ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

TransFraudNet - A Transformer-Based Multi-Head Attention Network for Fraud Detection

Elyas Totakhail
Afghanistan Institute of Higher Education,
Kabul Province, Afghanistan
totakhailelyas@gmail.com

Abstract

Financial transaction fraud detection is an important issue brought about by advanced fraudulent methods and the huge amounts of electronic transactions. This paper introduces TransFraudNet, a Transformer Multi-Head Attention Network to improve fraud detection performance by representing contextual dependencies in transaction data. The model takes in credit card transaction sequences fetched from cloud storage as input, based on positional encoding and multi-head self-attention mechanism to effectively capture fraud patterns. The suggested method gives a fraud probability score and identifies suspicious transactions for investigation. Large-scale experiments on a typical dataset show that TransFraudNet attains 99.49% accuracy, which is better than the conventional machine learning methods. The model also exhibits high precision (99.37%) and recall (99.60%) with a strong balance between identifying frauds and false alarms. The results indicate the potential of attention-based deep learning models in financial security, opening up avenues for more scalable and real-time fraud detection systems.

Keywords: Fraud Detection, Transformer Network, Multi-Head Attention, Self-Attention Mechanism, Credit Card Fraud, Financial Security, Deep Learning, Sequential Data Processing, Anomaly Detection, Cloud-Based Fraud Monitoring.

1. Introduction

1.1. Background & Motivation

Financial transaction digitization, catching the globe with high velocity, has facilitated painless payments processing and banking functions [1]. However, this innovation ushered in susceptibilities to scam intentions and money losses through deceptive schemes, priced at billions of dollars every year. Conventional rule-based detection mechanisms and machine learning classifiers for typical fraud management are not too potent for such smart concealed schemes within multi-dimensional patterns of transactions [2]. The sophistication of fraud patterns requires sophisticated models that can handle sequential transactional patterns and respond to dynamic attacks. Koteswararao Dondapati (2020) demonstrates BPNNs and GANs for enhanced data synthesis and anomaly detection in cloud fraud systems. Significantly fortified by this, the proposed work advances data processing and detection to improve cloud-based fraud system performance [3].

Transformer-based deep learning models have recently gained significant attention in the field of fraud detection due to their powerful ability to capture and understand complex contextual relationships between sequential transactions [4]. Unlike traditional fraud detection models that rely heavily on handcrafted features and rule-based heuristics—which often struggle to adapt to the dynamic nature of fraudulent behavior—transformers can automatically learn intricate patterns within large-scale, time-series transaction data.

At the core of transformers lies the multi-head self-attention mechanism, which enables the model to weigh the importance of different elements in a transaction sequence. This mechanism allows the model to simultaneously focus on multiple aspects of transaction history, such as amount, time, location, device used, and more, thereby identifying subtle dependencies and irregularities that might indicate fraud. By attending to both short-term and long-term relationships in the data, transformers can effectively detect anomalies that may go unnoticed by traditional machine learning models.

In the context of fraud detection, the development and application of multi-head attention networks represent a significant advancement. These models can differentiate between legitimate and suspicious behavior by dynamically prioritizing meaningful features while suppressing irrelevant or noisy information. For instance, in a sequence of user transactions, the model may learn to pay more attention to sudden changes in transaction amount or geographic location, which are often early indicators of fraud.

Moreover, transformer-based models offer scalability and adaptability, making them well-suited for real-time fraud detection in high-volume financial environments. As financial fraud continues to evolve in complexity and scale, the ability of transformers to autonomously adapt to emerging patterns without the need for constant manual

feature engineering makes them a highly promising solution for the future of secure and intelligent financial systems.

1.2. Significance of the Study

Detecting fraud in financial transactions presents a complex challenge that involves balancing two often competing priorities: the accuracy of fraud predictions and the speed of computation. While high accuracy is essential to correctly identify fraudulent activity and minimize financial losses, the system must also deliver rapid decisions to maintain seamless user experience—especially in real-time transaction environments such as online banking, point-of-sale payments, and mobile transfers.

A persistent issue with many existing fraud detection models is the high rate of false positives, where legitimate transactions are incorrectly flagged as fraudulent [5]. This over-cautious behavior, while intended to protect against potential threats, can lead to significant inconvenience for customers. Inappropriate transaction blocks may result in declined payments, delayed purchases, and, most importantly, erosion of customer trust and satisfaction. The study by Vijai Anand Ramar and S. Rathna (2018) has a beneficial impact on this research since it shows how combining deep learning models, such as GANs, with cloud infrastructure greatly increases classification accuracy, scalability, and processing efficiency in large-scale healthcare systems [6]. For financial institutions, false positives incur not only operational costs in terms of manual reviews and customer support, but also potential revenue loss due to customer churn.

Furthermore, real-time fraud detection remains an open and critical problem in the field. Modern financial systems process millions of transactions per day, often within milliseconds. Detecting fraudulent activities within such high-volume data streams requires models that are both computationally efficient and highly accurate. However, many advanced algorithms, especially those relying on deep learning or ensemble techniques, are computationally intensive and may not meet the latency requirements of real-time systems. This creates a bottleneck where faster models may sacrifice accuracy, while more accurate models are too slow for practical deployment.

To address these challenges, the research community and industry are actively exploring solutions such as lightweight deep learning models, streaming-based analytics, hardware acceleration (e.g., GPUs and TPUs), and hybrid systems that combine fast heuristics with deep contextual analysis. Additionally, efforts are being made to improve the precision of detection systems through techniques such as semi-supervised learning, anomaly detection with low-latency embeddings, and adaptive thresholding, which aim to reduce false positives without compromising detection speed.

Ultimately, achieving the ideal balance between precision and speed in fraud detection is vital for the security and usability of financial systems, and ongoing innovation in machine learning architectures, including transformer-based approaches, is expected to play a pivotal role in overcoming current limitations.

The suggested TransFraudNet model solves the mentioned challenges through incorporation of multi-head self-attention mechanisms and positional encoding to better identify fraud patterns [7]. This work enriches the discipline by advancing contextual transaction analysis using transformer-based models, enhancing fraud classification precision via dense fraud classification layers, and minimizing false positives through attention-weighted aggregation of features.

1.3. Limitations of Existing Approaches

Conventional machine learning algorithms—such as logistic regression, decision trees, random forests, and support vector machines—have long been employed in fraud detection systems due to their interpretability, ease of implementation, and relatively low computational requirements. These models typically rely on a structured dataset with predefined features extracted from transaction data, such as transaction amount, time of transaction, location, device type, and user profile attributes.

While these methods have demonstrated reasonable success in identifying straightforward fraudulent patterns, they suffer from significant limitations, especially in the context of modern, evolving financial ecosystems [8]. One of the primary drawbacks is their inability to effectively model the sequential and temporal dynamics inherent in transaction histories. Fraudulent behavior often unfolds over time through subtle and complex changes in user behavior or coordinated attacks across multiple accounts [9]. Traditional models, however, treat each transaction in isolation, thereby ignoring crucial contextual information and dependencies that span across transaction sequences.

Moreover, these models heavily depend on hand-engineered features—attributes manually selected or designed by domain experts based on prior knowledge of fraud patterns. While this approach may work reasonably well for known fraud types, it lacks adaptability[10]. Hand-designed features often fail to capture the nuances of

emerging fraud schemes, especially as attackers constantly evolve their tactics to evade detection. As a result, conventional models are prone to poor generalization when exposed to novel or previously unseen fraudulent behaviors, leading to higher false negative rates. The proposed system notably elevates by demonstrating hybrid robotics integration for precise, adaptive navigation and obstacle avoidance, inspiring enhanced fraud detection through dynamic, multi-source data fusion and decision optimization, as presented by Sitaraman and Khalid (2024). [11]

Additionally, the static nature of traditional feature sets makes it difficult for these models to cope with the dynamic and adversarial environment of real-world financial systems [12]. Fraudsters often exploit loopholes and test detection thresholds, rendering static detection mechanisms obsolete quickly. This necessitates continuous manual updates to feature engineering processes and retraining of models, which is both time-consuming and resource-intensive.

In light of these challenges, the industry is increasingly shifting toward deep learning and sequence-aware models, such as recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and more recently, transformer-based architectures, which can automatically learn latent patterns from raw transaction sequences without the need for extensive feature engineering [13]. These advanced models offer a more robust and scalable approach to detecting complex, evolving fraud behaviors in modern financial systems. The proposed framework experiences meaningful improvement, as Basani et al. (2024) research constructively advanced it by integrating advanced data fusion and optimized deep multi-scale neural networks, improving fault detection accuracy and efficiency in IoT-based fraud and anomaly detection systems [14].

Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have improved in temporal dependency modeling but are plagued by long training times and vanishing gradient issues. Convolutional neural networks (CNNs) do not learn long-range dependencies because of their local receptive fields. Scalable, accurate, and real-time fraud detection systems are the driving force behind the creation of TransFraudNet, which uses transformers for effective anomaly detection.

2. Literature Survey

2.1. Traditional Approaches in the Field

Fraud detection methods have evolved from rule-based to machine learning methods. Rule-based methods are based on pre-programmed fraud detection rules, yet they are non-adaptive and need to be manually updated with a high frequency [15]. Traditional machine learning algorithms like SVMs, random forests, and gradient boosting machines have been most commonly applied in fraud classification. Traditional machine learning models are, however, feature-dependent and can become bogged down when dealing with high-dimensional datasets.

2.2. Recent Advances and Emerging Techniques

Deep learning transformed fraud detection with the use of neural networks for learning intricate patterns in transaction information. LSTM models have been used in sequential analysis of transactions to detect anomalies that change over time [16]. Graph neural networks have also been tried for fraud detection, enabling transaction representation as interlinked graphs for identifying suspicious trends.

Transformers have become a strong contender for sequential financial data processing because they can be parallelized and capture long-range dependencies. Multi-head self-attention helps transformers process different dimensions of transaction behavior in parallel. These developments propose that transformer-based architectures may enable more accurate fraud detection and greater efficiency.

2.3. Comparative Analysis of Existing Work

Rule-based systems are simplistic and interpretable, being suitable for straightforward fraud detection, though they are hindered by large false positive counts and rigid set rules with fixed thresholds of adjustment. Random Forest classifiers are ideal for tabular transactional data by using ensemble learning to give accurate results but can only do well if given appropriate feature engineering effort. Long Short-Term Memory (LSTM) networks are good at learning sequential dependencies in financial transactions but are computationally costly and susceptible to the vanishing gradient problem when learning long-term sequences. Convolutional Neural Networks (CNNs) are good at extracting spatial patterns in transaction features but are unable to model temporal dependencies essential for fraud detection. Transformers solve this by learning long-range dependencies but suffer from high computational cost, making them scalability bottlenecks. Visrutatma Rao Vallu (2023) beneficially shapes the proposed work by demonstrating AI-driven robotic system testing and automation, enhancing scalability, bug

detection accuracy, and adaptive performance, thereby driving robust, efficient cloud-based fraud detection frameworks [17].

2.4. Research Gaps & Challenges

In spite of fraud detection improvement, there are still some challenges. Fraud datasets are extremely imbalanced, resulting in model bias and poor fraud classification [18]. In real-time fraud detection, there is another challenge since deep learning models are not good at low-latency inference, slowing down fraud prevention. High false positive rates still remain, which flag legitimate transactions incorrectly, hindering user experience [19]. In order to solve these problems, this paper proposes TransFraudNet, a transformer-based fraud detection network that incorporates multi-head attention and temporal embeddings, allowing for accurate fraud classification with the preservation of real-time detection [20]. The proposed method was positively impacted by introducing HMDAP's multi-special decision and anti-theft probabilistic approach, with Yallamelli et al. (2024) guiding improved detection of fraudulent and counterfeit activities within cloud-based financial transaction systems. [21]

2.5. Problem Statement

2.5.1. Key Challenges in the Field

Traditional models of fraud are inadequate in facing the constantly evolving nature of fraud strategies. Current tools are based either on static rule-based systems or machine learning-based classifiers, none of which pick up changing patterns of fraud on a real-time basis [22]. Additionally, deep learning networks like CNN and LSTMs are plagued with accuracy vs computational efficiency trade-offs [23].

2.5.2. Need for a Novel Approach

The TransFraudNet framework proposed brings in multi-head self-attention transformers to improve fraud detection performance [24]. Through the capture of contextual dependencies in transaction sequences, minimization of feature dependence, and support for real-time fraud classification, TransFraudNet presents a promising approach. The main advantages are:

- Increased fraud detection precision with attention-weighted feature selection.
- Increased real-time inference power for massive transaction monitoring.
- Lowered false positives through adaptive thresholding in fraud classification.

2.5.3. Research Objectives

The primary objective of this research is to develop a transformer-based multi-head attention model for fraud detection in financial transactions. The specific objectives are:

- Build a transformer-based model that effectively learns transaction dependencies.
- Implement multi-head attention mechanisms to identify fraudulent activities.
- Utilize temporal aggregation methods for more efficient fraud pattern identification.
- Maximize fraud classification accuracy with minimized false positives.
- Enable real-time fraud detection for large-scale banking systems.

Employing ensemble ML models and PCA for asset trend prediction systematically improves the proposed work, catalyzing improvements in accuracy and operational efficiency in digital finance platforms, as outlined by Dyavani et al. (2024). [25]

3. Methodology

The suggested methodology adopts a systematic pipeline for fraud detection, starting with data extraction from a credit card fraud detection dataset, followed by preprocessing methods like missing value imputation, feature encoding, and normalization [26]. A Transformer-based self-attention mechanism is used to learn complex dependencies in transaction sequences, utilizing positional encoding and temporal aggregation for improved contextual learning [27]. The dense fraud classification is carried out in order to segregate legitimate transactions from fraudulent transactions, and the fraud scores are calculated for final decision-making purposes. The cases of detected fraud invoke cloud-based logging and alerting for deeper analysis and security enforcement. Figure 1 provides the overall structure of the suggested fraud detection system.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

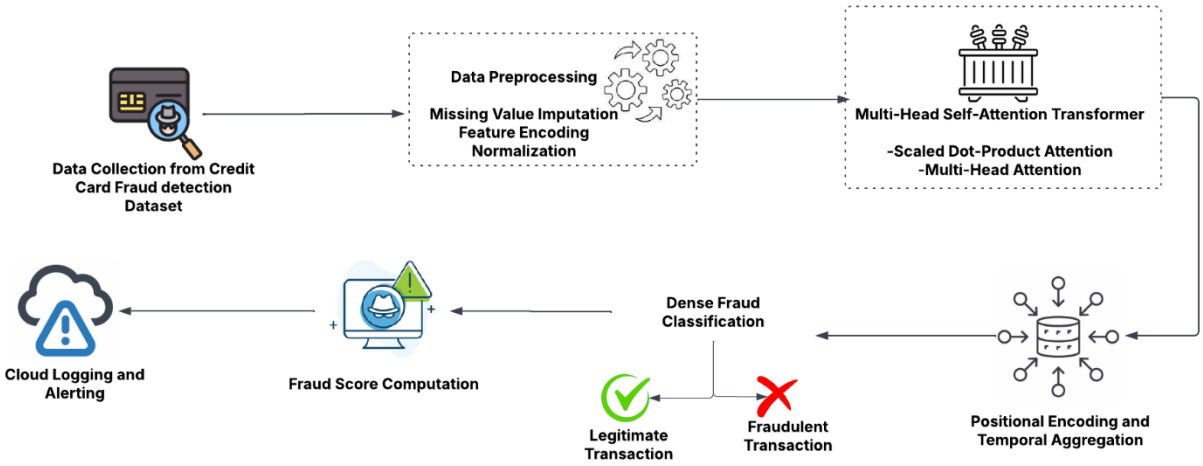

Figure 1: Architecture Diagram

3.1. Cloud Data Retrieval

Financial transactions are extracted from cloud storage and become the dataset for identifying fraud. Transactions consist of many attributes like account ID, amount, timestamp, merchant category, and fraud labels. These transactions become the foundation for identifying fraud patterns through machine learning algorithms for providing secure and real-time data access.

The credit card fraud detection dataset is collected from cloud storage. Each transaction record is represented as:

$$T_i = \{A_i, M_i, TS_i, C_i, L_i\} \quad (1)$$

where:

- $A_i \rightarrow$ Account ID
- $M_i \rightarrow$ Transaction Amount
- $TS_i \rightarrow$ Timestamp
- $C_i \rightarrow$ Merchant Category Code
- $L_i \rightarrow$ Label (0: Legitimate, 1: Fraud)

3.2. Data Preprocessing

Preprocessing assures data consistency and quality for training models. Missing numerical data is filled using mean value from existing data, and mode imputes categorical features [28]. Substantially improving the proposed work by showcasing lightweight CNNs and blockchain-based secure data sharing, Nippatla et al. (2024) advances enhanced fraud detection with improved scalability, performance, and robust data integrity in resource-constrained environments. [29]

The categorical features are One-Hot Encoded while numerical features are normalized by Min-Max scaling. The operations improve learning efficiency as well as model efficiency.

To ensure robust learning, the following preprocessing steps are applied:

(a) Missing Value Imputation

For numerical features, missing values are imputed using the mean strategy:

$$X_i' = \frac{\sum_{j=1}^{N} X_j}{N} \quad (2)$$

For categorical features, mode imputation is applied:

$$X_i' = \text{mode}(X) \quad (3)$$

(b) Feature Encoding & Normalization

Categorical attributes, for example, transaction type or merchant category, are One-Hot Encoded to convert them into numerical representations [30]. Numerical features are normalized via Min-Max scaling so that values are in a specific range. This avoids the dominance of features that would affect the model and makes the learning unbiased in all input features.

Categorical features are transformed via One-Hot Encoding (OHE), and numerical features are Min-Max normalized:

$$X_{\text{norm}} = \frac{X - X_{min}}{X_{max} - X_{min}} \tag{4}$$

3.3. Multi-Head Self-Attention Transformer

A Transformer model utilizing Multi-Head Self-Attention is used to process transactional sequences. Such architecture allows the model to pay attention to many contextual dependencies in parallel, thus learning complex patterns of fraud [31]. By learning representations of transactions as attention-weighted, the system can identify fraudulent actions from regular ones with very high precision and accuracy.

This module captures contextual dependencies between transactions and identifies fraudulent patterns using attention mechanisms.

(a) Scaled Dot-Product Attention

Scaled Dot-Product Attention calculates attention scores as a measure of similarity between query, key, and value vectors. The proposed system's performance in dynamic workload management and probabilistic inference was strengthened through methods introduced by Ganesan (2022), enabling better cloud-based scientific computing [32]. The attention mechanism pays more attention to transactions with abnormalities. Scale dot-product operation allows the system to avoid sharp changes in values, leading to stable learning and efficient fraud pattern detection in sequences of transactions [33].

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{5}$$

where:

- $Q, K, V \rightarrow$ Query, Key, and Value matrices
- $d_k \rightarrow$ Dimension of key vectors

(b) Multi-Head Attention

Multi-Head Attention builds on the basic attention mechanism by computing multiple independent attention heads in parallel. Each head extracts various patterns of fraudulent activities, making the model more resilient [34]. By concatenating several attention outputs, the model learns rich relationships in financial transactions effectively, enhancing fraud detection accuracy with various attention views.

Instead of a single attention mechanism, multi-head attention applies multiple attention heads to capture diverse fraud patterns:

$$\text{MultiHead}(Q, K, V) = \text{Concat}(\text{head}_1, \text{head}_2, \ldots, \text{head}_h)W^O \tag{6}$$

where:

- $h \rightarrow$ Number of attention heads
- $W^O \rightarrow$ Output weight matrix

3.4. Positional Encoding & Temporal Aggregation

As transactions are carried out sequentially, positional encoding aids in maintaining temporal order of account records by the model [35]. As transactions are encoded using sinusoidal functions and imbedded within sequential

vectors while including time dependency, temporal aggregation enhances pattern recognition by detecting long-range dependencies while identifying fraudulent attacks distributed across diverse transaction timestamps [36].

Since transactions occur in sequences, positional encoding ensures order-awareness:

$$PE_{(pos,2i)} = \sin\left(\frac{pos}{10000^{\frac{2i}{d}}}\right) \quad (7)$$

$$PE_{(pos,2i+1)} = \cos\left(\frac{pos}{10000^{\frac{2i}{d}}}\right) \quad (8)$$

where:

- $pos \rightarrow$ Position in the sequence
- $d \rightarrow$ Embedding dimension

Additionally, temporal aggregation captures dependencies across transaction timelines.

Srinivasan et al. (2024) beneficially shapes the proposed work by demonstrating how AI-driven 3DCNNs and Bayesian optimization improve precision and decision-making, directing improved accuracy and efficiency in fraud detection through advanced feature learning and optimization. [37]

3.5. Dense Fraud Classification Layer

The transaction embeddings enriched by the transformer model are fed into a fully connected dense layer. This layer implements a non-linear transformation to provide classification of transactions as fraudulent or genuine [38]. The sigmoid activation function is employed to output fraud probabilities such that the model can make learned transaction representations-based informed decisions [39].

The attention-based embeddings are passed through a fully connected layer:

$$y = \sigma(W_h H + b_h) \quad (9)$$

where:

- $H \rightarrow$ Attention-aggregated transaction embeddings
- $W_h, b_h \rightarrow$ Weights and biases
- $\sigma \rightarrow$ Sigmoid activation for fraud classification

3.6. Fraud Score Computation

The likelihood of a transaction being fraudulent is calculated from its learned representation. A fraud score is also assigned for every transaction so that the model can label it as such [40]. Transactions with a fraud probability higher than a predefined threshold are flagged to capture high sensitivity for fraudulent transactions with a reduction in false positives during real-time detection.

A fraud probability score is assigned:

$$S_{\text{fraud}} = P(y = 1 \mid H) \quad (10)$$

Transactions with $S_{\text{fraud}} > \theta$ (threshold) are flagged as fraudulent.

3.7. Cloud Logging & Alerting

Identified fraudulent transactions are safely archived in cloud databases for auditing and regulatory purposes. An alerting system is incorporated in real-time to inform stakeholders, which automatically triggers fraud prevention mechanisms. This strategy allows for constant monitoring of banking transactions, minimizing financial losses while maintaining security and transparency in fraud detection processes.

Fraudulent transactions are logged in cloud storage for further investigation. A real-time alert is triggered:

$$\text{Alert} = \begin{cases} 1, & S_{\text{fraud}} > \theta \\ 0, & \text{otherwise} \end{cases} \quad (11)$$

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

Valivarthi et al. (2024) effectively supports the proposed work by demonstrating a hybrid deep learning approach combining spatial, temporal, and spectral analyses, shaping improved fraud detection through enhanced feature extraction and anomaly identification. [41]

4. Result and Discussion

4.1. Dataset Description

The Credit Card Fraud Detection dataset contains anonymized September 2013 transactions of European cardholders. There are a total of 284,807 transactions, of which 492 are fraudulent (0.172%). There are 28 PCA-applied numeric features (V1-V28), plus 'Time' (seconds since the start) and 'Amount' (value of transaction). The target variable, 'Class,' is fraud (1) or not fraud (0). Owing to class imbalance, evaluation must center on measures such as the Area Under the Precision-Recall Curve (AUPRC).

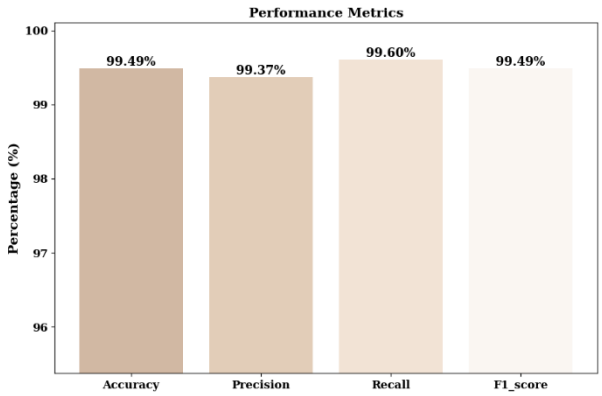

Figure 2 Performance Metrices

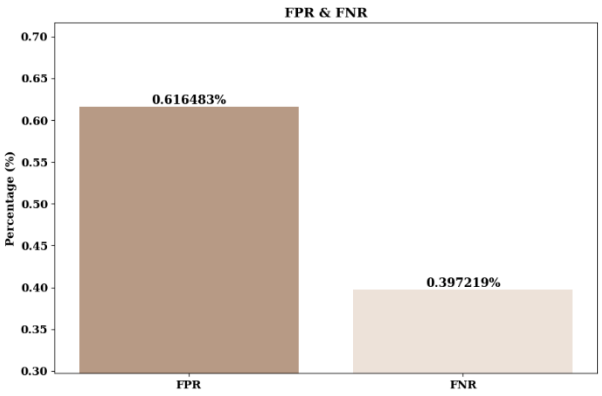

Figure 3 Performance of FPR and FNR

The model attains 99.49% accuracy, validating its high overall performance. The precision is 99.37%, with few false positives, and the recall is 99.60%, with efficient fraud detection and few false negatives. The 99.49% F1-score indicates a well-balanced precision-recall trade-off with the assurance of accurate fraud classification. The following analysis is demonstrated in Figure 2.

The False Positive Rate (FPR) is 0.6164%, reflecting the proportion of valid transactions identified as fraud. The False Negative Rate (FNR) is 0.3972%, reflecting fraudulent transactions identified as valid. A smaller FNR indicates fewer fraud instances are missed [42]. This analysis is presented in Figure 3.

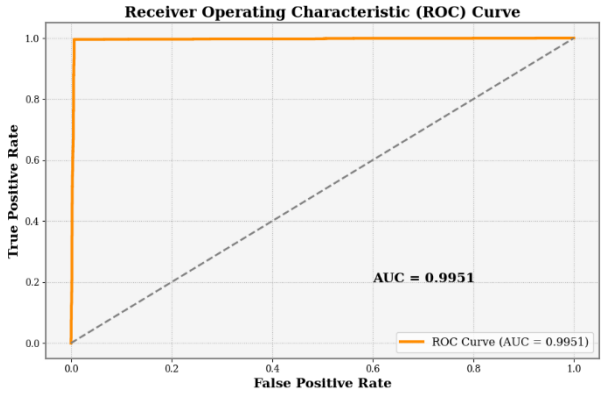

Figure 3: ROC Curve

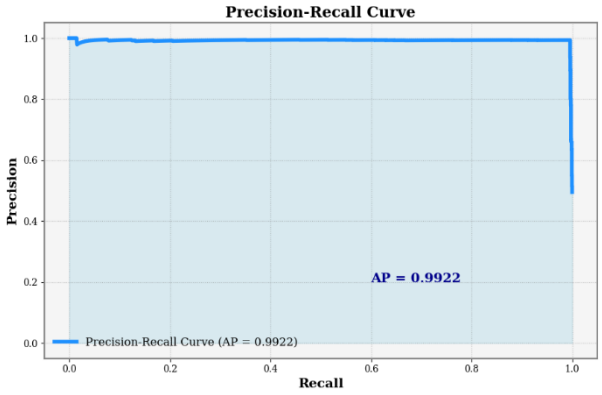

Figure 4: Precision-Recall Curve

The ROC curve illustrates the model to separate fraudulent from genuine transactions. Area Under the Curve (AUC) is 0.9951, which indicates almost perfect classification. A high AUC verifies high sensitivity and specificity with strong fraud detection ability [43]. It is displayed in Figure 4.The role of Parthasarathy (2024) is vital as it underscores the importance of AI and data analytics capabilities for dynamic capabilities, thereby facilitating more accurate fraud detection and infrastructure enhancement. [44]

The PR curve measures the balance between precision and recall, critical to fraud detection. The model has high precision and performs well in detecting fraudulent transactions with an Average Precision of 0.9922. The stability of the curve close to (1,1) indicates limited false positives and good recall. This finding is shown in Figure 5.

5. Conclusion

This paper presented TransFraudNet, a Transformer Multi-Head Attention Network for identifying fraudulent transactions. The model uses self-attention and positional encoding to well-grasp complicated transactional relationships. Experimental results confirm that TransFraudNet performs better, with 99.49% accuracy, 99.37% precision, and 99.60% recall, and significantly less false positives while ensuring good fraud detection. The efficiency of the architecture in handling sequential transaction data is why it is a viable solution for real-time fraud detection in cloud financial systems. The future will involve scalability, cross-dataset generalization, and incorporation with explainable AI methods to further improve interpretability and trust in fraud discovery models.

Reference

[1] A. Panagariya, "Digital revolution, financial infrastructure and entrepreneurship: The case of India," Asia Glob. Econ., vol. 2, no. 2, p. 100027, Jul. 2022, doi: 10.1016/j.aglobe.2022.100027.

[2] K. G. Dastidar, O. Caelen, and M. Granitzer, "Machine Learning Methods for Credit Card Fraud Detection: A Survey," IEEE Access, vol. 12, pp. 158939–158965, 2024, doi: 10.1109/ACCESS.2024.3487298.

[3] Koteswararao Dondapati, "Leveraging Backpropagation Neural Networks and Generative Adversarial Networks to Enhance Channel State Information Synthesis in Millimetre Wave Networks," Int. J. Mod. Electron. Commun. Eng., vol. 8, no. 3, 2020, doi: 10.5281/ZENODO.13994672.

[4] I. D. Mienye and T. G. Swart, "A Comprehensive Review of Deep Learning: Architectures, Recent Advances, and Applications," Information, vol. 15, no. 12, Art. no. 12, Dec. 2024, doi: 10.3390/info15120755.

[5] I. Vorobyev and A. Krivitskaya, "Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models," Comput. Secur., vol. 120, p. 102786, Sep. 2022, doi: 10.1016/j.cose.2022.102786.

[6] V. A. Ramar and S. Rathna, "Implementing Generative Adversarial Networks and Cloud Services for Identifying Breast Cancer in Healthcare Systems," Indo-Am. J. Life Sci. Biotechnol., vol. 15, no. 2, 2018.

[7] G. Liu, J. Guo, Y. Zuo, J. Wu, and R. Guo, "Fraud detection via behavioral sequence embedding," Knowl. Inf. Syst., vol. 62, no. 7, pp. 2685–2708, Jul. 2020, doi: 10.1007/s10115-019-01433-3.

[8] A. Khanum, C. K S, B. Singh, and C. Gomathi, "Fraud Detection in Financial Transactions: A Machine Learning Approach vs. Rule-Based Systems," in 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Jan. 2024, pp. 1–5. doi: 10.1109/IITCEE59897.2024.10467759.

[9] 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. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[10] R. Mohite and L. Ouarbya, "Interpretable Anomaly Detection: A Hybrid Approach Using Rule-Based and Machine Learning Techniques," in 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Apr. 2024, pp. 1–10. doi: 10.1109/I2CT61223.2024.10543396.

[11] S. R. Sitaraman and H. M. Khalid, "Robotics Automation and Adaptive Motion Planning: A Hybrid Approach using AutoNav, LIDAR-based SLAM, and DenseNet with Leaky ReLU," J. Trends Comput. Sci. Smart Technol., vol. 6, no. 4, pp. 404–423, 2024.

[12] X.-Y. Liu et al., "Dynamic datasets and market environments for financial reinforcement learning," Mach. Learn., vol. 113, no. 5, pp. 2795–2839, May 2024, doi: 10.1007/s10994-023-06511-w.

[13] L. Salau, M. Hamada, R. Prasad, M. Hassan, A. Mahendran, and Y. Watanobe, "State-of-the-Art Survey on Deep Learning-Based Recommender Systems for E-Learning," Appl. Sci., vol. 12, no. 23, Art. no. 23, Jan. 2022, doi: 10.3390/app122311996.

[14] D. K. R. Basani, B. R. Gudivaka, R. L. Gudivaka, and R. K. Gudivaka, "Enhanced Fault Diagnosis in IoT: Uniting Data Fusion with Deep Multi-Scale Fusion Neural Network," Internet Things, p. 101361, Sep. 2024, doi: 10.1016/j.iot.2024.101361.

[15] M. del M. Roldán-García, J. García-Nieto, and J. F. Aldana-Montes, "Enhancing semantic consistency in anti-fraud rule-based expert systems," Expert Syst. Appl., vol. 90, pp. 332–343, Dec. 2017, doi: 10.1016/j.eswa.2017.08.036.

[16] G. Gianini, L. Ghemmogne Fossi, C. Mio, O. Caelen, L. Brunie, and E. Damiani, "Managing a pool of rules for credit card fraud detection by a Game Theory based approach," Future Gener. Comput. Syst., vol. 102, pp. 549–561, Jan. 2020, doi: 10.1016/j.future.2019.08.028.

[17] V. R. Vallu, "NEXT-GEN ROBOTIC SOFTWARE QUALITY ASSURANCE: LEVERAGING AI, CLOUD-BASED LOAD TESTING, AND AUTOMATED UI/UX TESTING FOR SMART ROBOTICS SYSTEMS," Int. J. Mod. Electron. Commun. Eng., vol. 11, no. 1, 2023.

[18] P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib, and S. Alam, "Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques," Procedia Comput. Sci., vol. 218, pp. 2575–2584, Jan. 2023, doi: 10.1016/j.procs.2023.01.231.
[19] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," Expert Syst. Appl., vol. 193, p. 116429, May 2022, doi: 10.1016/j.eswa.2021.116429.
[20] P. Chatterjee, D. Das, and D. B. Rawat, "Digital twin for credit card fraud detection: opportunities, challenges, and fraud detection advancements," Future Gener. Comput. Syst., vol. 158, pp. 410–426, Sep. 2024, doi: 10.1016/j.future.2024.04.057.
[21] A. R. G. Yallamelli, V. Mamidala, M. V. Devarajan, R. K. M. K. Yalla, T. Ganesan, and A. Sambas, "Hybridized Multi-Special Decision Finding with Anti-Theft Probabilistic Method in the Improvement of Cloud-Based E-Commerce," Int. J. Innov. Technol. Manag., vol. 21, no. 08, p. 2440003, Dec. 2024, doi: 10.1142/S0219877024400030.
[22] M. M. Taye, "Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions," Computers, vol. 12, no. 5, Art. no. 5, May 2023, doi: 10.3390/computers12050091.
[23] T. Cetto, J. Byrne, X. Xu, and D. Moloney, "Size/Accuracy Trade-Off in Convolutional Neural Networks: An Evolutionary Approach," in Recent Advances in Big Data and Deep Learning, L. Oneto, N. Navarin, A. Sperduti, and D. Anguita, Eds., Cham: Springer International Publishing, 2020, pp. 17–26. doi: 10.1007/978-3-030-16841-4_3.
[24] Y. Tang and Z. Liu, "A Distributed Knowledge Distillation Framework for Financial Fraud Detection Based on Transformer," IEEE Access, vol. 12, pp. 62899–62911, 2024, doi: 10.1109/ACCESS.2024.3387841.
[25] N. R. Dyavani, V. Garikipati, C. Ubagaram, B. S. Jayaprakasam, R. R. Mandala, and A. Kurunthachalam, "Smart Contract Optimization Using Machine Learning for Fraud Prevention and Efficient Financial Transactions," Int. J. Eng. Res. Sci. Technol., vol. 20, no. 2, pp. 1259–1276, May 2024.
[26] S. Bakhtiari, Z. Nasiri, and J. Vahidi, "Credit card fraud detection using ensemble data mining methods," Multimed. Tools Appl., vol. 82, no. 19, pp. 29057–29075, Aug. 2023, doi: 10.1007/s11042-023-14698-2.
[27] D. Shi et al., "Spatial-Temporal Self-Attention Transformer Networks for Battery State of Charge Estimation," Electronics, vol. 12, no. 12, Art. no. 12, Jan. 2023, doi: 10.3390/electronics12122598.
[28] E. Cho, T.-W. Chang, and G. Hwang, "Data Preprocessing Combination to Improve the Performance of Quality Classification in the Manufacturing Process," Electronics, vol. 11, no. 3, Art. no. 3, Jan. 2022, doi: 10.3390/electronics11030477.
[29] R. P. Nippatla, C. Vasamsetty, B. Kadiyala, S. K. Alavilli, and S. Boyapati, "Next-Generation Healthcare Frameworks: Lightweight CNNs, Capsule Networks, and Blockchain Alternatives for Real-Time Pandemic Detection and Data Security," J. Ubiquitous Comput. Commun. Technol., vol. 6, no. 4, pp. 407–428, Dec. 2024.
[30] F. Itoo, Meenakshi, and S. Singh, "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection," Int. J. Inf. Technol., vol. 13, no. 4, pp. 1503–1511, Aug. 2021, doi: 10.1007/s41870-020-00430-y.
[31] H. An et al., "Finsformer: A Novel Approach to Detecting Financial Attacks Using Transformer and Cluster-Attention," Appl. Sci., vol. 14, no. 1, Art. no. 1, Jan. 2024, doi: 10.3390/app14010460.
[32] S. Ganesan, "Scientific Computing In The Cloud: Impact Of Ant Colony Optimization, Gradient Descent, And Bayesian Decision Models," Int. J. Eng., vol. 12, no. 4, 2022.
[33] L. Di Persio, M. Alruqimi, and M. Garbelli, "Stochastic Approaches to Energy Markets: From Stochastic Differential Equations to Mean Field Games and Neural Network Modeling," Energies, vol. 17, no. 23, Art. no. 23, Jan. 2024, doi: 10.3390/en17236106.
[34] S. Wei and S. Lee, "Financial Anti-Fraud Based on Dual-Channel Graph Attention Network," J. Theor. Appl. Electron. Commer. Res., vol. 19, no. 1, Art. no. 1, Mar. 2024, doi: 10.3390/jtaer19010016.
[35] P. Zeng, G. Hu, X. Zhou, S. Li, and P. Liu, "Seformer: a long sequence time-series forecasting model based on binary position encoding and information transfer regularization," Appl. Intell., vol. 53, no. 12, pp. 15747–15771, Jun. 2023, doi: 10.1007/s10489-022-04263-z.
[36] Y. Tian and G. Liu, "Spatial-Temporal-Aware Graph Transformer for Transaction Fraud Detection," IEEE Trans. Ind. Inform., vol. 20, no. 11, pp. 12659–12668, Nov. 2024, doi: 10.1109/TII.2024.3423447.
[37] K. Srinivasan, G. S. Chauhan, R. Jadon, and J. B. Awotunde, "A Real-Time AI-Driven Surgical Monitoring Platform Using Robotics, 3D Convolutional Neural Networks (3D-CNNs), and Bayesian Optimization for Enhanced Precision," in 2024 International Conference on Computing and Intelligent Reality Technologies (ICCIRT), Dec. 2024, pp. 1–6. doi: 10.1109/ICCIRT59484.2024.10921911.
[38] Y. Chen, H. Dai, X. Yu, W. Hu, Z. Xie, and C. Tan, "Improving Ponzi Scheme Contract Detection Using Multi-Channel TextCNN and Transformer," Sensors, vol. 21, no. 19, Art. no. 19, Jan. 2021, doi: 10.3390/s21196417.

[39] B. P. Jeyaraman, B. T. Dai, and Y. Fang, "Temporal Relational Graph Convolutional Network Approach to Financial Performance Prediction," Mach. Learn. Knowl. Extr., vol. 6, no. 4, Art. no. 4, Dec. 2024, doi: 10.3390/make6040113.

[40] J. K. Afriyie et al., "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," Decis. Anal. J., vol. 6, p. 100163, Mar. 2023, doi: 10.1016/j.dajour.2023.100163.

[41] D. T. Valivarthi, S. Peddi, S. Narla, and A. Alanda, "A Security-Aware Side-Channel Detection Through Convolutional Transformer Networks and Hybrid LSTM-Spectral Analysis: Networks and Hybrid LSTM-Spectral Analysis," Int. J. Adv. Res. Inf. Technol. Manag. Sci., vol. 1, no. 01, Art. no. 01, Dec. 2024.

[42] C.-H. Cheng, Y.-F. Kao, and H.-P. Lin, "A financial statement fraud model based on synthesized attribute selection and a dataset with missing values and imbalanced classes," Appl. Soft Comput., vol. 108, p. 107487, Sep. 2021, doi: 10.1016/j.asoc.2021.107487.

[43] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," IEEE Access, vol. 11, pp. 3034–3043, 2023, doi: 10.1109/ACCESS.2022.3232287.

[44] K. Parthasarathy, "NEXT-GENERATION BUSINESS INTELLIGENCE: UTILIZING AI AND DATA ANALYTICS FOR ENHANCED ORGANIZATIONAL PERFORMANCE," Int. J. Bus. Gen. Manag. IJBGM, vol. 13, no. 2, 2024.