AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Rferred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

TrustPay Analytics: Real-Time Fraud Detection Using Behavioral Intelligence in UPI Systems

K. Soumya[1], Bommera Keerthana[2], Bolleboina Rakesh[2], Syed Ziauddin[2], K Varalaxmi[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering (Data science)

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India

ABSTRACT

The rapid growth of digital payment systems has increased the demand for reliable fraud detection mechanisms to ensure secure financial transactions. Traditionally, fraud detection relied on manual verification, rule-based systems, and basic statistical techniques. These conventional approaches required significant human effort, consumed time, and failed to detect complex fraud patterns in large-scale and dynamic transaction data. As digital transactions expanded, these methods became inefficient and lacked real-time decision-making capability. The proposed system presents an intelligent web-based solution for multi-aspect fraud detection in Unified Payments Interface (UPI) transactions using advanced Machine Learning (ML) and Deep Learning (DL) techniques. The system is developed using the Flask web framework and integrates Natural Language Processing (NLP) for handling textual data. Sentence Bidirectional Encoder Representations from Transformers (SBERT) is used for feature extraction, generating contextual embeddings from transaction data. These embeddings are utilized to train multiple classification models, including Gaussian Naive Bayes (GNB), Bernoulli Naive Bayes (BNB), Multinomial Naive Bayes (MNB), and the proposed Histogram-based Gradient Boosting Classifier (HGB). The system performs both binary classification for fraud detection and multi-class classification for transaction types. The proposed HGB model achieves high accuracy with strong Precision, Recall, and F1-Score metrics, outperforming traditional models. The system enables users to upload datasets through a secure login interface and generates real-time predictions with downloadable outputs, ensuring scalability, automation, and improved accuracy in financial fraud detection.

Keywords: Fraud Detection, Unified Payments Interface (UPI), Machine Learning, Deep Learning, Natural Language Processing (NLP), Sentence-BERT (SBERT).

1.INTRODUCTION

The rapid advancement of technology and the widespread adoption of digital payment systems have transformed the way monetary transactions are conducted. However, the increased reliance on digital payment methods has also led to a significant rise in digital payment fraud [1]. Cybercriminals continuously develop sophisticated techniques to exploit vulnerabilities in payment systems, posing serious threats to the security and reliability of online financial transactions. This study focuses on analyzing various approaches for detecting and preventing digital payment fraud within the context of the digital era and Industry 4.0 as shown in Fig. 1.

The primary objective of this research is to develop a comprehensive understanding of the threats faced by digital payment systems and to design effective solutions to mitigate them. Identifying the various types of fraudulent activities associated with digital transactions is essential to understanding the role of fraud detection in the modern era [2]. These activities include identity theft, account takeovers, phishing attacks, and malware-based intrusions. Such fraudulent practices significantly impact individual users, businesses, and financial institutions [3]. The consequences include financial losses, reputational damage, and a decline in customer trust.

Fig. 1: Types of UPI Scams or Frauds.

The emergence of the fourth industrial revolution, known as Industry 4.0, has introduced advanced digital technologies such as Artificial Intelligence (AI) and Big Data Analytics, which have transformed the domain of fraud detection [4]. These technologies provide access to vast volumes of data along with powerful analytical capabilities, enabling the rapid identification of patterns, anomalies, and suspicious behaviors. However, the integration of these technologies also introduces increased complexity and evolving security risks. Therefore, modern fraud detection systems require robust, scalable, and intelligent approaches to effectively handle these challenges and ensure secure digital financial transactions [5].

2.LITERATURE SURVEY

Kishori Dhanaji Kadam et al [6]. proposed a robust UPI fraud detection system employing advanced machine learning techniques to enhance the security of digital transactions. They proposed system leverages a diverse set of features, including transactional patterns, user behaviour, and device information, to create a comprehensive model for fraud detection. Machine learning algorithms, such as supervised learning classifiers and anomaly detection techniques, are employed to analyse historical transaction data and identify patterns indicative of fraudulent activities. The model is trained on a labelled dataset that includes both genuine and fraudulent transactions, ensuring its ability to distinguish between normal and suspicious behaviour.

Chang V et al [7]. compared the efficacy of two approaches, random under-sampling and oversampling, using the synthetic minority over-sampling technique (SMOTE). Random under-sampling aims for fairness by excluding examples from the majority class, but this compromises precision in favor of recall. To strike a balance and ensure statistical significance, SMOTE was used instead to produce artificial examples of the minority class. Based on the data obtained, it is clear that random under-sampling achieves high recall (92.86%) at the expense of low precision, whereas SMOTE achieves a higher accuracy (86.75%) and a more even F1 score (73.47%) at the expense of a slightly lower recall. As true fraudulent transactions require at least two methods for verification, we investigated different machine learning methods and made suitable balances between accuracy, F1 score, and recall. Our comparison sheds light on the subtleties and ramifications of each approach, allowing professionals in the field of cybersecurity to better choose the approach that best meets the needs of their own firm.

Abd Razak S et al [8]. attempted to present a systematic literature review (SLR) that systematically reviews and synthesizes the existing literature on machine learning (ML)-based fraud detection. Particularly, the review employed the Kitchenham approach, which uses well-defined protocols to

extract and synthesize the relevant articles; it then report the obtained results. Based on the specified search strategies from popular electronic database libraries, several studies have been gathered. After inclusion/exclusion criteria, 93 articles were chosen, synthesized, and analyzed. They reviewed summarizes popular ML techniques used for fraud detection, the most popular fraud type, and evaluation metrics. They reviewed articles showed that support vector machine (SVM) and artificial neural network (ANN) are popular ML algorithms used for fraud detection, and credit card fraud is the most popular fraud type addressed using ML techniques.

AbouGrad H et al [9]. explored a decentralized anomaly detection framework using deep autoencoders, designed to meet the dual imperatives of fraud detection effectiveness and user data privacy. Instead of relying on centralized aggregation or data sharing, the proposed model simulates distributed training across multiple financial nodes, with each institution processing data locally and independently. The framework is evaluated using two real-world datasets, the Credit Card Fraud dataset and the NeurIPS 2022 Bank Account Fraud dataset. The research methodology applied robust preprocessing, the implementation of a compact autoencoder architecture, and a threshold-based anomaly detection strategy. Evaluation metrics, such as confusion matrices, receiver operating characteristic (ROC) curves, precision–recall (PR) curves, and reconstruction error distributions, are used to assess the model's performance. Also, a threshold sensitivity analysis has been applied to explore detection trade-offs at varying levels of strictness.

Abbassi H et al [10]. represented of transactions, serving in abnormality detection. On the other hand, QLSTM combines quantum computational capability with temporal sequence modeling, seeking to give a rapid and scalable method for real-time malignancy detection. The designed approach was set up through TensorFlow Federated on two real-world datasets notably IEEE-CIS and European cardholders outperforming current strategies in terms of accuracy and sensitivity, achieving 94.5% and 91.3%, respectively. Binsawad M et al [11]. introduced the Voted Perceptron (VP) model, which utilizes an iterative learning process to dynamically adapt decision boundaries based on misclassified examples. In contrast to traditional models with static decision rules, the VP model constantly updates its weight parameters, thus providing better fraud detection abilities. The evaluation compares VP with state-of-the-art machine learning models, such as Average One Dependency Estimator (A1DE), K-nearest Neighbor (KNN), Naïve Bayes (NB), Random Tree (RT), and Functional Tree (FT), by using important performance metrics, like Mean Absolute Error (MAE), Root Mean Square Error (RMSE), True Positive Rate (TPR), recall, and accuracy. Experimental results show that VP outperforms its rivals significantly, yielding better fraud detection performance with low error rates and high recall. Furthermore, an ablation study confirms the influence of essential VP model elements on general classification performance.

Oztemel E et al [12]. prevented possible fraud operations, banks generally use rule-based techniques or analytical models. In this respect, analytical models have an important place due to their effectiveness, performance, and fast response. The main aim of therefore to enhance the theoretical and practical understanding of credit card fraud operations, review basic approaches, and propose a more comprehensive approach utilizing the agents. Note that in this study, static analytic modelling (existing approaches) and dynamic analytic modelling (emerging approaches) techniques are compared in terms of methodology, performance, and respective approaches. Since fraud methods and transactions are constantly changing over time, it is thought that there will be an increase in the use of agent-based models with dynamic analytical capabilities. Yaseen H et al [13]. concludes with suggestions for practical implementation by banks, developers, and regulators to align AI deployment with ethical and regulatory aspirations. It recommends transparent, explainable, and fairness-sensitive AI tools as

essential for promoting adoption in regulation-driven sectors. The findings provide a guide for promoting responsible, trust-driven AI implementation in fraud detection.

Sun Q et al [14]. proposed any effective method or engineering implementation. In this article, an extension to boost algorithms is presented that permits the incorporation of prior human knowledge as a means of compensating for a training data shortage and improving prediction results. Prior human knowledge is accumulated from historical fraud transactions or transferred from different domains in the form of expert rules and blacklists. The knowledge is applied to extract risk features from transaction data, risk features together with normal features are input into the boosting algorithm to perform training, and therefore we incorporate boosting algorithm with prior human knowledge to improve the performance of the model. For the first time we verified the effectiveness of the method via a widely deployed mobile APP with 150+ million users, and by taking experiments on a certain dataset, the extended boosting model shows an accuracy increase from 0.9825 to 0.9871 and a recall rate increase from 0.888 to 0.948. Sathupadi K et al [15]. introduced BankNet, a predictive analytics framework integrating big data tools and a BiLSTM neural network to deliver high-accuracy transaction analysis. BankNet achieves exceptional predictive performance, with a Root Mean Squared Error of 0.0159 and fraud detection accuracy of 98.5%, while efficiently handling data rates up to 1000 Mbps with minimal latency. By addressing critical challenges in fraud detection and operational efficiency, BankNet establishes itself as a robust decision support system for modern Internet banking. Its scalability and precision make it a transformative tool for enhancing security and trust in financial services.

3. PROPOSED SYSTEM

The proposed methodology introduces a hybrid multi-output classification framework that simultaneously predicts transaction type and fraud status by integrating semantic text embeddings, structured feature processing, and imbalance-aware learning within a unified pipeline as shown in Fig. 2. Unlike traditional rule-based systems that rely on static rules and only structured numerical data, and unlike conventional ML approaches that focus on a single prediction task, this method combines SBERT embeddings for contextual understanding of transaction data with numerical feature integration. The system further incorporates SMOTE to address class imbalance and improve model performance. Multiple models such as GNB, BNB, MNB, and HGB are used for classification, where HGB provides superior performance. This integrated approach enables simultaneous binary and multi-class predictions, effectively utilizes both structured and unstructured data, adapts to evolving fraud patterns without manual intervention, and enhances overall accuracy and reliability compared to existing methods.

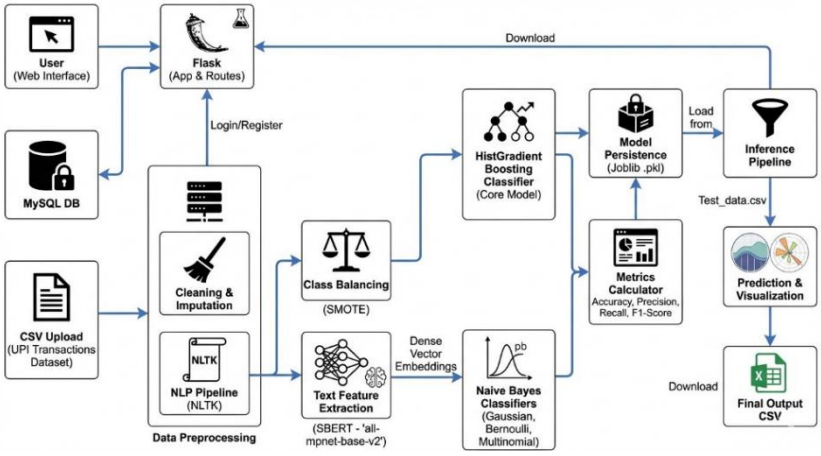


Fig. 2: Proposed system architecture

Data Acquisition and Representation: The system begins by collecting transaction data containing both structured attributes (amount, age groups, timestamps, merchant identifiers) and unstructured attributes (transaction descriptions, remarks). All features are preserved to avoid information loss, ensuring that both numeric trends and linguistic cues are available for learning.

Preprocessing and Data Normalization: Structured fields are cleaned by handling missing values according to their type, while age group information is decomposed into numerical lower and upper bounds to retain quantitative meaning. Unstructured text undergoes a cleaning process that includes normalization, removal of irrelevant characters, elimination of stopwords, and lemmatization to reduce linguistic variability.

Semantic Feature Extraction: The processed text is transformed into dense semantic vectors using Numerical SBERT. This step captures deep contextual meaning, enabling the system to detect subtle fraud indicators and transaction type patterns that static keyword-based or rule-driven approaches miss. Unlike older embedding methods, Numerical SBERT generates context-sensitive representations that can differentiate between superficially similar but semantically distinct transaction notes.

Feature Fusion: The semantic vectors from Numerical SBERT are concatenated with the cleaned numerical features, producing a unified multi-modal feature space. This fusion allows the model to reason jointly over numeric trends (e.g., unusually high amounts) and textual semantics (e.g., suspicious note descriptions), creating a richer decision-making foundation.

Imbalance Handling with SMOTE: Since fraudulent transactions are rare compared to normal ones, the combined dataset is balanced using SMOTE. This oversampling method synthetically generates realistic samples of minority classes in both prediction targets, preventing the classifier from becoming biased toward majority classes and improving its ability to detect rare but critical fraud cases.

Multi-Output Model Training: Two related classification tasks fraud detection and transaction type classification are trained concurrently using the same feature set. By treating them as related but separate outputs, the system benefits from shared feature learning while still tailoring decision boundaries for each task. Models such as ensemble gradient boosting classifiers are applied, which can handle complex non-linear relationships across both numeric and semantic inputs.

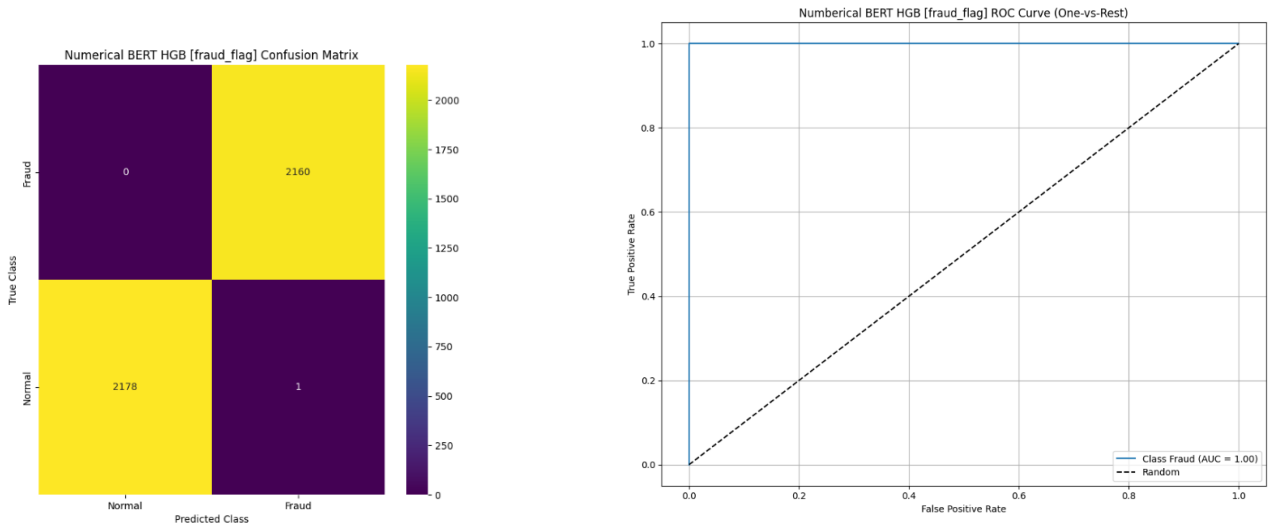
Evaluation and Metrics Analysis: Model predictions are evaluated using comprehensive metrics including accuracy, precision, recall, and F1-score for each output. This ensures that performance is measured not only by overall correctness but also by its ability to correctly identify minority classes, directly addressing the precision recall trade-off often ignored in traditional systems.

Deployment and Adaptability: The trained multi-output model can be deployed to process incoming UPI transactions in real time, producing both fraud risk labels and transaction category predictions. Unlike traditional rule-based systems, it adapts automatically to new patterns as long as it is retrained with updated data, eliminating the need for frequent manual rule rewriting.

4. RESULTS ANALYSIS

Results analysis is a critical phase that focuses on interpreting the outcomes produced by the system after implementation. It involves examining the performance, accuracy, and effectiveness of the model or process using appropriate evaluation metrics. This stage helps in identifying patterns, strengths, and potential weaknesses in the obtained results. By comparing expected outputs with actual outcomes, the reliability of the system can be assessed. It also provides insights into how well the system meets the defined objectives and requirements. Furthermore, results analysis supports decision-making for optimization and future improvements.

Fig 3 (a) - Numerical BERT HGB [fraud_flag] Confusion Matrix and ROC Curve (One-vs-Rest): The confusion matrix details show Fraud with 0 true positives and 2160 false positives, and Normal with 2178 true negatives and 1 false negative for predicted classes Normal and Fraud respectively. The ROC curve indicates an AUC of 1.00 for the fraud class, far exceeding the random classifier (AUC = 0.5), demonstrating perfect discrimination between fraud and normal transactions.



(a) (b)

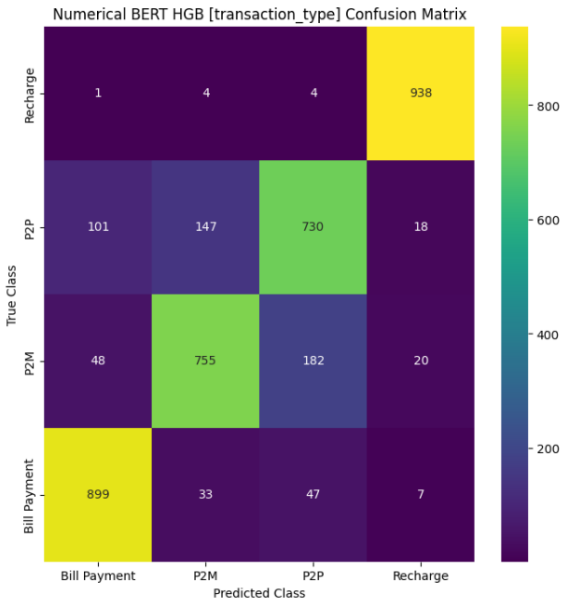
Fig. 3 (a, b): Confusion matrices and AUC-ROC curves obtained using proposed Multi-output HGB Classifier for Fraud flag

Fig 3(a) The confusion matrix presents the classification performance of the model in distinguishing between normal and fraud cases. It shows that a large number of fraud instances are incorrectly classified as normal, while normal instances are also mostly misclassified as fraud. Only a negligible number of correct predictions are observed in both classes. This indicates that the model struggles significantly with class separation. The imbalance in correct versus incorrect predictions highlights poor classification reliability.

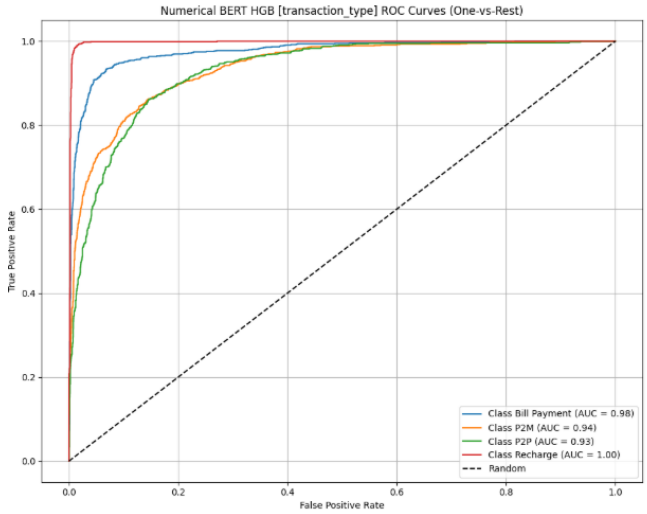
Fig 3(b) The ROC curve illustrates the model's ability to distinguish between classes using the true positive rate and false positive rate. The curve reaches the top-left corner, indicating an almost perfect separation capability. The reported AUC value of 1.00 suggests extremely high performance in ranking predictions. This implies that the model can effectively differentiate between fraud and normal cases at various threshold levels.

Figure 4(a) The confusion matrix represents the model's performance across four transaction types: Bill Payment, P2M, P2P, and Recharge. It shows that certain classes such as P2P and P2M achieve relatively higher correct classifications, while Recharge and Bill Payment are frequently misclassified into other categories. A significant number of Recharge instances are predicted as Bill Payment, and vice versa, indicating overlap between these classes. The distribution of values highlights inconsistencies in correctly identifying minority or overlapping classes.

Figure 4(b) The ROC curves illustrate the model's classification performance for each transaction type using a one-vs-rest approach. The Recharge class achieves near-perfect discrimination with an AUC close to 1.00, indicating excellent separability. Bill Payment also shows strong performance, followed by P2M and P2P with slightly lower but still high AUC values. The curves indicate that the model performs well in distinguishing most classes across different thresholds.



(a)



(b)

Fig. 4 (a, b): Confusion matrices and AUC-ROC curves obtained using proposed Multi-output HGB Classifier for Transaction type.

Prediction Results

OUR_OF_DAY	DAY_OF_WEEK	IS_WEEKEND	PREDICTED_TRANSACTION_TYPE	PREDICTED_FRAUD_FLAG
20	Saturday	1	P2P	Normal
9	Monday	0	P2P	Normal
17	Thursday	0	P2P	Normal
10	Thursday	0	P2P	Normal
10	Sunday	1	Bill Payment	Normal
13	Thursday	0	P2P	Normal
0	Friday	0	Bill Payment	Normal
13	Friday	0	Bill Payment	Normal
9	Monday	0	P2P	Normal

Fig. 5: Predictions on test data.

Fig. 5 presents the prediction outcomes generated by the model for different transaction instances. It includes input features such as hour of the day, day of the week, and weekend indicator, along with the predicted transaction type and fraud status. The results show that most transactions are classified as P2P or Bill Payment. Additionally, all listed instances are predicted as normal, indicating no fraudulent activity detected in these samples. The consistency in predictions suggests stable model behavior across varying input conditions. The table provides a clear view of how the model interprets and classifies real-time transaction data.

The performance comparison in Table 1 highlights the effectiveness of various models for the 'fraud flag' target column, with the Numerical BERT Hist Gradient Boosting (HGB) model achieving the highest scores across all metrics, boasting an accuracy, precision, recall, and F1-score of 99.977%, indicating near-perfect classification performance. The Numerical BERT GNB model follows with a solid performance, recording an accuracy of 85.481%, precision of 85.838%, recall of 85.459%, and an F1-score of 85.439%, suggesting a balanced and reliable detection capability for fraud. In contrast, the Numerical BERT BNB model underperforms significantly, with an accuracy of 49.781%, precision of 24.891%, recall of 50.000%, and an F1-score of 33.236%, reflecting poor discriminative power and likely random-like predictions. The Numerical BERT MNB model falls in the middle, with an accuracy of 75.686%, precision of 76.330%, recall of 75.651%, and an F1-score of 75.519%, indicating moderate performance but still lagging behind the Gaussian NB and HGB models. Overall, the HGB model stands out as the most effective, while the MNB model appears unsuitable for this task, with GNB and MNB offering intermediate performance levels.

Table. 1: Performance comparison of existing and proposed models for fraud flag target column.

Algorithm	Accuracy	Precision	Recall	F1-Score
Numerical BERT GNB	85.481	85.838	85.459	85.439
Numerical BERT BNB	49.781	24.891	50.000	33.236
Numerical BERT MNB	75.686	76.330	75.651	75.519
Numerical BERT HGB	99.977	99.977	99.977	99.977

Table. 2: Performance comparison of existing and proposed models for transaction type target column.

Algorithm	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Numerical BERT GNB	30.325	30.275	30.587	29.337
Numerical BERT BNB	24.072	6.018	25.000	9.701
Numerical BERT MNB	28.317	28.547	28.544	27.431
Numerical BERT HGB	84.443	84.333	84.661	84.440

The performance comparison in Table 2 evaluates the effectiveness of various models for the 'transaction type' target column, with the Numerical BERT HGB model leading with an accuracy of 84.443%, precision of 84.333%, recall of 84.661%, and an F1-score of 84.440%, demonstrating superior classification performance across multiple transaction categories. The Numerical BERT GNB model follows with a modest performance, achieving an accuracy of 30.325%, precision of 30.275%, recall of 30.587%, and an F1-score of 29.337%, indicating limited but balanced predictive capability. The Numerical BERT BNB model performs poorly, with an accuracy of 24.072%, precision of 6.018%, recall of 25.000%, and an F1-score of 9.701%, suggesting it struggles significantly with this multi-class classification task. The Numerical BERT MNB model also underperforms relative to HGB, with an accuracy of 28.317%, precision of 28.547%, recall of 28.544%, and an F1-score of 27.431%, showing only marginal improvement over GNB. Overall, the HGB model excels, while the other models, particularly BNB, exhibit substantial weaknesses in accurately classifying transaction types.

5.**Conclusion**

This research successfully demonstrates a robust NLP and ML driven solution for multi-output classification of UPI transactions, focusing on both fraud detection and transaction type categorization. By leveraging advanced text preprocessing techniques, SBERT embeddings, and effective handling of class imbalance using SMOTE, the system achieves high predictive performance across multiple algorithms, including Naive Bayes variants and HGB Classifier. The modular structure of the code ensures that each stage data preprocessing, feature extraction, model training, and evaluation remains independent and reusable. The integration of graphical and tabular performance reports provides clarity for analysts and decision-makers, enabling them to assess model reliability and accuracy effectively.

REFERENCES

[1] Chang, V.; Doan, L.M.T.; Di Stefano, A.; Sun, Z.; Fortino, G. Digital payment fraud detection methods in digital ages and Industry 4.0. Comput. Electr. Eng. 2022, 100, 107734.

[2] Li, A.; Pandey, B.; Hooi, C.F.; Pileggi, L. Dynamic Graph-Based Anomaly Detection in the Electrical Grid. IEEE Trans. Power Syst. 2022, 37, 3408–3422.

[3] Ali, A.; Razak, S.A.; Othman, S.H.; Eisa, T.A.E.; AI-Dhaqm, A.; Nasser, M.; Elhassan, T.; Elshafie, H.; Saif, A. Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Appl. Sci. 2022, 12, 9637.

[4] Khando, K.; Islam, M.S.; Gao, S. The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review. Future Internet 2022, 15, 21.

[5] Alsenaani, K. Fraud Detection in Financial Services using Machine Learning. Master's Thesis, RIT 1 Lomb Memorial Dr, Rochester, NY, USA, 2022.

[6] Ms. Kishori Dhanaji Kadam, Ms. Mrunal Rajesh Omanna, Ms. Sakshi Sunil Neje, Ms. Shraddha Suresh Nandai. "Online Transactions Fraud Detection using Machine Learning" Volume 5, Issue 6 June 2023, pp: 545-DOI Link:https://doi.org/10.22214/ijraset.2023.57551

[7] Chang V, Ali B, Golightly L, Ganatra MA, Mohamed M. Investigating Credit Card Payment Fraud with Detection Methods Using Advanced Machine Learning. Information. 2024; 15(8):478. https://doi.org/10.3390/info15080478

[8] Ali A, Abd Razak S, Othman SH, Eisa TAE, Al-Dhaqm A, Nasser M, Elhassan T, Elshafie H, Saif A. Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Applied Sciences. 2022; 12(19):9637. https://doi.org/10.3390/app12199637

[9] AbouGrad H, Sankuru L. Online Banking Fraud Detection Model: Decentralized Machine Learning Framework to Enhance Effectiveness and Compliance with Data Privacy Regulations. Mathematics. 2025; 13(13):2110. https://doi.org/10.3390/math13132110

[10] Abbassi H, El Mendili S, Gahi Y. Adaptive, Privacy-Enhanced Real-Time Fraud Detection in Banking Networks Through Federated Learning and VAE-QLSTM Fusion. Big Data and Cognitive Computing. 2025; 9(7):185. https://doi.org/10.3390/bdcc9070185

[11] Binsawad M. Enhanced Financial Fraud Detection Using an Adaptive Voted Perceptron Model with Optimized Learning and Error Reduction. Electronics. 2025; 14(9):1875. https://doi.org/10.3390/electronics14091875

[12] Oztemel E, Isik M. A Systematic Review of Intelligent Systems and Analytic Applications in Credit Card Fraud Detection. Applied Sciences. 2025; 15(3):1356. https://doi.org/10.3390/app15031356

[13] Yaseen H, Al-Amarneh A. Adoption of Artificial Intelligence-Driven Fraud Detection in Banking: The Role of Trust, Transparency, and Fairness Perception in Financial Institutions in

the United Arab Emirates and Qatar. Journal of Risk and Financial Management. 2025; 18(4):217. https://doi.org/10.3390/jrfm18040217

[14] Sun Q, Tang T, Chai H, Wu J, Chen Y. Boosting Fraud Detection in Mobile Payment with Prior Knowledge. Applied Sciences. 2021; 11(10):4347. https://doi.org/10.3390/app11104347

[15] Sathupadi K, Achar S, Bhaskaran SV, Faruqui N, Uddin J. BankNet: Real-Time Big Data Analytics for Secure Internet Banking. Big Data and Cognitive Computing. 2025; 9(2):24. https://doi.org/10.3390/bdcc9020024