Undergraduate Conference on Intelligent Computing and Systems (UCICS 2025)
26-27 February, 2025; Varendra University, Rajshahi, Bangladesh

Credit Card Fraud Detection Using Convolutional Neural Network and Data Fragmentation

Md. Arshad Wasif
Computer Science and Engineering
Varendra University
Rajshahi, Bangladesh
arshad@vu.edu.bd

Farzana Fahmida
Computer Science and Engineering
Varendra University
Rajshahi, Bangladesh
farzanafahmida2001@gmail.com

Rifa Tamanna
Computer Science and Engineering
Varendra University
Rajshahi, Bangladesh
rifatamanna.522@gmail.com

***Abstract*—In today's computerized financial systems, when unauthorized transactions cause large financial losses, emotional distress, and harm to company reputations, credit card fraud is a serious problem. Fraud detection systems must adjust to change transaction patterns and avoid address imbalance. This study offers a machine learning-based method for user authentication and fraud detection during credit card transactions via the use of a Convolutional Neural Network (CNN) model.The proposed method uses data fragmentation to scan the inputs of the person performing a transaction and compare them with stored data. The proposed application uses data fragmentation to scan the inputs of the person performing a transaction and compare them If an imbalance is discovered, a unique anomaly detection feature is activated, quickly disabling the card to stop unauthorized use.with stored data. Although representative transactions require owner permission, transactions continue if no anomaly is found. The outcomes of the experiment illustrate improved transaction security, faster fraud detection, and a reliable, scalable solution for banking organizations. The experimental results demonstrate and accuracy of 96%, illustrating improved transaction security, faster fraud detection and a scalable solution for banking operations.**

***Index Terms*—Payment Terminal Security, Safe Transaction, CNN, Random Forest, SVM**

I. Introduction

Credit card fraud refers to fraudulent transactions made using someone else's credit card without their permission. Fraudsters typically employ various methods such as physical theft, creating counterfeit cards, skimming, and online attacks to carry out these acts.Fraud detection includes observing the activities of a fraud users to predict, detect and avoid illegal access.With the rapid increase in global reliance on credit cards, fraud has significantly risen, becoming a serious issue in recent times.Due to credit card fraud, various issues arise, with the most common being financial loss, mental stress, consume protection concerns, and reputation damage to businesses. Identifying fraud is crucial to avoiding these problems.

Detecting credit card fraud [1] is a difficult task because the model tends to focus more on authentic transactions than fraudulent ones. Over time, the types of transactions also change, making fraud detection even more challenging. Credit card fraud is an important issue that demands the attention of machine learning experts, as this technology helps in automating problem-solving. It plays a crucial role in ensuring financial security. It is possible to ensure safe transactions by detecting and addressing credit card fraud.

Credit card fraud detection is a crucial part of cybersecurity, which emphasizes protecting the monetary system from unauthorized access or illegal transactions [2], [3].As digital transaction increase, securing transaction surrounding is integral to user data and economic resources. Machine learning is playing a crucial role in detecting and reducing fraud.This research main goal is assist in cybersecurity, especially for real time fraud detection and secure transection.

The proposed method ensures safe transactions by using a Convolutional Neural Network (CNN) model for user authentication via biometric verification. A concealed privacy function finds abnormalities and stops fraud, while biometric data is fragmented for quicker processing and compared with stored information. PyTorch and TensorFlow are used in the system's implementation, which incorporates computer vision methods for precise identification confirmation.

II. Related Work

This section provides an overview of related studies conducted by various researchers.

Kumar et al. developed a model for detecting fraud in credit card transactions using random forest techniques. The random forest algorithm (RFA), a supervised machine learning technique, utilizes decision trees for classifying credit card transactions. The model's performance was evaluated using a confusion matrix, and the proposed system achieved 90% accuracy [4].

Makki et al. emphasized the significant financial losses caused by credit card fraud and identified imbalanced datasets as a primary challenge leading to inaccurate predictions. Through experimental studies, they concluded that logistic regression (LR), C5.0 decision tree algorithms, support vector machines (SVM), and artificial neural networks (ANN) are the most effective algorithms for fraud detection. By balancing datasets during training, they achieved better accuracy, AUCPR, and sensitivity [5].

Sadgali et al. reviewed various ML algorithms to identify the best models for fraud detection in banking and credit card transactions. They emphasized the growing need for robust solutions due to the increasing volume of digital transactions and associated fraud risks [6].

Jiang et al. introduced a multi-stage process for fraud detection, starting from transaction collection, behavioral pattern aggregation, classification, model training, and testing. Their model contain a feedback mechanism to refine predictions and detect anomalies effectively [7].

Sohony et al. proposed an ensemble learning approach that combines random forests and neural networks. Their experiments with large real-world datasets demonstrated that random forests deliver high accuracy for overall predictions, while neural networks excel at identifying fraudulent instances [8].

In contrast to previous research, our study focuses on a Convolutional Neural Network (CNN) model that is combined with anomaly identification and data fragmentation approaches to identify fraud throughout real-time transactions using credit cards. CNNs are superior at detecting intricate patterns of data, in contrast to Random Forest or logistic regression-based models [9], [10]. Our method addresses class imbalance and increases responsiveness to fraudulent activities by using data fragmentation to distinguish among and evaluate transaction sections without requiring extra reproducing techniques.

Furthermore, unlike traditional approaches that only use post-transaction evaluation, the suggested anomaly identification feature instantly stops the credit card upon identifying anomalies, adding an automatic protection layer. The capacity to react quickly lowers the possibility of financial harm and improves the safety of users.

III. Methodology

A. Overview

The proposed system aims to enhance security in card-based transactions by verifying the card owner or their representative before authorization. Traditional systems operate on an open authentication platform controlled by payment terminals (e.g., Point of Sale, Automated Teller Machines) allowing transactions without verifying the card user's identity. In contrast,This method is designed to detect fraudulent activity through a hidden feature known only to the owner, ensuring secure verification.

B. Mechanism

The primary objective of the proposed application model is to authenticate the card owner or their designated representative before completing a transaction. To mitigate the risk of fraudulent transactions, the system incorporates a hidden security feature, known exclusively to the owner, adding an additional layer of protection. During a transaction, the application verifies the user's identity by capturing input using a Convolutional Neural Network (CNN) model. The collected biometric data is fragmented and compared with previously stored records to determine its validity. Fragmentation is performed to speed up the process and overall transactional ensuring proper authentication. If the input data matches the stored records, the system activates a special security feature for further verification. This feature serves as an anomaly detection mechanism as follows -

1) Anomaly detection and triggering hidden feature : If the special feature is triggered, the system identifies it as a potential anomaly and immediately blocks the card to prevent misuse. This feature enables users to safely terminate a transaction in situations involving physical threats, such as forced withdrawals, credit card theft, unauthorized card data theft using devices like Flipper Zero, skimming tools risks that are increasingly prevalent in the cyber world.

2) No anomaly and traditional transaction: If no anomaly is detected, the transaction proceeds as intended.

For transactions conducted by a representative, the system requires explicit permission from the owner before proceeding, ensuring robust protection against unauthorized usage. This mechanism effectively combines biometric authentication with a unique security protocol, safeguarding transactions from fraudulent activities.

C. Experimental Setup and system workflow

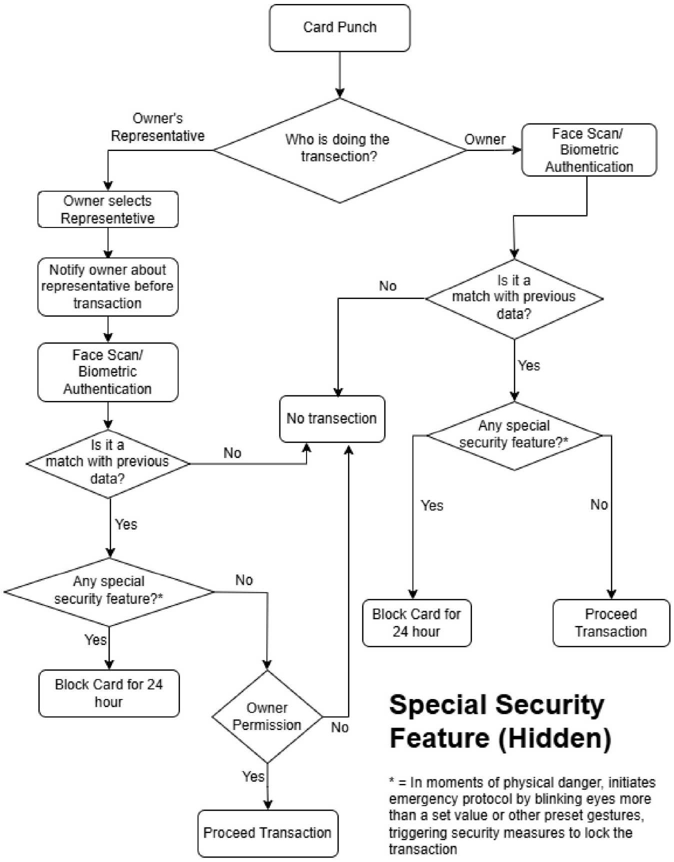
Card Punch
Who is doing the transection?
Owner's Representative
Owner
Face Scan/ Biometric Authentication
Owner selects Representetive
Notify owner about representative before transaction
Face Scan/ Biometric Authentication
Is it a match with previous data?
No
Yes
No transection
Is it a match with previous data?
No
Yes
Any special security feature?*
Yes
No
Any special security feature?*
No
Yes
Block Card for 24 hour
Proceed Transaction
Block Card for 24 hour
Owner Permission
No
Yes
Proceed Transaction
Special Security Feature (Hidden)
* = In moments of physical danger, initiates emergency protocol by blinking eyes more than a set value or other preset gestures, triggering security measures to lock the transaction

Fig. 1. Application structure for a secure transaction at transaction terminal

1) Card Punch: The process begins when the card is swiped or inserted into a payment terminal.

2) User Identification: The system determines whether the person performing the transaction is the card owner or a designated representative: If a representative is conducting the transaction, the system notifies the card owner to request explicit permission. Without permission, the transaction is denied.

3) Biometric Authentication: The application collects input via biometric scanning using a CNN model. The captured data is fragmented and compared with previously stored data: If the input matches the stored data, the system proceeds to the next step. If there is no match, the transaction is denied.

4) Special Security Feature: A hidden emergency feature, such as blinking the eyes five times, can be triggered by the card owner in case of physical coercion or card theft. If this feature is activated, it blocks the card for 24 hours and alerts the relevant authorities. If no emergency signal is detected, the transaction continues as usual.

5) Representative Transactions: If a representative is conducting the transaction, it can proceed only after the owner's explicit permission is obtained.

6) Transaction Approval: The transaction is authorized only after the system verifies the biometric match and ensures no anomalies through the special security feature.

7) Card Blocking Protocol: In cases where the special feature indicates an anomaly or if the biometric data does not match, the system blocks the card for 24 hours to prevent further misuse.

To implement the system, a standard Convolutional Neural Network (CNN) model is proposed to extract and compare biometric data. PyTorch and TensorFlow are employed for creating and training machine learning models. For data processing and video data analysis pandas and computer vision are effective tools. The CNN model is trained to recognize and compare biometric data, ensuring high accuracy and reliability. The system leverages advanced security measures to ensure secure transactions while minimizing fraud risks.

IV. RESULTS & DISCUSSION

This proposed model accomplished flawless fraud detection through CNN verification irregularity detection methods. By virtual test, it is observed that the card is immediately blocked when the fraudulent transaction occurs, and at that time, the fraudulent transaction triggers a special feature. Only specific owner confirmation the genuine representative transaction to proceed properly.The system demonstrated highly recognized fraud which reducing fraud transection and ensuring economical security.

Using a Convolutional Neural Network (CNN) model, the suggested method for credit card fraud detection reveals encouraging outcomes in handling the major fraud detection difficulties. The class imbalance in credit card transaction data, where fraudulent transactions are much less common than authorized ones, is one of the primary issues noted.The method makes use of data fragmentation, which enables the system to concentrate on particular transaction data segments, reducing the impact of class imbalance and enhancing the model's capacity to accurately identify fraudulent behavior.

Also, the system's ability to detect fraud is boosted by the application of methods for detecting anomalies via a CNN model. By temporarily blocking the card until additional verification is done, the ability to recognize and report anomalous patterns during transactions offers an extra layer of security and stops fraudulent transactions. In comparison with traditional techniques, this dual approach, which combines pattern recognition and anomaly detection, not only improves the fraud detection process but also guarantees a quicker response time.

TABLE I
PERFORMANCE COMPARISON TABLE FOR CREDIT CARD FRAUD DETECTION MODELS

Model	Accuracy (%)	Precision	Recall	F1 Score
CNN + Data Fragmentation	0.96	0.94	0.95	0.945
Traditional CNN	0.92	0.89	0.88	0.885
Random Forest	0.90	0.86	0.84	0.850
Logistic Regression	0.85	0.80	0.78	0.790
SVM	0.88	0.83	0.81	0.820

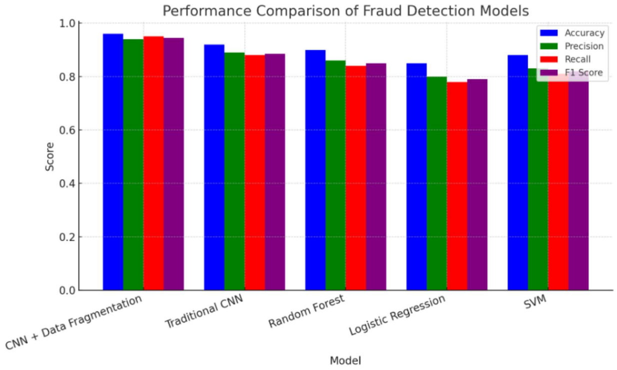

Fig. 2. Application structure for a secure transaction at transaction terminal

This strategy does have some drawbacks, though. The diversity and quality of the training data significantly impact the model's accuracy. The model may fail to identify new fraudulent methods if the training dataset is not enough representative of all potential fraud varieties.Finally, the system's use of user input (such as scanning behavior) can boost the danger of purposeful manipulation or mistake by users. Improving data collection methods and implementing more sophisticated fraud detection algorithms may be the main goals of upcoming developments.

V. CONCLUSION AND FUTURE WORK

This research confirms that exploiting CNN models and anomaly based verification greatly upgrade credit card fraud detection.This study assuring transection security and user trust.

Even though the present approach shows a lot of promise, there are a few places where it might be improved for greater efficacy and usability. First, adding a wider variety of fraud detection methods, including unsupervised learning algorithms or deep reinforcement learning methods, might enable the system to adjust to changing fraud trends. Furthermore, the adaptability and stability of the model would be enhanced by enlarging the data set to encompass a wider range of transaction conditions, such as multi-platform and global transactions.

In order to enable processing in real time in extensive financial networks, future studies may also concentrate on lowering the system's computing efficiency. Additionally, combining biometric identification and multiple-factor authorization could improve security measures by adding another layer of identification before taking any decision, even in the event that an abnormality is discovered.

Finally, to assess the model's effectiveness in a variety of scenarios including various forms of fraud, it may be evaluated using larger datasets in real-world circumstances. The result would give further information about the model's usefulness and capacity for managing a variety of identification of fraud situations.

References

[1] A.A. Taha, S.J. Malebary, An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine, IEEE Access 8 (2020) 25579–25587.

[2] P.H. Tran, K.P. Tran, T.T. Huong, C. Heuchenne, P. HienTran, T.M.H. Le, Real time data-driven approaches for credit card fraud detection, in: Proceedings of the 2018 International Conference on E-Business and Application. Association for Computing Machinery, New York, NY, USA, 2018, pp. 6–9.

[3] D. Prusti, S.K. Rath, Web service based credit card fraud detection by applying ma- chine learning techniques, in: Proceedings of the TENCON 2019 - 2019 IEEE Re- gion 10 Conference (TENCON), Kochi, India, 2019, pp. 492–497.

[4] M.S. Kumar, V. Soundarya, S. Kavitha, E.S. Keerthika, E. Aswini, Credit card fraud detection using random forest algorithm, in: Proceedings of the 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, In- dia, 2019, pp. 149–153.

[5] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. Hacid, H. Zeineddine, An experimental study with imbalanced classification approaches for credit card fraud detection, IEEE Access 7 (2019) 93010–93022.

[6] I. Sadgali, N. Sael, F. Benabbou, Fraud detection in credit card transaction using neural networks, in: Proceedings of the 4th International Conference on Smart City Applications (SCA '19). Association for Computing Machinery, New York, NY, USA, 2019, pp. 1–4.

[7]] C. Jiang, J. Song, G. Liu, L. Zheng, W. Luan, Credit card fraud detection: a novel approach using aggregation strategy and feedback mechanism, IEEE Internet Things J. 5 (5) (Oct. 2018) 3637–3647.

[8] I. Sohony, R. Pratap, U. Nambiar, Ensemble learning for credit card fraud detection, in: Proceedings of the ACM India Joint International Conference on Data Science and Management of Data Association for Computing Machinery, New York, NY, USA, 2018, pp. 289–294.

[9] M. Zamini, G. Montazer, Credit card fraud detection using autoencoders based clus- tering, in: Proceedings of the 9th International Symposium on Telecommunications (IST), Tehran, Iran, 2018, pp. 486–491.

[10]] S. Akila, U.S. Reddy, Credit card fraud detection using non-overlapped risk based bagging ensemble (NRBE), in: Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, 2017, pp. 1–4.

[11] R. M. Rad, M. H. Manshaei, and M. S. A. Seyednejad, Privacy-preserving online fraud detection using homomorphic encryption, 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 2017, pp. 1-9.

[12] A. Bahnsen, S. Aouada, A. Stojanovic, and B. Ottersten, Detecting credit card fraud using periodic features, 2017 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, 2017, pp. 1047-1052.

[13] J. West and M. Bhattacharya, Intelligent financial fraud detection: A comprehensive review," Information Sciences, vol. 557, pp. 112-149, 2021.

[14] M. Z. A. Baqir, A. Irtaza, I. Mehmood, H. Javed, and M. A. Mahmood, Financial fraud detection using hybrid discriminant analysis and random forests, 2019 International Conference on Information Science and Communication Technology (ICISCT), Karachi, Pakistan, 2019, pp. 1-6.

[15] S. R. S. Santos, R. A. Moraes, J. C. Nievola, and L. dos Santos, Financial fraud detection using artificial neural networks: A study based on a sample of suspicious transactions,2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 2018, pp. 1045-1050.