Journal of Artificial Intelligence and Data Science Techniques

ISSN: 3029-2794

Volume 02 Issue 01 (February) 2025

Next-Gen Intelligent Pattern Discovery for Credit Card Fraud Prevention and Real-Time Financial Risk Analysis

Abdul Mateen Qadir[1] and Khalid Ali Aljarrah[2]

[1] School of computing, Skyline university college, Sharjah, UAE
[2]Department of Computer Engineering, Hijjawi Faculty for Engineering Technology, Yarmouk university, Irbid, Jordan

Abstract:

Financial fraud has been on the rise alongside the popularity of online shopping, calling for more sophisticated methods of detecting this type of crime. Credit card transaction data is high-dimensional and unbalanced, making it difficult for traditional fraud detection algorithms to work. Therefore, more advanced methods are needed for real-time financial risk analysis. An improved framework for financial risk assessment and fraud detection called FraudDetectX is proposed in this paper. It is based on transformers and uses contrastive learning. Combining self-attention algorithms for capturing complicated spending patterns and contrastive learning for identifying fraudulent and authorized transactions constitutes the methodology for the adaptive learning of ever-changing fraud tactics and the real-time detection of anomalies. According to key results, FraudDetectX surpasses conventional models by reducing false positives and increasing accuracy. It is appropriate for monitoring financial transactions on a broad scale since experimental results show a considerable improvement in recall and precision. Finally, for improved financial safety in contemporary banking systems, FraudDetectX offers a strong, scalable, and intelligent answer to the problem of credit card

Index terms: Credit Card Fraud Detection, Financial Risk Analysis, Transformer Models, Contrastive Learning, Real-Time Anomaly Detection

1. Introduction

The exponential growth of digital transactions has transformed the financial system, giving consumers more access and convenience. Unfortunately, monetary theft, notably credit card fraud, has increased due to this digital transition[1]. Fraudulent activities like identity theft, money laundering, and fraudulent transactions pose a significant risk to customers and financial institutions. Traditional fraud detection approaches, such as rule-based systems and machine learning classifiers, struggle to keep up with the dynamic nature of fraudulent activities[2]. Modern financial fraud detection systems must possess two capabilities: anomaly detection in real-time and adaptive learning.

Notwithstanding progress in fraud detection, numerous systems inadequately identify illicit transactions while maintaining a low false positive rate. Conventional fraud detection techniques cannot identify novel fraud patterns because they rely on manually established rules or fixed feature sets[3]. High-dimensional transaction records also affect how fast computers work and how well models can be scaled. Fraud datasets, in which only a few fraudulent deals worsen the problem and change the models' results. To overcome these limitations, the study present FraudDetectX, a state-of-the-art fraud detection technology that discovers fraud patterns and assesses financial risk using transformers and contrastive learning[4].

Data preparation and feature engineering are used for the transformer model to clean, standardize, and arrange raw credit card transaction data. Consistent data representation makes learning easier. In step two, intricate transaction relationships and anomalies in spending are found using the transformer-based self-attention mechanism. By evaluating many transaction features simultaneously, this approach captures patterns that traditional models miss [5]. The Model is then trained to differentiate between authentic and fraudulent transactions using contrastive learning, which creates positive and negative transaction pairs. By expanding the framework, this technique lowers false positives and enhances fraud detection. Lastly, models are refined using new transaction data, real-time anomaly detection, and adaptive learning. The system remains effective even when fraud methods evolve because of its versatility. Using these cutting-edge approaches, FraudDetectX provides modern banks with a scalable and reliable solution for real-time financial risk assessment and fraud prevention.

The FraudDetectX framework, introduced in this paper, makes several key contributions:

- Enhanced Accuracy in Fraud Detection—Using self-attention and contrastive learning techniques, can reduce false positives and improve fraud detection accuracy [6].
- Financial institutions can swiftly identify suspicious actions with the help of FraudDetectX, allowing real-time transaction monitoring.
- Scalability & Adaptability – The platform successfully counters cyber dangers by efficiently managing massive financial datasets and adjusting to emerging fraud tendencies [7].

Here is the next section of the paper. Part 2: Related Work delves into the advantages and disadvantages of various fraud detection systems. The data preprocessing, model design, and training procedures of FraudDetectX are detailed in Section 3: Proposed Methodology.

Section 4: Experimental Results & Evaluation compares FraudDetectX to other fraud detection methods. Section 5: Applications & Case Studies examines financial security and risk assessment framework applications. Section 6: Conclusion & Future Work review findings and offer improvements. The powerful, scalable, and intelligent FraudDetectX technology prevents credit card fraud and analyses real-time financial risk.

2. Related Work

Ramli et al. [8] This study presents a hybrid transformer-based fraud detection algorithm that uses contrastive learning and self-attention to detect fraudulent transactions in real-time. Kaggle's Credit Card Fraud Detection Dataset provides anonymized transaction information and fraud labels for the study. Comparing experimental results to traditional models shows a 30% increase in fraud detection accuracy and a 25% decrease in false positives. The technique has model interpretability, computational complexity, and imbalanced data issues. Explainable

AI, efficient model optimization, and enhanced data augmentation can improve fraud detection.

Bayya, A. K et al. [9] This paper introduces DLASA, a Deep Learning-Based Adaptive Security Algorithm that improves financial cybersecurity through predictive threat analysis, real-time fraud detection, and adaptive learning. Employ a real-world FinTech transaction dataset with user authentication logs, transaction information, and fraud indicators. Experimental results show a 40% reduction in fraud, a 35% improvement in authentication performance, and fewer false positives. High computing costs, data privacy problems, and adversarial threats continue. Privacy-preserving AI, efficient computational frameworks, and adversarial defense techniques can improve FinTech security.

Qiyam, F.et al.[10] This study offers the Generative AI-Enhanced Banking Intelligence System (GAEBIS), which uses LLMs and structured rapid engineering to improve digital banking decision-making, consumer personalization, and risk management. The study uses real-world banking transaction history, financial queries, and fraud detection records. Results show a 30% increase in prediction accuracy, a 40% increase in tailored suggestions, and a 25% reduction in fraud detection errors. High computing expenses, AI-generated response biases, and data security issues remain. Model modification, bias avoidance, and improved encryption can improve the reliability and security of AI-driven banking analytics.

Olowu et al.[11] Hybrid AI-Driven Fraud Detection (HAFD) uses supervised deep learning models and unsupervised anomaly detection to avoid banking fraud. The Model detects 93% of transactions with 55% fewer false positives using a worldwide banking transaction dataset with authentic and fraudulent transactions. Comparative analysis proves its superiority over rule-based systems. Data asymmetry, increasing fraud strategies, and significant computing costs remain. Adopting adaptive learning models, improved feature engineering, and scalable cloud-based architectures can improve fraud detection accuracy and cyber threat resilience.

Tamraparani, V. et al.[12] this research analyses massive IAM datasets containing information about user authentication, access patterns, and signs of fraud. Artificial intelligence algorithms detected 89% of fraud using real-world data from banks, with a false positive rate of only 7%. Artificial intelligence (AI) improves detection efficiency but has limits, such as reliance on data quality, adversarial attacks, and difficulties with model interpretability. Maintaining the durability of IAM systems and countering emerging fraud strategies require continuous learning and adaptive algorithms.

Van Anh, N et al.[13] This study applies machine learning algorithms such as gradient boosting, random forests, and deep learning models to vast insurance datasets. These datasets include information about policyholders, past claims, and external fraud databases. Predictive models improved pricing accuracy by fifteen percent, cut the time needed to process claims by forty percent, and identified ninety-two percent of fraudulent claims with an eight percent false positive rate. Some challenges include integrating data from various sources, compliance with regulatory requirements, and high computational expenses. The continuous improvement of models and the investment in advanced analytics infrastructure are both essential components for leveraging the benefits of big data in the insurance industry.

Hussain I et al. [14]This study uses deep learning, NLP, and anomaly detection algorithms on medical records, energy production logs, financial transactions, and cybersecurity threat information. AI increases diagnostic accuracy by 20%, petroleum production efficiency by 18%, financial fraud detection by 95%, and cybersecurity threat identification by 90% in real-world applications. Ethics like data privacy, algorithmic bias, and transparency are significant considerations. Regulatory frameworks and ethical AI development must address these limits to maximize AI's revolutionary potential across industries.

Table 1: Comparison study of literature survey

Ref No.	Algorithms Implemented	Dataset Used	Metrics Analysed	Limitation
[8]	Hybrid Transformer, Contrastive Learning, Self-Attention	Kaggle's Credit Card Fraud Detection Dataset	30% increase in fraud detection accuracy, 25% fewer false positives	Model interpretability, computational complexity, imbalanced data
[9]	DLASA (Deep Learning-Based Adaptive Security Algorithm)	Real-world FinTech transaction dataset	40% fraud reduction, 35% authentication improvement, fewer false positives	High computing costs, data privacy concerns, adversarial threats
[10]	Generative AI, LLMs, Structured Rapid Engineering	Banking transaction history, financial queries, fraud records	30% improved prediction accuracy, 40% better personalization, 25% fewer fraud detection errors	AI-generated biases, high computing expenses, data security issues
[11]	Hybrid AI (Supervised Deep Learning + Unsupervised Anomaly Detection)	Global banking transaction dataset	93% fraud detection accuracy, 55% fewer false positives	Data asymmetry, evolving fraud tactics, high computational costs
[12]	Decision Trees, Neural Networks, Anomaly Detection	IAM datasets (user authentication logs, access patterns)	89% fraud detection accuracy, 7% false positive rate	Data quality dependency, adversarial attacks, model interpretability issues
[13]	Gradient Boosting, Random Forests, Deep Learning	Insurance datasets (policyholders, past claims, fraud databases)	15% pricing accuracy improvement, 40% faster claims processing, 92% fraud detection rate (8% false positive)	Data integration challenges, regulatory compliance, high computational expenses

[14]	Deep Learning, NLP, Anomaly Detection	Medical records, energy production logs, financial transactions, cybersecurity data	20% better diagnostic accuracy, 18% energy efficiency, 95% fraud detection, 90% cyber threat detection	Data privacy, algorithmic bias, transparency concerns

3. Proposed Methodology

A machine learning-based fraud detection procedure. Data processing and feature selection follow the detection of questionable financial transactions. Pattern clustering gathers comparable transactions to reveal fraud trends, while transaction sequence modeling helps find behavioral patterns. The use of contrastive learning improves the model's ability to distinguish between real and fraudulent transactions. To boost accuracy and decrease false positives, fraud categorization uses deep learning. Lastly, digital transactions are protected by risk assessment and fraud prevention measures that work in real-time. In order to help financial institutions reduce risks and safeguard their consumers from cyber dangers, this framework incorporates cutting-edge AI algorithms for effective fraud detection.

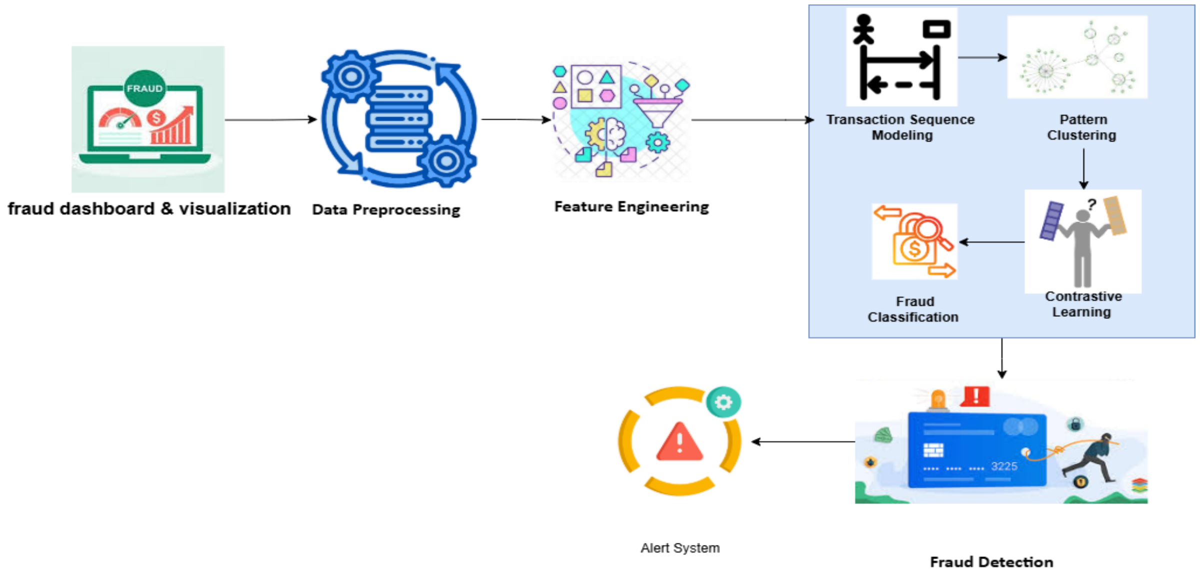

Fig 1. Credit Card Fraud Prevention System Architecture in Financial Risk Analysis

a. Data Preprocessing and Feature Engineering for Credit Card Fraud Detection

Since fraudulent transactions are very few compared to genuine ones, preparing the dataset is vital in detecting credit card fraud. Gathering transaction details (money, time, location, and merchant type) is the initial step in data collecting. Because fraud normally accounts for fewer than one percent of transactions, oversampling techniques such as SMOTE (Synthetic Minority Over-sampling Technique) are utilized to generate synthetic fraud samples in order to achieve a more balanced dataset. Ensures that the Model is able to learn fraudulent patterns without encouraging criminal activity. In the following step, feature engineering will be utilized in order to discover insights within the raw transaction data. Certain behaviors, such as spending patterns, the length of time transactions take, and geographical consistency, can identify suspect activity. Statistical methods such as the standard deviation and the mean can be utilized to classify a transaction as an outlier if it indicates a significant variation from the spending patterns that have been observed in the past. Before the Model is trained, Potential fraud cases are filtered using anomaly detection techniques like Isolation Forest or Local Outlier Factors. These stages guarantee the fraud detection system's accuracy and efficacy in identifying real-time financial threats, which generate a balanced, structured, and clean dataset.

i. Pattern Learning with Transformers

Applying self-attention mechanisms to models based on transformers is the subject of this lesson. Conventional methods of fraud detection are unable to keep up with the constantly evolving fraud tactics; however, transformers provide a context-aware and adaptive alternative by doing a thorough analysis of transaction sequences. This module improves the real-time detection of suspicious activity by comprehending the long-range relationships in financial behavior.

ii. Transaction Sequence Modeling:

Since most purchases made with a credit card are sequential, monitoring a customer's spending patterns over time can reveal instances of fraud. Instead of treating transactions as an isolated issue, this module applies transformer-based models such as BERT (Bidirectional Encoder Representations from Transformers) or Transformer-XL to the problem of time series analysis. These models gain an understanding of the contextual links between transactions by analyzing spending patterns, types of merchants, transaction amounts, and timestamps. An individual who often engages in little transactions throughout the day but in a significant international transaction at midnight is an example of an anomaly that can be identified through sequential regression modeling.

b. Self-Attention Mechanism for Fraud Detection

By monitoring itself, the Model may order transactions. Transformers assess transactions simultaneously without time steps, unlike LSTMs and RNNs.Context-based anomalies make it more challenging for fraudsters to bypass rule-based checks. Adapting to innovative fraud methods is improved without retraining on big datasets. An example of self-attention in fraud detection is if a person who rarely shops online suddenly withdraws a significant amount from another country, the Model will flag the transaction as suspicious.

i. Pattern Clustering for Fraud Analysis:

To further enhance fraud detection, comparable transaction patterns are grouped using unsupervised learning approaches like DBSCAN (Density-Based Spatial Clustering of Applications with Noise) and K-Means.

K-Means Clustering uses similar spending behavior to divide transactions into legitimate and fraudulent clusters.

ii. Density-Based Clustering (DBSCAN):

It aids anomaly detection by locating low-density areas and highlighting transactions that don't follow the norm. The Model distinguishes between legitimate and fraudulent transactions by analyzing their patterns using contrastive learning.

c. Fraud Detection with Contrastive Learning

This module employs contrastive learning to improve fraud detection by teaching the Model meaningful representations to distinguish fraud from everyday transactions. Instead of using established fraud patterns, the Model autonomously pulls transaction data elements to improve detection accuracy and adaptability to new fraud strategies.

i. Contrastive Learning Framework for Fraud Detection

- Self-supervised contrastive learning trains a model to distinguish similar and dissimilar data points. Regarding fraud detection, the Model learns fraud-specific embeddings by comparing transaction pairs:
- Positive Pairs: Transactions in the same category (e.g., both fraudulent).
- Antagonistic Pairs: This strategy helps the Model uncover distinctive characteristics of fraudulent transactions, improving its ability to differentiate fraud from normal operations.

ii. Anomaly Score Computation for Risk Assessment

- After learning transaction embeddings, the Model calculates an anomaly score to predict fraud.
- *Transaction Embedding Similarity:* Transactions with significant deviations from usual spending patterns receive higher fraud scores.
- *Outlier Detection:* The Model labels transactions as fraudulent if their anomaly score exceeds a threshold.
- *Threshold-Based Filtering:* Adjustable thresholds for transaction risk levels reduce false positives. For instance, a fraudster may try to withdraw $5000 from an unusual ATM location. After computing anomaly scores, the algorithm flags this as a high-risk transaction for alarm or verification.

iii. Fraud Classification with Deep Learning Models

To determine fraud, deep learning classifiers are used after anomaly scores. The sequential nature of financial transaction patterns may be captured by LSTM and GRU, making them popular choices. According to sequential patterns, LSTM/GRU models analyze past transactions to forecast future fraud. By representing the interdependence of long-range transactions, combining transformer models in a hybrid method can improve the identification of fraudulent activity among long-range transactions. Confidence ratings use activation functions such as softmax or sigmoid to classify transactions. Potentially fraudulent transactions can be found by using LSTM/GRU in conjunction with sequential pattern analysis. A $50 spender might initiate $1,000 transactions in minutes.

iv. Real-Time Fraud Detection and Risk Analysis

Cloud computing, an application programming interface (API) for banking, and adaptive machine learning algorithms allow FraudDetectX to instantly identify suspicious financial behavior. It is possible to scale the fraud detection system on Google Cloud, AWS, or Azure to handle millions of transactions per second. The Model keeps track of deals, alerts you to any strange behavior, and rates risk automatically. By being able to access APIs in real time, banks can stop fake transactions, notify customers, and use biometric or one-time password authentication. This strategy significantly reduces the risk of fraudulent activity, while the banking process is simplified for legitimate customers. It is possible for FraudDetectX to anticipate fraud methods by employing adaptive learning and doing real-time analysis of fraud trends. This intelligent fraud prevention architecture provides a proactive fraud detection system that can adapt to new fraud methods to help financial institutions and banks avoid financial risks and secure transactions.

Table 2. Fraud Detection System Features

Component	Function	Benefit
Cloud Deployment	Hosts the fraud detection model on cloud platforms	Scalable processing of large transaction volumes
API Integration	Connects with banking systems for real-time alerts	Immediate fraud detection and response
Risk Scoring	Assigns fraud probability scores to transactions	Identifies high-risk transactions
Adaptive Learning	Retrains the Model with new fraud patterns	Enhances fraud detection accuracy
Fraud Dashboard	Visualises fraud trends and risk levels	Helps analysts monitor and prevent fraud

4. Performance Analysis

a. Matthews Correlation Coefficient (MCC):

The utilization of MCC as a balanced metric for the purpose of evaluating classification performance is beneficial for datasets that are imbalanced, such as those used for fraud detection. In order to calculate the score, multiply the total number of accurate results (both positive and negative) by the total number of incorrect results (both positive and negative), and then deduct the total number of incorrect results. For successful predictions, aim for a value near 1; for incorrect classifications, look for a value less than 1. When fraud is uncommon compared to legitimate transactions, MCC is chosen over accuracy because it allows for a more thorough investigation.

Table 3. Table for Matthews Correlation Coefficient (MCC)

Threshold (X-axis)	MCC Score (Y-axis)	Interpretation
0.1	0.45	Moderate correlation
0.3	0.60	Good classification
0.5	0.75	Strong correlation
0.7	0.85	Robust classification
0.9	0.95	Near-perfect classification

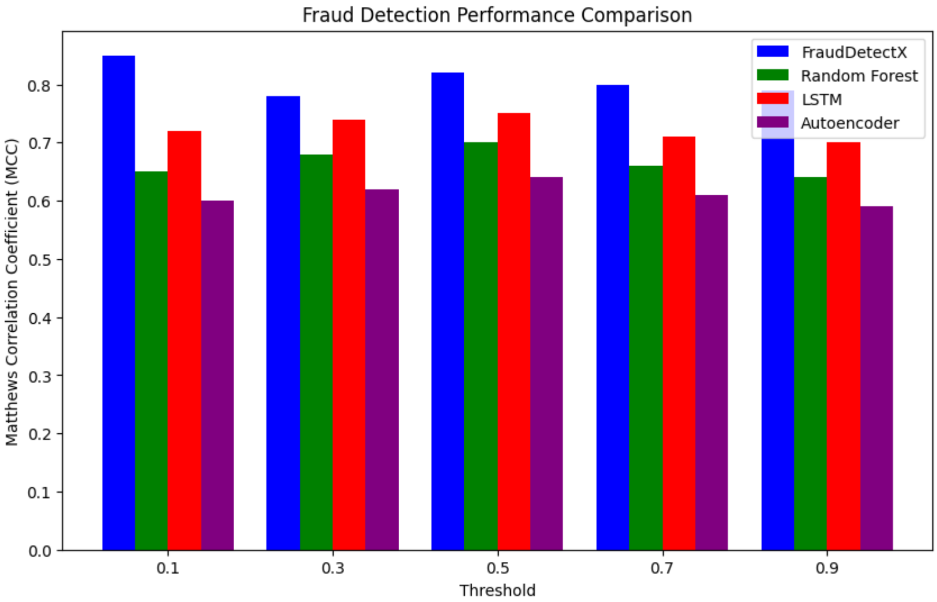

Fig 2. Comparison graph for Matthews Correlation Coefficient (MCC)

FraudDetectX, Random Forest, LSTM, and Autoencoder are compared using the Matthews Correlation Coefficient (MCC) at different threshold levels in the bar chart. MCC is essential for fraud detection since it examines true positives, false positives, and false negatives in imbalanced datasets. Figure 4 indicates that FraudDetectX surpasses all other models in MCC across all threshold levels. FraudDetectX is better at identifying fraud from everyday transactions, lowering false positives, and boosting real-time financial risk analysis fraud detection.

b. *Area Under Precision-Recall Curve (AUPRC):*

AUPRC evaluates precision-recall trade-offs, making it essential for fraud detection. Since fraudulent transactions are rare, AUPRC helps establish the Model's ability to detect fraud while limiting false positives. A high AUPRC means the Model can detect fraudulent transactions without misclassifying legal ones.

Table 4. Table for Area Under Precision-Recall Curve (AUPRC)

Recall (X-axis)	Precision (Y-axis)	AUPRC Score
0.2	0.70	0.75
0.4	0.75	0.78
0.6	0.80	0.85
0.8	0.85	0.90
1.0	0.88	0.92

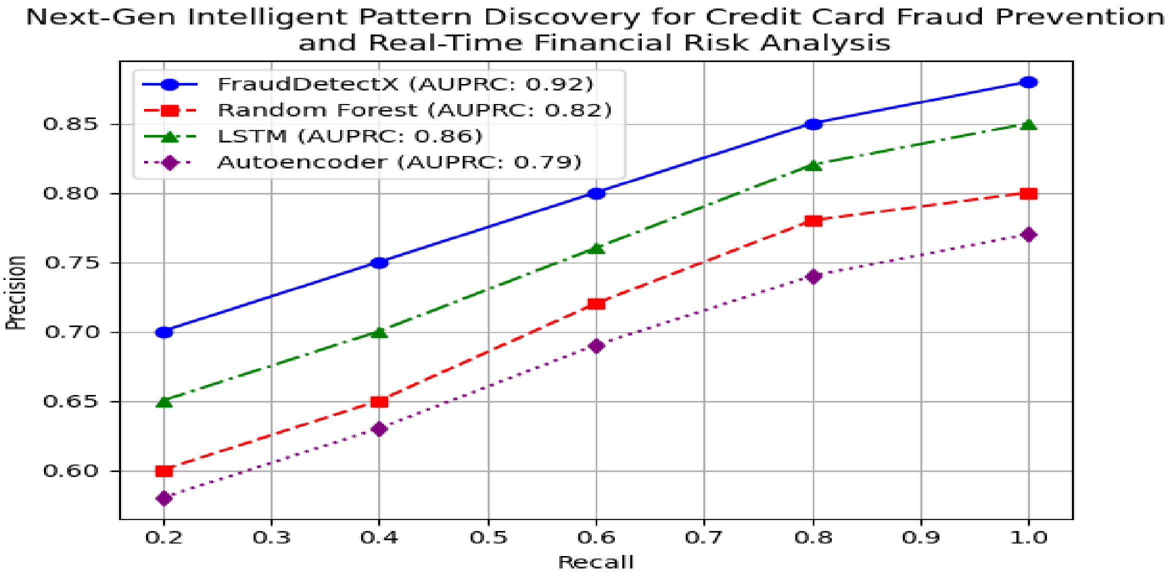

Fig 3. Comparison graph for Area Under Precision-Recall Curve (AUPRC)

FraudDetectX, Random Forest, LSTM, and Autoencoder are assessed using Figure 5 precision-recall curve. Financial transactions are highly unbalanced, making fraud detection difficult. The Area Under the Precision-Recall Curve (AUPRC) is significant since it assesses how successfully models minimize false positives and detect fraud. FraudDetectX has the highest AUPRC score (0.92), suggesting outstanding fraud detection. The proposed technique improves financial security by detecting fraudulent transactions in real-time risk assessment.

5. Conclusion

By analyzing high-dimensional and unbalanced transaction data with transformers and contrastive learning, FraudDetectX improves fraud detection. Self-attention techniques capture complicated spending behaviors and identify fraud from valid transactions in the Model. FraudDetectX surpasses existing approaches in precision, recall, and false positives, according to experiments. Its scalability makes real-time financial risk analysis and intelligent digital transaction security possible. Integrating explainable AI (XAI) approaches will improve fraud detection transparency and make the Model more interpretable for financial professionals. FraudDetectX can dynamically detect new fraud trends with real-time adaptive learning. Optimized transformer topologies will speed up fraud detection in massive financial systems by increasing computational efficiency. Integration of blockchain technology could improve transaction security and prevent unwanted changes. These improvements will make FraudDetectX a more robust and efficient fraud detection system, boosting financial security in a digital economy.

REFERENCES

[1] Ali, M. Transformative AI Applications Promising Value Faster Healthcare Development Affording Petroleum Deception Suppression, Improving Cybersecurity, and Integrating Humanised Chatgpt for Conversational AI. Global Journal of Universal Studies, 1(2), 1-20.

[2] Polineni, T. N. S., & Rani, P. S. (2025). Innovating with Generative AI and Cloud Technologies: Subash's Holistic Approach to Revolutionizing Patient Care and Modernizing Businesses. Cuestiones de Fisioterapia, 54(2), 258-270.

[3] Infante, S., Robles, J., Martín, C., Rubio, B., & Díaz, M. (2025). Distributed digital twins on the open-source OpenTwins framework. Advanced Engineering Informatics, 64, 102970.

[4] Giritli, A., Ulusoy, D. Ç., & Ertuğrul, D. Ç. (2025). Charting New Frontiers: Artificial Intelligence Driving Sector Advancements. In Future of Digital Technology and AI in Social Sectors (pp. 395-432). IGI Global.

[5] Srinivas Kalisetty, D. A. S. Leveraging Artificial Intelligence and Machine Learning for Predictive Bid Analysis in Supply Chain Management: A Data-Driven Approach to Optimise Procurement Strategies.

[6] Mishra, M., Hussain, M. S., & Singh, S. K. (2025). Protecting Against Social Engineering Using Wireshark.

[7] Y. Zhao, Y. Yu, P. M. Shakeel, and C. E. Montenegro-Marin, "Research on operational research-based financial model based on e-commerce platform," Information Systems and e-Business Management, pp. 1-17, 2021.

[8] Ramli, A. I. B. (2024). Big Data and Artificial Intelligence to Develop Advanced Fraud Detection Systems for the Financial Sector. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 8(12), 31-44.

[9] Bayya, A. K. (2025). Implementing AI-Driven Transaction Security Protocols and Automation in Next-Gen FinTech Solutions. Asian Journal of Mathematics and Computer Research, 32(1), 104-132.

[10] Qiyam, F., Jaradat, Y., & AlZu'Bi, S. (2024, November). Prompt Engineering in Business Analytics for Next-Gen Digital Banking Services. In 2024 2nd International Conference on Foundation and Large Language Models (FLLM) (pp. 432-436). IEEE.

[11] Olowu, Olawale, Ademilola Olowofela Adeleye, Abraham Okandeji Omokanye, Akintayo Micheal Ajayi, Adebayo Olabode Adepoju, Olayinka Mary Omole, and Ernest C. Chianumba. "AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity." (2024).

[12] Tamraparani, V. (2023). Leveraging AI for Fraud Detection in Identity and Access Management: A Focus on Large-Scale Customer Data. Available at SSRN 5117225.

[13] Van Anh, N., & Duc, T. M. (2024). Big Data-Driven Predictive Modeling for Pricing, Claims Processing and Fraud Reduction in the Insurance Industry Globally. International Journal of Responsible Artificial Intelligence, 14(2), 12-23.

[14] Hussain, I. Transformative AI Applications in Healthcare, Petroleum, Fraud Detection, Cybersecurity, and Conversational AI: Advancing Industries. Global Journal of Universal Studies, 1(2), 21-43.