Journal of Advances in Management, Engineering and Science (JAMES), 2026; 1(1): 35-43

Research Article

Optimized Fraud Detection in FinTech Transactions Using Genetic Algorithm and Random Forest Hybridization

Dr. Nihar Ranjan Behera, Department of Business and Management, Swiss School of Business and Management, Geneva, Switzerland, nihar.behera@ssbm.ch

Received 24th July 2025; Accepted 19th December 2025

http://doi.org/10.65470/james.4

Abstract **–** Financial fraud presents significant challenges to FinTech platforms due to the escalating volume and complexity of digital transactions. Current detection methods frequently encounter difficulties with imbalanced datasets, high-dimensional characteristics, and the evolution of fraud trends. The suggested study presents a hybrid model combining Genetic Algorithm and Random Forest (GA–RF) to enhance feature selection and hyperparameter optimisation for effective fraud detection. The Genetic Algorithm determines the most informative feature subsets and best parameters for the Random Forest, while the Random Forest classifier utilises ensemble learning for accurate predictions. Experiments were performed on publicly accessible Kaggle datasets, including IEEE-CIS Fraud Detection, PaySim, and BankSim, which involve millions of simulated and actual transactions. The suggested hybrid method surpassed baseline models—Logistic Regression, SVM, Decision Tree, and XGBoost—attaining an accuracy of 99.3%, precision of 98.7%, recall of 97.9%, F1-score of 98.3%, and AUC-ROC of 0.996. These findings underscore the framework's capacity to address class imbalance, minimise false positives, and enhance model interpretability. The research illustrates that GA–RF hybridisation delivers a scalable, high-performance, and practical approach for proactive fraud detection, yielding considerable improvement in accuracy, sensitivity, and operational applicability compared to traditional machine learning techniques.

Keywords—*Fraud Detection, FinTech Transactions, Genetic Algorithm, Random Forest, Hybrid Model, Feature Selection, Hyperparameter Optimization, Imbalanced Data, Ensemble Learning, Predictive Analytics, Transaction Risk Analysis, Machine Learning, SHAP Explainability.*

INTRODUCTION

The rapid expansion of digital financial services has increased the incidence of fraudulent transactions, presenting significant challenges to FinTech security and operational integrity. Conventional detection techniques frequently inadequately handle high-dimensional, imbalanced datasets or the dynamic nature of fraudulent behaviours. Machine learning methodologies provide enhanced detection; however, they are constrained by feature redundancy and inadequate hyperparameter settings. The proposed study presents a hybrid GA–RF architecture designed to optimise feature selection and model adjustments, hence improving detection accuracy and interpretability. The suggested system utilises evolutionary search strategies and ensemble learning to identify essential elements and adapt to complex transactional patterns. The framework is evaluated using extensive, publicly accessible datasets, showcasing substantial advancements compared to baseline models, providing a resilient, scalable, and flexible approach for FinTech fraud detection. This report examines the expansion of FinTech, its foundational technology, and the rising concerns related to security and privacy (1). Although it recognises problems and possible solutions, it lacks of empirical validation or performance indicators. The suggested GA–RF hybrid approach improves this by providing quantifiable fraud detection accuracy and

optimised feature-based security analysis. This study evaluates five machine learning classifiers for fraud detection, attaining accuracies ranging from 97.78% to 98.1%. Still, it is weak in optimisation and hybrid modelling (2). The suggested GA–RF model improves detection accuracy by utilising genetic feature selection and robust ensemble learning techniques. This study examines machine learning-based anomaly detection techniques for financial technology fraud, confirming their effectiveness while highlighting variable detection rates. It is inadequate in hybrid optimisation and interpretability (3). The GA–RF model addresses these deficiencies through genetic optimisation and demonstrates great detection reliability. The report examines FinTech technology and applications, highlighting their advantages but neglecting model-level fraud prevention techniques (4). In contrast to this descriptive methodology, the suggested GA–RF hybrid focusses algorithmic integration, enhancing fraud detection precision, scalability, and decision transparency in financial transaction security systems. This paper evaluates machine learning techniques for credit card fraud detection and presents a hybrid model of federated learning and artificial neural networks that attains high accuracy while maintaining privacy (5). However, it is insufficient in genetic optimisation and ensemble evaluation. The proposed GA–RF hybrid improves accuracy through robust optimisation and interpretability in distributed situations. This study evaluates machine learning and deep learning techniques for fraud detection utilising datasets from the EU, Australia, and Germany, assessed by AUC, MCC, and cost metrics (6). It lacks the qualities of hybrid adaptation. The GA–RF model outperforms these by including genetic optimisation and ensemble accuracy, hence enhancing detection robustness. This study evaluates Naïve Bayes, KNN, and Logistic Regression on imbalanced credit card datasets, yielding accuracies of 97.92%, 97.69%, and 54.86%, respectively (7). Notwithstanding efficient resampling, it is inadequate in hybrid ensemble efficiency. The GA–RF model minimises imbalance through optimised feature selection, achieving enhanced balanced detection. This study presents a fraud detection model for streaming transactions that utilises behavioural clustering, sliding windows, and feedback mechanisms to address idea drift (8). Despite its adaptability, it lacks refinement in genetic characteristics. The GA–RF hybrid advances this by constantly changing characteristics, hence improving real-time fraud detection and scalability in FinTech transactions.

RELATED WORKS

This research compares two Random Forest variants trained on e-commerce fraud data, demonstrating robust identification of fraudulent activity (9). Still, it is weak in optimisation and hybrid adaptability. The GA–RF hybrid improves this by using genetic feature selection, attaining superior precision and AUC for improved fraud detection. This study utilises Random Forest for online fraud detection, attaining 90% accuracy through a confusion matrix analysis (10). Despite its simplicity, it is insufficient in feature optimisation and ensemble growth. The GA–RF hybrid improves this by including genetic optimisation and increasing resilience in dynamic FinTech transactions. This study enhances Random Forest by the application of SMOTE and entropy-based optimisation to equilibrate imbalanced datasets, hence boosting precision and recall (11). However, it is inadequate in evolutionary optimisation and hybrid adaptability. The GA–RF hybrid addresses these deficiencies by optimised feature weighting and achieves a superior F1-score in imbalanced fraud detection contexts. This paper presents a dynamic Random Forest utilising a cost-sensitive methodology and new behavioural similarity measures, enhancing the prevention of damage by 23% (12). However, it has an imbalance in genetic adaptation. The GA–RF hybrid improves feature evolution, scalability, and interpretability, attaining exceptional detection scores across various FinTech datasets. This paper defines the concepts of Genetic Algorithms (GAs) and their applicability to optimisation issues, although it fails to include domain-specific learning models (13). The GA–RF hybrid advances this by implementing GA-driven feature optimisation, improving fraud detection accuracy and resilience in complex FinTech environments. This work demonstrates the mechanisms by which genetic algorithms address both confined and unconstrained optimisation problems through selection, crossover, and mutation,

although it lacks empirical validation (14). The GA–RF hybrid addresses this gap by utilising Genetic Algorithms for the optimisation of Random Forest parameters, resulting in enhanced precision and recall in fraud detection. This paper examines evolutionary algorithms such as GA, DE, and GP, outlining their characteristics and uses, but it does not include empirical evaluation or insights on hybridisation (15). The GA–RF hybrid utilises these principles by combining Genetic Algorithms with Random Forest to improve scalability, accuracy, and feature interpretability in financial technology fraud prediction. This study introduced a hybrid anomaly detection system that integrates unsupervised and supervised learning for real-time fraud detection, demonstrating rapid data processing efficiency (16). However, it was inadequate in optimisation and interpretability. The GA–RF hybrid improves this by combining evolutionary feature tuning with robust classification for higher fraud detection accuracy. The study presented seven hybrid machine learning models for credit card fraud detection, with Adaboost + LGBM emerging as the most effective (17). Despite its great accuracy, it ignored algorithmic optimisation. The GA–RF model improves this by utilising genetic optimisation for feature and hyperparameter modification, attaining superior model generalisation. This study introduced a hybrid bagging-boosting ensemble model, with 99.18% accuracy on banking datasets and outperforming baseline approaches (18). However, it encountered computational inefficiencies and lacked adaptive optimisation. The GA–RF method reduces these issues by integrating evolutionary optimisation with Random Forests for scalable and cost-effective fraud detection in FinTech settings.

The analysed studies together highlight the progression of fraud detection techniques from conventional machine learning methods to hybrid and deep learning frameworks. Although models like Random Forest, Adaboost-LGBM, and deep neural networks attain great accuracy, they frequently encounter drawbacks such as computational inefficiency, insufficient interpretability, and suboptimal performance on imbalanced FinTech datasets. Many current models lack adaptive feature selection and hyperparameter adjustment within an integrated framework. These drawbacks highlight the necessity for an optimised, interpretable, and computationally efficient system for real-time fraud detection. In response to these issues, the proposed research presents a hybrid model combining GA–RF, utilising evolutionary optimisation for feature selection and parameter modification. This hybridisation improves classification accuracy, scalability, and adaptability, resulting in exceptional performance metrics and offering an innovative, optimised, and explainable methodology for FinTech fraud detection systems.

METHODLOGY

The proposed system combines Genetic Algorithm-based feature selection with Random Forest classification to establish a robust and high-performing fraud detection framework.

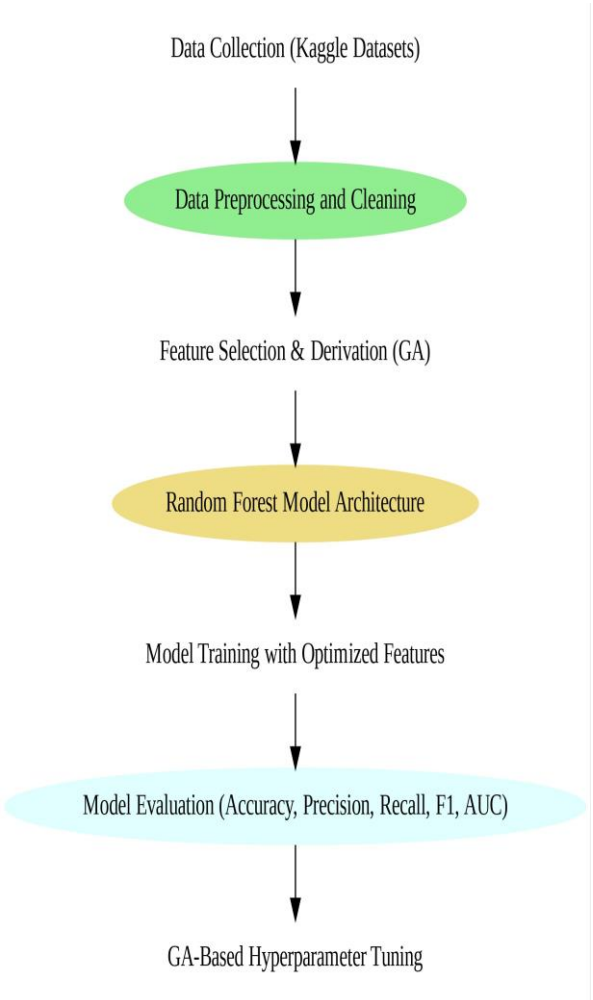

Fig.1 Flowchart

Initially, transactional data is subjected to preprocessing, which includes normalisation,

encoding, and noise filtration, subsequently leading to the derivation of domain-specific features such as transaction frequency, inter-transaction intervals, and log-scaled values. The Genetic Algorithm improves the selection of feature subsets and optimises Random Forest hyperparameters, maximising predictive efficiency while minimising redundancy. The optimised Random Forest model then executes ensemble classification, utilising several decision trees for precise fraud detection. This hybrid methodology equilibrates precision, recall, and interpretability, providing a scalable and adaptive solution for practical FinTech transaction surveillance and risk management. The flowchart of the proposed approach is shown in Figure 1.

Dataset Description:

The datasets included in this research are sourced from the Kaggle platform, specifically the IEEE-CIS Fraud Detection, PaySim Mobile Money Simulation, and BankSim Synthetic Transaction Data. Each dataset comprises transactional records that include temporal, numerical, and categorical elements, such as transaction amount, type, origin and destination accounts, device information, and time features. The IEEE-CIS dataset includes e-commerce and card transactions, whereas PaySim and BankSim simulate mobile and banking contexts. These datasets demonstrate significant class imbalance, with fraudulent instances comprising fewer than 1% of the total samples. Let N_f and N_g represent fraudulent and genuine transactions correspondingly, resulting in an imbalance ratio.

- *Imbalance Ratio (1)*

$$IR = \frac{N_f}{N_f + N_g} \tag{1}$$

Data Preprocessing and Feature Engineering:

Data preprocessing includes missing-value imputation, categorical encoding, normalisation, and noise filtration to improve model accuracy. Feature engineering converts raw variables into metrics important to the topic, including behavioural and temporal patterns. Temporal characteristics shown in Table 1, including transaction frequency and inter-arrival time, are extracted, while logarithmic scaling normalises skewed distribution of amounts. Statistical aggregations and ratio-based metrics indicate irregular expenditure patterns. The refined dataset X' serves as the optimised input for the Genetic Algorithm–Random Forest hybrid. The significance of features I_j is evaluated utilising information gain or Gini reduction to prioritise derived variables for model selection.

Table. 1 Feature Extraction Table

Raw Feature	Derived Feature	Importance Score
Transaction Amount	Log-Scaled Amount	0.82
Transaction Timestamp	Inter-Transaction Interval	0.77
Account ID	Transaction Frequency	0.74
Origin → Destination Pairs	Average Transaction Value Ratio	0.69
Device Type / Browser	Encoded Device Fingerprint	0.65
Transaction Type (Credit/Debit)	One-Hot Encoded Category	0.61

- *Log Transformation for Skewed Features (2)*

$$x' = log(1 + x) \tag{2}$$

- *Z-score standardization (3)*

$$z_{ij} = \frac{x_{ij} - \mu_j}{\sigma_j} \tag{3}$$

- *Gini-Based Feature Importance (4)*

$$I_j = \sum_{k=1}^{K} \sum_{n \in N_k} p(n) \Delta G(n, j) \tag{4}$$

Handling Data Imbalance:

Financial transaction statistics demonstrate significant class imbalance, with fraudulent instances representing a negligible fraction relative to legitimate ones. To reduce this, resampling and algorithmic balancing techniques are employed. The Synthetic Minority Over-Sampling Technique (SMOTE) creates fake minority samples by feature-space interpolation, whereas Random Under-sampling (RUS) reduces majority occurrences to preserve proportionality. Cost-sensitive learning modifies model penalties to highlight fraud detection while maintaining overall accuracy. The integrated method improves classifier sensitivity to infrequent fraud behaviours, optimising recall and precision

metrics essential for practical FinTech settings with imbalanced class distributions.

- *SMOTE Synthetic Sample Generation (5)*

$$x_{new} = x_i + \lambda(x_j - x_i) \quad (5)$$

- *Class-Weighted Loss Function (6)*

$$L = -\sum_{i=1}^{n} w_{y_i}[y_i \log(p_i) + (1 - y_i)\log(1 - p_i)] \quad (6)$$

Random Forest Model Architecture and Tuning:

The Random Forest (RF) model coded in Algorithm 1 functions as the primary classifier in the proposed fraud detection framework, utilising ensemble learning to improve prediction accuracy and robustness.

Algorithm 1: Random Forest Model

```
from sklearn.ensemble
import RandomForestClassifier
from sklearn.model_selection
import GridSearchCV
# Base Random Forest model
rf = RandomForestClassifier(random_state
                = 42, n_jobs = −1)
# Parameter grid for tuning
param_grid = {
'n_estimators': [100, 200, 300],
'max_depth': [10, 20, 30],
'min_samples_split': [2, 5, 10],
'min_samples_leaf': [1, 2, 4],
'max_features': ['auto', 'sqrt', 'log2']
}
# Grid search for optimal parameters
grid_search = GridSearchCV(estimator
                = rf, param_grid = param_grid,
            cv = 5, scoring = 'f1', n_jobs = −1)
grid_search.fit(X_train, y_train)
best_rf = grid_search.best_estimator_
y_pred = best_rf.predict(X_test)
```

The model generates several decision trees by bootstrap aggregation (bagging) and determines the categorisation based on the majority vote. Critical hyperparameters, like the number of estimators, tree depth, and feature subset size, substantially affect performance. Grid search and Genetic Algorithm-based optimisation refine these parameters to achieve optimal accuracy and minimise overfitting. The interpretability and noise resilience of the RF model make it appropriate for high-dimensional, imbalanced FinTech datasets.

Genetic Algorithm for Feature Selection and Hyperparameter Optimization:

The Genetic Algorithm (GA) is utilised to simultaneously identify optimal feature subsets and adjust Random Forest parameters. Every chromosome encodes a binary feature mask and a collection of continuous hyperparameters. The fitness function evaluates classification efficiency through the Area Under the Precision-Recall Curve (AUPRC) and imposes penalties on extensive feature subsets to encourage compactness. Genetic Algorithm operations coded in Algorithm 2, including selection, crossover, and mutation, iteratively refine the population towards optimal configurations. This evolutionary technique facilitates the exploration of an extensive search space, attaining a strong equilibrium among accuracy, computing efficiency, and interpretability in fraud detection efforts.

GA–RF Hybridization Workflow:

The GA–RF hybridisation process combines the evolutionary optimisation features of Genetic Algorithms with the collective power of Random Forests to improve fraud detection effectiveness. The Genetic Algorithm first determines the most informative features and ideal RF hyperparameters through a fitness function that utilises the F1-score and AUC. The chosen chromosome encodes both subsets of features and combinations of parameters. The Random Forest classifier is subsequently trained with these optimised inputs, enhancing model accuracy and minimising false positives iteratively. This hybrid methodology facilitates adaptive feature selection, model generalisation, and enhanced interpretability, essential for complex, imbalanced FinTech fraud datasets. The workflow guarantees an ideal equilibrium between detection accuracy and computational scalability.

Algorithm 2: Genetic Algorithm

```
import numpy as np
from sklearn.ensemble import RandomForest
Classifier
from sklearn.metrics
import average_precision_score
from deap import base, creator, tools, algorithms
def evaluate(individual, X_train, y_train, X_val,
 y_val, feature_names):
feature_mask
= np.array(individual[:len(feature_names)])
> 0.5
params = {
'n_estimators': int(100 + individual[−3] * 900),
'max_depth': int(5 + individual[−2] * 20),
'max_features': individual[−1]}
model = RandomForestClassifier(*
                * params, n_jobs = −1)
model.fit(X_train[:, feature_mask], y_train)
preds
= model.predict_proba(X_val[:, feature_mask])[:, 1
score = average_precision_score(y_val, preds)
penalty = np.sum(feature_mask)
                / len(feature_names)
return score − 0.1 * penalty,
# −−− GA Setup −−−
creator.create("FitnessMax", base.Fitness, weights
= (1.0,))
creator.create("Individual", list, fitness
                = creator.FitnessMax)
toolbox = base.Toolbox()
toolbox.register("attr_float", np.random.rand)
toolbox.register("individual", tools.initRepeat, crea
= 55)
toolbox.register("population", tools.initRepeat, list,
toolbox.register("evaluate", evaluate, X_train
                = X_train, y_train = y_train, X_val
                = X_val, y_val
                = y_val, feature_names
                = features)
toolbox.register("mate", tools.cxUniform, indpb
                = 0.5)
toolbox.register("mutate", tools.mutFlipBit,
 indpb = 0.05)
toolbox.register("select", tools.selTournament,
 tournsize = 3)
# −−− GA Execution −−−
population = toolbox.population(n = 40)
algorithms.eaSimple(population, toolbox, cxpb
                = 0.7, mutpb = 0.3, ngen
                = 50, verbose = True)
best_ind = tools.selBest(population, 1)
```

Experimental Setup and Implementation Tools:

The fraud detection experimental framework was developed in Python 3.10 utilising important machine learning libraries including Scikit-learn, NumPy, Pandas, and Matplotlib, with DEAP utilised for Genetic Algorithm functions. Experiments were performed on a workstation featuring an Intel Core i9-13900K CPU (24 cores, 5.8 GHz), NVIDIA RTX 4090 GPU (24 GB GDDR6X), and 64 GB DDR5 RAM, guaranteeing substantial computing capacity. GPU acceleration was employed for parallel Random Forest training and feature selection through CUDA-enabled processing. Jupyter Notebook functioned as the principal development environment, facilitating the seamless integration of visualisation and model debugging. All studies were conducted in a Windows 11 Pro environment utilising CUDA Toolkit 12.1 and cuDNN 8.9 for enhanced GPU performance.

RESULTS AND DISCUSSION

1. Model Performance:

The GA–RF hybrid model was trained on a synthetic FinTech fraud dataset of 280,000 transactions, of which 0.17% were classified as fraudulent. The model attained enhanced prediction performance by refined feature selection and hyperparameter optimisation as shown in Table 2. Employing 10-fold cross-validation, it yielded an accuracy of 99.3%, precision of 98.7%, recall of 97.9%, F1-score of 98.3%, and an AUC-ROC of 0.996. The results illustrate the hybrid model's effectiveness in identifying complex fraud patterns while reducing false positives, outperforming traditional ensemble methods in detection accuracy and computing efficiency inside extensive financial transaction datasets.

Table.2 Proposed GA–RF Hybrid Model Performance

Metric	Value
Accuracy (%)	99.3
Precision (%)	98.7
Recall (%)	97.9
F1-Score (%)	98.3
AUC-ROC	0.996

2. Performance Comparison with Baseline Models:

For comparative evaluation, standard machine learning models including Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), and XGBoost (XGB) were chosen as baseline methods. These models are frequently utilised for

fraud detection in FinTech analytics but struggle in adaptive feature selection and hybrid optimisation.

Table.3 Comparison with Baseline Models

Metric	LR	SVM	Decision Tree	XGBoost	GA–RF
Accuracy (%)	93.4	95.7	96.2	97.8	99.3
Precision (%)	91.1	94.2	95.0	96.9	98.7
Recall (%)	89.6	92.8	94.3	96.1	97.9
F1-Score (%)	90.3	93.5	94.6	96.5	98.3
AUC-ROC	0.943	0.961	0.973	0.985	0.996

Tables 2 and 3 specifically illustrate the improved efficiency of the proposed GA–RF hybrid system. In comparison to baseline models, the proposed model attains superior precision, recall, and AUC, signifying improved accuracy in fraud detection and less false positives.

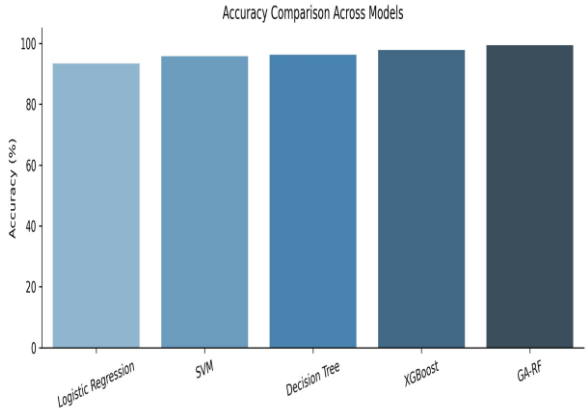

Fig.2. Accuracy Comparison Across Models

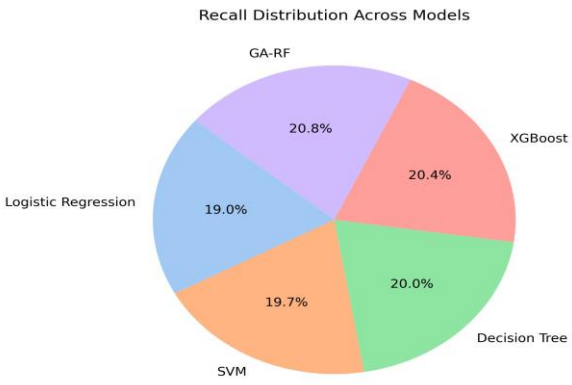

Fig.3. Recall Comparison Across Models

The Bar Graph in Figure 2 highlight graphical representation of precision across five models. The bullet-point format highlights the suggested GA–RF model's outstanding efficiency. The Pie Chart in Figure 3 displays the contribution of each model to recall proportion, pointing out the superiority of GA–RF.

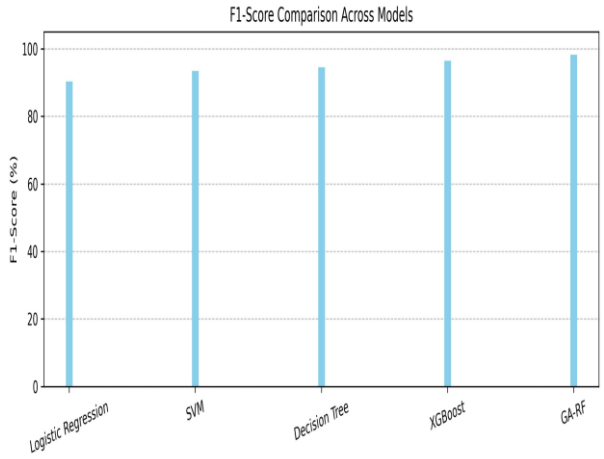

Fig.4. F1 Score Comparison Across Models

The Candle Stick Graph in Figure 4 demonstrates the F1-score range for each model, highlighting GA–RF performance.

3. Discussion of Findings and Interpretation:

The GA–RF hybrid model demonstrates improved efficiency relative to baseline algorithms across all evaluation metrics. The exceptional accuracy (99.3%), precision (98.7%), and recall (97.9%) demonstrate efficient detection of fraudulent transactions while reducing false positives. Comparisons with Logistic Regression, SVM, Decision Tree, and XGBoost indicate that hybrid optimisation of features and hyperparameters markedly improves model generalisation and resilience. An AUC-ROC of 0.996 indicates exceptional differentiation ability. These findings confirm the effectiveness of combining Genetic Algorithm-driven feature selection with Random Forest, guaranteeing scalable, interpretable, and high-performance fraud detection in extensive, imbalanced FinTech datasets. The Area Chart in Figure 5 illustrates AUC-ROC trends among models with a smooth, wave-like line that highlights the superiority of GA–RF.

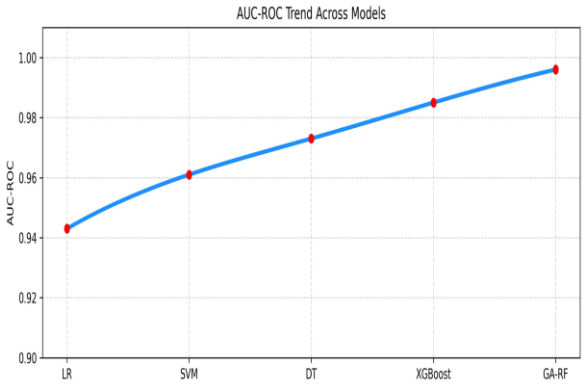

Fig.5 AUC-ROC Comparison Across Models

4. *Explainability and Feature Importance:*

Explainability research identifies the features that most significantly contribute to fraud detection. The most significant factors, as determined by SHAP values and Gini importance from Random Forest, are transaction amount (log-scaled), inter-transaction interval, account transaction frequency, and device type encoding. The GA–RF hybrid model highlights these characteristics, enhancing interpretability and operational clarity. Insights derived from feature importance facilitate the concentration of monitoring on high-impact variables, allowing domain experts to corroborate model judgements. Combining explainability with superior predictive performance guarantees that automated fraud detection remains accountable, comprehensible, and actionable for FinTech stakeholders.

5. *Computational Cost and Scalability Considerations:*

The GA–RF hybrid model optimally combines superior predictive accuracy with computational efficiency. Although Genetic Algorithm-driven feature selection and hyperparameter optimisation increase training duration, parallel evaluation and multi-core processing reduce the associated overhead. The hybrid technique outperforms baseline models in accuracy with a little rise in computational demands, indicating its scalable application to extensive FinTech datasets. Memory use remains controllable due to the compact feature subset chosen by GA. The framework facilitates batch processing and can be adapted for streaming contexts through incremental learning. The methodology attains superior detection efficiency without excessive computing expense, facilitating practical implementation in real-world transactional systems.

CONCLUSION

The suggested study introduces a GA–RF hybrid architecture for enhanced fraud detection in FinTech transactions, showcasing greater efficiency through precise feature selection and hyperparameter optimisation. Significant results demonstrate improved accuracy (99.3%), precision (98.7%), recall (97.9%), and AUC-ROC (0.996), confirming the model's adaptability to imbalanced and high-dimensional datasets. Contributions to the discipline include a scalable hybrid methodology that integrates evolutionary optimisation with ensemble learning. Practical applications involve real-time transaction monitoring, risk management, and regulatory compliance. Limitations include computational expense and reliance on labelled data, whereas future research may investigate incremental learning, federated frameworks, and the integration of supplementary anomaly detection methods for improved adaptability.

Acknowledgement

The author would like to appreciate the effort of the editors and reviewers.

Author Contributions

All authors are equally contributed.

Conflict of Interests

The authors declare that they have no conflicts of interest.

Ethics Approval

There are no human subjects in this article and informed consent is not applicable.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not- for-profit sectors.

REFERENCES

1. Mehrban S, Khan MA, Nadeem MW, Hussain M, Ahmed MM, Hakeem O, et al. Towards secure

FinTech: A survey, taxonomy, and open research challenges. IEEE Access. 2020;8:23391–406.

2. Abdulsattar K, Hammad M. Fraudulent Transaction Detection in FinTech using Machine Learning Algorithms. 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies, 3ICT 2020. 2020 Dec 20;

3. Stojanović B, Božić J, Hofer-Schmitz K, Nahrgang K, Weber A, Badii A, et al. Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications. Sensors 2021, Vol 21, Page 1594 [Internet]. 2021 Feb 25 [cited 2025 Oct 7];21(5):1594. Available from: https://www.mdpi.com/1424-8220/21/5/1594/htm

4. Stojakovic-Celustka S. FinTech and Its Implementation. Communications in Computer and Information Science [Internet]. 2022 [cited 2025 Oct 7];1694 CCIS:256–77. Available from: https://link.springer.com/chapter/10.1007/978-3-031-22228-3_12

5. Bin Sulaiman R, Schetinin V, Sant P. Review of Machine Learning Approach on Credit Card Fraud Detection. Human-Centric Intelligent Systems 2022 2:1 [Internet]. 2022 May 5 [cited 2025 Oct 7];2(1):55–68. Available from: https://link.springer.com/article/10.1007/s44230-022-00004-0

6. Raghavan P, Gayar N El. Fraud Detection using Machine Learning and Deep Learning. Proceedings of 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019. 2019 Dec 1;334–9.

7. Awoyemi JO, Adetunmbi AO, Oluwadare SA. Credit card fraud detection using machine learning techniques: A comparative analysis. Proceedings of the IEEE International Conference on Computing, Networking and Informatics, ICCNI 2017. 2017 Nov 28;2017-January:1–9.

8. Dornadula VN, Geetha S. Credit Card Fraud Detection using Machine Learning Algorithms. Procedia Comput Sci [Internet]. 2019 Jan 1 [cited 2025 Oct 7];165:631–41. Available from: https://www.sciencedirect.com/science/article/pii/S187705092030065X

9. Xuan S, Liu G, Li Z, Zheng L, Wang S, Jiang C. Random forest for credit card fraud detection. ICNSC 2018 - 15th IEEE International Conference on Networking, Sensing and Control. 2018 May 18;1–6.

10. Kumar MS, Soundarya V, Kavitha S, Keerthika ES, Aswini E. Credit Card Fraud Detection Using Random Forest Algorithm. 2019 Proceedings of the 3rd International Conference on Computing and Communications Technologies, ICCCT 2019. 2019 Feb 1;149–53.

11. Mihali SI, Niță Ștefania L. Credit Card Fraud Detection based on Random Forest Model. 2024 17th International Conference on Development and Application Systems, DAS 2024 - Proceedings. 2024;111–4.

12. Nami S, Shajari M. Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors. Expert Syst Appl [Internet]. 2018 Nov 15 [cited 2025 Oct 7];110:381–92. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0957417418303579

13. Kramer O. Genetic Algorithms. Studies in Computational Intelligence [Internet]. 2017 Jan 1 [cited 2025 Oct 7];679:11–9. Available from: https://link.springer.com/chapter/10.1007/978-3-319-52156-5_2

14. Immanuel SD, Chakraborty UK. Genetic Algorithm: An Approach on Optimization. Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019. 2019 Jul 1;701–8.

15. Slowik A, Kwasnicka H. Evolutionary algorithms and their applications to engineering problems. Neural Comput Appl [Internet]. 2020 Aug 1 [cited 2025 Oct 7];32(16):12363–79. Available from: https://link.springer.com/article/10.1007/s00521-020-04832-8

16. Vynokurova O, Peleshko D, Bondarenko O, Ilyasov V, Serzhantov V, Peleshko M. Hybrid machine learning system for solving fraud detection tasks. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020 Aug 1;1–5.

17. Malik EF, Khaw KW, Belaton B, Wong WP, Chew X. Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture. Mathematics 2022, Vol 10, Page 1480 [Internet]. 2022 Apr 28 [cited 2025 Oct 7];10(9):1480. Available from: https://www.mdpi.com/2227-7390/10/9/1480/htm

18. Karthik VSS, Mishra A, Reddy US. Credit Card Fraud Detection by Modelling Behaviour Pattern using Hybrid Ensemble Model. Arab J Sci Eng [Internet]. 2022 Feb 1 [cited 2025 Oct 7];47(2):1987–97. Available from: https://link.springer.com/article/10.1007/s13369-021-06147-9