Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Artificial Intelligence in Fraud Detection: Strengthening Identity Data Security in Open Banking

Vijay Kumar Soni

Expert Application Engineer
Discover Financial Services, USA

Abstract

Open banking allows banks to share information with third-party providers in an easy manner through secure channels that result in enhanced usability of financial services as well as innovations. Increased connectivity of the system creates more susceptibility to fraud activities and identity theft. The paper proposes an Artificial Intelligence (AI) detection system for protecting Open Banking transactions and protecting user identity information. Machine learning algorithms such as XGBoost and Random Forest empower the system to identify fraud accurately in real-time with high precision and recall scores. Data imbalance issue needs preprocessing via Synthetic Minority Over-sampling Technique (SMOTE) that improves model sensitivity. The system adopts Representational State Transfer (REST) Application Programming Interface via OAuth2 and Open Identity (OpenID) Connect for secure deployment and employs AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) encryption to secure sensitive user information. Multi-factor authentication and tokenization provide additional identity protection. Machine Learning Operations (MLOps) allows the system to undertake continuous learning and model retraining and adaptation for identifying new fraud patterns. Experimental results highlight the superior detection accuracy and AUC (Area under the Curve) of Extreme Gradient Boosting (XGBoost), which determines the effectiveness of the system in real-world financial settings.

Keywords: Open Banking, Fraud Detection, Identity Protection, Artificial Intelligence, Machine Learning, Data Security, Random Forest, XGBoost, SMOTE, MLOps

1. Introduction

The financial sector is experiencing revolutionary changes because digital transformation enables open banking through standardized APIs, allowing banks to exchange data easily with third-party service providers. Customers gained financial freedom through this structure, together with personalized service options, while fintech environments experienced improved innovation due to it. Businesses that utilize customer banking data through Open Banking obtain significant operational efficiency and open new markets enabled by developer access to compliant customer information [7][9]. The open connections from data sharing issues cause serious problems with privacy protection, identity safety, and financial fraud incidents. The reliance on APIs, together with decentralized architectural structures, creates many

breach points, which allows criminals to carry out credential stuffing attacks, account takeovers, and real-time transaction frauds [8][10].

Banks traditionally detected suspicious activity patterns through their manual audits and rule-based systems, according to [11]. Known fraud patterns are detected successfully by static rule systems, yet these systems remain unable to follow sophisticated cybercriminal techniques that purposefully evade static rule mechanisms. Open Banking environments now contain such large and speedy data volumes that human monitoring of these datasets becomes impractical [12]. The current situation demands a transformation to automatic intelligent detection systems. The capability of Artificial Intelligence and Machine Learning to perform fraud detection programs stands robust. They reveal hidden patterns through data learning and deliver precise real-time predictions and learning capabilities from past information [13]. ML models in fraud detection build their capabilities to adapt to emerging attack methods while continuously monitoring activities, which significantly reduces financial loss and increases response speed [14].

This study presents a risk-resistant Open Banking AI-based fraud detection system that adapts to the needs of this specific banking sector [20]. The system incorporates Random Forest, XGBoost ensemble methods, and AES and RSA encryption algorithms for identity data security while detecting anomalous transactions [15]. Microservices architecture is employed in the development of the system, which provides SCA, liability, and security during integration into the current banking framework. The security of the system depends on MFA authentication alongside token control of sensitive information [16]. The proposed system contains a crucial function built on MLOps-enabled feedback loops which allow the model to gain knowledge from newly labeled data for sustaining its performance against changing fraud patterns [17]. This architecture combines identity protection, fraud detection, and safe software execution techniques to provide a comprehensive solution for future Open Banking threats [18][19].

1.1. Financial Impact of Data Breaches in Open Banking

Worldwide financial losses from data breaches are increasing in prominence because open banking is in the news. Research statistics indicate that cybercrime will cause $10.5 trillion worth of harm to the world economy in 2025. Financial losses attributed to Open Banking include direct fraud plans and regulatory fines together with reputational harm plus associated judicial costs. International Business Machines Corporation (IBM) indicates United States data breach expenditures averaged $9.48 million throughout the year 2023. General Data Protection Regulation (GDPR) imposed fines totaling over €2.9 billion throughout the European Union as of when their directive went into effect in 2018. India incurs average data breach expenses of INR 17.6 crore which translates to about $2.1 million every single time, based on Ponemon Institute statistics. Chinese authorities have put in place stringent cybersecurity laws that impose ¥50 million fines on entities which violate the Personal Information Protection Law. Measures to secure data and robust fraud controls should be implemented immediately on such stringent data points. Open Banking accounts maintained by financial institutions should proactively adopt defense strategies to counter threats so as to reduce the regulatory threats and retain client confidence and avoid monetary loss.

1.2. Regulatory Compliance and Industry Standards

Open Banking implementations need to meet GDPR laws of Europe along with PSD2 regulations from Europe and Dodd-Frank in the US and California Consumer Privacy Act (CCPA) standards from California. The handling of user data by all affected entities follows strict rules with clear financial consequences for security breaches. The OpenID Foundation together with the Financial Data Exchange (FDX) organizes important work to establish safe interoperable industry standards. For example, the FDX, Application Programming Interface (API) standard enables secure consumer-permission data sharing, while OpenID Connect provides strong user authentication mechanisms that form the basis of identity protection in Open Banking.

2. Research context

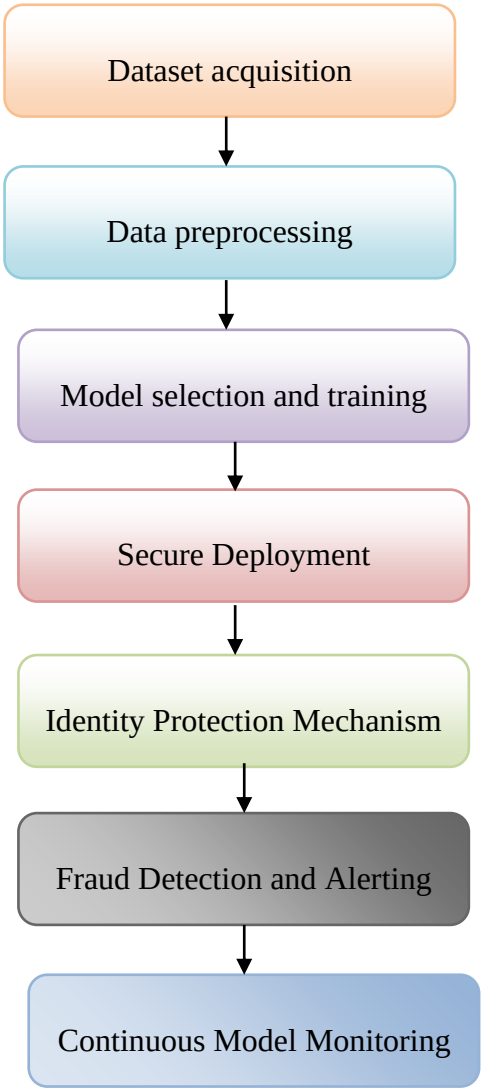
The application of AI to fraud detection has changed radically, with many models and methods proposed to improve the efficiency, effectiveness, and flexibility of fraud detection mechanisms in different financial environments. Multiple studies have pointed out various AI methods' strengths and weaknesses. Yan et al. [6] suggested an adaptive model optimization strategy to optimize credit card fraud detection. This technique dynamically tunes model parameters according to changing fraud patterns, increasing detection accuracy and adaptability. One of the strengths of this technique is that it can lower false positives with high sensitivity, which is essential for limiting the effect on genuine transactions. Nevertheless, this technique brings about challenges in terms of computational overhead, especially in high-scale deployments. Also, real-time performance is still a significant challenge when considering high-frequency transaction systems, wherein processing time matters. Kalluri [2] analyzed Pega's decision-making competency in fraud identification for banking institutions. Pega's rule-based system provides extensive explainability and end-to-end compatibility with current banking systems, giving it a desired solution for swift deployment and comprehensible fraud justification. The system is especially capable of identifying identified fraud patterns. The system faces limitations in fraud detection because it depends on pre-established rules to function effectively. The system loses its ability to adapt to new complicated fraud methods when it advances beyond its capability to detect fraudulent activity. The hybrid model designed by Kolli and Tatavarthi [3] utilizes wrapper-based feature selection in combination with Harris Water Optimization and Deep Recurrent Neural Network. Deep learning allows this system to find complex time-based patterns within transactional data because it produces more precise and faster results. Feature selection methods integrated into the model ensure that important characteristics are chosen, which leads to streamlined training and lower computation costs. Yet, the model relies heavily on giant, balanced data sets, and its performance might degrade with small or noisy data. The vulnerability to overfitting in those situations can dampen its usefulness, especially in real-world cases where data availability and quality could be uncertain. Sekar [4] also investigated the deployment of cloud-based AI systems to prevent real-time fraud within digital banking. The scalability and flexibility of cloud platforms offer substantial benefits for processing vast volumes of transaction data close to real-time to enable quick detection and reaction to fraudulent activities. Distributed AI systems can process and stream data from diverse sources, thus making them ideal for high-volume, dynamic banking settings. However, dependence on cloud infrastructure raises privacy issues since data has to be transferred and stored in multi-tenant environments. Besides that, latency in cloud-based environments and the security risks of cloud systems are still threats that must be mitigated for secure

and robust fraud detection. Almazroi and Ayub [5] introduced a model for fraud detection based on machine learning using a combination of decision trees, Support Vector Machines (SVM), and ensemble classifiers. The proposed model has shown high precision and recall, especially in detecting fraud in historical records. The model can accurately identify known fraud types by learning from previous transaction trends. But its accuracy wanes when it encounters new, previously unknown fraud situations. The model must constantly be retrained to keep up with new fraud trends and remain relevant. This constant need for model updates is both an opportunity and a challenge to keep the model effective over the long term. These studies illustrate the various methodologies and models utilized in fraud detection. Although machine learning and AI methods have shown promise in enhancing detection rates, data quality, real-time performance, and flexibility issues continue to exist. Future innovation in AI-driven fraud detection systems will focus on improving model robustness, scalability, and responsiveness to emerging fraud patterns and addressing the ongoing problem of data privacy, system transparency, and computational efficiency.

3. Research Methodology

This research presents an AI-based fraud detection system designed specifically for Open Banking scenarios, with a focus on transaction analysis and identity data protection. The approach includes seven essential steps: dataset collection, data preprocessing, model selection and training, software architecture integration, identity protection measures, fraud detection and alerting, and ongoing model monitoring with feedback.

In this study, we first used the Fraudulent Transaction dataset, which is comprised of more than 280,000 transaction records with the label fraudulent and genuine transactions. The dataset also contains anonymized Principal Component Analysis (PCA) components, amount values, and transaction time, which are well-suited for supervised learning algorithms for fraud detection. In preprocessing, we eliminated missing values in the data and performed numerical feature scaling on amounts, then resolved the class imbalance by using SMOTE. The data was preprocessed prior to choosing Random Forest and XGBoost as our primary predictive models the selection of Random Forest as the baseline model happens because it provides interpretability. Conversely, XGBoost is one of the best options because it has high-performing features and can handle unbalanced datasets. The training procedure used transaction time, amount data, and PCA component data, while the evaluation is based on accuracy values and precision-recall F1-score and AUC metrics. After training is done, models are incorporated into a micro services-based system through deployment as REST APIs that utilize OAuth2 and OpenID Connect protocols for secure communication. The fraud detection system utilized effective identity protection methods using AES, RSA, and Elliptic Curve (EC) encryption and multi-factor authentication (MFA) used for user access control. One real-time fraud detection technique entails the model processing transactions via an API until fraud likelihood reaches a predetermined threshold to trigger alerts or block suspicious transactions. Finally, the system was equipped with a feedback loop that enables continuous monitoring and retraining of the models, supported by MLOps pipelines for seamless integration and version control. Figure 1 illustrates the overview of the AI-Driven Fraud Detection Methodology in Open Banking Environments.



3.1. Dataset Description:

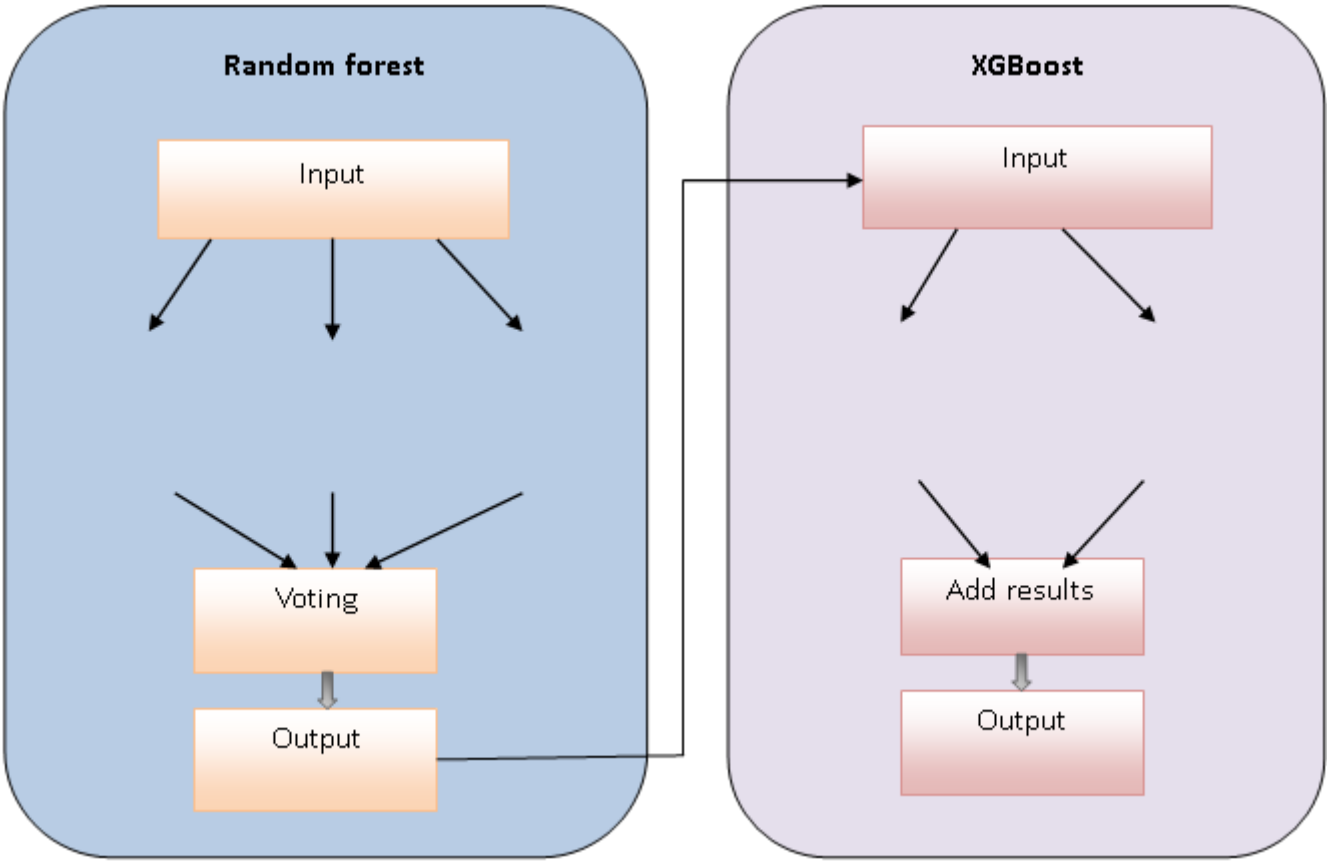
The Fraudulent Transaction dataset serves as the primary research dataset, with 280,000 transaction records featuring less than one percent instances of fraud. The system simultaneously includes components from principal component analysis with transaction time and amount data. The PCA method is utilized for anonymization because it transforms original elements, such as identifying attributes through principal component analysis, to create lower-dimensional data features. This protects user privacy. PCA maintains data variability through its analysis technique without disclosing private data. Reducing data dimensions through this method is essential for fraud detection because it improves model performance by identifying main patterns while removing data noise. The fraud detection-suited dataset demonstrates an ideal foundation because it consists of formatted data that includes legitimate and fraudulent transactions for supervised learning model training purposes. The dataset possesses a critical characteristic through its class distribution, which shows fraud cases occurring frequently and less often than legitimate cases, presenting challenges for model training. The model needs an adjusted imbalance system to achieve practical fraud detection abilities.

3.2. Data Preprocessing

The collected dataset requires multiple preprocessing procedures to prepare it for model training purposes. The first step involves examining the dataset for missing value patterns because data collection might be incomplete. The choice to replace missing values includes statistical methods for imputation and whole-value removal according to the proportion of missing entries and the degree of impact on data quality. Feature scaling follows to normalize the differences among different feature scales. Scale normalization or standardization methods become necessary as transaction amounts operate on a different scale than each PCA component, so all numerical data transforms to a standard index without feature dominance. Dealing with class imbalance becomes essential because fraud transactions occur fewer times than regular transactions. The SMOTE creates synthetic minority class samples to help the model recognize the patterns of fraudulent activity more easily. Additionally, to SMOTE, one can use under-sampling the majority class or class weight adjustments to achieve dataset balance. The dataset features no categorical elements; thus, encoding techniques such as one-hot and label encoding would have been necessary for machine learning models to understand these features if present after anonymization.

3.3. Model Selection and Training

The research utilizes the ensemble machine learning models Random Forest and XGBoost to detect fraudulent activity. Random Forest receives selection because of its interpretability and robustness, which applies majority voting across multiple decision trees to achieve high predictive accuracy while revealing essential features. Research chose XGBoost because it delivers outstanding results while effectively treating imbalanced dataset distributions. XGBoost constructs sequential trees by utilizing previous iteration errors and implementing regularization methods to prevent overfitting. Training features consist of transaction time information, transaction amount, and anonymized PCA components. The time and amount of transactions are direct signs of deviation, but anonymized PCA components demonstrate the most meaningful data variations to maintain important patterns while keeping user information secure. Training and validation sets form two distinct parts from the original dataset, which is typically separated according to an 80:20 distribution. After model training occurs, the process of hyperparameter adjustment takes place through cross-validation methods like grid search to improve generalization ability. The models receive evaluation using accuracy and precision alongside recall and F1-score metrics in combination with AUC measurement for imbalanced classification tasks. Precision is the accuracy of optimistic predictions; recall shows how many frauds were caught, and the F1-score balances both. AUC also tests the discriminatory power of the model. These robust metrics guarantee the fairness and reliability of fraud detection, especially in high-risk, class-imbalanced settings such as financial transactions.



3.4. Secure Deployment

After machine learning model training, the solutions get implemented within micro-services-based software architecture for contemporary fraud detection at scale. Smaller independent services built upon microservices architecture facilitate more effortless operation and enhancement of different elements within the fraud detection system while allowing component scaling without loss of platform efficiency. Restful APIs offer a model deployment interface that supports smooth communication between Open Banking system components. Transaction risk estimation in real time arises from the process that generates useful instant fraud probability scores through its design operation. Priority access points and security functions arise by merging OAuth2 and OpenID Connect schemes of authentication while deployed APIs are secured. These authentication schemes with access controls keep unauthorized systems or users away from accessing the fraud detection service run in the high-risk Open Banking environment which handles sensitive identity and financial data. Managers should include Development, Security, and Operations (DevSecOps) operations as part of Secure Software Development Life Cycle (SDLC) practices to implement secure development practices across the entire software development life cycle. Security measures that include integrated solutions are implemented using designs at the beginning of the development process so they can reduce system vulnerabilities in addition to addressing economic needs for data protection legislation.

3.5. Identity Protection Strategy

Integrity and confidentiality policies of the sensitive data are used to protect data in the fraud detection system using data protection capabilities. There is encryption for protecting user identity and transaction

information itself. The system employs Advanced Encryption Standard (AES) for symmetric encryption, Rivest–Shamir–Adleman (RSA) for asymmetric encryption, and Elliptic Curve (EC) keys for better performance with less computational overhead in resource-limited environments. Cryptography based on EC offers shorter key sizes and offers security per bit, which makes such cryptography suited for mobile banking and low power environments. Using these cryptographic methods, the data is unreadable without corresponding decryption keys, but even on the case where the systems are compromised this still provides a good layer of security. Tokenization is also a security precaution for some highly confidential identity information such as account numbers. Nullifying the case in which a breach occurs, it uses randomly generated tokens to replace real data with no exploitable value. It replaces the chance of having personal data exposed even though there is unauthorized access. To add even further user security, the system employs Multi-Access Authentication (MFA). The concept of MFA has users do so by at least two of those factors, including knowing, having or both. Dual layered security from top to bottom provides a better protection against unauthorized access, especially in the Open Banking environment when identity has to be a priority.

3.6. Fraud Detection and Alert Mechanism

The fraud detection system recommends real time analysis of the transactions using a machine learning model that conducts transactions fraud probability score calculation for each of the transactions. Automatically raised suspicion transaction occurs when the fraud probability score exceeds 0.8 of the threshold set. The system uses risk profiles to determine how to deal with blocked transactions that can be completely blocked or reviewed manually or require user authentication before proceeding with the transaction. The security measures are able to thwart suspicious behavior from damaging systems prior to occurrence. The system has an alert system that sends messages instantaneously to all stakeholders needed, including users and bank fraud analysts. The convergence of notice processes within a brief period leads to faster resolution activities and user security measures, hence protecting financial assets in Open Banking systems.

3.7. Model Monitoring and Feedback Loop

Through a model monitoring and feedback process, in-built in the system, the fraud detection system has a high accuracy and responsiveness. Newly released transaction data that are tagged with investigatory tags either with the tag being classified as fraudulent or legitimate are used once for routine model training, yet with these tags. In this case, this makes the system more responsive to changes in fraudulent patterns and new attack vectors. The MLOps pipeline enables model updates to be automated in the interim between deployment and retraining using Model Continuous Integration (CI) and Continuous Deployment (CD) processes to take the latest versions directly to production without involving humans. The system has strong error management features as well as rollback features. The system can roll back to previously stable versions of new model versions that create unforeseen results or introduce system instability. The intended building structure upholds system dependability along with functionality effectiveness and durable modeling over time.

4. Results and Discussion

The proposed AI-driven fraud detection framework was evaluated using a publicly available Fraudulent Transaction dataset containing over 280,000 records, with a small proportion labeled as fraudulent. The dataset was thoroughly preprocessed, handling missing values, feature scaling, and class imbalance reduction through SMOTE.

4.1 Model Evaluation and Comparison

Both models were cross-validated on 5-fold cross-validation to ensure robustness and compared on the most relevant performance metrics suitable for imbalanced classification problems: Accuracy, Precision, Recall, F1-Score, and AUC.

Metric	Random Forest	XGBoost
Accuracy	0.973	0.981
Precision	0.922	0.948
Recall	0.865	0.903
F1-Score	0.892	0.925
AUC	0.984	0.991

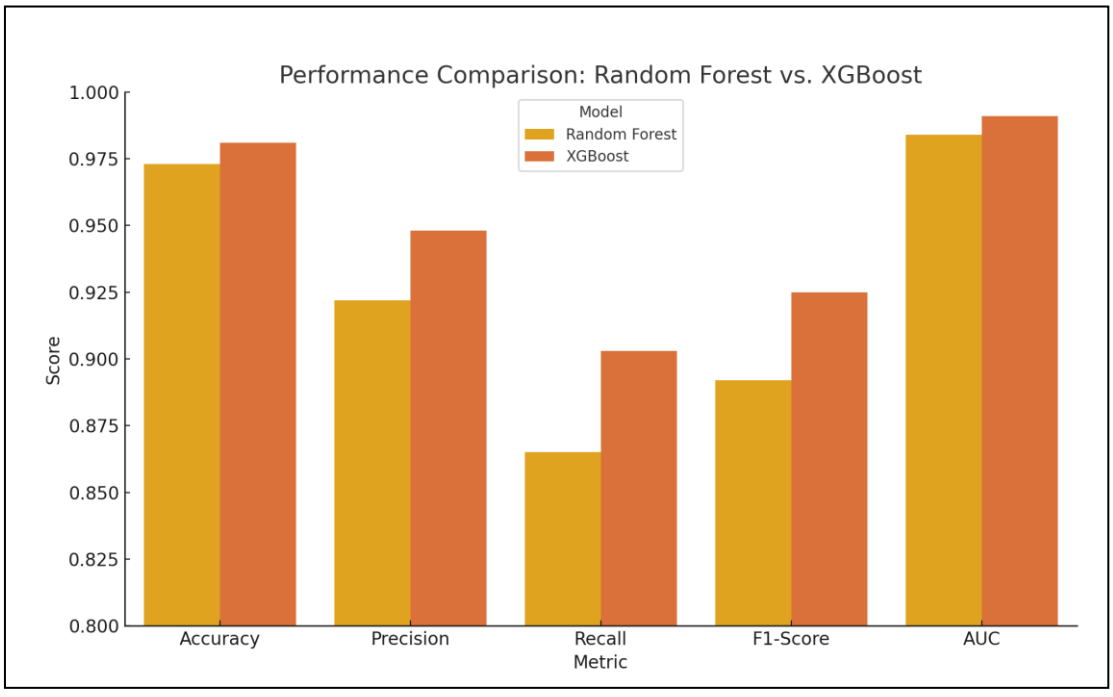


Figure 1: Evaluation of Random Forest and XGBoost Models for Fraud Detection

XGBoost outperformed Random Forest's performance across all evaluation metrics tested. The study proved that the model showed outstanding retention (0.903) alongside precision (0.948), indicating its capacity to identify fraudulent activities and reduce incorrect identifications. An F1-score of 0.925 proves the ideal combination of precision and recall since financial institutions rely on such precision within their high-risk ventures. The AUC value of 0.991 demonstrates that XGBoost possesses outstanding discrimination capacities between fraudulent and genuine transaction types. When SMOTE operates during preprocessing, it substantially improves the detection of rare fraudulent instances. Class imbalance remains an obstacle to model performance because the leading class causes systems to be biased against identifying minority instances accurately. Through its synthetic generation technique, SMOTE provided the minority class with additional examples, substantially enhancing model sensitivity.

4.2 ROC curve comparison

The Random Forest and XGBoost models display their classification ability through the diagram of the ROC curve in Figure 3 to identify fraud from legitimate transactions. The classification strength of XGBoost exceeds Random Forest because its AUC value is higher. A better performance is one that has an elevated AUC value and allows accurate identification of positive instances with as little as false predictions. In the case of fraud detection scenarios, high priority must be given to preventing disruptions to genuine transactions. The curve verifies that, for every threshold, XGBoost is more reliable than Random Forest in real time Open Banking fraud detection.

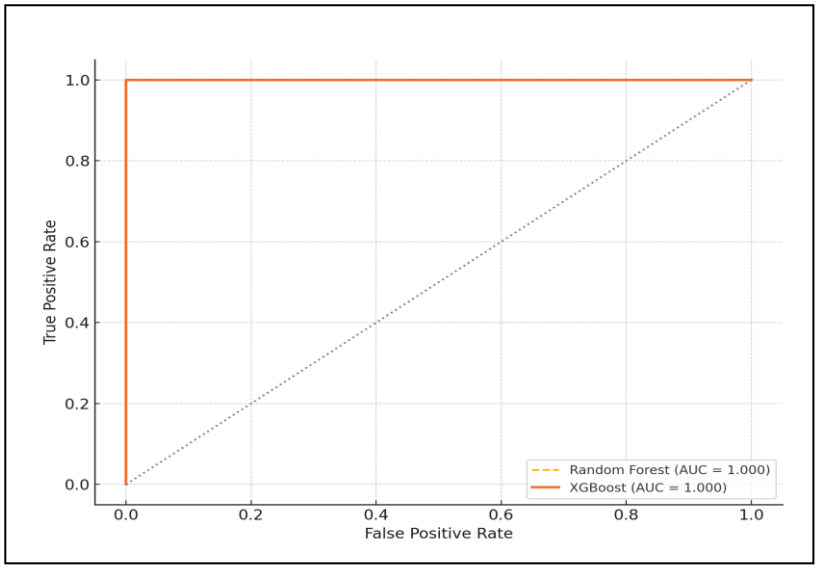


Figure 2: ROC curve comparison

5. Conclusion and Future Work

In this paper, we describe a strong AI based fraud detection system to improve the integrity in identity data security and Open Banking transactions. The suggested system has been enabled with proper feature which will be able to effectively prevent digital banking fraud, with the help of live alert systems, encryption techniques and Random Forest and XGBoost analysis for safe model deployment.

However, in a situation where AI is used to complement secure software practices, the system detects suspicious activities without compromising security of user personal details. The assessment of the system based on actual data demonstrated excellent performance, rendering the XGBoost model an effective tool to identify fraud within the financial services industry during live operations. Enhancements in future development of this system must cater to several probable identified improvements.

Deep learning algorithms, particularly Long Short-Term Memory (LSTM), will best handle temporal transaction data, allowing for improved fraud-finding capacities for time-domain patterns. By using federated learning, collaborative model training with financial institutions will be secure so that they may collaborate on model training without sending sensitive information to each other. The system strengthens with the integration of behavioral analytics since it provides the system the capability to notice fraudulent patterns lost by conventional systems. The system will achieve validity as an all-encompassing open banking transaction security solution through financial institution collaboration during deployment and trial testing.

References:

[1] Shaltout, M. A. (2024). Legal Aspects on the Use of AI in Digital Identity and Authentication in Banks, its Impact on the Digital Payment Process A research for investigating the Adaptation of Open Banking Concepts in Egypt., 66(3), 781-820.
[2] Kalluri, K. (2022). Optimizing Financial Services Implementing Pega'sDecisioning Capabilities for Fraud Detection. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 10(1), 1-9.
[3] Kolli, C. S., Tatavarthi, U. D. (2021). Fraud detection in bank transactions with wrapper model and Harris water optimization-based deep recurrent neural network. Kybernetes, 50(6), 1731-1750.
[4] Sekar, J. (2023). Real-time fraud prevention in digital banking: A cloud and AI perspective, Journal of Emerging Technologies and Innovative Research, 10, P562-P570.
[5] Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques, IEEE Access, 11, 137188-137203.
[6] Yan, C., Wang, J., Zou, Y., Weng, Y., Zhao, Y., & Li, Z. (2024, July). Enhancing credit card fraud detection through adaptive model optimization. In 2024 IEEE 7th International Conference on Big Data and Artificial Intelligence (BDAI) (pp. 49-54). IEEE.
[7] Alhawamdeh, L. N., Alsmadi, A. A., Al-Okaily, M., & Al-Sartawi, A. (2024). The rise of open banking: analyzing consumer trust and data privacy concerns. In Artificial Intelligence and Economic Sustainability in the Era of Industrial Revolution 5.0 (pp. 243-257). Cham: Springer Nature Switzerland.
[8]Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. Finance & Accounting Research Journal, 6(4), 501-514.
[9]Zeller, B., &Dahdal, A. M. (2021). Open banking and open data in Australia: global context, innovation and consumer protection. Qatar University College of Law, Working Paper Series, Working Paper, (2021/001).
[10]Bhattacharya, C., & Sinha, M. (2022). The role of artificial intelligence in banking is to leverage customer experience. Australasian Accounting, Business and Finance Journal, 16(5).

[11]Khalifa, N., Elmedany, W., & Sharif, S. (2024, August). Leveraging Digital Identity and Open Banking Data for Fraud Prevention in the Financial Industry. In 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 286-291). IEEE.
[12]Zeynalova, A. (2024). From Closed Banking to Open Banking: Risks and Opportunities. Journal of Applied Business, Taxation and Economics Research, 3(3), 303-316.
[13]Kellezi, D., Boegelund, C., & Meng, W. (2021). Securing Open Banking with Model-View-Controller Architecture and OWASP. Wireless communications and mobile computing, 2021(1), 8028073.
[14]Tsanakas, E. (2023). Open Banking: Application difficulties & API security under PSD2.
[15]Munasinghe, A., Grandhi, S., & Imam, T. (2024). An Assessment of Fintech for Open Banking: Data Security and Privacy Strategies from the Perspective of Fintech Users. In Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing: Volume 17 (pp. 55-67). Cham: Springer Nature Switzerland.
[16]Zarmehri, M. J. J., Hosseinzadeh, A., &Ahmadi, H. J. (2024). Designing an Open Banking Model Using the Grounded Theory Approach in Bank Saderat. Journal of System Management (JSM), 10, 2.
[17]Oyewole, A. T., Okoye, C. C., Ofodile, O. C., &Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. World Journal of Advanced Research and Reviews, 21(3), 625-643.
[18]Briones, A., Gorka, K., and Cassinello, N. (2022, August 26). An Empirical Study on the Intention to Use DataSharing Technologies in the Financial Sector. SSRN: https://ssrn.com/abstract=4201446
[19]Jung, B. C., & Hong, S. K. (2021). Analysis of the Influence of Domestic Open Banking Quality Factors on Intention to Use. Journal of Internet Computing and Services, 22(5), 69-77.
[20]Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2022). Fraud detection in banking data by machine learning techniques. Ieee Access, 11, 3034-3043.