# Adaptive Systems for Fraud Detection in Financial Transactions: A Survey on Multi-Modal Biometrics and Real-Time Analytics

Shubhangi Vairagar[1] and Vaishnavi Babar[2]
[1]*Department of AI and Data Science,Dr. D.Y. Patil Institute of Technology, Pune, India*
[2]*Artificial Intelligence and Data Science, Dr. D.Y. Patil Institute of Technology, Pune, India*

Keywords: Adaptive Fraud Detection, Multi-Modal Behavioral Biometrics, RealTime Predictive Analytics, Machine Learning, Anomaly Detection, Financial Transactions, Blockchain Technology, Risk Assessment, Explainable AI, Typing Patterns, Mouse Movements, Facial Recognition, Fraud Prevention, Dynamic Thresholds, Transaction Transparency.

Abstract: The paper takes a revolutionary approach to countering financial fraud through adaptive fraud detection using multi-modal behavioral biometrics and real-time predictive analytics. Current systems are based on static rules and historical data that fail to counter modern and sophisticated techniques of fraud. This system builds an adaptive, all-inclusive user profile by including behavioral biometrics such as typing patterns, mouse movements, and emotional cues captured through facial recognition. Advanced machine learning algorithms improve on anomaly detection, enabling a system to adapt to in real-time changes in behavior of the user and changing fraud patterns, thereby strongly reducing false positives while the detection rates are improved. **Real-time predictive analytics** identify and stop fraudulent transactions prior to their occurrence, thus reducing monetary losses. The model will also use **blockchain technology**, where suspicious transactions can be logged safely for transparent audit purposes, hence increasing trust levels and transparency in transactions. The system adds layers of precision to fraud detection by utilizing live behavioral data for dynamic risk assessments. Its explainable AI mechanisms are transparent, which fosters user trust, and its adaptability supports resilience against evolving fraud tactics. The proposed system marks a significant leap forward, promising a safer and more efficient environment for financial transactions, ultimately revolutionizing fraud prevention strategies in the financial sector.

## 1 INTRODUCTION

In this digital era, the upsurge in online financial transactions has drastically altered the face of business. Even though at times easier to people's lifestyles, the increased rate of fraud against the financial system is one aspect that needs to be weighed with much consideration. As indicated by the Association of Certified Fraud Examiners, each year organizations lose an estimated 5Adaptive fraud detection systems are crucial and particularly needed to better improve the effectiveness of identifying fraudulent transactions. The research introduces a new approach with multi-modal behavioral biometrics, incorporating typing patterns, mouse movement, and emotional responses through facial recognition in building up a complete user profile. Continuously, this proposed system will analyse the different behavioral indicators and thus be able to adapt it in real time to changes in user behavior and emerging patterns of fraud. For instance, behavioral biometrics may also monitor for deviations in typical patterns by a user-thus changes in the typing speed or unusual mouse movements are likely indicators of fraudulent attempts. The incorporation of real-time predictive analytics makes the value of this system double since anomalies can be identified even before fraudulent transactions are actually performed. This is because, through machine learning algorithms, the system not only identifies transactions that are not in line with already established behavioral patterns but also predicts attempts made in real-time with fraudulent intentions, so financial losses for consumers and businesses could be significantly reduced. This predictive ability is very important in the high-speed digital paradigm wherein the transactions are made within milliseconds, thus it allows responding swiftly to potential fraud. Although there have been many leaps in recent years through



Vairagar, S. and Babar, V.
Adaptive Systems for Fraud Detection in Financial Transactions: A Survey on Multi-Modal Biometrics and Real-Time Analytics.
DOI: 10.5220/0013615200004664

In *Proceedings of the 3rd International Conference on Futuristic Technology (INCOFT 2025) - Volume 3*, pages 321-328
ISBN: 978-989-758-763-4

new fraud detection methodologies, many such gaps are identified in the literature. Most such existing systems are still more or less based on historical data and do not make allowance for the dynamic character of user behavior. Furthermore, many approaches focus the bias between detection accuracy and user experience wrongly and tend to increase false positives up to an undesirable point. For example, while some systems might gain accurate fraud detection, they may yield a large amount of true positives, and this leads to customer frustration and loss of user trust. This paper bridges these gaps by proposing a dynamic risk assessment model that adaptively adjusts contextual thresholds from live behavioral data, thus enhancing accuracy in fraud detection while maintaining user satisfaction. In this research work, our primary objective is to devise and implement an adaptive fraud detection system using multimodal behavioral biometrics along with advanced machine learning algorithms. More specifically, for this research, this combination of supervised learning and unsupervised learning techniques will be utilized to develop a hybrid model that can learn from the labeled data while discovering new patterns associated with fraud. The primary intention is to develop a highly accurate framework in terms of fraudulent transactions identification and is able to explain the decision-making process for the users to gain maximum trust and transparency. This paper integrates existing technologies with innovative features to redefine the approach toward fraud prevention in the financial sector. Besides improved accuracy in fraud detection, some more implications arise from implementing the blockchain technology on the proposed system. All such flagged transactions will be transparently logged, ensuring their secure record and thus thorough auditing. This degree of detail supports not only compliance with the regulations but will also enhance the confidence of the users as they interact with various financial systems. Additionally, with the use of explainable AI mechanisms, users are able to understand decisions made in the fraud detection process, hence building further trust in the system. The paper is outlined in the following sections: In Section II, pertinent literature will be reviewed in order to focus the evolution of methodologies detecting fraud and its integration with behavioral biometrics. Section III shall hold the architecture proposed, which shall elucidate the algorithms used and their place in the detection process. Section IV shall be comprised of experimental results on the effectiveness demonstrated by rigorous testing and validation. Lastly, Section V puts together the discussion and possible further work related to the findings within this domain. This paper addresses the limitation of existing methodologies and proposes a user-centric approach to fraud detection with the aim of significantly contributing to the field of financial security in its path toward the robust defence against fraudulent activities for digital transactions. Integration of multi-modal behavioral biometrics and real-time analytics will enhance the current technology and has tremendous potential in fighting financial fraud, thereby creating a more secure environment for financial transactions and enhancing the resilience of businesses to changing threats..

## 2 LITERATURE SURVEY

•Here, Alazizi et al. (2020) (Alazizi, Habrard, et al. 2021) present a comprehensive study on anomaly detection techniques tailored for fraud detection. In doing so, the authors point out that highquality datasets play a crucial role in the performance of anomaly detection models as such performance lies in the characteristics of the data upon which they are built. The authors propose a framework integrating various anomaly detection algorithms, namely supervised and unsupervised learning methods, to identify fraudulent activities. One of the major advantages of their methodology is that it is highly adaptable to multiple datasets, thus bettering its practicability in a vast range of fraud scenarios. However, one major drawback in the framework is that it is not capable of dealing with the dynamic aspect of fraudulent behaviors, thus requiring periodic updates of their model. Their models have a good degree of accuracy; however, their system does not offer an instant detection process.

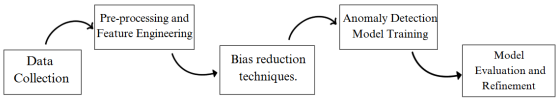


Figure 1: Anomaly Detection Work Flow for Fraud Detection

•Fawcett and Provost (1997) (Fawcett and Provost, 1997) discussed adaptive fraud detection methods using a decision tree. This method enables continuous learning of new data and continually refines the model towards a higher accuracy over time. The methodology has the ability to adapt to new patterns of fraud at automatic times, which is really important in this fast-evolving fraud landscape of today. However, it has been found to adapt in some considerable time, which could be a drawback in cases where

near-instant detection is the need. The authors have mentioned high precision and recall, but there could be scope for lag in adaptation that may leave holes in real-time fraud detection

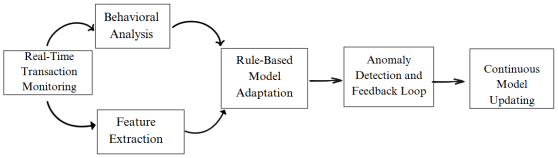


Figure 2: Adaptive Fraud Detection Framework

•Lebichot et al. (2017) (Lebichot, Paldino, et al. 2017) proposed incremental learning strategies specifically designed for credit-card fraud detection. Their strategy relies on using decision trees in an adaptive manner to learn from the arriving data. The most significant merit of this strategy is its ease of handling streaming data, which constitutes one of the primary requirements for fraud detection systems. In the paper, though, some restrictions on feature selection are encountered that would prevent the model from recognizing sophisticated fraud patterns. Their model's accuracy is appreciable; however, it does not provide a comprehensive behavioral analysis.

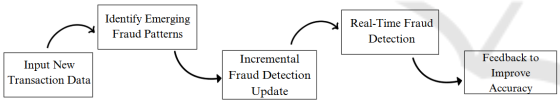


Figure 3: Incremental learning Strategy for Credit card Fraud Detection

•Makki, et al. (2021) (Makki, Assaghir et al. 2020) concentrates on class-imbalanced techniques for the detection of credit card frauds. They applied random forest and oversampling approaches to face the prevalent class-imbalance problem of the fraud dataset. A major benefit of their proposed technique is the improvement of the detection rates associated with the minority classes, which is a significant aspect in scenarios associated with fraud. Oversampling may also incorporate noise into the dataset, which may lead to false positives. It reports high accuracy levels, but the approach may not scale up well to large-sized datasets.

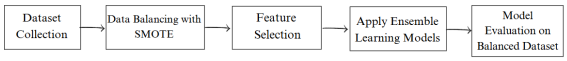


Figure 4: Imbalanced Classification Approach for Fraud Detection

• Carcillo et al. (2020) (Carcillo, Borgne et al. 2020) discusses streaming active learning strategies in credit card fraud detection in reallife scenarios. Their framework uses active learning to respond to developments in the model as stream data keeps flowing in. The main advantage of their approach is its dynamic update of patterns in fraud detection. However, the authors caution that selection bias may prevail in their sampling methods to the detriment of fraud cases. Although they note very high accuracy of their model, coverage may not be all-inclusive for any kind of transaction.

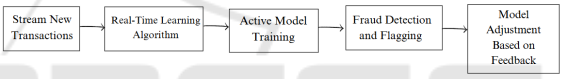


Figure 5: Streaming Active Learning for Real-Time Fraud Detection

•Alarfaj et al. (2020) (Alarfaj, Malik et al. 2020) analyzed the current day-to-day techniques of the related literature using some state-of- the-art machine learning and deep learning algorithms for credit card fraud detection. The authors have used CNN and LSTM network techniques, and their models achieved high accuracy based on the result. However, this deep learning method results in expensive compu- tational costs and a slower response time, which can be dangerous in a real-time fraud detection scenario. Where their approach is quite strong, that is, in a very high detection capability, the constraints in terms of speed and computational requirements pose associated challenges.

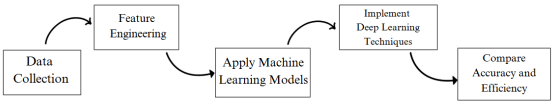


Figure 6: Big Data Medicare Fraud Detection System

•Herland et al. (2019) (Herland, Khoshgoftaar,

2018) detail ways fraud can be followed by using big data analytics in several Medicare data sources. If combined datasets are a reflection of depth and width, then detection would be even more precise. While the study has adopted an all-roundedness that employed the richness of big data, handling a significant volume of data may become cumbersome or even delaying in detection. This point has brought out the greater need for more efficient data management techniques

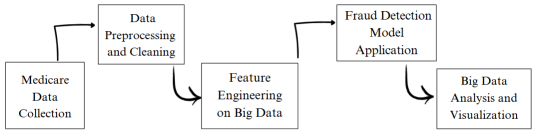


Figure 7: Behavioral Transaction-Based Fraud Detection Model

• According to transaction behavior analysis, Kho and Vea (2017) (Kho and Vea, 2017) engage focus and work on the detection of fraudulent credit cards. The methodology applied proceeds with an understanding of the patterns of transaction of the user to detect anomalies suitably. Probably, their approach concentrates on various user-specific behaviors, which will improve detection accuracy. But their method may lack sophistication against sophisticated fraudsters trying to mimic legitimate behavior patterns.

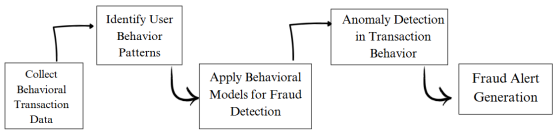


Figure 8: Fraud Detection in Distributed Graph Databases

•Srivastava and Singh(Srivastava and Singh, 2019) introduced a fraud detection methodology based on distributed graph databases, that has shown to do well with the detection of fraud across interlinked networks. Their approach is strong regarding determination of relationship-based analysis within the data that helps discover even hidden patterns of fraud but is not suitable in most individual transactions.

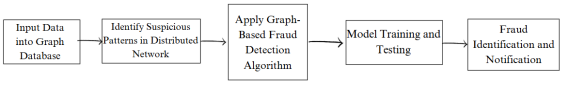


Figure 9: Hybrid Ensemble Model for Behavioral Fraud Detection

•Karthik et al. (Karthik, Mishra, et al. 2019) proposes a hybrid ensemble model for credit card fraud detection based on modeling user behavior patterns. Their strategy is an amalgamation of several classifiers in order to immensely improve the accuracy of the detection process. The benefits of this strategy include very high detection rates but challeng- ing for its implementation in terms of complexity and increased computational requirements.

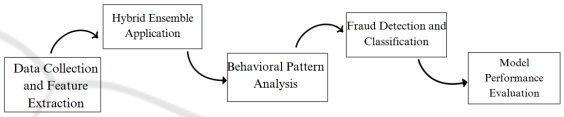


Figure 10: Realistic Modeling and Novel Learning Strategy for Fraud Detection

• Hashemi et al. (Hashemi, Mirtaheri, et al. 2020) discuss fraud detection from banking data by considering different types of machine learning techniques. Efficient results are obtained by using some classifiers, which are nothing but Support Vector Machines (SVM) and Random Forests. The major drawback in their approach is that it often needs you to retrain the system for the appearance of new fraudulent patterns. Accuracy rates reported are impressive though the requirement of manual intervention to make updates limits the operational efficiency.

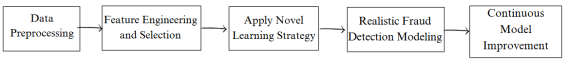


Figure 11: Banking Data Fraud Detection Using Machine Learning Techniques

•Jiang et al. (Jiang, Song, et al. 2020) propose a new approach in credit card fraud detection using aggregation strategy with feed- back mechanism. The strategy they have suggested is integrating several strategies to enhance the performance continuously.

Their approach lacks effectiveness at ex- tremely real-time scenarios and may lose track of the required fraud cases on time.

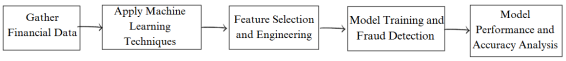


Figure 12: Feedback-Based Aggregation for Credit Card Fraud Detection

•Abdul Salam et al. finally dealt with the federated learning technique with the methods being incorporated into credit card fraud detection and data balancing. In this research, the benefits lie in not losing any personal data since the models are locally trained, leaking no private information. However, federated learn- ing is decentralized, and it results in slower updates and less information sharing that develops inefficient overall solutions.

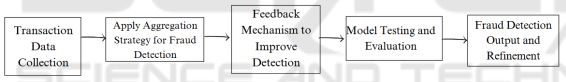


Figure 13: Federated Learning Model for Fraud Detection

• In the work of Zareapoor et al. (Zareapoor, Yari, et al. 2021), an ensemble system on fraud detection feature selection techniques combined with ensemble learning is discussed. As the authors noted: ”the importance of the selection of the most relevant features, as the presence of irrelevant features will reduce the accuracy of a detection model.” Their approach utilizes multiple classifiers that leverage boosting both Logistic Regression and Decision Trees. Among its strengths would be that it’s easy to cut down computational complexity focusing on only the meaning- ful features. Probably one of its major weaknesses is dependency on static feature sets thus probably maybe less adaptable in cases of a changing pattern. Despite the very high accuracy rates reported, there are also feature set update challenges.

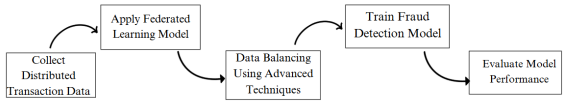


Figure 14: Adaptive Fraud Detection Using Multi-Modal Biometrics

•According to Yang et al. (2021) (Yang, Zhang, et al. 2021), this is an application of deep learning in credit card fraud detection. Here, they apply Convolutional Neural Network in their model, which is based on the pattern extracted from transaction data and also from the user behavior pattern. One of the important features of this method is that it uses deep learning; thus the models capture much more complex data patterns than other approaches. However, the deep learning models require huge amounts of labeled data for training in the fraud-detection domain as labelled instances are scarce. Their approach works well and has accuracy, but there is no real-time adaptability.

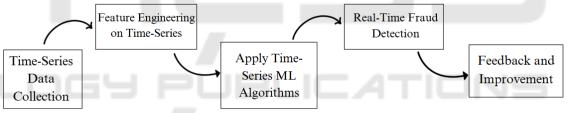


Figure 15: Real-Time Predictive Analytics in Fraud Detection

•Choudhary et al. (2022) (Choudhary, Tiwari, et al. 2022) comes up with a novel credit card fraud detection framework. This combines rein- forcement learning with typical classification techniques. Their focus is on the dynamic concept attributed to fraud detection because they have designed their model to alter its policy of decision based on the feedback received from the environment. The strength of this framework lies in learning errors from earlier moves and thus improves over time. Conversely, actual complexity involved in implementing reinforcement learning might act as an in- hibitor to its practical applicability. The authors reported improvement in terms of accuracy detection performance, but perhaps the time it takes to train the system could be an obstruction to its timeliness when urgent action is warranted.

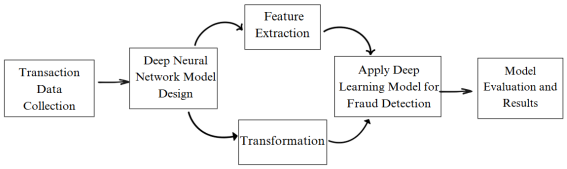


Figure 16: Blockchain-Integrated Fraud Detection System

•Another highly relevant study is that of Mahmood et al. (2022) (Mahmood, Khedher et al. 2022) that deals with researching techniques of Natural Language Processing for fraud detection ap- plications in financial transactions. Here, the authors utilize sentiment analysis for assessing descriptions in transactions and communications by users in terms of a number of fraud indicators. One of the salient advantages of this strategy involves innovative exploitation of text information that may provide supplementary contextual input for the system to detect fraud. However, in the cases where transaction data are mostly numeric, the technique has disadvantages. The reported accuracy is encouraging but becomes susceptible to the quality of textual data utilized.

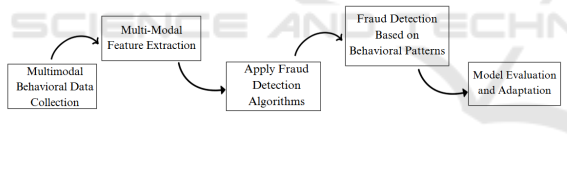


Figure 17: Risk-Based Dynamic Fraud Detection Model

•Finally, authors Akinwande et al. (2023) (Akinwande, Ajayi et al. 2023) present a federated learning framework especially designed for fraud detection in mobile payment systems. Their ap- proach is based on building the model across distributed data sets while ensuring both privacy and security for users. The key advantage is that the privacies of users are preserved such that sensitive data stay on the local de- vices. The authors mention data heterogeneity as a factor that impacts the quality of the model while commenting on the method's applicability. Very acceptable accuracy has been achieved; however, the challenges associated with federated learning limit the real-time responsiveness of the system.

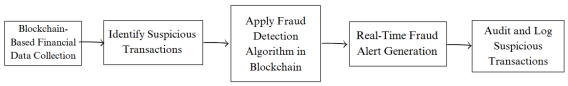


Figure 18: Explainable AI in Fraud Detection

# 3 GAP FINDINGS

The literature review demonstrates that, even when all fraud detection systems had been improved in many ways, the problems were still enormous. Indeed, most of the studies applying traditional machine learning methods with models such as Random Forests and Support Vector Machines have not addressed the real-time adaptability of fraud detection systems and ignored that fraud patterns have always changed with time and that even historical data might be insufficient for fraud detection systems where new fraud patterns are emerging. Besides, papers based on static behavioral biometrics are mostly concentrated on single-modal data such as keystroke dynamics or mouse movement with very limited capabilities of capturing holistic user behavior under changing conditions.Most of the models were enhanced in detection accuracy using deep learning algorithms such as Convolutional Neural Networks, but most of them lack scalability and computational efficiency in large-scale, real-time applications. Other ensemble methods increased detection rates but suffer from high false-positive rates, which may eventually become a painful user experience. In addition, nearly all the modelbased reviews are tested on static datasets while the realtime environment with continuous changes in behavior can be questioned. In addition, although integrating with blockchain to enhance the transparency of transactions is under-explored in most systems, it leaves a potential flaw in auditing and identifying fraudulent activities. Most of the papers using SMOTE balancing data techniques have not taken into account dynamic trends in fraud, nor do they provide an explanation regarding the role of multimodal biometric modes, like emotional recognition, and facial recognition modes. Lastly, although many algorithms have been developed targeting the specific aspects of fraud detection, none of them integrates, to a full extent, a comprehensive multi-modal, real-time predictive analytics approach that adapted in a balanced way both between the aspects of detection accuracy and computational efficiency as fraud tactics continuously evolve.

# 4 CONCLUSIONS

Adaptive Fraud Detection in Financial Transactions Using Multi-Modal Behavioral Biometrics and Real-Time Predictive Analytics: A Novel Perspective on Modern Advanced Financial Fraud Challenges, a paper posits a new approach to the extensive challenges emerging in modern advanced financial fraud. It uses adaptive evolving patterns of fraud that observe behavioural biometrics, combined with real-time analytics and advanced machine learning, to further decrease false positives in fraud detection, thus making the detection more effective and accurate. There is a combination of overall behavioral inputs, such as dynamics of typing, mouse movement, facial recognition, and traditional financial data in the proposed model, so that an all-inclusive view of user behavior comes up to ensure very efficiency against sophisticated fraud strategies. With the implementation of blockchain technology, it would be possible to audit flagged transactions also, thereby enhancing the transparency and security associated with fraud detection. The proposed solution is real-time in nature, making fraud prevention proactive as possible; thus, it minimizes financial losses further while strengthening the trust of users in digital transactions. This adaptive system is far more efficient at detecting fraud with minimal interruptions to legitimate transactions as compared to extant systems that are based solely on static mechanisms built around rules, and provide high false positives. Scope for Personalizing Fraud Detection with Individual User Behavior This dynamic risk assessment model has the scope for personalizing fraud detection based on individual user behavior, which indicates how security and convenience can be balanced. Future work will probably rely on expanding the scope of the system by incorporating a much wider variety of behavioral biometrics apart from user behaviors. The future work may also include the healthcare and e-commerce domains. Therefore, an absolute scaling optimization of the system will be absolutely required in conjunction with more complex and large financial infrastructures for mass deployment of the system. In conclusion, the paper is an important step for fraud detection techniques, since it is innovative, avoiding the weaknesses of current techniques and providing a basis for further innovations related to adaptive behaviorbased fraud detection. This proposed system probably will revolutionize ways of securing transactions inside a financial industry moving toward higher levels of digitalization and fluidity.

# REFERENCES


Ayman Alazizi, Amaury Habrard, Franc¸ois Jacquenet, and Liyun HeGuelton, "Anomaly Detection, Consider your Dataset First: An illustration on Fraud Detection," 2021.

T. Fawcett and F. Provost, "Adaptive Fraud Detection," NYNEX Science and Technology, White Plains, NY, 1997.

B. Lebichot, G. M. Paldino, W. Siblini, L. He-Guelton, F. Oble´, and G. Bontempi, "Incremental Learning Strategies for Credit Card Fraud Detection," in Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 2017, pp. 180-187.

S. Makki, Z. Assaghir, Y. Taher, R. Haque, M.-S. Hacid, and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," IEEE Access, vol. 8, pp. 157685-157695, 2020.

F. Carcillo, Y.-A. Le Borgne, O. Caelen, and G. Bontempi, "Streaming Active Learning Strategies for Real-Life Credit Card Fraud Detection: Assessment and Visualization," IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 3, pp. 826-838, Mar. 2020.

F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, vol. 8, pp. 189102-189120, 2020.

M. Herland, T. M. Khoshgoftaar, and R. A. Bauder, "Big Data Fraud Detection Using Multiple Medicare Data Sources," Journal of Big Data, vol. 5, no. 1, pp. 1-15, 2018.

J. R. D. Kho and L. A. Vea, "Credit Card Fraud Detection Based on Transaction Behavior," International Journal of Computer Applications, vol. 159, no. 8, pp. 1-5, 2017.

S. Srivastava and A. K. Singh, "Fraud Detection in the Distributed Graph Database," in Proceedings of the 2019 IEEE 2nd International Conference on Data Science and Information Technology (DSIT), Bangkok, Thailand, 2019, pp. 168-173.

V. S. S. Karthik, A. Mishra, and U. S. Reddy, "Credit Card Fraud Detection by Modelling Behaviour Pattern using Hybrid Ensemble Model," International Journal of Computer Applications, vol. 182, no. 40, pp. 1-7, 2019

A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learn- ing Strategy," IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3782-3794, Aug. 2018.

S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," Applied Sciences, vol. 10, no. 2, p. 641, 2020.

C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," International Journal of Information Technology, vol. 12, no. 2, pp. 1-8, Apr. 2020.

M. Zareapoor, M. Yari, and F. Abdollahzadeh, "An Ensemble Learning Approach for Fraud Detection Using Feature Selection Techniques," Journal of Information Security and Applications, vol. 57, p. 102704, 2021

X. Yang, Y. Zhang, and X. Zhou, ”Deep Learning for Credit Card Fraud Detection: A Comprehensive Review,” IEEE Transactions on Computational Social Systems, vol. 8, no. 2, pp. 157-173, Apr. 2021.

A. Choudhary, S. Tiwari, and A. K. Mishra, ”Reinforcement LearningBased Framework for Credit Card Fraud Detection,” Journal of King Saud University - Computer and Information Sciences, 2022.

H. Mahmood, A. M. A. Khedher, and A. M. Anis, ”Sentiment Analysis in Credit Card Fraud Detection: A Natural Language Processing Approach,” Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. 1, pp. 273-284, Jan. 2022.

A. Akinwande, O. Ajayi, and F. I. Oyetunji, ”Federated Learning Framework for Credit Card Fraud Detection in Mobile Payment Systems,” Future Generation Computer Systems, vol. 142, pp. 244-257, Feb. 2023.