Leveraging the Variational Autoencoder with the Blockchain Smart Contracts Model for Strengthening Fraud Detection in Financial Sectors

Khalid Hamed Allehaibi
Computer Science Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
kallehaibi@kau.edu.sa (corresponding author)

Received: 14 July 2025 | Revised: 30 July 2025, 21 August 2025, 2 September 2025, and 9 September 2025 | Accepted: 11 September 2025

 DOI: https://doi.org/10.48084/etasr.13371

ABSTRACT

Financial fraud has increased and evolved alongside recent technological developments, raising the need for systems that are able to detect and prevent it. One such system is Blockchain (BC), which enables computerized functionality and on-the-spot verification, while being both cost-efficient and adequately productive, and it is expected to influence domains such as accountancy and its related services. Additionally, combining the security and transparency of BC with the analytical capabilities of Machine Learning (ML) can offer a more promising system for detecting and preventing financial fraud than a standalone BC. Motivated by this idea, this study presents the Leveraging Variational Autoencoder with Smart Contracts to Strengthen Fraud Detection (LVAESC-SFD) model, which aims to examine the contribution of Smart Contracts (SCs) in enhancing security and fraud detection in financial applications. The model operates by employing the Correlation-based Feature Selection (CFS) technique for selecting an optimal subset of features, and then a Variational Autoencoder (VAE) for performing fraud detection and classification. The LVAESC-SFD model was evaluated using a financial fraud detection dataset listing millions of transactions and achieved an accuracy of 98.24%, outperforming existing models.

Keywords-fraud detection; smart contracts; financial sector; variational autoencoder; blockchain; correlation-based feature selection

I. INTRODUCTION

The growing reliance of everyday transactions on digital finance has resulted in an increased need for advanced fraud-prevention mechanisms to ensure transaction security. An example of such a mechanism is Smart Contracts (SCs), which support secure, automated transactions, and especially their integration into Blockchain (BC) ecosystems has revolutionized sectors such as banking by reducing intermediaries, simplifying processes, and enhancing security and transparency [1-3]. However, auditing SCs remains challenging due to i) their complex transactional logic, making fraudulent behavior harder to identify, and ii) their issues related to compliance and scalability [1, 2]. At the same time, traditional rule-based fraud detection systems further struggle to keep pace with rapidly evolving fraud attack patterns [4]. Therefore, with financial networks becoming increasingly interconnected, reinforcing fraud-detection capabilities is essential to counteract growing cyberattacks and fraudulent schemes [5], preventing financial losses, maintaining user trust, ensuring regulatory compliance [6], and upholding transaction integrity across financial systems [7].

A proposed approach to counteract these limitations is the integration of Artificial Intelligence (AI) and BC, where Machine Learning (ML) models can analyze transactional data to identify anomalies and adapt to evolving fraud strategies [8], resulting in higher detection accuracy, fewer false alarms, and faster response times. Several recent studies highlight promising developments in this area. For instance, authors in [9] utilized a Deep Learning (DL)-driven SC within a Private Ethereum Consortium Blockchain (PEC-BC), where the Dynamic Butterfly-Billiards Optimizer Algorithm (DB-BOA) is used to select leader blocks and tuning, followed by the application of Adaptive Deep Temporal Context Networks (ADTCN) in the elected novel leader block, and the use of consensus mechanisms to secure SCs. Authors in [10] investigated AI techniques emphasizing differential privacy and Federated Learning (FL) for secure data utilization, while authors in [11] introduced a novel AI framework incorporating a Convolutional Neural Network (CNN). Additionally, authors in [12] proposed an Integrated Blockchain and Artificial Intelligence (IBAI) method that leverages decentralized storage with swift AI-driven analysis, while authors in [13] examined the combined integration of BC and Internet of Things (IoT).

In other attempts, in [14], the combination of ML, Natural Language Processing (NLP), and BC was examined, while authors in [15] further investigated the AI-BC combination in conventional financial processes, and authors in [16] reviewed ML and DL methods for banking fraud detection. Moreover, authors in [17] introduced an enhanced Variational Autoencoder-Generative Adversarial Network (VAE-GAN) with a CNN-based oversampling strategy, and authors in [18] proposed a semi-decentralized fraud detection system integrating VAE-Quantum Long Short-Term Memory (VAE-QLSTM) technique with FL to improve real-time detection accuracy. Lastly, authors in [19] investigated DL models such as Autoencoders (AE), CNN, Recurrent Neural Networks (RNNs), and Generative Adversarial Networks (GANs) to improve anomaly detection.

Despite the promising results from the combinations of AI, DL, and BC, significant challenges remain regarding scalability, privacy, and system complexity, leaving an evident research gap in developing an efficient, scalable, and privacy-preserving fraud-detection model suitable for real-time financial applications. This study aims to fill this gap by proposing the Leveraging Variational Autoencoder with Smart Contracts to Strengthen Fraud Detection (LVAESC-SFD) model. The model utilizes i) the decentralized nature of BC to reduce fraud risks while streamlining auditability and compliance, ii) a Correlation-based Feature Selection (CFS) to identify optimal feature subsets, and iii) a VAE to effectively detect and classify fraudulent activities. This framework offers a novel and scalable solution that merges decentralized contract automation with advanced data-driven analytical methods, providing a robust and scalable solution for counteracting the growing fraud challenges in digital finance.

II. PROPOSED METHOD

Figure 1 illustrates the complete workflow of the proposed LVAESC-SFD model, which integrates BC, data preparation, Feature Selection (FS), and a fraud detection process.

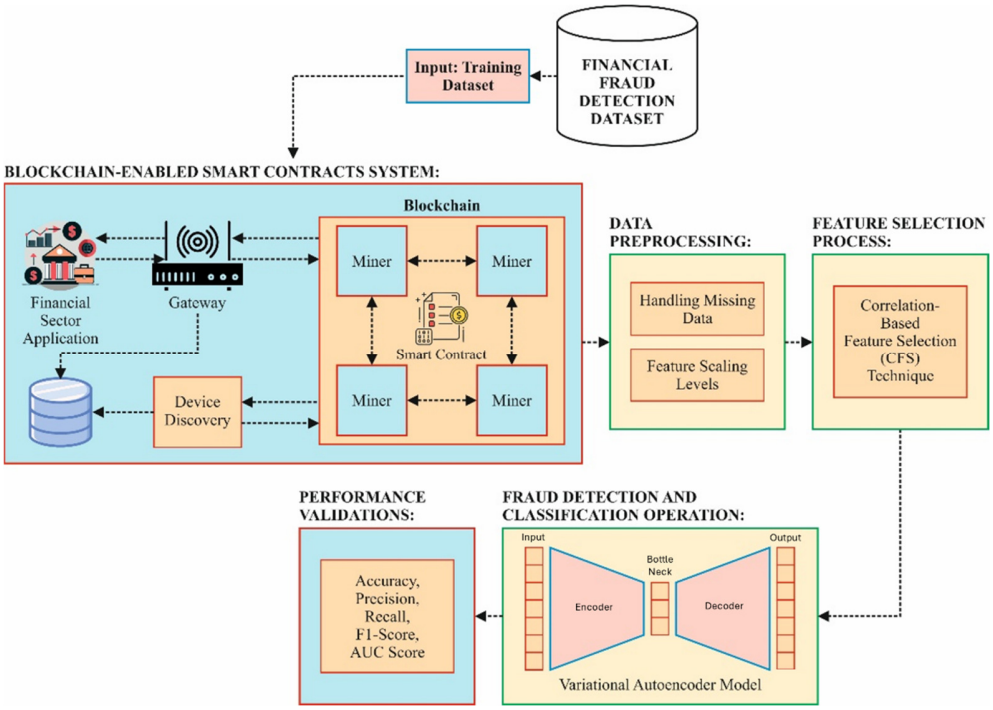

Fig. 1. Complete workflow process of LVAESC-SFD model.

A. BC-Enabled SCs

In the proposed framework, BC-enabled SCs are first employed to enhance fraud recognition in financial systems [20].

BC platforms are generally categorized into public platforms, such as Bitcoin and Ethereum. Public BC relies on decentralized probabilistic consensus, whereas Ethereum supports SCs via the Ethereum Virtual Machine (EVM), making it suitable for complex SC deployment. Each Ethereum node executes the EVM, ensuring uniform rule execution, and is widely used to develop Decentralized Applications (DApps).

On the other hand, SCs are executable scripts on top of BC that automate agreements between mutually untrusted parties, while their decentralized structure also improves scalability and resilience.

B. Data Preparation

In this framework, the preprocessing steps involved handling missing data and feature scaling. Missing values were imputed using mean imputation, calculated as:

$$X_{imputed} = \frac{\Sigma X_i}{n} \quad (1)$$

where n signifies the observation counts and X_i indicates every observed value. For feature scaling, all features were normalized using Min-Max scaling to the range [0,1], defined as:

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (2)$$

where X signifies the feature value, and X_{min} and X_{max} refers to the minimum and maximum feature values.

C. Feature Subset Selection

In order to reduce the dimensionality of the initial feature vector while retaining relevant features, the LVAESC-SFD model implements the CFS technique [21]. Specifically, CFS evaluates a feature subset based on correlation with the target class and inter-feature redundancy using:

$$M_s = \frac{k\overline{r_{cf}}}{\sqrt{k + k(k-1)\overline{r_{ff}}}} \quad (3)$$

where k is the number of features, M_s depicts the correlation between the set of features and class, $\overline{r_{ff}}$ denotes the average inter-feature correlation and $\overline{r_{cf}}$ signifies the average correlation between features and class.

Among the typical CFS heuristic searching approaches (forward selection, backward elimination, and best-first strategy), the best-first approach is employed, terminating when no improvement is observed on the correlation coefficient index over five consecutive generated subsets

D. Fraud Detection and Classification Model

The last part of the proposed framework is the VAE, responsible for the fraud detection and classification operation [22]. VAE is chosen for its ability to model complex data distributions, detect anomalies, and handle imbalanced datasets, while reducing input dimensionality, learning latent representations, and addressing overfitting present in other conventional AEs.

VAE consists of an encoder and a decoder. The encoder learns the posterior probability distribution $q_\phi(z \mid x)$, which models the latent variable z given the input x, while the decoder learns the likelihood distribution $p_\theta(x \mid z)$, which reconstructs the input x from the latent variable z. The subscripts θ and ϕ denote the decoder and encoder network parameters, respectively. In an optimal scenario, the reconstruction error, which is the difference between the original input and its reconstructed version, should be as close to zero as possible. The latent variable z also becomes useful for FS and dimensionality reduction, improving downstream fraud classification.

The VAE minimizes a loss function that combines a reconstruction term and a regularization term, defined as:

$$L(q) = E_{z\sim q_\phi(z|x)}\big(\log p_\Theta(x|z)\big) - KL\left(q_\phi(z|x) \parallel p(z)\right) \quad (4)$$

where $E_{z\sim q_\phi(z|x)}\big(\log p_\Theta(x|z)\big)$ measures the decoder's reconstruction quality (i.e., how accurately x is recovered from z), while $KL\left(q_\phi(z|x) \parallel p(z)\right)$ enforces similarity between the encoder's latent distribution and the prior distribution $p(z)$, thus shaping and constraining the latent space.

E. Algorithmic Steps for Fraud Detection: Integrating BC and VAE

Algorithm 1 outlines the key steps used in the model:

```
Algorithm 1: BC-Enabled VAE-based Fraud Detection
Input: Financial fraud detection data
Output: Fraud, Not Fraud
Step 1: Preprocessing
1.1. Handle missing data and apply feature scaling
Step 2: Feature Selection
2.1. Use CFS for choosing crucial features
Step 3: BC SCs
3.1. Utilize SCs to securely store and verify transactions
Step 4: Fraud Detection and Classification using VAE
4.1. Train VAE on chosen features
4.2. Detection of anomalies based on reconstruction error
4.3. If reconstruction error > threshold, classify as fraud; otherwise, classify as not fraud
```

III. EXPERIMENTAL ANALYSIS

All experiments were conducted using Python 3.6.5 on a system equipped with an Intel i5-8600k Central Processing Unit (CPU), a 4 GB Graphics Processing Unit (GPU), 16 GB Random Access Memory (RAM), a 250 GB Solid-State Drive (SSD), and a 1 TB Hard Disk Drive (HDD). The model was trained with a learning rate of 0.01, Rectified Linear Unit (ReLU) activation, 500-3,000 epochs, a dropout rate of 0.5, and a batch size of 5.

The simulation validation of the LVAESC-SFD model was examined using the financial fraud detection dataset in [23], comprising 10,000 samples evenly distributed between "isFraud_Yes" and "isFraud_No" classes. The dataset contains 10 features: step, type, amount, nameOrig, oldbalanceOrg, newbalanceOrig, nameDest, oldbalanceDest, newbalanceDest, and isFraud. For model training, 8 features were selected, excluding nameOrig and nameDest due to their low predictive relevance. Each of the samples corresponds to a balanced subset representing the broader distribution of millions of real-world transactions. Table I summarizes the distribution of financial transaction types in the dataset (CASH_OUT, PAYMENT, CASH_IN, TRANSFER, and DEBIT).

TABLE I. TRANSACTION TYPE DISTRIBUTION IN THE DATASET

Type	Count
PAYMENT	2,151,495
TRANSFER	532,909
CASH_OUT	2,237,500
DEBIT	41,432
CASH_IN	1,399,284

A. Model Evaluation

Figure 2 presents the confusion matrices of the LVAESC-SFD model evaluated at multiple epochs (500-3,000). At 500 epochs, the model achieved 4,766 True Positives (TP), 4,891 True Negatives (TN), 234 False Negatives (FN), and 109 False Positives (FP), demonstrating reasonable classification but with some misclassifications. By 3,000 epochs, the model improved to TP = TN = 4,912 and FP = FN = 88, increasing overall accuracy from 96.57% to 98.24%.

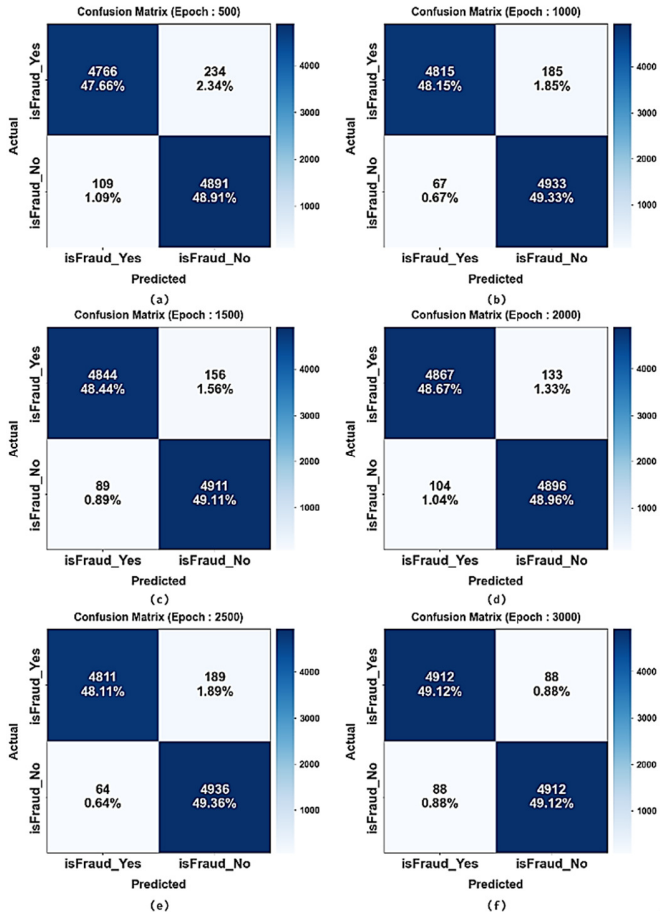

Fig. 2. Confusion matrices of LVAESC-SFD model: (a-f) epochs 500 to 3,000.

In addition, Table II summarizes all the performance metrics of the model across the epochs, including accuracy, precision, recall, F1-score, and Area Under Curve (AUC) score.

A similar pattern, as shown in the confusion matrices, is seen in the improvement of metrics as epochs increase, where performance steadily increases from 500 to 1,500 epochs and starts stabilizing at 2,500 epochs, while the best performance is achieved at 3,000 epochs. At 500 epochs, the LVAESC-SFD approach achieved an accuracy of 96.57%, a precision of 96.60%, a recall of 96.57%, an F1-score of 96.57%, and an AUC score of 96.57%, while at 3,000 epochs it achieved a uniform 98.24% across all metrics.

TABLE II. FRAUD DETECTION OUTCOME OF THE LVAESC-SFD TECHNIQUE UNDER DISTINCT EPOCHS

Class Labels	Accuracy %	Precision %	Recall %	F1-score %	AUC score %
Epoch - 500					
isFraud_Yes	-	97.76	95.32	96.53	96.57
isFraud_No	-	95.43	97.82	96.61	96.57
Average	96.57	96.60	96.57	96.57	96.57
Epoch - 1000					
isFraud_Yes	-	98.63	96.30	97.45	97.48
isFraud_No	-	96.39	98.66	97.51	97.48
Average	97.48	97.51	97.48	97.48	97.48
Epoch - 1500					
isFraud_Yes	-	98.20	96.88	97.53	97.55
isFraud_No	-	96.92	98.22	97.57	97.55
Average	97.55	97.56	97.55	97.55	97.55
Epoch - 2000					
isFraud_Yes	-	97.91	97.34	97.62	97.63
isFraud_No	-	97.36	97.92	97.64	97.63
Average	97.63	97.63	97.63	97.63	97.63
Epoch - 2500					
isFraud_Yes	-	98.69	96.22	97.44	97.47
isFraud_No	-	96.31	98.72	97.50	97.47
Average	97.47	97.50	97.47	97.47	97.47
Epoch - 3000					
isFraud_Yes	-	98.24	98.24	98.24	98.24
isFraud_No	-	98.24	98.24	98.24	98.24
Average	98.24	98.24	98.24	98.24	98.24

These results indicate that the model consistently improves detection as epochs increase, which is meaningful for fraud detection; nevertheless, the improvements are modest, showing lesser returns with additional training.

B. Comparative Analysis

Table III compares the LVAESC-SFD model performance of 3000 epochs against recent approaches, including Light Gradient Boosting Machine Long Short-Term Memory (LightGBM-LSTM) hybrid, Adaptive Boosting (AdaBoost), K-Neural Network (KNN), Classical Autoencoder (CAE), Quantum One-Class SVM (QO-SVM), Random Forest with Synthetic Minority Oversampling Technique (RF+SMOTE), and Sparse Autoencoder with Generative Adversarial Networks (SAE+GAN).

The proposed model was the most competitive model, achieving the highest metrics across the board, followed by the RF+SMOTE, the QO-SVM, and the AdaBoost approaches.

TABLE III. COMPARATIVE STUDY OF LVAESC-SFD TECHNIQUE WITH RECENT MODELS

Approach	Accuracy %	Precision %	Recall %	F1-score %
LightGBM-LSTM Hybrid [24]	91.67	90.53	94.72	92.41
AdaBoost [25]	94.89	94.23	96.34	91.87
KNN [25]	95.78	91.26	90.70	89.12
CAE [26]	92.20	98.05	93.47	90.46
QO-SVM [26]	94.31	94.91	93.65	94.30
RF+SMOTE [27]	95.64	95.94	96.44	95.02
SAE+GAN [27]	93.51	91.56	89.68	89.79
LVAESC-SFD [Proposed]	98.24	98.24	98.24	98.24

IV. CONCLUSION

In this study, the Leveraging Variational Autoencoder with Smart Contracts to Strengthen Fraud Detection (LVAESC-SFD) model was proposed to enhance financial fraud detection in financial applications. The framework leverages Blockchain (BC)-enabled Smart Contracts (SC) to strengthen data security during fraud detection. The workflow includes data pre-processing to handle missing values and scale features, feature subset selection using the Correlation-based Feature Selection (CFS) technique, and finally, fraud detection and classification using a Variational Autoencoder (VAE) model.

Experimental evaluation on a financial fraud detection dataset demonstrated the effectiveness of LVAESC-SFD, achieving an accuracy, precision, recall, and F1-score and Area Under Curve (AUC) score of 98.24%, outperforming existing benchmark models.

Despite its strong performance, the main limitations of the proposed model were i) challenges in handling large-scale, heterogeneous data and ensuring seamless interoperability across diverse financial systems, and ii) needing to optimize computational resource usage and reduce latency for real-time deployment. Addressing these issues can result in more robust, effective fraud detection frameworks tailored for dynamic financial environments.

REFERENCES

[1] L. Liu, W.-T. Tsai, Md. Z. A. Bhuiyan, H. Peng, and M. Liu, "Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum," *Future Generation Computer Systems*, vol. 128, pp. 158–166, Mar. 2022, https://doi.org/10.1016/j.future.2021.08.023.

[2] C. Ubagaram, R. R. Mandala, B. S. Jayaprakasam, V. Garikipati, N. R. Dyavani, and G. A. Ogunmola, "An Improved Fedformer-Dilated Residual CNN Framework with Cross-Attentive Fusion for Cloud-Based Cyber Threat Detection and Financial Fraud Prediction," *International Journal of Innovation and Technology Management*, Oct. 2025, https://doi.org/10.1142/S021987702540005X.

[3] S. Sh. Taher, S. Y. Ameen, and J. A. Ahmed, "Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12822–12830, Feb. 2024, https://doi.org/10.48084/etasr.6641.

[4] H. O. Bello, C. Idemudia, and T. V. Iyelolu, "Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention," *World Journal of Advanced Research and Reviews*, vol. 23, no. 1, pp. 056–068, July 2024, https://doi.org/10.30574/wjarr.2024.23.1.1985.

[5] S. Lakkaraju, "Using Machine Learning to Combat E-Commerce Fraud," *International Journal of Information Technology and Management Information Systems*, vol. 16, no. 1, pp. 844–859, Feb. 2025, https://doi.org/10.34218/IJITMIS_16_01_060.

[6] A. A. Alhashmi, A. M. Alashjaee, A. A. Darem, A. F. Alanazi, and R. Effghi, "An Ensemble-based Fraud Detection Model for Financial Transaction Cyber Threat Classification and Countermeasures," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12433–12439, Dec. 2023, https://doi.org/10.48084/etasr.6401.

[7] A. Louja, A. Jamali, and N. Naja, "Blockchain-Powered Artificial Intelligence for Healthcare Systems Data Orchestration," in *Proceedings of the Third ICMDS'24: Machine Learning, Inverse Problems and Related Fields*, vol. 1466, A. Laghrib and A. Ghazdali, Eds. Cham: Springer Nature Switzerland, 2025, pp. 155–163.

[8] B. Annane, A. Alti, and A. Lakehal, "A Blockchain Semantic-based Approach for Secure and Traceable Agri-Food Supply Chain," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18131–18137, Dec. 2024, https://doi.org/10.48084/etasr.8908.

[9] S. C. Prabanand and M. S. Thanabal, "Advanced financial security system using smart contract in private ethereum consortium blockchain with hybrid optimization strategy," *Scientific Reports*, vol. 15, no. 1, Feb. 2025, Art. no. 6764, https://doi.org/10.1038/s41598-025-89404-3.

[10] F. Yuan *et al.*, "AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection," *Algorithms*, vol. 18, no. 5, May 2025, Art. no. 263, https://doi.org/10.3390/a18050263.

[11] H. Louati *et al.*, "Adopting Artificial Intelligence to Strengthen Legal Safeguards in Blockchain Smart Contracts: A Strategy to Mitigate Fraud and Enhance Digital Transaction Security," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 19, no. 3, pp. 2139–2156, Aug. 2024, https://doi.org/10.3390/jtaer19030104.

[12] A. Alenizi, S. Mishra, and A. Baihan, "Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence," *Ain Shams Engineering Journal*, vol. 15, no. 6, June 2024, Art. no. 102733, https://doi.org/10.1016/j.asej.2024.102733.

[13] O. S. Adanigbo, F. S. Ezeh, U. S. Ugbaja, C. I. Lawal, and S. C. Friday, "Advances in Blockchain and IoT Applications for Secure, Transparent, and Scalable Digital Financial Transactions," *International Journal of Advanced Multidisciplinary Research and Studies*, vol. 4, no. 6, pp. 1863–1869, Dec. 2024, https://doi.org/10.62225/2583049X.2024.4.6.4158.

[14] O. Odeyemi, C. C. Okoye, O. C. Ofodile, O. B. Adeoye, W. A. Addy, and A. O. Ajayi-Nifise, "Integrating AI with Blockchain for Enhanced Financial Services Security," *Finance & Accounting Research Journal*, vol. 6, no. 3, pp. 271–287, Mar. 2024, https://doi.org/10.51594/farj.v6i3.855.

[15] T. K. Vashishth, V. Sharma, V. Kaushik, and K. K. Sharma, "Blockchain-Driven Innovations in the Banking and Financial Sectors: Harnessing the Power of Automated Machine Learning," in *Advances in Finance, Accounting, and Economics*, D. Darwish and S. Kumar, Eds. IGI Global, 2024, pp. 555–578.

[16] M. F. Manzoor and A. Muhammad Faran, "Enhancing Banking Fraud Detection: Role of Machine Learning and Deep Learning Methods," *Premier Journal of Artificial Intelligence*, 2025, Art. no. 100014, https://doi.org/10.70389/PJAI.100014.

[17] B. R. Gudivaka, M. Almusawi, M. S. Priyanka, M. R. Dhanda, and M. Thanjaivadivel, "An Improved Variational Autoencoder Generative Adversarial Network with Convolutional Neural Network for Fraud Financial Transaction Detection," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, Hassan, India, May 2024, pp. 1–4, https://doi.org/10.1109/ICDSIS61070.2024.10594271.

[18] H. Abbassi, S. El Mendili, and Y. Gahi, "Adaptive, Privacy-Enhanced Real-Time Fraud Detection in Banking Networks Through Federated Learning and VAE-QLSTM Fusion," *Big Data and Cognitive Computing*, vol. 9, no. 7, July 2025, Art. no. 185, https://doi.org/10.3390/bdcc9070185.

[19] S. R. Peddinti, A. Tanikonda, and S. R. Katragadda, "Deep Learning for Anomaly Detection in E-commerce and Financial Transactions: Enhancing Fraud Prevention and Cybersecurity," *SSRN Electronic Journal*, vol. 10, no 30s, pp. 70-77, Feb. 2025, https://doi.org/10.2139/ssrn.5251213.

[20] H. Elsharkawi, E. Elbeltagi, M. S. Eid, W. Alattyih, and H. Wefki, "Construction Payment Automation Through Scan-to-BIM and Blockchain-Enabled Smart Contract," *Buildings*, vol. 15, no. 2, Jan. 2025, Art. no. 213, https://doi.org/10.3390/buildings15020213.

[21] E. Godini, H. Zareiforoush, A. Bakhshipour, Z. Lorigooini, and S. H. Payman, "Intelligent Grading of Green Cardamom Using Data Fusion of Electronic Nose and Computer Vision Methods," *Food Science & Nutrition*, vol. 13, no. 4, Apr. 2025, Art. no. e4645, https://doi.org/10.1002/fsn3.4645.

[22] H. Hamdaouy, E. M. Benghoulam, M. Chaibi, M. Berrada, and A. E. Hmaidi, "Estimating daily global solar radiation using deep learning," *Results in Engineering*, vol. 27, Sept. 2025, Art. no. 106132, https://doi.org/10.1016/j.rineng.2025.106132.

[23] *Financial Fraud Detection Dataset*. (2023), S. H. Eedala. [Online]. Available: https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset.

[24] M. Akouhar, M. Ouhssini, M. El Fatini, A. Abarda, and E. Agherrabi, "Dynamic oversampling-driven Kolmogorov–Arnold networks for credit card fraud detection: An ensemble approach to robust financial security," *Egyptian Informatics Journal*, vol. 31, Sept. 2025, Art. no. 100712, https://doi.org/10.1016/j.eij.2025.100712.

[25] K. H. Ahmed, S. Axelsson, Y. Li, and A. M. Sagheer, "A credit card fraud detection approach based on ensemble machine learning classifier with hybrid data sampling," *Machine Learning with Applications*, vol. 20, June 2025, Art. no. 100675, https://doi.org/10.1016/j.mlwa.2025.100675.

[26] C. Huot, S. Heng, T.-K. Kim, and Y. Han, "Quantum Autoencoder for Enhanced Fraud Detection in Imbalanced Credit Card Dataset," *IEEE Access*, vol. 12, pp. 169671–169682, 2024, https://doi.org/10.1109/ACCESS.2024.3496901.

[27] S. Shi, W. Luo, and G. Pau, "An attention-based balanced variational autoencoder method for credit card fraud detection," *Applied Soft Computing*, vol. 177, June 2025, Art. no. 113190, https://doi.org/10.1016/j.asoc.2025.113190.