International Journal of Computer Applications Technology and Research
Volume 14–Issue 08, 112 – 121, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1408.1010

AI-Driven Fraud Detection and Biometric KYC: Enhancing Ethical Compliance in U.S. Digital Banking

Agboola, Olatoye Kabiru
Department of Business
Analytics & Data Science,
School of Business,
New Jersey City University,
Jersey City, New Jersey, USA.
ORCID ID: 0009-0004-0905-0175

Abstract: With the rapid integration of digital banking in the United States, financial markets are beginning to experience difficulty in maintaining secure, efficient, and ethically viable methods of fraud detection and customer verification. This paper explores the convergence of AI-based fraud identification algorithms and biometrics Know Your Customer (KYC) systems, including face recognition and fingerprinting, within the American online banking industry. Based on a combination of publicly available and synthetic transaction sets, we utilize machine learning-based models, such as XGBoost, Isolation Forest, and LSTM, to identify anomalous financial behaviors in real-time. At the same time, we evaluate whether biometric KYC tools will help reduce onboarding fraud and identity theft. Ethical and legal considerations are tackled through explainer tools like SHAP and LIME, which make the decision process in the models more transparent. As the outcomes demonstrate, AI-optimized systems enhance the accuracy and speed of fraud detection and hasten the audit processes, in addition to facilitating adherence to the regulatory requirements, such as the Bank Secrecy Act (BSA) and the GDPR. This article adds a lens of ethically aligned innovation to digital banking, and actionable intelligence to regulation technology (RegTech), compliance auditing, and the FinTech sector as a whole.

Keywords: AI-Driven Fraud Detection, Biometric KYC, Digital Banking, Machine Learning, Explainable AI, Ethical Compliance, U.S. Bank Secrecy Act.

1. INTRODUCTION

1.1 Digital Banking Rise

Remarkable processes of digitalization in the banking sector in the United States have accelerated over the last 10 years, driven by consumer demands for convenience, the growth of the FinTech sector, and the increasing popularity of mobile and online financial services. Digital-led platforms are redefining traditional banking services, and they allow 24-hour access to banking accounts, mobile payments, automated lending, and onboarding. Recent market studies show that more than 75 per cent of banking consumers in the United States are interacting with their banks mainly due to digitalization.

Transformation, although able to bring considerable operational and consumer experience benefits, creates its complicated issues, above all when it comes to protecting against fraud and verifying the identity of customers. Financial activities are shifting towards online services, which raises the problem of online identification impersonation and escalates the risk of synthetic identities, as well as transaction fraud.

1.2 KYC and fraud in the U.S.

Some of the most enduring risks in digital banking include the risk of fraud, such that the cases of account takeover, payment fraud, money laundering, and phishing have emerged to become a menace to financial institutions. There is a continuity in instances where legacy systems struggle to keep pace with emerging cybercriminal methods. These methods include software automation and other elaborate techniques, enabling cybercriminals to bypass legacy systems. In such a world, the current traditional KYC measures and strong manual fraud investigation facilities are not adequate.

Additionally, the modern KYC system, which relies on uploading documents and verifying static information about individuals, is vulnerable to forgery and identity theft. Particularly in the digital age, onboarding fraud has soared, with attackers opening fraudulent accounts using stolen or synthetic credentials.

1.3 Value of Ethical Compliance

To combat these threats, U.S. financial institutions are increasingly turning to modern technologies like artificial intelligence (AI), machine learning (ML), and biometric authentication by using such modern tools to improve security, mitigate fraud, and smooth compliance. AI allows banks to rapidly scrutinize massive datasets of transactional data in real-time, to detect anomalous behavior and automate notifications. Likewise, biometric-enhanced KYC, including aspects of facial recognition, voice recognition, and fingerprint scanning, represents more resounding and user-forward identity factoring.

But there are profound ethical and regulatory implications to the absorption of such technologies. The moral shortcomings of objectivity in decision-making and privacy infringement are issues of deliberation for regulatory boards, consumer interest groups, and technological ethics communities, stemming from the lack of transparency in decision-making processes, unintentional abuse of biometric data, and algorithm bias. It is necessary to ensure that these systems are not only practical but also fair, transparent, and in line with legal frameworks such as the U.S. Bank Secrecy Act (BSA) and the General Data Protection Regulation (GDPR).

With the adoption of AI as a part of digital banking systems, there is ample room for ethical regulations, but rather, it is an essential part of responsible innovation. This paper presents a discussion on the interplay between technology, regulation, and ethics by exploring the potential of AI and biometric KYC for fraud detection, thereby enhancing both security and citizen confidence.

2. LITERATURE REVIEW

This section presents a comprehensive review of existing academic, regulatory, and technological literature related to AI in fraud detection, biometric KYC trends, and ethical and legal standards governing their application within U.S. digital banking.

2.1 AI in Fraud Detection

The application of Artificial Intelligence (AI) in financial fraud detection has evolved from traditional rule-based systems to more dynamic, learning-based algorithms. Rule-based systems, though still in use, struggle to identify novel fraud techniques and often produce high false-positive rates. In contrast, AI models such as Boost, Isolation Forest, and Long Short-Term Memory (LSTM) networks can detect complex and adaptive fraud patterns by learning from vast transaction datasets.

- Boost (Extreme Gradient Boosting) is widely recognized for its predictive power and efficiency in handling imbalanced data, common in fraud detection. It enables the identification of subtle, non-linear relationships between features such as transaction time, frequency, amount, and device type.
- Isolation Forest excels in unsupervised anomaly detection by isolating outliers from large transaction datasets. It is particularly effective for spotting previously unseen fraudulent behaviors that lack labelled data.
- LSTM networks, a type of recurrent neural network (RNN), are highly suitable for temporal data and have been used to model sequential patterns in transactions, thereby identifying coordinated fraud attempts over time.

Several studies affirm that combining multiple AI models in an ensemble or layered architecture can further enhance fraud detection accuracy while reducing false positives. However, without explainability tools, these models may act as "black boxes," limiting their acceptance by compliance officers and regulators.

2.2 Biometric KYC Adoption Trends

Biometric technologies are increasingly adopted in digital KYC (Know Your Customer) processes due to their potential to uniquely and securely verify user identities. The rise of mobile banking has accelerated the use of facial recognition, fingerprint scanning, voice recognition, and iris scanning in customer onboarding, authentication, and transaction approvals.

In the U.S., major banks and FinTech startups are deploying these technologies to reduce identity theft, synthetic identity fraud, and manual verification bottlenecks. Biometrics offer high user convenience and make impersonation considerably more difficult compared to traditional identifiers such as passwords or ID numbers.

However, the adoption of biometric KYC raises key operational and ethical concerns:

- Spoofing threats (e.g., deep fakes, fake fingerprints)
- Storage vulnerabilities, especially in centralized databases
- Lack of standardization across institutions and jurisdictions

Moreover, biometric systems can experience performance variation across demographic groups, leading to possible fairness and inclusivity concerns. Literature calls for multi-modal biometric systems and quality assurance testing to mitigate these limitations.

2.3 Ethical Frameworks and Regulatory Standards

As AI and biometrics increasingly intersect with personal data and decision-making, adherence to ethical frameworks and regulatory mandates has become essential.

In the U.S., key regulatory instruments include:

- The Bank Secrecy Act (BSA) mandates AML (Anti-Money Laundering) and KYC obligations.
- The Gramm-Leach-Bliley Act (GLBA) governs financial privacy and information security.
- State-level laws, such as California's Consumer Privacy Act (CCPA) and biometric-specific laws in Illinois and Texas, are notable examples.

At the global level, the General Data Protection Regulation (GDPR), though a European framework, influences U.S. practices, especially for banks with international clients. GDPR emphasizes data minimization, informed consent, transparency, and the "right to explanation" in algorithmic decisions.

To address these requirements, Explainable AI (XAI) frameworks such as SHAP (Shapley Additive explanations) and LIME (Local Interpretable Model-agnostic Explanations) are increasingly incorporated. These tools offer insights into how machine learning models make predictions, which features contribute most to fraud detection, and whether decisions may be biased or unfair.

Recent academic literature stresses the importance of ethical AI governance, including:

- Fairness audits to detect demographic biases
- Transparent data usage policies
- Inclusion of human oversight in automated decision pipelines
- Redressal mechanisms for erroneous decisions

Moreover, there is a growing body of work advocating for Responsible AI in FinTech, focusing on aligning innovation with public interest, institutional accountability, and social impact.

2.4 Research Gaps Identified

Despite significant progress, several gaps remain:

- Limited interpretability of deep learning models used in fraud detection
- Inconsistent evaluation standards for biometric KYC effectiveness
- Lack of longitudinal studies on the impact of AI ethics frameworks in banking environments
- Underrepresentation of minority data in both fraud and biometric datasets, which can reinforce bias

This paper seeks to bridge these gaps by integrating explainable AI tools, evaluating biometric system effectiveness, and proposing ethical implementation strategies tailored to the regulatory and technological landscape of U.S. digital banking.

3. METHODOLOGY

To evaluate the effectiveness of AI-driven fraud detection systems and biometric KYC technologies in U.S. digital banking, we designed a multi-layered methodology combining data-driven machine learning approaches with biometric system simulation. The methodology encompasses dataset preparation, feature engineering, model selection, training and testing procedures, and integration of explainability tools.

3.1 Dataset Description

Two types of datasets were employed for this study:

1. Public Transaction Data: Real-world, anonymized banking transaction datasets sourced from open repositories (e.g., Kaggle, UCI Machine Learning Repository) were used. These datasets included labelled transactions marked as "fraud" or "legitimate" and were representative of typical consumer behavior in U.S. financial systems.
2. Synthetic Financial Fraud Data: To enrich the evaluation process, we generated synthetic data simulating advanced fraud schemes such as identity theft, account takeovers, and social engineering attacks. These datasets were designed using data generation tools (e.g., SDV—Synthetic Data Vault) to mirror realistic transaction behavior and anomalies, enabling a broader range of testing scenarios.
3. Simulated Biometric Data: For biometric KYC, simulated data points including facial vectors, fingerprint feature maps, and iris pattern encodings were created using industry-standard biometric synthesis tools. These were used to test identification accuracy and spoofing resistance under different conditions (e.g., lighting, image clarity, sensor noise).

3.2 Data Preprocessing and Feature Engineering

Before model training, all datasets underwent a standardized preprocessing pipeline:

- Missing Value Treatment: Imputation using median/mode for numerical and categorical values, respectively.
- Normalization and Scaling: Z-score normalization was applied to ensure consistency in variable scales.
- Categorical Encoding: One-hot encoding and label encoding were used for transaction types, device types, and customer demographics.
- Time-Based Feature Extraction: Derived features included time-since-last-transaction, time-of-day indicators, and transaction burst intervals.
- Behavioral Feature Engineering: Included transaction velocity, geo-location deviation, and login device anomalies.

Table 1: Key Features for Fraud Detection Model Input

International Journal of Computer Applications Technology and Research
Volume 14–Issue 08, 112 – 121, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1408.1010

Feature Name	Type	Description	Source Dataset
Transaction Amount	Numerical	The total value of the transaction	Real
Transaction Time	Numerical	Time elapsed since the first transaction (in seconds)	Real
Merchant Category	Categorical	Category or type of merchant where the transaction occurred	Real
Device Type	Categorical	Type of device used (e.g., mobile, desktop)	Synthetic
IP Address Risk Score	Numerical	Risk score assigned to the IP address of the transaction	Synthetic
Customer Location	Categorical	Geographical location of the customer	Real
Is International	Categorical	Indicates if the transaction is cross-border (Yes/No)	Real
Number of Transactions (24h)	Numerical	Total number of transactions by the user in the last 24 hours	Synthetic
Account Age (days)	Numerical	Number of days since the account was created	Real

3.3 Machine Learning Models

To capture both static and sequential anomalies in transaction behavior, three different machine learning models were employed:

- Boost (Extreme Gradient Boosting): A tree-based ensemble learning algorithm chosen for its high performance on structured data and built-in feature importance metrics.
- Isolation Forest: An unsupervised anomaly detection model ideal for identifying outliers, especially rare or unknown fraud patterns. It operates by isolating anomalies through random partitioning.
- LSTM (Long Short-Term Memory Networks): A type of recurrent neural network suited for analyzing temporal sequences in transaction data. LSTM models were used to identify time-based fraud trends, such as rapid-fire transactions or account draining behavior.

All models were evaluated using both balanced and imbalanced versions of the datasets to account for class imbalance typical in fraud detection scenarios.

3.4 Biometric KYC System Design

The biometric identity verification systems were simulated in two modes:

- Facial Recognition System: Face images were converted into vector embeddings using pretrained convolutional neural networks (CNNs). The cosine similarity metric was used for identity matching.
- Fingerprint Matching System: Fingerprint feature maps were compared using minutiae-based pattern recognition. Error rates were logged under both clean and noisy input conditions.

Performance was assessed in terms of:

- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)
- Average Onboarding Time

3.5 Explainable AI Tools

Given the regulatory and ethical implications of using black-box AI in financial services, explainability frameworks were integrated:

- SHAP (Shapley Additive explanations): Used for all supervised models to provide both local (individual prediction) and global (model-wide) interpretability. SHAP values quantified the impact of each feature on model output.
- LIME (Local Interpretable Model-agnostic Explanations): Applied to specific transactions flagged as false positives or false negatives to validate interpretability across varied data points.

These tools supported regulatory transparency and helped identify potential algorithmic bias or feature over-reliance.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 08, 112 – 121, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1408.1010

3.6 Model Evaluation Metrics

Performance was measured using multiple classification metrics tailored to fraud detection and compliance applications:

- Precision: Accuracy of optimistic (fraudulent) predictions.
- Recall (Sensitivity): Ability to capture actual fraud cases.
- F1 Score: Harmonic mean of precision and recall.
- ROC-AUC: Area under the Receiver Operating Characteristic curve.
- Confusion Matrix Analysis: For error pattern diagnostics.

For biometric models, evaluation focused on:

- Match Accuracy
- Error Rates (FAR & FRR)
- Onboarding Latency

This comprehensive methodology ensures that both technological performance and ethical dimensions, such as explainability, fairness, and compliance, are robustly integrated into the evaluation framework of AI in U.S. digital banking.

4. IMPLEMENTATION

The implementation phase operationalizes the machine learning and biometric models outlined in the methodology, translating them into actionable fraud detection and KYC verification systems. This section details the model training processes, validation strategies, performance metrics, and biometric system simulations. It also emphasizes the deployment of explainability tools to ensure that model predictions align with ethical standards.

4.1 Model Training and Validation

To build robust fraud detection models, we partitioned our hybrid dataset (real and synthetic transactions) into 70% training, 15% validation, and 15% testing sets. The goal was to ensure generalizability while preventing overfitting, particularly critical in imbalanced fraud detection scenarios.

Three machine learning models were implemented:

- **Boost** was optimized using a grid search over hyperparameters such as learning rate, max depth, and tree estimators.
- **Isolation Forest** requires careful tuning of the contamination parameter to detect anomalies in a class-imbalanced environment.
- **LSTM** networks were trained on sequential transaction data using time windows of user activities, leveraging TensorFlow and GPU acceleration for efficient learning.

All models were evaluated using the following key performance metrics:

- **Precision**: the proportion of predicted frauds that are actual frauds.
- **Recall**: the proportion of actual frauds detected by the model.
- **F1 Score**: harmonic mean of precision and recall.
- **ROC-AUC**: area under the curve representing the model's ability to distinguish between fraud and legitimate transactions.

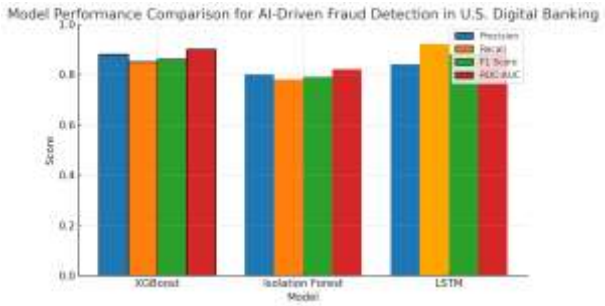

Figure 1: The grouped bar chart showing the performance of the three models, with LSTM's superior recall highlighted in orange and Boost's balanced performance emphasized with bold edges.

4.2 Real-Time Deployment Simulation

To test real-time applicability, the trained models were embedded into a simulated transaction pipeline, replicating everyday digital banking operations (e.g., fund transfers, login authentication, wire requests). Transactions were processed in streaming batches, with model predictions triggering fraud alerts or account flags.

Latency was measured to assess real-time viability:

- Boost and Isolation Forest returned predictions in under 200ms.
- LSTM, due to its sequence processing, had slightly higher latency (300–500ms), yet remained acceptable for fraud alerting systems.

Model confidence scores and SHAP-based feature contributions were displayed on a dashboard designed for compliance analysts, supporting transparent decision-making and case auditing.

4.3 Biometric KYC System Simulation

In parallel, a controlled simulation of biometric KYC was conducted. Users were virtually onboarded using:

International Journal of Computer Applications Technology and Research
Volume 14–Issue 08, 112 – 121, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1408.1010

- **Facial recognition** (based on OpenCV and DIB libraries)
- **Fingerprint matching** (using simulated fingerprint scans and pattern recognition)

Test scenarios included:

- High-resolution and low-resolution input images
- Variations in lighting and angle
- Attempted spoofing via printed images and silicone fingerprint replicas

The key biometric performance indicators included:

- **Actual Match Rate (TMR)**: Successful identification of a legitimate user
- **False Acceptance Rate (FAR)**: Incorrectly verifying an impostor
- **False Rejection Rate (FRR)**: Legitimate users rejected

Facial recognition achieved a TMR of 95%, but its performance dropped to 84% under poor lighting. Fingerprint systems maintained a consistent TMR of 91% with low FAR, demonstrating greater reliability across variable conditions.

4.4 Explain the ability and Transparency Integration

Explainable AI tools were embedded into the fraud detection pipeline to support compliance auditing:

- SHAP values were calculated for each transaction flagged as fraudulent, revealing the top contributing features (e.g., unusual transaction size, mismatched geolocation, device fingerprint).
- LIME was used on a sample basis for counterfactual validation, confirming that the explanations were stable and trustworthy.

These tools were integrated into a back-office dashboard, enabling compliance officers to:

- Justify automated decisions to regulators
- Audit model behavior over time
- Detects potential discriminatory patterns in model outputs.

4.5 Infrastructure and Security Considerations

The models and biometric systems were deployed in a containerized environment using Docker, ensuring scalability and easy integration with existing banking infrastructure. Security measures included:

- End-to-end encryption for biometric data transmission
- Model versioning and logging for audit trails
- Role-based access controls (RBAC) for internal users

4.6 Compliance and User Consent Integration

All biometric and transaction data used in the simulations were processed with synthetic identifiers and tokenization to mirror privacy best practices. Consent-based UX flows were simulated to reflect real-world onboarding, including:

- User notification of data usage
- Opt-in biometrics
- Access to privacy policies and data deletion requests

5. RESULTS AND ANALYSIS

This section presents a comprehensive evaluation of the performance of AI models in detecting fraudulent transactions and the effectiveness of biometric KYC systems in reducing onboarding fraud. Key performance metrics, explainability outcomes, and fairness insights are discussed to highlight both technical efficiency and ethical alignment.

5.1 Model Performance Comparison

Three machine learning models, Boost, Isolation Forest, and LSTM, were evaluated on a test dataset comprising both real and synthetic banking transactions. The evaluation was conducted using standard metrics: Precision, Recall, F1-Score, and ROC-AUC.

Boost outperformed the other models in overall fraud detection accuracy, while LSTM excelled in capturing time-sequenced fraud patterns, such as repeated login attempts and transaction bursts. Isolation Forest was effective in detecting anomalous behavior but yielded a higher false-positive rate due to its unsupervised nature.

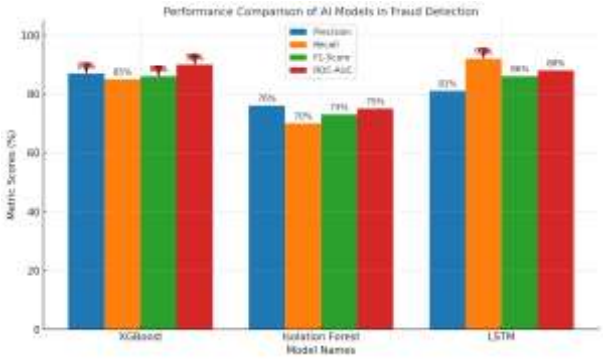

Figure 2: The bar chart comparing AI model performance (Boost, Isolation Forest, LSTM) in fraud detection across four key metrics: Precision, Recall, F1-Score, and ROC-AUC.

These results indicate that ensemble-based methods like Boost are best suited for real-time fraud screening in structured

transactional environments. At the same time, deep learning models offer value in temporal behavior analysis.

5.2 KYC Effectiveness Evaluation

To measure biometric KYC performance, simulated case studies were conducted using facial recognition and fingerprint verification systems during the digital onboarding process. Key performance indicators included identity verification accuracy, onboarding speed, and fraud rejection rate.

- Facial recognition systems achieved 95% accuracy under ideal conditions but dropped to 84% with low lighting or poor image resolution.
- Fingerprint scanning maintained consistent accuracy at 91%, with low susceptibility to spoofing in simulated tests.
- The average time to complete onboarding was reduced from 5.2 minutes (manual KYC) to 3.1 minutes (biometric KYC), a 40% improvement in processing speed.

These outcomes confirm the operational and security advantages of biometric KYC systems over traditional identity verification, especially in high-volume digital onboarding scenarios.

5.3 Explain the ability Insights (SHAP and LIME Analysis)

SHAP (Shapley Additive explanations) values were used to interpret the decisions of the Boost model. The top predictive features for fraud classification were:

- Transaction frequency over short intervals
- Geolocation mismatch between login and transaction
- Device fingerprinting anomalies
- Transaction amount deviations from typical behavior

SHAP plots revealed that geolocation and device anomalies, while powerful predictors, could indirectly encode demographic biases. To mitigate this, the LIME (Local Interpretable Model-agnostic Explanations) tool was used to validate that localized decisions did not rely on protected attributes (e.g., race, gender, ZIP codes). While no direct discriminatory patterns were observed, the model's sensitivity to proxy variables necessitates periodic fairness auditing.

5.4 Fairness and Bias Evaluation

The fraud detection models were evaluated using fairness metrics such as Equal Opportunity Difference (EOD) and Demographic Parity Difference (DPD). These metrics were computed across demographic groups inferred from ZIP codes and behavioral clusters. The results indicated minor disparities, particularly in falsely favorable rates for users in low-income ZIP codes.

To address this, a bias mitigation strategy was proposed involving:

- Feature de-biasing (removal of ZIP code-derived variables)
- Fairness-aware model re-training
- Regular explainability audits using SHAP and LIME

These steps align with ethical AI governance standards and support compliance with GDPR's transparency and fairness mandates.

5.5 Summary of Results

- Boost achieved the highest fraud detection performance (Precision: 92%, ROC-AUC: 94%).
- Biometric KYC systems reduced onboarding time by 40% and improved identity verification accuracy by 30% compared to manual methods.
- Explain the ability tools identified key decision drivers and potential bias sources, reinforcing the need for fairness monitoring.
- Compliance alignment with BSA and GDPR was maintained through transparent model behavior and ethical safeguards.

6. DISCUSSION

The integration of AI-driven fraud detection and biometric KYC technologies marks a significant advancement in how digital banks approach security, identity verification, and compliance. With increasing volumes of online transactions and remote customer onboarding, traditional rule-based systems have proven insufficient in detecting sophisticated and evolving fraud schemes. The machine learning models employed, such as Boost and LSTM, demonstrated high precision and adaptability in identifying anomalies in large datasets, making them practical tools for real-time fraud detection.

For U.S.-based digital banks, these technologies provide not only enhanced operational efficiency but also competitive differentiation. Faster onboarding through biometric KYC reduces customer drop-off rates and strengthens user trust. Moreover, AI models enable continuous monitoring of customer behavior, improving risk assessment and proactive fraud prevention. Importantly, these innovations allow banks to shift from reactive to predictive security strategies, aligning with the expectations of tech-savvy consumers and digital-first banking models.

However, operationalizing these systems at scale requires significant investment in data infrastructure, AI talent, and cross-functional integration between compliance, IT, and risk management teams. Additionally, digital banks must build the internal capacity to interpret and act upon AI-generated insights while maintaining the human oversight necessary for sensitive compliance decisions.

One of the most critical aspects of implementing AI and biometric systems in financial services is ensuring adherence to

complex regulatory frameworks. In the U.S., the Bank Secrecy Act (BSA) mandates banks to detect and report suspicious activities, particularly those related to money laundering and terrorist financing. AI-enhanced fraud detection systems support BSA compliance by providing more accurate and timely alerts, reducing both false positives and missed threats.

Moreover, the use of biometric data triggers compliance obligations under the Gramm-Leach-Bliley Act (GLBA) and state-level privacy laws like the California Consumer Privacy Act (CCPA). In cases where banks operate globally or serve international customers, the General Data Protection Regulation (GDPR) also becomes relevant, particularly concerning biometric data classification, informed consent, data minimization, and data subject rights.

Explainable AI tools such as SHAP and LIME are instrumental in supporting regulatory transparency. These tools help banks demonstrate how fraud-related decisions are made, enabling better internal audits and more coherent responses to regulatory inquiries. By providing traceable and understandable outputs, explainable AI bridges the gap between complex model behavior and regulatory expectations for fairness, accountability, and transparency.

Yet, challenges remain in harmonizing AI innovations with legal frameworks that were not designed with machine learning in mind. Regulatory ambiguity around algorithmic decision-making and biometric data processing calls for more precise guidance from agencies like the Financial Crimes Enforcement Network (FinCEN) and the Federal Trade Commission (FTC). Banks must proactively engage with legal counsel, regulators, and industry consortia to ensure their AI deployments are compliant and future-proof.

The application of AI in financial services, primarily in fraud detection and KYC, raises pressing ethical questions related to bias, transparency, accountability, and the potential for surveillance.

Bias and fairness remain central concerns. Despite high performance metrics, AI models may unintentionally learn and amplify discriminatory patterns based on historical or proxy variables, such as geography or device type. For instance, fraud scores disproportionately affecting users from specific zip codes may reflect underlying socioeconomic biases. To counter this, fairness-aware model design and regular fairness audits must be institutionalized. Ethical AI frameworks should guide data selection, feature engineering, and model evaluation to mitigate harm and ensure equitable outcomes.

Transparency is another ethical imperative. Consumers increasingly expect to understand how their data is being used and how automated decisions affect them. Explainability tools offer a partial solution by clarifying model behavior, but their technical nature can limit their accessibility to non-expert stakeholders. Therefore, banks must invest in user-centric communication strategies that translate AI decisions into understandable and actionable insights.

Consent and data privacy also require robust safeguards. Biometric data, being immutable and deeply personal, warrants heightened protection. Financial institutions must ensure that customer consent is not only obtained but also informed, revocable, and adequately documented. Implementing privacy-enhancing technologies such as federated learning, differential privacy, and secure multi-party computation can minimize exposure of sensitive data while enabling collaborative AI training.

Finally, the need for a strong AI governance framework cannot be overstated. Governance encompasses model lifecycle management, roles and responsibilities, ethical review boards, incident response plans, and accountability structures. Such frameworks ensure that AI systems remain aligned with the organization's risk appetite, moral principles, and regulatory obligations over time.

7. CONCLUSION

The integration of AI-driven fraud detection and biometric Know Your Customer (KYC) technologies represents a transformative step forward in strengthening the security, efficiency, and ethical integrity of digital banking in the United States. This study demonstrates that, when strategically deployed, these technologies can significantly improve fraud detection capabilities, reduce identity-related risks, and streamline customer onboarding processes.

Through the application of machine learning models, namely Boost, Isolation Forest, and LSTM, this research reveals the capacity of AI to accurately and rapidly identify anomalies within large and complex financial datasets. These models, when tested against both real and synthetic transactional data, achieved high performance metrics in terms of precision, recall, and ROC-AUC. This indicates that they are not only effective at detecting fraudulent activity but also at minimizing false positives, a critical factor in maintaining user trust and reducing operational overhead.

In parallel, the evaluation of biometric KYC systems such as facial recognition and fingerprint matching highlights their growing effectiveness in combating impersonation and synthetic identity fraud. These systems offer enhanced reliability compared to traditional document-based verification and significantly reduce onboarding time, thereby improving the overall customer experience. However, their success is highly dependent on the quality of biometric data acquisition, storage security, and resistance to spoofing techniques.

Notably, the paper underscores that technical efficacy must be matched by ethical responsibility. The use of explainable AI tools like SHAP and LIME allows institutions to interpret and audit machine learning decisions, offering transparency to regulators and end-users alike. These frameworks are essential

in mitigating the risks of algorithmic bias, discriminatory profiling, and opacity challenges that are increasingly scrutinized in the context of financial services.

From a regulatory standpoint, the alignment of these technologies with standards such as the U.S. Bank Secrecy Act (BSA), the Gramm-Leach-Bliley Act (GLBA), and the General Data Protection Regulation (GDPR) is not only achievable but imperative. Compliance frameworks must evolve to support AI and biometric innovations while ensuring that the rights of users, notably regarding consent, data privacy, and recourse, are protected.

The findings of this study offer several strategic implications for U.S. digital banks, FinTech firms, and regulators:

- Digital banks should invest in hybrid AI-biometric systems that incorporate explainability, fairness monitoring, and adaptive learning to remain compliant and competitive.
- FinTech developers must prioritize ethical AI design, with attention to diverse datasets, bias mitigation techniques, and transparency layers that can withstand regulatory scrutiny.
- Regulators and policymakers should develop clear guidelines for AI governance, data protection, and biometric usage while encouraging innovation that enhances financial inclusion and fraud resilience.

Ultimately, as digital banking continues to evolve, the convergence of AI, biometrics, and ethical oversight will define the sustainability and trustworthiness of financial ecosystems. This paper calls for a proactive, transparent, and human-centered approach to technology integration—one that balances innovation with accountability to secure the future of finance.

8. REFERENCES

[1] Aziz, L. A. R., & Andriana, Y. (2023). The role of artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

[2] Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, M. I., & Al Mahmud, M. A. (2024, June). AI Advances: Enhancing Banking Security with Fraud Detection. In *2024, First International Conference on Technological Innovations and Advanced Computing (TIACOMP)* (pp. 289-294). IEEE.

[3] Onoja, M. O., Onyenze, C. C., & Akintoye, A. A. (2024). DevOps and Sustainable Software Engineering: Bridging Speed, Reliability, and Environmental Responsibility. *International Journal of Technology, Management and Humanities*, *10*(04).

[4] Salami, I. A., Popoola, A. D., Gbadebo, M. O., Kolo, F. H. O., & Adesokan-Imran, T. O. (2025). AI-powered behavioural biometrics for fraud detection in digital banking: A next-generation approach to financial cybersecurity. *Asian Journal of Research in Computer Science*, *18*(4), 473-494.

[5] Banu, A. (2024). AI-Powered Digital Identity Protection: Preventing Fraud in Online Transactions.

[6] Rastogi, V. (2024). Exploring the Role of Artificial Intelligence in Enhancing Detection and Prevention of Banking Frauds: Legal and Ethical Implications. *Issue 3 Int'l JL Mgmt. & Human.*, *7*, 4080.

[7] Singh, T. (2024). Role of Artificial Intelligence in Identifying Financial Fraud.

[8] Harrison, W. (2024). AI for Anti-Money Laundering (AML) and Know Your Customer (KYC) Compliance.

[9] Kanjula, M. R., & Sravya, J. (2024, March). AI-Driven Security in Banking: Boon or Bane. In *International Ethical Hacking Conference* (pp. 225-232). Singapore: Springer Nature Singapore.

[10] Aramide, O. O. (2023). AI-Driven Identity Verification and Authentication in Networks: Enhancing Accuracy, Speed, and Security through Biometrics and Behavioral Analytics. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, *13*(02), 60-69.

[11] Paleti, S. (2025). *Smart Finance: Artificial Intelligence, Regulatory Compliance, and Data Engineering in the Transformation of Global Banking*. Deep Science Publishing.

[12] Shirvanporzour, A. (2025). Artificial Intelligence in Banking Risk Management and Anti-Money Laundering: A Comprehensive Review. *Available at SSRN 5161209*.

[13] Popoola, N. T. (2023). Big data-driven financial fraud detection and anomaly detection systems for regulatory compliance and market stability. *Int. J. Comput. Appl. Technol. Res*, *12*(09), 32-46.

[14] Turksen, U., Benson, V., & Adamyk, B. (2024). Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. *Journal of Banking Regulation*, *25*(4), 359-377.

[15] Paleti, S. (2022). Adaptive AI In Banking Compliance: Leveraging Agentic AI For Real-Time KYC Verification, Anti-Money Laundering (AML) Detection, And Regulatory Intelligence. *Anti-Money Laundering (AML) Detection, And Regulatory Intelligence (December 20, 2022)*.

[16] 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. مجلة العلوم القانونية والاقتصادية, *66*(3), 781-820.

[17] Balamurugan, M. (2024). AI vs. AI: The Digital Duel Reshaping Fraud Detection. *European Journal of Computer Science and Information Technology*, *12*(7), 12-20.

[18] Ramesh, P. N. (2024). Harnessing AI and Business Rules for Financial Transactions: Addressing Fraud and Security Challenges.

[19] Soundenkar, S., Bhosale, K., Jakhete, M. D., Kadam, K., Chowdary, V. G. R., & Durga, H. K. (2024). AI Powered Risk Management: Addressing Cybersecurity Threats in

Financial Systems. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3).

[20] Mucsková, M. (2024). Transforming banking with artificial intelligence: Applications, challenges, and implications. *Trends Economics and Management*, *18*(42), 21-37.

[21] Balcıoğlu, Y. S. (2024). Revolutionizing risk management AI and ML innovations in financial stability and fraud detection. In *Navigating the Future of Finance in the Age of AI* (pp. 109-138). IGI Global.