

## **literature Review : AI-Based Real-Time Fraud Detection in Digital Service Requests” How can organization activate AI to mitigate fraud**

Table of contents:

- Summary research paper's
- Critical Analysis:
- Connections
- Conflicts between the findings
- Synthesis Matrix for Literature Review
- References

---

## Summarized Research Papers

### 1. Bendhi, 2025

- **Summary Research Paper:** This study investigates real-time fraud detection in digital financial transactions using various AI techniques. It specifically highlights the effectiveness of Long Short-Term Memory (LSTM) networks. The research reports that LSTM achieved high performance metrics (precision 0.96, recall 0.94, F1 score 0.95, AUC 0.98) with very low latency (85 milliseconds) and a significant reduction in false positives (from 3.7% to 0.8%) compared to traditional systems. The implementation was in a real-time operational setting using a public credit card dataset.
- **Critical Analysis:** The paper presents strong quantitative evidence for the superiority of LSTM in this context, demonstrating clear improvements in accuracy and efficiency. The use of a public dataset enhances reproducibility, but its generalizability to diverse proprietary financial data could be further explored. The study's focus on a single type of digital financial transaction (credit cards) might limit its direct applicability to other digital services. While it highlights reduced false positives, the specific mechanisms within LSTM contributing to this reduction could be elaborated.
- **Connections:** This paper strongly supports the overall theme that AI/ML methods outperform traditional rule-based systems in fraud detection. Its specific findings on LSTM's low latency and high accuracy connect well with the need for real-time processing emphasized across the literature. It aligns with Olowu et al. (2024) in promoting AI's effectiveness.
- **Conflicts between Findings:** No direct conflicts with other findings are apparent; rather, its results provide strong empirical backing for the broad claims made in other, more general or review-based studies.
- **References:** Bendhi, Manish Reddy. "Fraud Detection: Leveraging Artificial Intelligence to Identify Transaction Anomalies in Real-Time and Minimize False Positives." *International Journal Of Engineering And Computer Science*, 2025.

### 2. Fallah et al., 2024

- **Summary Research Paper:** This study explores the integration of artificial intelligence with blockchain technology for real-time fraud detection in financial services. Utilizing Gradient Boosting and Recurrent Neural Networks within a permissioned blockchain environment, the research demonstrates high accuracy with an error rate below 2%. A key finding is its ability to process up to 1200 transactions per second, emphasizing how AI-blockchain integration enhances security and throughput. The implementation was based on simulation experiments.

- **Critical Analysis:** The novelty of this paper lies in its exploration of AI-blockchain synergy, addressing scalability and security concurrently. The high transaction processing speed is a significant advantage. However, as it's based on simulation experiments rather than a fully deployed real-world system, the practical challenges and overheads of such an integration in a live financial environment might be underestimated. The specific details of how Gradient Boosting and RNNs are integrated with the blockchain, and the nuances of the "permissioned" aspect, could be more thoroughly detailed.
- **Connections:** This paper connects to the broader theme of real-time processing and scalability. Its focus on blockchain complements other studies that discuss real-time streaming frameworks (Tyagi et al., 2025) and highlights an alternative approach to achieving high throughput. It supports the general notion of AI enhancing security, as also mentioned by Kandregula (2019).
- **Conflicts between Findings:** While not a direct conflict, this paper's reliance on simulation and high processing speed (1200 transactions/second) sets a very high bar, which might contrast with the lower processing speeds or scalability challenges noted in other studies that focus on more traditional AI deployment environments (e.g., Pothireddy and Algubelli, 2016 which mentions scalability as a challenge).
- **References:** Fallah, M. H., Ms. G. Sheeba, Dharmapuri Siri, Himanshu Sharma, G. R. Kumar, and Dr. A. Devendran. "AI- Powered Blockchain Systems for Real-Time Fraud Detection in Financial Services." *2024 International Conference on IoT, Communication and Automation Technology (ICICAT)*, 2024.

### 3. Pothireddy and Algubelli, 2016

- **Summary Research Paper:** This paper focuses on real-time fraud detection using AI on financial streaming data, employing supervised machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and Artificial Neural Network (ANN). The study highlights high precision and minimal latency, concluding that AI methods outperform traditional rule-based systems. However, it also identifies scalability and data quality as significant challenges in practical implementation.
- **Critical Analysis:** This paper provides early empirical evidence for AI's superiority in real-time financial fraud detection. The explicit mention of scalability and data quality as challenges is crucial for a balanced view of AI deployment. However, the lack of quantified precision and latency metrics makes it difficult to directly compare its performance with other studies. The specific details on how data quality affects the models and what "minimal latency" entails are not provided.
- **Connections:** This study reinforces the overarching conclusion that AI surpasses rule-based systems. Its identification of scalability as a challenge provides a valuable counterpoint or area for further exploration compared to papers that emphasize AI's scalability. It aligns with Olowu et al. (2024) and the broader literature on AI's performance benefits.
- **Conflicts between Findings:** This paper explicitly states "scalability and data quality are challenges," which stands in contrast to studies like Fallah et al. (2024) and Prem Sai (2024) that highlight or design for high scalability. This suggests that the realization of

scalability in real-world AI systems for fraud detection can vary significantly depending on the implementation context and specific technologies used.

- **References:** Pothireddy, Nirup Kumar Reddy, and Bipinkumar Reddy Algubelli. "Real-Time Fraud Detection Using AI on Financial Streaming Data." *International Journal of Scientific Research in Science and Technology*, 2016.

#### 4. Olowu et al., 2024

- **Summary Research Paper:** This is a systematic review analyzing artificial intelligence and data science approaches in banking fraud detection, based on a meta-analysis of 47 studies. It concludes that various machine learning and deep learning algorithms, especially integrated supervised/unsupervised approaches, yield detection rates ranging from 87% to 94% and reduce false positives by 40-60% compared to rule-based systems. It emphasizes that integrated approaches are best for detecting novel fraud patterns.
- **Critical Analysis:** As a systematic review, this paper provides a valuable high-level synthesis of the field, reinforcing the general efficacy of AI. The aggregation of findings from multiple studies strengthens its conclusions on detection rates and false positive reductions. However, as it's a review, it doesn't offer specific technical implementation details or primary empirical data from a single study. The specific methodologies employed for the meta-analysis are not detailed in the abstract, which limits the ability to critically assess its synthesis process.
- **Connections:** This paper serves as a foundational agreement across the literature, confirming the general consensus that AI outperforms traditional methods. Its emphasis on integrated supervised/unsupervised approaches connects with the idea of addressing novel fraud patterns and complements papers focusing on anomaly detection.
- **Conflicts between Findings:** This paper's broad findings are generally in agreement with the individual studies it synthesizes. Any "conflicts" would likely be at a more granular level, regarding specific algorithm performance differences or implementation challenges, which a meta-analysis typically smooths out into general trends.
- **References:** Olowu, Olawale, Ademilola Olowofela Adeleye, Abraham Okandeji Omokanye, Akintayo Micheal Ajayi, Adebayo Olabode Adepoju, Olayinka Mary Omole, and Ernest C Chianumba. "AI-Driven Fraud Detection in Banking: A Systematic Review of Data Science Approaches to Enhancing Cybersecurity." *GSC Advanced Research and Reviews*, 2024.

#### 5. Tyagi et al., 2025

- **Summary Research Paper:** This study explores the role of artificial intelligence in risk management and fraud detection, specifically highlighting the use of Autoencoders, Isolation Forests, and statistical methods for anomaly detection. It emphasizes the integration of these techniques with real-time frameworks like Kafka and Spark for high-dimensional transaction data. A key finding is the effectiveness of anomaly detection for new fraud types and integration with real-time frameworks, but it also notes scalability and regulatory compliance as significant deployment challenges.

- **Critical Analysis:** The paper's focus on anomaly detection for novel fraud types is important, addressing a key limitation of rule-based systems. The mention of specific real-time frameworks (Kafka, Spark) adds practical value. However, the study does not quantify performance metrics, making it difficult to assess the exact impact of its proposed methods. The challenges of "scalability and regulatory compliance" are identified but not explored in depth, leaving questions about their specific nature and potential solutions.
- **Connections:** This paper strongly connects with the theme of detecting novel fraud patterns and the importance of real-time processing frameworks. Its identification of scalability and regulatory compliance as challenges aligns with Pothireddy and Algubelli (2016) and supports the "Summary of Conflicts" in the original content, providing specific examples of these ongoing issues.
- **Conflicts between Findings:** Similar to Pothireddy and Algubelli (2016), this paper identifies scalability as a "deployment challenge," which conflicts with the implied or stated ease of scalability in systems like Fallah et al. (2024) or Prem Sai (2024). This highlights a nuanced reality of AI system deployment where theoretical scalability doesn't always translate smoothly into practice due to integration complexities and regulatory hurdles.
- **References:** Tyagi, Swati, Anuj Tyagi, Dr. S. Rani, A. Suraj Kumar, Dr. Sunil Adhav, and Dr. Sumeet Gupta. "The Role of Artificial Intelligence in Risk Management and Fraud Detection in Financial Services." *Journal of Informatics Education and Research*, 2025.

#### 6. Kandregula, 2019

- **Summary Research Paper:** This paper discusses leveraging artificial intelligence for real-time fraud detection in financial transactions from a FinTech perspective. It broadly mentions machine learning, deep learning, and natural language processing (NLP) as methods. The key findings include that AI reduces false positives/negatives, increases reliability, and reduces manual costs. It also notes that NLP adds security through sentiment/entity analysis.
- **Critical Analysis:** This paper provides a high-level overview of AI's benefits in FinTech fraud detection, particularly introducing NLP as a method, which is unique among the selected papers. However, it lacks specific algorithmic details, implementation context, and quantifiable performance metrics. The claims about reduced costs and increased reliability are qualitative and lack empirical backing within the paper's summary. This makes it more of a conceptual or review-oriented piece than an empirical study.
- **Connections:** This paper contributes to the general consensus about AI's ability to reduce false positives/negatives and improve reliability. Its mention of NLP introduces a new dimension to AI methods for fraud detection, potentially opening avenues for richer data analysis beyond numerical transactions. It broadly supports the positive outcomes of AI mentioned in Olowu et al. (2024).
- **Conflicts between Findings:** There are no direct conflicts with other papers, but its lack of detailed quantification or specific implementation context makes it less comparable in terms of performance metrics than other empirical studies (e.g., Bendhi, 2025). Its contribution is more in introducing a broader scope of AI applications (like NLP).

- **References:** Kandregula, Narendra. "Leveraging Artificial Intelligence for Real-Time Fraud Detection in Financial Transactions: A Fintech Perspective." *World Journal of Advanced Research and Reviews*, 2019.
- 

### Connections

The selected papers collectively demonstrate a strong consensus on the effectiveness of AI/ML in surpassing traditional rule-based systems for real-time fraud detection in digital financial services (Bendhi, 2025; Pothireddy and Algubelli, 2016; Olowu et al., 2024). Specifically, there's a recurring theme of AI leading to significant reductions in false positives and improved overall accuracy (Bendhi, 2025; Olowu et al., 2024; Kandregula, 2019). The emphasis on **real-time processing** is central across all chosen studies, with various architectural solutions proposed, from specific streaming frameworks like Kafka/Spark (Tyagi et al., 2025) to novel blockchain integrations (Fallah et al., 2024). The importance of **advanced AI techniques** like deep learning (LSTM in Bendhi, 2025; RNNs in Fallah et al., 2024) and ensemble/integrated supervised/unsupervised methods (Olowu et al., 2024; Tyagi et al., 2025) is consistently highlighted for their superior performance and ability to detect novel fraud patterns. Furthermore, several papers touch upon the broader benefits beyond just detection rates, such as enhanced security (Fallah et al., 2024; Kandregula, 2019) and operational efficiency.

### Conflicts between the Findings

While there is a general agreement on AI's benefits, a notable conflict arises concerning **scalability and implementation ease**. Pothireddy and Algubelli (2016) and Tyagi et al. (2025) explicitly identify **scalability as a significant challenge** and a deployment hurdle, respectively, often citing integration with legacy systems and regulatory compliance as barriers. In contrast, Fallah et al. (2024) present a highly optimistic view of scalability with their AI-blockchain integration, boasting 1200 transactions per second. Prem Sai (2024), though not explicitly summarized here, is also noted in the original content as "designed for scalability," and Kandregula (2019) claims ML/DL/NLP improve scalability. This divergence suggests that while AI *can* be scalable, achieving it in real-world, complex financial environments poses considerable practical difficulties that are not uniformly addressed or overcome across all implementations. Additionally, there's a variation in the **level of quantitative reporting**: some studies provide detailed performance metrics (Bendhi, 2025; Fallah et al., 2024), while others make qualitative claims about accuracy or efficiency without specific numbers (Pothireddy and Algubelli, 2016; Tyagi et al., 2025; Kandregula, 2019). This lack of consistent quantification makes direct, granular comparisons between methodologies challenging and points to a potential gap in standardized reporting.

### Synthesis Matrix for Literature Review

|                          |                                                               |                                      |                                             |                                                   |                                                                          |                                           |
|--------------------------|---------------------------------------------------------------|--------------------------------------|---------------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------|
| Theme/Paper              | Bendhi, 2025 (LSTM)                                           | Fallah et al., 2024 (AI-Blockchain ) | Pothireddy & Algubelli, 2016 (RF, SVM, ANN) | Olowu et al., 2024 (Systematic Review)            | Tyagi et al., 2025 (Autoencoders, IF)                                    | Kandregula, 2019 (ML, DL, NLP)            |
| AI/ML Methods            | LSTM, RF, Isolation Forest, Autoencoders, DT, NN, RNN, hybrid | Gradient Boosting, RNN               | Random Forest, SVM, ANN (supervised )       | Various ML/DL, integrated supervised/unsupervised | Autoencoders, Isolation Forests, statistical methods (anomaly detection) | ML, DL, NLP                               |
| Real-time Processing     | Yes (85ms latency)                                            | Yes (1200 TPS, blockchain )          | Yes (minimal latency)                       | Yes (consistent need for real-time)               | Yes (Kafka, Spark frameworks)                                            | Yes (FinTech context, real-time analysis) |
| Detection Accuracy       | High (P 0.96, R 0.94, F1 0.95, AUC 0.98)                      | High (error <2%)                     | High precision (not quantified)             | High (87-94% detection rate)                      | Focus on high accuracy (not quantified)                                  | Improved accuracy (not quantified)        |
| False Positive Reduction | Yes (from 3.7% to 0.8%)                                       | Yes (implied by low error rate)      | Yes (AI outperforms rule-based)             | Yes (40-60% reduction)                            | Focus on minimizing false alarms (not quantified)                        | Yes (reduces false positives/negatives)   |

|                        |                                                                                        |                                                                              |                                                                         |                                                                                   |                                                                          |                                                                         |
|------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Theme/Paper            | Bendhi, 2025 (LSTM)                                                                    | Fallah et al., 2024 (AI-Blockchain )                                         | Pothireddy & Algubelli, 2016 (RF, SVM, ANN)                             | Olowu et al., 2024 (Systematic Review)                                            | Tyagi et al., 2025 (Autoencoders, IF)                                    | Kandregula, 2019 (ML, DL, NLP)                                          |
| Scalability            | No mention found                                                                       | Scalable (permissioned blockchain )                                          | Challenge                                                               | Key consideration for real-time systems                                           | Deployment challenge                                                     | Improves scalability (ML/DL/NLP)                                        |
| Key Contributions      | Strong empirical evidence for LSTM; quantified performance ; false positive reduction. | AI-blockchain integration ; high throughput; enhanced security (simulated) . | Early validation of AI; identifies scalability/data quality challenges. | Comprehensive review; meta-analysis confirming AI superiority for novel patterns. | Anomaly detection for new fraud types; specific real-time frameworks.    | Broad benefits of AI in FinTech; introduces NLP for security/sentiment. |
| Limitations/Challenges | Generalizability of public dataset; details of LSTM contribution                       | Simulation-based; real-world deployment challenges                           | Lack of quantified metrics; scalability/data quality challenges.        | Meta-analysis nature (no primary data/implementation specifics).                  | No quantified performance; scalability/regulatory compliance challenges. | Lack of quantitative data; broad conceptual claims without empirical    |

|                |                                      |                                      |                                                     |                                        |                                                          |                                           |
|----------------|--------------------------------------|--------------------------------------|-----------------------------------------------------|----------------------------------------|----------------------------------------------------------|-------------------------------------------|
| Theme/Paper    | Bendhi, 2025 (LSTM)                  | Fallah et al., 2024 (AI-Blockchain ) | Pothireddy & Algubelli, 2016 (RF, SVM, ANN)         | Olowu et al., 2024 (Systematic Review) | Tyagi et al., 2025 (Autoencoders, IF)                    | Kandregula, 2019 (ML, DL, NLP)            |
|                | to FPR.                              | not fully explored.                  |                                                     |                                        |                                                          | backing.                                  |
| Unique Aspects | Detailed LSTM performance for fraud. | Blockchain integration .             | Early clear identification of practical challenges. | Meta-analysis across 47 studies.       | Focus on anomaly detection with specific streaming tech. | Introduction of NLP; FinTech perspective. |

## References

- Abikoye, B., Akinwunmi, T., Adelaja, A., Umeorah, S. C., & Ogunsuji, Y. M. (2024). Real-Time Financial Monitoring Systems: Enhancing Risk Management Through Continuous Oversight. *GSC Advanced Research and Reviews*.
- Bendhi, M. R. (2025). Fraud Detection: Leveraging Artificial Intelligence to Identify Transaction Anomalies in Real-Time and Minimize False Positives. *International Journal Of Engineering And Computer Science*.
- Fallah, M. H., Sheeba, G., Siri, D., Sharma, H., Kumar, G. R., & Devendran, A. (2024). AI- Powered Blockchain Systems for Real-Time Fraud Detection in Financial Services. *2024 International Conference on IoT, Communication and Automation Technology (ICICAT)*.
- Jeyachandran, P., Vardhan Akisetty, A. S. V., Subramani, P., Goel, O., Singh, S. P., & Shrivastav, A. (2024). Leveraging Machine Learning for Real-Time Fraud Detection in Digital Payments. *Integrated Journal for Research in Arts and Humanities*.
- Kandregula, N. (2019). Leveraging Artificial Intelligence for Real-Time Fraud Detection in Financial Transactions: A Fintech Perspective. *World Journal of Advanced Research and Reviews*.
- Olowu, O., Olowofela Adeleye, A., Omokanye, A. O., Ajayi, A. M., Adepoju, A. O., Omole, O. M., & Chianumba, E. C. (2024). AI-Driven Fraud Detection in Banking: A Systematic Review of Data Science Approaches to Enhancing Cybersecurity. *GSC Advanced Research and Reviews*.

- Pothireddy, N. K. R., & Algubelli, B. R. (2016). Real-Time Fraud Detection Using AI on Financial Streaming Data. *International Journal of Scientific Research in Science and Technology*.
- Premasai, R. (2024). INTEGRATING AI IN IDENTITY AND ACCESS MANAGEMENT FOR IMPROVED CYBERSECURITY POSTURE. *International Scientific Journal of Engineering and Management*.
- Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019). Real-Time Credit Card Fraud Detection Using Machine Learning. *Confluence*.
- Tyagi, S., Tyagi, A., Rani, S., Kumar, A. S., Adhav, S., & Gupta, S. (2025). The Role of Artificial Intelligence in Risk Management and Fraud Detection in Financial Services. *Journal of Informatics Education and Research*.