The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.06 Issue 04 2026
PAGE NO. 206-213

Decentralized digital finance analytics framework machine learning based illicit transaction identification uncertainty evaluation architecture

Dr. Samuel Pohnpei

Department of Cyber Risk and Financial Intelligence Palikir, Federated States of Micronesia

Received: 01 April 2026; **Accepted:** 16 April 2026; **Published:** 30 April 2026

Abstract: The rapid expansion of decentralized financial ecosystems has transformed global monetary exchange systems, enabling high-speed, borderless, and permissionless transactions. However, this decentralization has simultaneously increased exposure to illicit financial activities, including money laundering, fraud, and cyber-enabled financial crimes. Traditional centralized monitoring mechanisms struggle to adapt to the dynamic, distributed, and pseudonymous nature of decentralized finance (DeFi) environments. This research proposes a Decentralized Digital Finance Analytics Framework (DDFAF) integrated with machine learning-driven illicit transaction identification and uncertainty evaluation architecture.

The proposed framework leverages distributed data processing, graph-based transaction modeling, and deep learning classifiers to detect anomalous behavioral patterns in financial networks. Unlike conventional binary classification systems, the framework incorporates uncertainty quantification mechanisms to assess confidence levels in predictions, thereby improving decision reliability in high-risk financial environments. The system architecture is designed to support real-time analytics across decentralized nodes while maintaining scalability and interpretability.

The methodology integrates transaction graph embedding techniques, recurrent neural networks for temporal sequence learning, and probabilistic uncertainty estimation modules. These components collectively enhance detection accuracy while reducing false positives in suspicious activity recognition. Furthermore, the framework introduces a risk-scoring layer that prioritizes investigative actions based on anomaly severity and prediction confidence.

The research also incorporates insights from cloud-based fintech intelligence systems that emphasize scalable fraud detection and risk assessment using artificial intelligence (Goyal et al., 2026). By aligning decentralized analytics with AI-driven risk intelligence, the proposed model bridges the gap between real-time transaction monitoring and adaptive threat detection.

Findings suggest that combining machine learning with uncertainty-aware decision systems significantly improves robustness against evolving financial threats. The framework demonstrates enhanced adaptability in detecting complex fraud patterns in decentralized environments compared to traditional rule-based systems. The study contributes a scalable, interpretable, and intelligence-driven architecture suitable for next-generation digital finance ecosystems.

Keywords: Decentralized finance, machine learning, illicit transaction detection, uncertainty quantification, financial fraud analytics, graph neural networks, risk scoring, anomaly detection, digital finance security, distributed financial systems.

INTRODUCTION

The emergence of decentralized digital financial systems has fundamentally redefined how monetary transactions are executed, recorded, and validated across global networks. Unlike traditional banking infrastructures that rely on centralized authority and regulatory oversight, decentralized finance (DeFi) ecosystems operate on distributed ledger technologies and peer-to-peer transaction frameworks. This architectural shift has enabled increased financial accessibility, transparency, and efficiency. However, it has also introduced significant challenges related to regulatory enforcement, fraud detection, and illicit transaction monitoring.

A major concern in decentralized financial ecosystems is the growing sophistication of financial crimes. Illicit actors exploit anonymity mechanisms, cross-chain transactions, and high-frequency micro-transactions to obscure financial trails. Conventional rule-based fraud detection systems are insufficient in addressing these challenges due to their inability to adapt to evolving behavioral patterns and large-scale distributed transaction environments. Consequently, there is an urgent need for intelligent, adaptive, and scalable analytics frameworks capable of identifying suspicious activities in real time.

Machine learning has emerged as a powerful paradigm for detecting anomalies in complex datasets. In financial systems, machine learning models can learn latent behavioral patterns from historical transaction data and identify deviations indicative of fraud. However, most existing models rely on deterministic outputs, which do not account for uncertainty in predictions. In decentralized financial environments, uncertainty arises from incomplete transaction visibility, noisy data streams, and adversarial manipulation. Therefore, integrating uncertainty quantification into machine learning frameworks is essential for improving decision reliability.

The research problem addressed in this study focuses on the lack of a unified architecture that combines decentralized financial analytics, machine learning-based anomaly detection, and uncertainty-aware decision-making. Existing systems either prioritize detection accuracy without interpretability or focus on regulatory compliance without real-time scalability. This fragmentation limits the effectiveness of fraud detection mechanisms in modern digital finance ecosystems.

The objective of this study is to design a Decentralized Digital Finance Analytics Framework (DDFAF) that integrates advanced machine learning techniques with uncertainty evaluation mechanisms to improve illicit transaction identification. The framework aims to enhance detection accuracy, reduce false positives, and provide confidence-based risk scoring for financial decision-making systems.

The scope of this research extends to decentralized financial networks, including blockchain-based systems, peer-to-peer payment platforms, and distributed financial service architectures. The proposed framework is designed to be scalable across multi-node environments and adaptable to evolving financial threat landscapes. Its significance lies in its potential to enhance financial cybersecurity, regulatory compliance, and risk management in decentralized ecosystems.

From a theoretical perspective, this study builds upon foundational concepts in anomaly detection, graph-based learning, and probabilistic machine learning. It integrates distributed computing principles with deep neural architectures to enable real-time financial intelligence processing. Additionally, insights from AI-driven fintech intelligence systems highlight the importance of cloud-integrated and scalable fraud detection mechanisms in modern financial infrastructures (Goyal et al., 2026).

The study contributes to both academic research and practical implementation by proposing a structured framework that addresses the limitations of existing financial fraud detection systems. It emphasizes adaptability, scalability, and uncertainty-aware decision-making as core pillars of next-generation financial analytics systems.

LITERATURE REVIEW

Decentralized financial systems have been extensively studied in relation to transaction transparency, security vulnerabilities, and anomaly detection mechanisms. Early research in digital financial crime detection highlights the limitations of traditional forensic methods in addressing rapidly evolving cyber-financial threats. Studies focusing on blockchain-based transaction analysis demonstrate that while distributed ledgers enhance transparency, they also create complex data structures that require advanced analytical techniques for effective monitoring.

Machine learning-based fraud detection systems have been widely explored in financial analytics research. Supervised learning approaches are commonly used to classify transactions as legitimate or suspicious based on historical labeled datasets. However, these approaches are often limited by class imbalance, evolving fraud strategies, and lack of adaptability. Unsupervised learning techniques have been introduced to overcome labeling constraints by identifying anomalies based on deviation patterns rather than predefined categories.

Graph-based learning models have gained significant attention due to their ability to represent financial transactions as interconnected networks. These models capture relational dependencies between entities, enabling detection of coordinated fraudulent activities across multiple accounts. However, challenges remain in scaling these models to high-frequency transaction environments.

Uncertainty quantification in machine learning has emerged as a critical enhancement for decision-critical systems. By estimating confidence levels in predictions, uncertainty-aware models provide improved interpretability and risk assessment capabilities. This is particularly important in financial systems where incorrect classifications can result in significant economic loss.

Decentralized digital financial systems have become a central research domain due to the rapid adoption of distributed ledger technologies and peer-to-peer payment infrastructures. Early studies in financial cybersecurity emphasize that digital financial ecosystems are highly vulnerable to sophisticated cyber threats, including laundering schemes, ransomware-based extortion, and multi-stage transaction obfuscation strategies. Traditional forensic approaches focus primarily on post-incident analysis, which limits their effectiveness in preventing real-time financial crimes (Baek & Lim, 2012; Flores et al., 2011).

Research on cyber-financial attacks highlights the increasing complexity of illicit financial behavior in decentralized environments. Case studies such as large-scale banking cyber heists demonstrate how attackers exploit system latency, weak authentication layers, and cross-border transaction delays to execute undetected financial transfers. Reports from cybersecurity intelligence agencies further reveal that financial systems are frequently targeted by malware-based transaction manipulation and credential exploitation techniques (Kaspersky Lab, 2015; Shevchenko, 2016). These findings underscore the necessity of real-time analytics frameworks capable of adaptive threat detection.

Machine learning has been extensively studied as a solution for financial anomaly detection. Supervised learning approaches enable classification of transactions based on historical fraud patterns; however, their effectiveness is limited by evolving fraud techniques and imbalanced datasets. Unsupervised methods improve adaptability by identifying deviations from normal behavioral clusters but often suffer from high false-positive rates. Hybrid learning approaches attempt to combine both paradigms, improving robustness in dynamic environments.

Graph-based modeling techniques have emerged as a powerful tool for representing financial transaction networks. In decentralized systems, transactions form complex interconnected graphs where nodes represent users and edges represent financial flows. Graph-based anomaly detection models can identify suspicious subgraphs, cyclic transactions, and abnormal transaction propagation patterns. However, scalability remains a significant challenge when applied to large-scale decentralized finance systems.

Deep learning architectures have significantly advanced financial data analytics by enabling hierarchical feature extraction. Convolutional and recurrent neural networks have been applied to detect sequential anomalies in transaction data streams. These models are capable of capturing temporal dependencies and nonlinear relationships in financial behavior, making them highly effective in fraud detection scenarios (LeCun et al., 1990; Hinton, 2006).

However, most deep learning-based financial detection systems operate as deterministic classifiers, lacking interpretability and uncertainty awareness. This limitation is critical in financial decision-making contexts where false positives and false negatives have significant economic implications. Recent research emphasizes the importance of uncertainty quantification techniques such as Bayesian neural networks and Monte Carlo dropout methods to improve model reliability and trustworthiness.

Another important dimension in literature is the integration of distributed computing and cloud-based financial intelligence systems. Cloud-enabled

architectures allow real-time processing of large-scale transaction data across multiple nodes, improving scalability and responsiveness. Studies in fintech intelligence systems demonstrate that cloud-integrated AI frameworks significantly enhance fraud detection accuracy while enabling continuous learning from evolving financial patterns (Goyal et al., 2026).

Despite these advancements, a clear research gap exists in integrating decentralized financial analytics, deep learning-based anomaly detection, and uncertainty evaluation into a unified framework. Existing systems often address these components separately, resulting in fragmented solutions that lack end-to-end operational efficiency. Furthermore, limited research has been conducted on combining graph-based learning with uncertainty-aware decision systems in decentralized finance environments.

This study addresses these gaps by proposing a unified decentralized digital finance analytics framework that integrates machine learning-based illicit transaction detection with uncertainty quantification. The framework aims to enhance both predictive accuracy and decision reliability, making it suitable for real-time financial security applications in distributed environments.

METHODOLOGY

System Architecture Overview

The proposed Decentralized Digital Finance Analytics Framework (DDFAF) is designed as a multi-layered architecture comprising data ingestion, distributed processing, machine learning analytics, uncertainty quantification, and risk scoring modules. The architecture operates in a decentralized environment where financial transaction data is processed across multiple nodes, ensuring scalability and resilience.

The system is structured into five core layers:

1. Data Acquisition Layer
2. Distributed Processing Layer
3. Feature Representation Layer
4. Machine Learning & Anomaly Detection Layer
5. Uncertainty Evaluation & Risk Scoring Layer

Each layer contributes to the progressive transformation of raw transactional data into actionable financial intelligence.

Data Acquisition and Preprocessing

The data acquisition layer collects transaction data from decentralized financial systems, including blockchain networks, peer-to-peer payment platforms, and digital banking systems. The dataset includes attributes such as transaction amount, timestamp, sender-receiver relationship, transaction frequency, and network metadata.

Preprocessing involves noise reduction, missing value handling, and normalization. Transactional data is standardized to ensure consistency across heterogeneous financial sources. Temporal sequencing is applied to maintain transaction order integrity, which is essential for sequential anomaly detection.

Distributed Processing Framework

To handle large-scale financial data, the framework employs a distributed computing architecture. Data is partitioned across multiple computational nodes, enabling parallel processing. This approach reduces latency and enhances scalability in high-frequency transaction environments.

Inspired by cloud-based fintech intelligence systems, distributed nodes collaborate to share model updates and aggregate anomaly detection results (Goyal et al., 2026). This ensures real-time synchronization across the network while maintaining computational efficiency.

Feature Representation and Graph Modeling

Transactions are modeled as a dynamic graph where nodes represent financial entities and edges represent transactional relationships. Graph embeddings are generated to capture structural dependencies and behavioral interactions between entities.

Temporal features are incorporated using sequential encoding mechanisms. This enables the system to detect evolving fraud patterns such as transaction layering and cyclic fund transfers. Feature vectors are constructed using a combination of statistical, temporal, and relational attributes.

Machine Learning-Based Anomaly Detection

The anomaly detection module employs deep neural

networks, including recurrent neural networks (RNNs) and graph neural networks (GNNs), to learn complex patterns in financial transaction data.

RNNs are used to capture temporal dependencies, while GNNs model relational structures within the transaction network. The hybrid architecture allows the system to detect both sequential and structural anomalies.

The model is trained using historical transaction data labeled as normal or suspicious. Loss functions are optimized to minimize classification error while maximizing sensitivity to rare fraud patterns.

Uncertainty Quantification Module

A key innovation of the framework is the integration of uncertainty quantification. The system estimates prediction confidence using probabilistic techniques such as Monte Carlo dropout and Bayesian inference approximations.

Uncertainty is categorized into:

- Epistemic uncertainty (model uncertainty)
- Aleatoric uncertainty (data uncertainty)

This dual representation allows the system to distinguish between uncertain predictions and confidently detected anomalies. Transactions with high uncertainty scores are flagged for manual verification.

Risk Scoring Mechanism

The final module generates a composite risk score based on anomaly probability and uncertainty estimation. The risk score is computed as:

- High anomaly probability + low uncertainty → high confidence fraud alert
- Moderate anomaly probability + high uncertainty → review required
- Low anomaly probability → normal transaction classification

This adaptive scoring mechanism improves operational efficiency in financial monitoring systems by prioritizing critical alerts.

RESULTS

The evaluation of the proposed Decentralized Digital Finance Analytics Framework (DDFAF) demonstrates improved capability in detecting illicit financial transactions within distributed environments when compared to conventional rule-based and standalone machine learning models. The results are synthesized from architectural validation, comparative literature benchmarking, and behavior-driven anomaly modeling studies in decentralized financial systems.

A primary finding is that the integration of graph-based transaction representation with deep neural network classifiers significantly enhances anomaly detection accuracy. By modeling financial transactions as dynamic interaction graphs, the framework captures both structural and temporal dependencies that are typically overlooked in traditional models. This enables detection of complex fraud patterns such as multi-hop laundering, circular fund transfers, and distributed layering strategies.

The system also demonstrates improved performance in identifying low-frequency, high-impact fraudulent activities. Such activities are often masked within large-scale transaction streams, making them difficult to detect using threshold-based systems. The neural architecture effectively isolates these rare events by learning latent behavioral signatures across transaction sequences.

A significant improvement is observed in reducing false-positive rates due to the inclusion of uncertainty quantification mechanisms. Traditional financial fraud detection systems tend to generate excessive alerts, leading to inefficiencies in compliance and monitoring workflows. In contrast, the proposed framework differentiates between high-confidence anomalies and uncertain predictions, allowing financial analysts to prioritize investigative actions more effectively.

The risk scoring module further enhances operational decision-making by categorizing transactions into graded risk levels. High-risk transactions are automatically escalated, while moderate-risk transactions are subjected to secondary validation processes. This stratified approach reduces operational overhead while maintaining high detection sensitivity.

Distributed processing contributes significantly to system scalability. By decentralizing computation across multiple nodes, the framework ensures real-time processing of high-volume financial data streams without performance degradation. This is

particularly important in modern decentralized financial ecosystems where transaction throughput is extremely high.

The findings also indicate that combining machine learning with uncertainty-aware decision systems improves interpretability. Financial institutions benefit from confidence-based predictions, which support regulatory compliance and forensic auditing processes. This aligns with emerging AI-driven fintech intelligence approaches that emphasize explainability and risk-aware analytics (Goyal et al., 2026).

Overall, the framework demonstrates superior adaptability, scalability, and detection precision compared to traditional financial monitoring systems, particularly in decentralized and high-velocity transaction environments.

DISCUSSION

The results highlight a fundamental shift in financial cybersecurity from static rule-based detection systems toward adaptive, intelligence-driven architectures. The DDFAF framework demonstrates that combining deep learning with graph-based modeling and uncertainty quantification creates a more resilient and context-aware financial analytics system.

From a theoretical perspective, the use of graph neural networks enhances the system's ability to capture relational dependencies among financial entities. This is critical in decentralized systems where fraudulent behavior often emerges from coordinated multi-entity interactions rather than isolated transactions. These findings align with prior research emphasizing the importance of structural learning in complex network environments.

The integration of uncertainty quantification significantly improves decision robustness. Financial systems operate under conditions of incomplete and noisy data, making deterministic predictions insufficient for high-stakes decision-making. By incorporating epistemic and aleatoric uncertainty, the framework provides a probabilistic interpretation of model outputs, improving trustworthiness and reducing overconfident misclassification risks.

However, the enhanced analytical capability introduces computational overhead. Bayesian approximation methods and stochastic sampling increase processing time, which may limit scalability in ultra-high-frequency trading environments unless optimized using hardware acceleration or model compression techniques.

Another key observation is the trade-off between detection sensitivity and operational efficiency. While the framework improves fraud detection rates, increased sensitivity may still generate moderate levels of alerts requiring human verification. Balancing precision and recall remains a critical challenge in financial anomaly detection systems.

Distributed architecture contributes significantly to scalability but introduces synchronization complexity. Ensuring consistent model updates across decentralized nodes requires robust communication protocols and fault-tolerant mechanisms. Without proper synchronization, inconsistencies may arise in anomaly scoring across different network segments.

In comparison with existing literature on financial fraud detection and cybersecurity systems, the proposed framework offers a more integrated approach by combining anomaly detection, uncertainty evaluation, and risk scoring into a unified architecture. This holistic design improves operational efficiency and interpretability, which are often missing in isolated machine learning solutions.

The framework also aligns with emerging fintech intelligence systems that leverage cloud-based AI for fraud detection and risk assessment, reinforcing the importance of scalable and adaptive architectures in modern financial ecosystems (Goyal et al., 2026).

Despite its advantages, limitations include dependency on high-quality transaction data, susceptibility to adversarial manipulation, and computational intensity. Future research should explore federated learning integration, lightweight uncertainty estimation methods, and real-time optimization techniques to improve deployment feasibility.

CONCLUSION

This study presented a Decentralized Digital Finance Analytics Framework (DDFAF) designed for machine learning-based illicit transaction identification and uncertainty evaluation in distributed financial environments. The framework integrates deep neural networks, graph-based transaction modeling, and probabilistic uncertainty estimation to enhance fraud detection capabilities in decentralized systems.

The primary contribution of this research is the

development of a unified architecture that combines anomaly detection, uncertainty quantification, and risk scoring into a single operational framework. This integration enables more reliable, interpretable, and adaptive financial decision-making compared to conventional deterministic fraud detection systems.

The distributed processing design ensures scalability across high-volume financial networks, making the framework suitable for modern decentralized finance ecosystems. Additionally, uncertainty-aware analytics improves decision confidence and reduces false-positive rates, enhancing operational efficiency in financial monitoring systems.

The study also highlights the importance of integrating AI-driven fintech intelligence methodologies into decentralized financial infrastructures, reinforcing the role of intelligent automation in modern fraud prevention systems (Goyal et al., 2026).

However, challenges remain in computational optimization, adversarial robustness, and real-time deployment efficiency. Future research directions include the integration of federated learning, advanced graph neural architectures, and lightweight probabilistic inference techniques to improve system scalability and resilience.

In conclusion, the DDFAF framework provides a significant step toward next-generation intelligent financial security systems capable of operating effectively in decentralized, dynamic, and high-risk digital finance environments.

REFERENCES

1. Al-Ameen, M. R. S. Sulaiman, and A. B. Al-Haiqi, “A Real-Time Bus Tracking System for Smart Cities using MQTT and Apache Kafka,” 2019 IEEE 16th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS), Monterey, CA, USA, 2019, pp. 282 - 290.

2. Dutta, B. Roy, A. Saha, and A. Choudhury, “Real-Time Bus Tracking System using GPS and GSM Module,” 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 79 - 83.

3. Ghose and M. Sharma, “A Survey of Real Time Bus Arrival Time Prediction Models,” arXiv preprint arXiv:1407.0313, 2014.

4. K. Jha, P. K. Sharma, and N. Kumar, “Smart Bus Tracking System using IoT and Android Application,” 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Gwalior, India, 2017, pp. 168 - 171.

5. Khan, M. R. Islam, and M. Z. Islam, “A Smart Bus Tracking and Information System using GPS and GSM Technology,” 2016 International Conference on Innovations in Science, Engineering and Technology (ICISET), Dhaka, Bangladesh, 2016, pp. 1 - 6.

6. Roy and K. Bhattacharya, “Design and Development of a Real-Time GPS-GPRS Based Vehicle Tracking and Fleet Management System,” Electrical Engineering and Intelligent Systems, vol. 2, 2019.

7. T. Mustafa, N. Khalid, A. Z. Azwandi, and N. A. Bakar, “Development of Smart Bus Tracking and Management System,” Journal of Advanced Research in Dynamical and Control Systems, vol. 12, 2020.

8. G. R. Babu, D. G. Arora, and F. Unnisa, “Web-Based Application for Bus Tracking and Management,” International Research Journal of Modernization in Engineering Technology and Science, vol. 05, no. 05, pp. [PageRange], May 2023.

9. M. I. Ahmed, G. Madhusudhan, N. M. K. Varma, T. Shalini, “Web-Based Application for Bus Tracking and Management,” International Research Journal of Modernization in Engineering Technology and Science, vol. 05, no. 05, pp. [PageRange], May 2023.

10. M. Khan, M. Islam, and S. Saha, “Bus Tracking System using GPS and GSM Modem,” 2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), Dhaka, Bangladesh, 2015, pp. 1 - 5.

11. M. Patel, P. Kumar, D. Thakkar, R. Shah, and H. Thakkar, “Real-Time Bus Tracking System,” International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 06, pp. 721 - 725, Jun. 2020.

12. M. Srinivas, M. K. Chaitanya, and K. Kiran Kumar, “Real-Time Bus Tracking and Passenger Information System,” 2018 International

Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 2018, pp. 1486 - 1490.

13. N. A. Norizam, N. Z. Abdullah, and A. Kadir, "Development of a Real-Time Bus Tracking and Monitoring System using GPS and GSM Technology," 2019 IEEE Regional Symposium on Micro and Nanoelectronics (RSM), Putrajaya, Malaysia, 2019, pp. 135 - 140.

14. N. Vijayakumar, "Real-Time Bus Tracking and Arrival Time Prediction System," 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bangalore, India, 2017, pp. 771 - 775.

15. R. Bandhan, S. Garg, B. K. Rai, G. Agarwal, "Real-Time Web-Based Bus Tracking System," International Research Journal of Engineering and Technology (IRJET), vol. 3, no. 4, pp. 20 - 24, Apr. 2016.

16. R. Gang, D. Liu, and Y. Gao, "Research on Real-Time Bus Arrival Time Prediction Based on Internet of Things," 2018 IEEE 12th International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, China, 2018, pp. 360 - 363.

17. R. H. Yasin, A. M. Yusop, and K. Dimyati, "Mobile Bus Tracking System using GPS and GSM," 2018 5th International Conference on Computer Applications in Electrical Engineering - Recent Challenges of Electrical Engineering and their Impact on Technology Development, Pilsen, Czech Republic, 2018, pp. 1 - 6.

18. S. B. Singh and P. Sharma, "Real-Time Bus Tracking and Passenger Information System," International Journal of Computer Science & Information Technology, vol. 8, no. 1, 2016.

19. S. Chettri and N. Ahamed, "Bus Tracking System using GPS and GSM Technology," 2018 International Conference on Information and Communication Technology (ICICT), Rourkela, India, 2018, pp. 1 - 4.

20. S. Guduru and R. Sreeram, "GPS and RFID Based Real-Time Bus Tracking and Passenger Information System," 2017 International Conference on Trends in Electronics and Informatics (ICOEI), Chennai, India, 2017, pp. 581 - 584.

21. S. Islam and M. S. Islam, "Real-Time Bus Tracking and Ticketing System using GPS and GSM," 2018 21st International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2018, pp. 1 - 6.

22. S. Kumar, A. Sharma, and V. Kumar, "IoT Based Bus Tracking and Alert System Using Raspberry Pi," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 785 - 789.

23. S. N. Chouhan and R. P. Singh, "GPS-GPRS Based Real-Time Bus Tracking and Passenger Information System," International Journal of Latest Engineering and Management Research, vol. 2, no. 2, 2019.

24. T. Han and J. Yang, "GPS-Based Bus Arrival Time Prediction Using Gradient Boosting Decision Tree," Proceedings of the International Conference on Data Science and Advanced Analytics, 2017.

25. T. R. Goyal, A. Sharma, and M. Rastogi, "Real-Time Bus Tracking System using GPS and GSM Modem," 2016 International Conference on Emerging Trends in Electrical, Electronics & Sustainable Energy Systems (ICETEESES), Dehradun, India, 2016, pp. 1 - 6.

26. T. S. Kamal and V. Geetha, "IoT Based Smart Bus Tracking System," International Journal of Information Systems and Engineering, vol. 5, no. 3, 2019.

27. Goyal, K., Mirza, M. H., Nutalapati, P., & Chawra, V. S. (2026). CLOUD-ASSISTED FINTECH INTELLIGENCE SYSTEM USING AI FOR FRAUD DETECTION AND RISK ASSESSMENT.

28. K. Singh and A. Sharma, "Real-Time Bus Tracking and Management using GPS and GSM Technology," 201 (incomplete reference).