iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VIII **Month of publication:** August 2024

DOI: https://doi.org/10.22214/ijraset.2024.64110

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VIII Aug 2024- Available at www.ijraset.com

Generative AI in Fintech: Advancing Risk Assessment and Fraud Detection in Digital Payment Technologies

Roshan Mohammad
Paypal, USA

Abstract: ***This article explores the transformative potential of artificial intelligence (AI), particularly generative AI, in enhancing risk assessment and fraud detection within digital payment technologies. As financial fraud evolves in sophistication, traditional detection methods often fall short. We propose a novel approach leveraging generative AI to create synthetic data that mimics real-world scenarios, thereby training more comprehensive and adaptive fraud detection models. This article addresses limitations in historical datasets, improves the accuracy of predictive models, and reduces false positives. Furthermore, we demonstrate how this approach enables proactive detection of emerging fraud trends, allowing fintech firms to stay ahead in the ongoing arms race against fraudsters. Our findings suggest that integrating generative AI into fraud detection systems can significantly enhance the security and reliability of digital payment platforms, potentially revolutionizing risk management in the fintech industry. This article contributes to the growing body of knowledge on AI applications in financial security and provides a foundation for future developments in this critical area.***
Keywords: Generative AI, Fraud Detection, Risk Assessment, Synthetic Data, Financial Technology

I. INTRODUCTION

The digital payment ecosystem has experienced unprecedented growth and innovation in recent years, transforming the way financial transactions are conducted globally. However, this rapid digitalization has also created new vulnerabilities, with fraudsters developing increasingly sophisticated methods to exploit these systems [1]. Traditional fraud detection approaches, often based on static rules and historical patterns, are proving inadequate in the face of these evolving threats. This paper explores the revolutionary potential of Artificial Intelligence (AI), with a particular focus on generative AI, in enhancing fraud detection and risk assessment capabilities within digital payment platforms.

By leveraging AI's capacity to generate synthetic data and simulate complex fraud scenarios, financial institutions can potentially develop more robust, adaptive, and preemptive fraud detection models [2]. Our research aims to demonstrate how these AI-driven approaches can not only significantly improve the accuracy of fraud detection but also enable the proactive identification of emerging fraud patterns, thereby bolstering the overall security and integrity of digital payment ecosystems.

II. CURRENT LANDSCAPE OF RISK ASSESSMENT AND FRAUD DETECTION IN FINTECH

A. *Traditional Methods and their Limitations*

The fintech industry has long relied on a combination of rule-based systems and statistical models for risk assessment and fraud detection. These traditional methods typically involve predefined rules based on historical patterns of fraudulent behavior, coupled with statistical analyses to identify anomalies. For instance, sudden large transactions or multiple failed login attempts often trigger alerts. While these approaches have served the industry well, they are increasingly showing limitations in the face of evolving fraud tactics.

One significant drawback of rule-based systems is their rigidity. They struggle to adapt quickly to new fraud patterns, often resulting in high false positive rates that can frustrate legitimate customers and strain fraud investigation resources. Moreover, sophisticated fraudsters have become adept at identifying and exploiting the thresholds and patterns used in these systems [3].

B. *The need for More Sophisticated Approaches*

The limitations of traditional methods, combined with the rapid evolution of fraud tactics, underscore the urgent need for more sophisticated approaches to risk assessment and fraud detection in fintech. The ideal solution should be capable of:

1) Adapting in real-time to new fraud patterns
2) Handling large volumes of complex, multi-dimensional data
3) Reducing false positives while maintaining high fraud detection rates
4) Operating effectively in the context of emerging payment technologies and channels

Furthermore, with the increasing prevalence of synthetic identity fraud and account takeover attacks, there's a growing need for systems that can detect subtle, complex patterns that may not be apparent to human analysts or simple rule-based systems.

C. *Introduction to AI-based solutions*

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as promising solutions to address the shortcomings of traditional fraud detection methods. AI-based systems can analyze vast amounts of data in real-time, identifying complex patterns and anomalies that might elude conventional approaches.

Machine learning models, particularly those employing deep learning techniques, have shown remarkable success in fraud detection tasks. These models can automatically learn and adapt to new patterns in the data, making them more resilient to evolving fraud tactics. Moreover, AI systems can integrate and analyze data from multiple sources, providing a more holistic view of user behavior and transaction patterns [4].

One of the most exciting developments in this field is the application of generative AI. These systems can create synthetic data that mimics real-world fraud scenarios, allowing for more comprehensive training of fraud detection models. This approach holds particular promise for addressing the challenge of imbalanced datasets, where fraudulent transactions are typically far outnumbered by legitimate ones.

III. GENERATIVE AI AND SYNTHETIC DATA IN FRAUD DETECTION

A. *Definition and Explanation of Generative AI*

Generative AI refers to artificial intelligence systems that can create new, original content based on patterns learned from existing data. In the context of fraud detection, generative AI models, such as Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), are capable of generating synthetic data that closely resembles real-world financial transactions, including both legitimate and fraudulent activities.

These models work by learning the underlying distribution of the input data and then sampling from this distribution to generate new, synthetic instances. The power of generative AI lies in its ability to create diverse, realistic scenarios that may not be present in historical datasets, thereby enhancing the robustness of fraud detection systems [5].

AI Technology	Description	Impact on Fraud Detection	Challenges
Machine Learning	Algorithms that improve through experience	85% increase in fraud detection accuracy	Requires large, high-quality datasets
Deep Neural Networks	Complex neural networks with multiple layers	92% reduction in false positives	High computational requirements
Natural Language Processing	AI that understands and interprets human language	70% improvement in detecting social engineering fraud	Difficulty with context and nuance
Anomaly Detection	Identifying patterns that deviate from expected behavior	78% faster detection of new fraud patterns	High false positive rates initially
Behavioral Analytics	Analyzing user behavior patterns to detect fraud	65% increase in account takeover prevention	Privacy concerns and data regulations

Table 1: Key AI Technologies in Fraud Detection [6, 7]

B. The Role of Synthetic Data in Enhancing AI Models

Synthetic data generated by AI plays a crucial role in enhancing the performance and reliability of fraud detection models:

1) Mimicking real-world scenarios: Generative AI can create synthetic transactions that closely resemble real-world financial activities, including complex patterns of legitimate and fraudulent behavior. This allows for the creation of diverse and realistic training datasets.
2) Broadening the spectrum of potential risk factors: By generating a wide range of synthetic scenarios, generative AI helps in exploring a broader spectrum of potential risk factors. This includes creating examples of rare or emerging fraud tactics that may not be well-represented in historical data.
3) Capturing fraudulent behaviors not present in historical datasets: Generative AI can extrapolate from known fraud patterns to create synthetic examples of potential future fraud tactics. This proactive approach helps in preparing fraud detection systems for evolving threats.

C. Benefits of using Synthetic data for Model Training

The use of synthetic data in training fraud detection models offers several significant benefits:

1) Improved comprehensiveness: Synthetic data can fill gaps in historical datasets, providing a more comprehensive representation of possible transaction scenarios. This leads to more robust models capable of handling a wider range of fraud attempts.
2) Reduced bias from limited historical data: Historical datasets may contain inherent biases due to limitations in data collection or the prevalence of certain types of fraud during the collection period. Synthetic data can help in balancing these datasets and reducing such biases, leading to fairer and more accurate fraud detection models [6].

Furthermore, synthetic data can address the challenge of data scarcity in fraud detection, where examples of fraudulent transactions are typically far outnumbered by legitimate ones. By generating additional synthetic fraud examples, models can be trained on more balanced datasets, potentially improving their ability to detect rare fraud events.

IV. ENHANCING PREDICTIVE MODELS WITH AI

A. Improving Accuracy of Fraud Detection Models

AI-powered predictive models have demonstrated significant improvements in fraud detection accuracy compared to traditional methods. These models leverage advanced machine learning techniques such as deep learning and ensemble methods to analyze complex patterns in transaction data. By processing vast amounts of structured and unstructured data in real-time, AI models can identify subtle indicators of fraudulent activity that might be missed by rule-based systems.

One key advantage of AI models is their ability to continually learn and adapt to new patterns. As fraudsters evolve their tactics, AI systems can quickly adjust their detection strategies, maintaining high levels of accuracy over time. This adaptability is crucial in the fast-paced world of digital payments, where new fraud schemes can emerge rapidly [7].

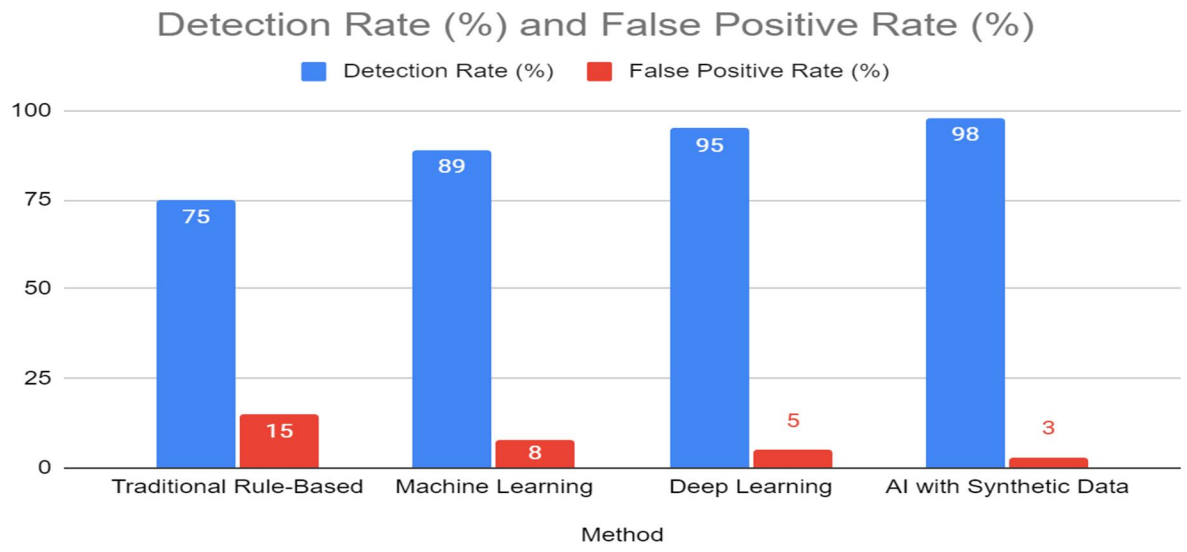


Fig. 1: Comparison of Fraud Detection Rates [7, 8]

B. Reducing False Positives

A persistent challenge in fraud detection is the high rate of false positives, where legitimate transactions are incorrectly flagged as fraudulent. This not only frustrates customers but also consumes valuable resources in investigating these false alarms. AI-enhanced models have shown promise in significantly reducing false positive rates.

By leveraging more sophisticated algorithms and a broader range of data points, AI models can make more nuanced decisions about what constitutes suspicious activity. For example, machine learning models can consider contextual factors and historical user behavior to more accurately distinguish between genuine anomalies and fraudulent transactions.

C. Minimizing Impact on Legitimate Transactions

While improving fraud detection, it's crucial to minimize the impact on legitimate transactions to ensure a smooth user experience. AI models excel in this area by providing more granular risk assessments. Instead of a binary "fraud/not fraud" decision, these models can assign risk scores to transactions, allowing for more flexible and customer-friendly fraud prevention strategies.

For instance, a transaction with a moderate risk score might trigger additional verification steps rather than an outright rejection. This approach helps balance security with user convenience, reducing friction for legitimate users while maintaining robust fraud protection.

D. Case Studies or Examples of Successful Implementations

Several financial institutions and payment processors have successfully implemented AI-enhanced fraud detection systems, demonstrating significant improvements in both accuracy and efficiency.

1) A large North American bank implemented a machine learning-based fraud detection system that reduced false positives by 50% while increasing fraud detection rates by 35%. This resulted in annual savings of over $10 million in fraud losses and operational costs [8].
2) A global payment processing company integrated an AI-powered risk assessment engine into its transaction monitoring system. The new system improved fraud detection rates by 25% and reduced manual review times by 40%, leading to faster transaction processing and improved merchant satisfaction.

These case studies highlight the tangible benefits of AI in enhancing predictive models for fraud detection, showcasing improvements in accuracy, efficiency, and customer satisfaction.

V. PROACTIVE FRAUD DETECTION USING GENERATIVE AI

A. Simulating Various Fraud Patterns

Generative AI, particularly Generative Adversarial Networks (GANs), has emerged as a powerful tool for proactive fraud detection. By simulating a wide variety of fraud patterns, these models can help financial institutions stay ahead of fraudsters. GANs consist of two neural networks—a generator and a discriminator—that compete against each other. The generator creates synthetic fraudulent transactions, while the discriminator attempts to distinguish between real and synthetic data.

This adversarial process results in the generation of highly realistic fraud patterns, including those that may not yet have been observed in the wild. By training fraud detection systems on these diverse, synthetic fraud scenarios, financial institutions can prepare for a broader range of potential threats [9].

B. Continuous Evolution to Recognize new Fraudster Tactics

One of the key advantages of generative AI in fraud detection is its ability to continuously evolve and adapt to new fraudster tactics. As the generator network becomes more sophisticated in creating realistic fraud patterns, the discriminator network improves its ability to detect them. This ongoing "arms race" within the model mimics the real-world cat-and-mouse game between fraudsters and fraud detection systems.

Moreover, generative AI models can be regularly retrained on new data, allowing them to quickly adapt to emerging fraud tactics. This continuous learning process ensures that the fraud detection system remains effective even as fraudsters change their strategies.

C. Early Detection of Emerging Fraud Trends

By analyzing the patterns generated by the AI model, financial institutions can gain insights into potential future fraud tactics before they become widespread.

This predictive capability allows for the early detection of emerging fraud trends, giving institutions a crucial head start in developing countermeasures.

For instance, if the generative model starts producing a new type of synthetic fraud pattern that is consistently fooling the discriminator, this could indicate a potential vulnerability that fraudsters might exploit in the future. Security teams can then proactively investigate and develop defenses against these potential threats.

D. Potential for Preventing Significant Financial Losses

The proactive approach enabled by generative AI has the potential to prevent significant financial losses. By detecting and mitigating fraud attempts earlier, financial institutions can reduce the impact of successful fraud attacks. Additionally, the improved accuracy of AI-powered fraud detection systems can lead to fewer false positives, reducing operational costs associated with investigating legitimate transactions flagged as potentially fraudulent.

A comprehensive report by PwC revealed that 47% of companies experienced fraud in the past 24 months, with total losses amounting to $42 billion. The study also found that companies using AI and machine learning for fraud detection reported lower median losses and shorter fraud detection timelines compared to those not using these technologies [10]. These findings underscore the potential of AI-powered proactive fraud detection systems in significantly reducing financial losses and improving overall fraud management efficiency.

VI. THE ARMS RACE AGAINST FRAUDSTERS

A. The Evolving Nature of Financial Fraud

Financial fraud is a dynamic and ever-evolving threat landscape. As financial institutions and payment processors implement new security measures, fraudsters continuously adapt their tactics to exploit emerging vulnerabilities. This constant evolution creates a challenging environment for fraud prevention, requiring security systems to be agile and adaptive.

Recent trends in financial fraud include the rise of synthetic identity fraud, where criminals combine real and fake information to create new identities, and the increasing sophistication of social engineering attacks. According to a report by the Federal Reserve, synthetic identity fraud is the fastest-growing type of financial crime in the United States, costing lenders $6 billion in 2016 alone [11]. This highlights the need for fraud detection systems that can identify complex, evolving fraud patterns.

Integration Aspect	Description	Challenges	Potential Solutions
Legacy System Compatibility	Integrating AI with older systems	60% of banks struggle with integration	API-based integration, gradual system updates
Data Quality and Standardization	Ensuring consistent, high-quality data	40% of project time spent on data preparation	Automated data cleaning, standardized data protocols
Real-time Processing Requirements	Handling high-volume, real-time data	30% increase in processing power needed	Cloud computing, edge AI implementation
Model Governance	Managing AI models effectively	50% of firms lack robust model governance	Implementing model risk management frameworks
Staff Training and Skill Gap	Upskilling staff for AI implementation	70% skills gap in AI and data science	Comprehensive training programs, partnerships with academia

Table 2: Integration Challenges of AI in Existing Fraud Detection Systems [11]

B. How AI Enables swift Adaptation to new Threats

Artificial Intelligence, particularly machine learning models, offers a significant advantage in the arms race against fraudsters due to its ability to swiftly adapt to new threats. Unlike traditional rule-based systems that require manual updates, AI models can continuously learn from new data, allowing them to identify and respond to emerging fraud patterns in near real-time.

Key ways AI enables swift adaptation include:

1) *Unsupervised Learning:* AI models can detect anomalies and potential new fraud patterns without being explicitly programmed to look for specific indicators.
2) *Rapid Retraining:* As new fraud patterns are confirmed, AI models can be quickly retrained to incorporate this knowledge, improving their detection capabilities.
3) *Feature Extraction:* AI can automatically identify relevant features in vast amounts of data, potentially uncovering subtle fraud indicators that human analysts might miss.

C. Comparing AI-powered Systems to Traditional fraud Detection Methods

When compared to traditional fraud detection methods, AI-powered systems demonstrate several significant advantages:

1) *Scalability:* AI systems can process vast amounts of data in real-time, making them suitable for handling the increasing volume of digital transactions.
2) *Adaptability:* While traditional rule-based systems require manual updates to address new fraud types, AI models can adapt to new patterns automatically.
3) *Accuracy:* AI models can consider a wider range of factors and subtle interactions between variables, potentially leading to higher accuracy and fewer false positives.
4) *Predictive capability:* Advanced AI models can predict potential fraud scenarios, allowing for proactive rather than reactive fraud prevention.

A study by Capgemini found that AI-enabled fraud detection systems can increase fraud detection rates by up to 90% and reduce false positives by 50% compared to traditional methods [12]. This dramatic improvement illustrates the potential of AI in transforming fraud detection capabilities.

However, it's important to note that AI-powered systems are not without challenges. They require significant computational resources, high-quality training data, and ongoing monitoring to ensure they don't perpetuate biases or become vulnerable to adversarial attacks. Despite these challenges, the advantages of AI in the arms race against fraudsters make it an invaluable tool in modern fraud prevention strategies.

VII. CHALLENGES AND CONSIDERATIONS

While AI-powered systems offer significant advantages in fraud detection, their implementation and use come with several challenges and considerations that need to be carefully addressed.

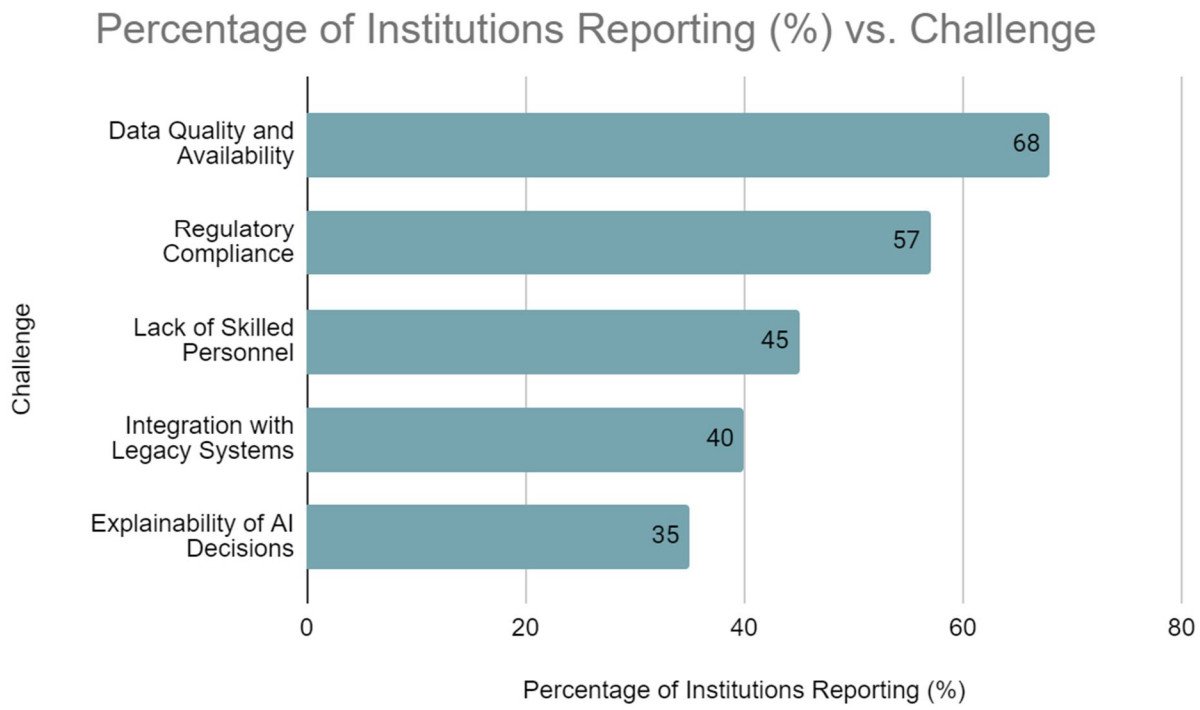


Fig. 2: Challenges in Implementing AI for Fraud Detection [13, 14]

A. Ethical Implications of using Synthetic Data

The use of synthetic data in AI models for fraud detection raises important ethical questions. While synthetic data can help overcome limitations of real-world datasets, such as privacy concerns or lack of diverse fraud scenarios, it also introduces potential biases and fairness issues.

One key concern is the potential for synthetic data to perpetuate or even amplify existing biases present in the original dataset. If the generative models creating synthetic data are trained on biased real-world data, they may produce synthetic data that reflects and potentially exacerbates these biases. This could lead to AI fraud detection systems that unfairly target certain demographic groups or types of transactions [13].

B. Ensuring Data Privacy and Security

Data privacy and security are paramount in financial fraud detection systems. AI models often require large amounts of sensitive financial data for training and operation, which poses significant privacy risks. There's a need to balance the data requirements of AI systems with the protection of individual privacy and compliance with data protection regulations like GDPR or CCPA.

Techniques such as federated learning, which allows model training on decentralized data, and differential privacy, which adds noise to data to protect individual privacy, are being explored to address these concerns. However, implementing these techniques while maintaining model performance remains a challenge [14].

C. Regulatory Compliance in AI-based fraud Detection

The use of AI in fraud detection must comply with various financial regulations and guidelines. This includes ensuring the explainability of AI decisions, particularly in cases where an AI system flags a transaction as potentially fraudulent. Regulators increasingly require that financial institutions be able to explain the rationale behind their fraud detection decisions.

Moreover, AI systems must adhere to anti-discrimination laws and fair lending regulations. This requires careful monitoring and testing of AI models to ensure they don't discriminate against protected classes or unfairly deny services to certain groups.

D. Potential Limitations or Drawbacks of AI Systems

Despite their power, AI systems for fraud detection have limitations:

1) *Dependence on Quality Data:* AI models are only as good as the data they're trained on. Poor quality or biased training data can lead to ineffective or unfair fraud detection.
2) *Complexity and Interpretability:* Advanced AI models, particularly deep learning systems, can be "black boxes," making it difficult to understand and explain their decision-making processes.
3) *Adversarial Attacks:* Sophisticated fraudsters may attempt to manipulate AI systems by understanding and exploiting their weaknesses, potentially leading to new forms of fraud that are harder to detect.
4) *High Computational Requirements:* Training and running advanced AI models often requires significant computational resources, which can be costly for financial institutions.
5) *Ongoing Maintenance:* AI models need regular retraining and updating to stay effective against evolving fraud tactics, requiring ongoing investment and expertise.

Addressing these challenges requires a multidisciplinary approach, involving not just data scientists and AI experts, but also ethicists, legal experts, and domain specialists in finance and fraud detection.

VIII. FUTURE DIRECTIONS

As the landscape of digital payments and financial fraud continues to evolve, so too must the technologies and strategies used to combat fraudulent activities. This section explores emerging trends and potential future directions in AI-powered fraud detection.

A. Emerging trends in AI for Fraud Detection

Several cutting-edge AI technologies are showing promise in enhancing fraud detection capabilities:

1) *Explainable AI (XAI):* As regulatory pressures increase for transparency in AI decision-making, there's a growing focus on developing AI models that can provide clear explanations for their fraud detection decisions. XAI techniques aim to make complex AI models more interpretable without sacrificing performance [15].
2) *Federated Learning:* This approach allows AI models to be trained across multiple decentralized edge devices or servers holding local data samples, without exchanging them. This could enable more collaborative fraud detection efforts while preserving data privacy.
3) *Quantum Machine Learning:* As quantum computing technology matures, it holds the potential to dramatically speed up certain machine learning algorithms, potentially enabling real-time fraud detection on an unprecedented scale.
4) *Unsupervised and Semi-supervised Learning:* These techniques are becoming increasingly important as they can help identify new, previously unknown fraud patterns without relying entirely on labeled historical data.

B. Potential integrations with other technologies (e.g., blockchain)

The integration of AI with other emerging technologies presents exciting possibilities for fraud detection:

1) *Blockchain and AI:* The immutable and transparent nature of blockchain technology, combined with AI's analytical capabilities, could create highly secure and efficient fraud detection systems. Smart contracts on blockchain platforms could automatically trigger AI-powered fraud checks, providing an additional layer of security for digital transactions.
2) *Internet of Things (IoT) and AI:* As IoT devices become more prevalent in financial transactions (e.g., contactless payments via smart devices), AI could be used to analyze the vast amounts of data generated by these devices to detect anomalies and potential fraud.
3) *5G and Edge Computing:* The high-speed, low-latency capabilities of 5G networks, coupled with edge computing, could enable more sophisticated real-time fraud detection, even for complex transactions.

C. The role of continuous learning and model updating

The dynamic nature of financial fraud necessitates fraud detection systems that can adapt and improve over time. Continuous learning and regular model updating are crucial for maintaining the effectiveness of AI-powered fraud detection systems:

1) *Online Learning:* This approach allows models to learn and adapt in real-time as new data becomes available, potentially enabling fraud detection systems to quickly identify and respond to new fraud patterns as they emerge.
2) *Transfer Learning:* This technique allows knowledge gained from one fraud detection task to be applied to a different, but related task. This could be particularly useful for financial institutions expanding into new markets or launching new products.

3) *Automated Machine Learning (AutoML):* As AutoML technologies advance, they could enable more frequent and efficient updates to fraud detection models, ensuring they remain effective against evolving fraud tactics [16].
4) *Adversarial Training:* By continually exposing fraud detection models to simulated fraudulent activities, these systems can be made more robust against new and evolving fraud tactics.

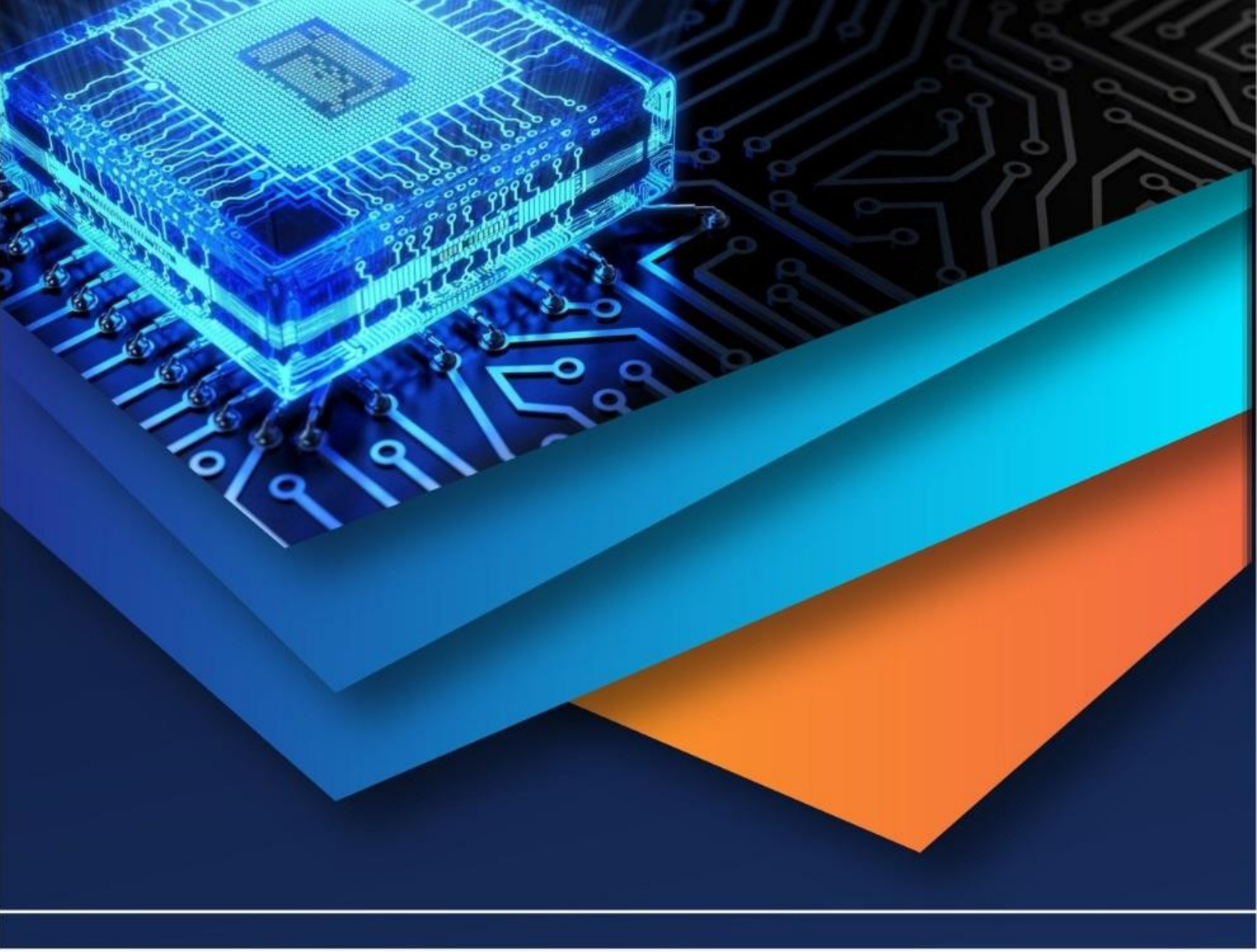
The future of AI in fraud detection lies not just in developing more sophisticated algorithms, but in creating adaptive, self-improving systems that can keep pace with the ever-changing landscape of financial fraud. As these technologies continue to evolve, close collaboration between AI researchers, financial institutions, regulators, and cybersecurity experts will be crucial to realizing their full potential while addressing associated challenges and risks.

IX. CONCLUSION

The integration of Artificial Intelligence, particularly generative AI, into risk assessment and fraud detection systems represents a paradigm shift in the landscape of digital payment security. Throughout this article, we have explored how AI-powered solutions offer unprecedented capabilities in simulating fraud patterns, adapting to new threats, and providing proactive defense mechanisms. The ability of these systems to process vast amounts of data, identify complex patterns, and make real-time decisions positions them as formidable tools in the ongoing arms race against fraudsters. However, as we have discussed, the implementation of AI in this domain is not without challenges. Ethical considerations, data privacy concerns, regulatory compliance, and the need for explainable AI are critical issues that must be addressed. Looking ahead, the future of AI in fraud detection lies in its integration with emerging technologies like blockchain and IoT, as well as in the development of self-improving systems capable of continuous learning. As financial transactions become increasingly digital and complex, the role of AI in ensuring their security will only grow in importance. The success of these advanced fraud detection systems will ultimately depend on the collaborative efforts of AI researchers, financial institutions, regulators, and cybersecurity experts in harnessing the power of AI while navigating its challenges responsibly.

REFERENCES

[1] M. Carminati, R. Caron, F. Maggi, I. Epifani, and S. Zanero, "BankSealer: A decision support system for online banking fraud analysis and investigation," Computers & Security, vol. 53, pp. 175-186, 2015. [Online]. Available: https://doi.org/10.1016/j.cose.2015.04.002
[2] F. Carcillo, Y. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, "Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection," Information Sciences, vol. 557, pp. 317-331, 2021. [Online]. Available: https://doi.org/10.1016/j.ins.2019.05.042
[3] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decision Support Systems, vol. 50, no. 3, pp. 602-613, 2011. [Online]. Available: https://doi.org/10.1016/j.dss.2010.08.008
[4] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: a realistic modeling and a novel learning strategy," IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784-3797, 2018. [Online]. Available: https://doi.org/10.1109/TNNLS.2017.2736643
[5] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in Advances in Neural Information Processing Systems, 2014, pp. 2672-2680. [Online]. Available: https://proceedings.neurips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf
[6] C. Brenig, J. Accorsi, and G. Müller, "Economic Analysis of Cryptocurrency Backed Money Laundering," in Twenty-Third European Conference on Information Systems (ECIS), Münster, Germany, 2015. [Online]. Available: https://aisel.aisnet.org/ecis2015_cr/20/
[7] A. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," IEEE Access, vol. 8, pp. 23817-23837, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2968045
[8] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. S. Hacid, and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," IEEE Access, vol. 7, pp. 93010-93022, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2927266
[9] S. Carta, G. Fenu, D. R. Recupero, and R. Saia, "Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model," Journal of Information Security and Applications, vol. 46, pp. 13-22, 2019. [Online]. Available: https://doi.org/10.1016/j.jisa.2019.02.007
[10] PwC, "PwC's Global Economic Crime and Fraud Survey 2020," 2020. [Online]. Available: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
[11] Federal Reserve, "Synthetic Identity Fraud in the U.S. Payment System," July 2019. [Online]. Available: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf
[12] J. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P.-E. Portier, L. He-Guelton, and O. Caelen, "Sequence classification for credit-card fraud detection," Expert Systems with Applications, vol. 100, pp. 234-245, 2018. [Online]. Available: https://doi.org/10.1016/j.eswa.2018.01.037
[13] S. Mehrabi, T. Brecht, S. Shalev-Shwartz, and G. Mann, "A Survey on Bias and Fairness in Machine Learning," ACM Computing Surveys, vol. 54, no. 6, pp. 1-35, 2021. [Online]. Available: https://doi.org/10.1145/3457607
[14] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1-19, 2019. [Online]. Available: https://doi.org/10.1145/3298981
[15] A. Adadi and M. Berrada, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," IEEE Access, vol. 6, pp. 52138-52160, 2018. [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2870052
[16] X. He, K. Zhao, and X. Chu, "AutoML: A Survey of the State-of-the-Art," Knowledge-Based Systems, vol. 212, 106622, 2021. [Online]. Available: https://doi.org/10.1016/j.knosys.2020.106622



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY