International Journal on Smart & Sustainable Intelligent Computing
Vol. 02, Iss. 03, S. No. 01, pp. 1--12, Sept 2025
ISSN (Online): 3048-8508

Received: 29 Aug 2025, Accepted: 05 Oct 2025, Published: 07 Oct 2025
Digital Object Identifier: https://doi.org/10.63503/j.ijssic.2025.163

Review Article

LSTM–Based Anomaly Detection for Fraud and Financial Crime.

Blessing Oloko[1], Xiaochun Cheng[2*]

[1] Department of Computer Science, Faculty of Science, University of Lagos, Nigeria.

[2,] Department of Computer Science, Swansea Wales, UK

karodan01@gmail.com[1], xiaochun.cheng@swansea.ac.uk[2]

*Corresponding author: Xiaochun Cheng, xiaochun.cheng@swansea.ac.uk

ABSTRACT

Anomaly detection is a vital weapon for financial institutions in the war on fraud and financial crime, now more sophisticated and widespread in the wake of the COVID-19 pandemic's expansion of online transactions. This paper suggests a powerful, unsupervised, LSTM-based time-series anomaly detection model to solve the problem of detecting fraudulent transactions in financial data, which tend to be missing labelled anomaly information. Our approach utilizes the special capacity of LSTMs to learn temporal patterns by dynamically learning an anomaly threshold from prediction errors instead of utilizing limited anomaly labels. By performing a number of large-scale experiments on a financial transaction dataset, the proposed LSTM model was found to perform better than a number of state-of-the-art anomaly detection methods. The results show its better performance on major indicators, especially recall and F1-score, validating its high accuracy in detecting financial crimes. This study showcases the importance of sophisticated deep learning models in enhancing fraud detection ability and provides a strong, flexible solution for financial institutions to manage risks proactively. Our future work will involve extending this scheme for identifying deepfake-related fraud and enhancing its capability in processing more general complex time series data.

Keywords: *Fraud, Financial, Crime, Anomaly, Outlier, Deep learning, Machine learning, Artificial intelligence.*

1. Introduction

Economic and financial crimes are defined as non-violent offenses leading to financial loss (like fraud, money laundering, and tax evasion), and are hard to eliminate [1] [2]. This is because criminals constantly find new ways to perpetrate them despite existing laws [3] [4]. Synthetic identity fraud, phishing, and deepfakes are among the crimes that have increased significantly as a result of the growth of cyberspace transactions, which the COVID-19 pandemic has particularly accelerated. [5].

The ability of artificial intelligence (AI) to process large amounts of data reliably and efficiently makes it a promising tool for financial fraud detection. AI can enhance fraud detection by:

- **Automatically learning features**: From raw data, deep learning models can uncover intricate, hidden fraud patterns. [6][7].
- **Managing temporal and sequential patterns**: Recurrent neural networks (RNNs) and long short-term memory (LSTM) networks are capable of analysing transaction sequences over time to identify irregularities such as account takeovers. [8][9][10].
- **Anomaly detection with autoencoders**: These models flag deviations from normal transaction patterns, even for previously unknown fraud types [11] [12] [13] – [22] [23].
- **Graph Neural Networks (GNNs):** GNNs analyse relationships between entities to uncover fraudulent networks [17] - [24].
- **Real-time detection and adaptability**: AI systems can process transactions in real-time and adapt quickly to new fraud schemes [25] [26] [27] [11].
- **Improved performance metrics**: AI aids in lowering false negatives and false positives in fraud detection. [28].

- **Combining data types**: Deep learning can integrate both structured and unstructured data for comprehensive analysis [25].

AI integration into financial systems has the following advantages and disadvantages:

- **Enhanced accuracy and speed**: AI quickly identifies subtle patterns in large datasets [20].
- **Adaptive learning**: AI systems can rapidly adjust to new fraud tactics [29] [30] [31] 32].
- **Proactive risk management**: AI helps anticipate and prevent risks [25, 27, 38].
- **Operational efficiency**: It automates routine tasks, saving resources [33] [9] [34].
- **Improved customer experience**: Fewer false positives mean less inconvenience for legitimate customers [35] [36].
- **Network analysis**: AI uncovers organized crime and money laundering schemes [24] – [17].
- **Regulatory compliance**: AI assists in meeting Anti-Money Laundering (AML) and other regulatory requirements [37].

The risks associated with the integration of AI into the financial system are as follows:

- **Algorithmic bias:** AI models can perpetuate or amplify existing biases from training data [28, 9, 35].
- **Lack of explainability ("Black Box" Problem**): It can be hard to understand how complex AI models make decisions, posing challenges for audits and disputes [9].
- **Data privacy concerns**: AI requires access to sensitive data, raising privacy issues [37]
- **Adversarial attacks:** Criminals can manipulate AI systems to bypass detection [3, 43].
- **High costs**: Implementing and maintaining AI systems is expensive [12] [38] [39].
- **Regulatory uncertainty**: Legal frameworks for AI are still developing [40] [33] [3].
- **Over-reliance and deskilling**: Excessive dependence on AI can reduce human analytical skills.
- **Job displacement:** Automation by AI may lead to job losses, especially for job roles that require routine operations or performance.

The documents make a distinction between anomalies (unexpected, unusual values which should not normally exist) and outliers (known data points usually caused by errors) [11] [9]. Anomaly detection is important for financial stability and data integrity since it entails the detection of data points which fundamentally diverge from normal behaviour [3] [24]. Anomalies are classified as:

• Data Point-Based: Single irregular data points.

• Context-Based: Individual data points are normal, but abnormal when placed in a given context.

• Pattern-Based: Patterns or trends that deviate from past experience.

The study highlights that time series data (temporally gathered data points) forms a key element of financial systems. Time Series Analysis (TSA) employs statistical techniques to discover patterns and predict trends, taking into account elements such as level, trend, seasonality, noise, and cyclical components. Outliers in time series data may be:

• Point Outliers: Individual outlying data points at a particular time.

• Subsequence Outliers: Successive points whose joint behaviour is outlying.

• Outlier Time Series: a rare time series as a whole.

A key obstacle for applying AI to anomaly detection in finance, particularly following the switch to more online-based transactions in the post-COVID-19 era, is a paucity of anomaly labels in large datasets and variety of data obtained from different devices employed in executing financial transactions [41].

To do this, the research sets out a LSTM-based anomaly detection approach. This approach adopts an unsupervised learning method to derive error thresholds so that dependence on labelled anomaly data is lessened. Improved prediction performance across a range of datasets is also a target for the LSTM model, which will make it applicable to a variety of financial instruments and datasets. Testing on a Kaggle financial dataset is said to demonstrate its value over other forms of anomaly detection [42].

This research aims to enhance fraud detection using deep learning method, assess its effectiveness in mitigating financial crimes, examine how AI may help with regulatory compliance, and how machine learning can be used to spot unidentified illicit activity patterns.

The study is set up like this. Literature review Section examines relevant research in the areas of deep learning techniques, time-series data prediction and anomaly detection, and fraud and financial crime. The methods and data are presented in research methodology section. Implementation, comparison of the suggested model with alternative anomaly detection methods, and experiment results for the proposed model's performance evaluation are covered in result and discussion section. Concluding section brings this study to a close and identifies a topic for further investigation.

2. Literature review (Related work)

The proliferation of Artificial Intelligence (AI) and other cutting-edge technologies has created a normality in the financial sector. Artificial Intelligence simultaneously contribute to and combat financial fraud and cybercrime. Traditional rule-based Machine learning systems are proving to be increasingly ineffective in this evolving landscape. This literature review synthesizes research on AI's dual role, examining its use by fraudsters, its application as a defence mechanism, the specific AI technologies being leveraged, and the broader ethical and societal considerations.

Fraudsters are using AI to enhance the sophistication and scale of their criminal activities. Generative AI presents new and significant tool for the fraudsters since it enables them to create highly convincing fraudulent materials.

Content Generation: AI can generate persuasive phishing emails, vishing contents, fraudulent advertisements, and even fabricated images for insurance claims, making it difficult for victims to discern genuine content from fake [43, 44].

Deepfake Technology: Deepfake videos are used for impersonation, bypassing identity verification systems like "selfie video ID" in banks, and creating clickbait content. This is an alarming development for the financial industry [4, 101].

Automation and Targeting: Machine learning can analyse vast datasets to identify vulnerabilities and create highly personalised spear-phishing messages while AI-enabled chatbots can automate the manipulation of potential victims at scale. AI also enhances brute-force attacks against banking systems by developing subtle and powerful strategies to exploit vulnerabilities [4].

The increasing accuracy of DeepFake technology poses serious consequences, significant disruptions to social, economic, and political and systems, including privacy violations. The challenge of distinguishing genuine media from fabricated content necessitates robust defence mechanisms [5].

Despite the risks, AI is an indispensable tool in the fight against fraud and financial crime. It significantly improves fraud detection and prevention by analysing massive volumes of data in real-time, far surpassing the capabilities of traditional methods. According to research, state-of-the-art AI systems may reduce false positives by 40–60% and achieve detection rates of 87% to 94%. [29, 5, 32, 14, 22].

Fraud Detection and Efficiency: AI examines past data to identify questionable practices, such as fraudulent credit card transactions and fraudulent payments. Automating routine operations also increases operational efficiency by freeing up human experts to work on more complicated issues.

Combating AI-Generated Threats: AI is being developed to counter AI-generated threats, such as gathering intelligence on fraudulent networks and identifying deepfakes [4].

The absence of efficient techniques for utilizing big data analytics for fraud detection and prevention, however, is a significant challenge for IT Managers. Data exchange across financial institutions is essential in crime fighting and prevention, but it is hampered by a number of issues, such as privacy issues, inconsistent data formats, and complicated regulatory issues [43, 8, 57].

Research shows that certain deep learning (DL) and machine learning (ML) models outperform traditional rule-based systems in identifying and preventing financial crime.

Hybrid and Ensemble Models: Convolutional Neural Networks (CNNs) and LSTMs are examples of deep learning architectures that routinely outperform standalone approaches when combined with ensemble techniques like Random Forest and XGBoost [8, 29, 32, 35, 38, 40].

Graph Neural Networks (GNNs): GNNs hold great promise for enhancing real-time fraud detection at scale by examining relationships in financial transaction data [37, 38, 46, 58].

Large Language Models (LLMs): LLMs like ChatGPT offer a less resource-intensive alternative to fine-tuning for financial statement fraud detection by using prompt engineering. Additionally, these models have enhanced query resolution and authentication accuracy in financial institutions [40].

Explainable AI (XAI): XAI is essential for comprehending the intricacies of deep learning models and fulfilling legal and regulatory obligations. It fosters openness and trust by enabling financial institutions to defend AI-driven fraud detection decisions [45, 46, 21, 26, 48, 49].

Anomaly Detection: Time series data abnormalities and malicious behaviour are detected using a variety of models, such as ALGAN, F-SE-LSTM, and LSTM-based VAE-GAN [48, 55, 43]. Furthermore, the K-Star system has proven to be incredibly effective in detecting credit card fraud; in one research, it achieved 100% classification accuracy [47].

Financial fraud prevention involves more than just technological fixes; it also involves larger ethical and societal issues. It is concerning that fraud has becoming more commonplace; research has shown that certain Nigerian hip-hop songs dehumanize victims, justify fraud, and exalt fraudulent activity, all of which contribute to narratives that minimize the victims' pains [49].

The regulatory and ethical implications of using advanced AI models, particularly LLMs, are paramount. The transparent, responsible, and ethical application of these technologies is essential, along with upholding the Consumer Duty to ensure fair treatment and protection against fraudulent activities [50, 19, 20]. The battle is described as an "arms race" between fraudsters and defenders. Consequently, collaboration among organizations, governments, and international bodies is vital for establishing robust ethical and legal frameworks to mitigate AI-related financial crimes [45, 10, 21, 26, 48, 49].

The paper focuses on a comparison of several anomaly detection models with the LSTM anomaly detection model, aiming to determine which model is more effective among these models using the same dataset and comparing their performance metrics in detecting and preventing fraud and financial crime in the financial industry.

3. Research Methodology

The dataset, originating from a financial institution, contains bank transactions with a target indicating fraudulent (1) or normal (0) transactions, making it suitable for supervised learning. However, the study adapts it for unsupervised learning.

Key data preparation steps include:

- Checking for and handling missing values.
- Dropping attributes with only one unique entry.
- Transforming categorical variables into numerical values.
- Addressing data imbalance (a common issue in fraud datasets) by oversampling with SMOTE (Synthetic Minority Oversampling Technique) to prevent under-fitting and overfitting before splitting the dataset.
- Merging 'transaction date' and 'transaction time' into a 'timestamp' field.

For unsupervised learning, a 200,000-data-point dataset with 24 attributes, named ‘Bank Transaction_ Fraud.csv’, was used to train the deep learning model.

The core of the system is an LSTM anomaly detection model trained on time-series data 'Bank Transaction_ Fraud_Detection.csv'.

- **Training Phase:** The first half of a time-series sequence is used as "normal" data for training an LSTM model. The data is pre-processed into rolling windows, where the LSTM predicts the Tth time step value using the previous T-1 steps.
- **Prediction and Error Calculation**: The trained LSTM predicts values across the entire time series (both training and testing halves). The Mean Absolute Error (MAE) is calculated between predicted and actual outputs.
- **Anomaly Thresholding:** A threshold for prediction error is set using the 95th percentile (top 5%) of the training prediction errors. Any error exceeding this boundary is flagged as an anomaly.
- **Anomaly Detection**: This established threshold is then applied to the testing data. Errors in the testing set higher than this threshold are classified as anomalies.

This unsupervised approach works because training only on "normal" data teaches the model to recognize typical patterns. When it encounters an anomaly in unseen data, its prediction will significantly deviate, resulting in a high error that crosses the predefined threshold.

Software Environment and Libraries:

The project utilizes Python 3.12.4 (Anaconda distribution) and several key libraries:

- Pandas for data manipulation.
- Scikit-learn for machine learning and pre-processing.
- NumPy for numerical computations.
- TensorFlow 2.19.0 for deep learning.
- Additional libraries like Statsmodels, Seaborn, Plotly, SciPy, Keras, and Matplotlib for data analysis.

The studies also emphasize rigorous processing of real-world, imperfect data, including handling missing values, outliers, and incorrect entries. [9]][51][52][46] [49] [31] [44] [53] [25] [29] [12].

Dataset Splitting and Model Evaluation

The data set is methodically separated into:

- Training Set (60-80%): Used for model learning.
- Testing Set (10-20%): For evaluating performance on unseen data (generalization ability).
- Validation Set (10-20%): An optional subset from the training split, used for experimentation, prototyping, and detecting overfitting during iterative model training. The model must never train on validation or test sets to ensure unbiased evaluation [9].

Machine Learning Paradigms

The machine learning paradigms are:

- **Supervised Learning:** Models (such as classification and regression) learn from labelled data.
- **Unsupervised Learning:** Models (such as Dimensionality Reduction and Clustering) identify patterns in unlabelled data.
- **Semi-supervised Learning:** Combining elements of supervised and unsupervised learning is known as semi-supervised learning. [9].

Model Evaluation Metrics

The importance of detailed model evaluation beyond simple accuracy is emphasized, especially for imbalanced datasets.

Loss Functions: Common loss functions include:

- For classification, use log loss or cross-entropy loss.
- For regression, the mean-squared error (MSE) is used.

Confusion Matrix: Provides a detailed view of performance by categorizing predictions into:

- True Positive (TP)
- False Positive (FP) (Type I error/false alarm)
- True Negative (TN)
- False Negative (FN) (Type II error/missed detection)

Key Classification Metrics:

• **Precision:** The percentage of expected positives that turn out to be actual positives.
• **Recall (Sensitivity):** The percentage of true positives that were accurately identified.
• **F1-measure (F1-Score):** The precision and recall harmonic means.
• **True Negative Rate (Specificity)**: The percentage of real negatives that are accurately detected.
• **Precision-Recall Trade-off and ROC AUC**: Talks about how to balance precision and recall, as well as how the Receiver Operating Characteristic (ROC) curve uses Area Under the Curve (AUC) to distinguish across classes overall.

Regression Metrics: Unlike classification, regression models predict continuous, real-valued outputs. The primary metrics measure the deviation between predicted and true values:

• The Mean Squared Error (MSE) is susceptible to anomalies.
• The Mean Absolute Error (MAE) is more resilient to anomalies.
• Mean Absolute Percentage Error (MAPE) is beneficial for data that is quite variable.

Overfitting and Bias-Variance Tradeoff

A model is said to be overfit when it performs poorly on unknown data (low bias, high variance) because it has learned the training data—including noise—too well. [41, 55, 9]. Underfitting happens when a model performs badly on both training and test data (high bias) because it is either too simplistic or not sufficiently trained. When performance is the same in both datasets, generalization is accomplished.

Preventing Overfitting and Enhancing Generalization

Strategies include:

- Loss Penalty (Regularization)
- Reducing Complexity
- Data Processing
- Hyperparameter Tuning (e.g., using Grid Search)
- Adding Training Data
- Validation Strategies: It is emphasized that models must never train on validation or test sets and that hold-out validation and K-Fold Cross-Validation are essential for avoiding overfitting, model selection, and hyperparameter tweaking.

Deep Learning Concepts and LSTM Implementation

The papers provide an overview of deep learning, focusing on Artificial Neurons, Activation Functions (Sigmoid, Tanh, ReLU, Softmax), Neural Network Structure (input, hidden, output layers), Forward and Backward Pass (Backpropagation), and the "Black Box" Problem of explainability. It also details Loss Functions (MSE, MAE, MAPE for regression; Binary/Categorical Cross-Entropy for classification) and Gradient Descent variants (SGD, Mini-batch, Batch) for optimizing parameters.

LSTMs (Long Short-Term Memory) were created to solve the problems of traditional RNNs (Recurrent Neural Networks). Unlike RNNs, which tend to remember everything and struggle with long sequences, LSTMs can selectively remember important information and forget what's irrelevant. This ability allows them to handle both short and long-term dependencies effectively.

The Gated Mechanism of LSTMs

LSTMs achieve their selective memory through a unique architecture featuring a cell and three types of gates that control the flow of information:

- **Forget Gate:** This gate decides what information to discard from the previous state.

- **Input Gate:** This gate determines how much new information to let into the current state.
- **Output Gate**: This gate controls what part of the cell's state gets passed on to the next hidden state.

By using these gates to control the information flow, LSTMs are able to avoid the vanishing gradient problem that hinders the training of RNNs. This selective approach makes their training process more efficient and stable. The gates use sigmoid and tanh activation functions to process information and determine which values to keep or discard.

The enhanced LSTM anomaly detection system has two main parts:

- **Offline Component:** This component trains an LSTM (Long Short-Term Memory) model to predict time-series data.
- **Online Component:** This component uses the trained LSTM model to detect anomalies. It does this by comparing the actual data with the values predicted by the model. If the difference between the measured and predicted values (the prediction error) exceeds a specific threshold, an anomaly is flagged.

A more precise LSTM model and a novel technique for determining the error threshold to efficiently detect anomalies are the system's two primary enhancements.

Table 2:1 Performance comparison of the different Anomaly Detection Algorithms on the Bank financial fraud dataset

Classifier	**Accuracy**	**Precision**	**Recall**	**F1- Score**
Isolation Forest	0.9045	0.0532	0.0532	0.0532
One-Class SVM for Anomaly Detection	0.9048	0.053	0.0526	0.0528
LSTM Anomaly Detection	0.949	0.0725	0.0052	0.0097
RRCF	0.9111	0.1148	0.1137	0.1142
Anomaly Detection	0.9472	0.05	0.0052	0.0094
RNN Anomaly Detection	0.9438	0.0424	0.006	0.0106

Anomaly Detection System Evaluation

The suggested anomaly detection system, utilizing the LSTM model, was rigorously evaluated:

- **Overall Anomaly Detection Performance:** The LSTM model was compared against four state-of-the-art methods (Isolation Forest, One-Class SVM for Anomaly Detection, Anomaly Detection, and RNN Anomaly Detection). It achieved a precision of 0.9490, a recall of 0.0052, and an F1-score of 0.0097. While its precision was slightly lower than "Anomaly Detection model" (0.05), its recall and F1-score were significantly higher than those of all other methods. This superior performance is attributed to its ability to utilize the time correlation of data and its adaptability.

- **LSTM Model Performance**: The LSTM model consistently showed the lowest error values across all metrics when compared to RNN and anomaly detection models. The LSTM model slightly outperformance as depicted in the comparison below (Figure 2-11).

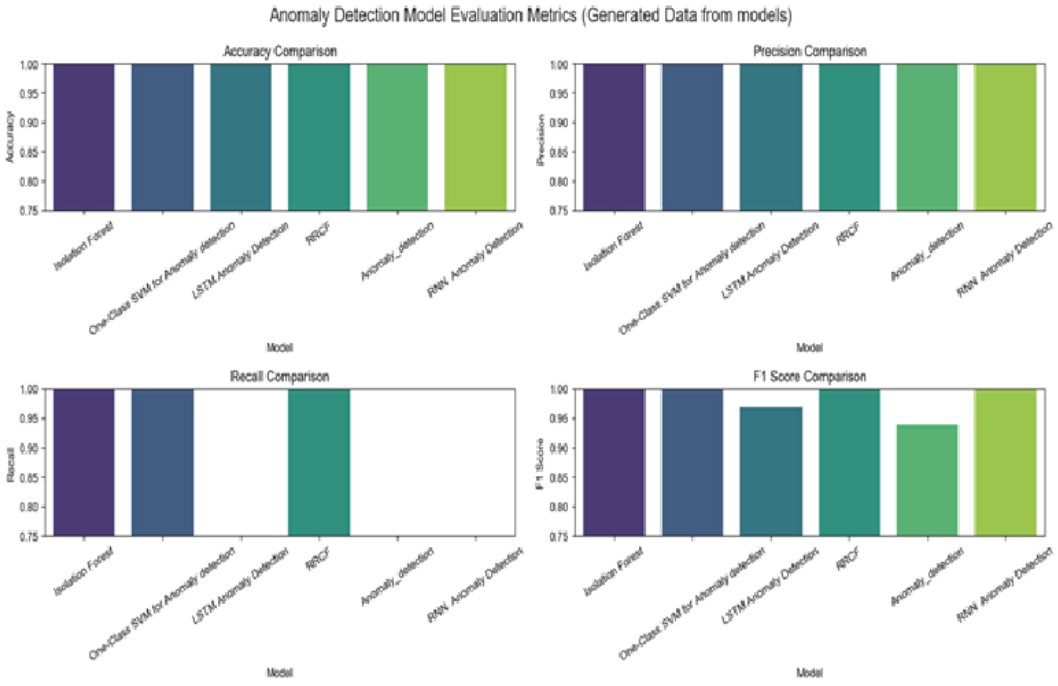

Figure 2-1: Comparison of the metrics of different models.

4. Results and Discussion

The evaluation of the anomaly detection system using three metrics: precision (Pr), recall (Re), and the F1-Score. Precision measures the system's ability to correctly identify anomalies without mistaking normal points for anomalies, while Recall measures its ability to detect anomalies without missing any. The F1-score combines both Precision and Recall to provide a comprehensive measure of overall performance.

The research paper presents several key findings across three main experiments:

- **Comparison with Other Methods:** The LSTM-Based Anomaly detection system was compared against four other state-of-the-art anomaly detection methods, including Isolation Forest, Robust Random Cut Forest, Twitter-AD, and autoencoders. The LSTM method outperformed all others in recall and F1-score, demonstrating a stronger ability to detect anomalies in time-series data. Although Twitter-AD had a slightly higher precision, the LSTM method's strengths in adaptability and handling time correlations make it more effective for complex financial fraud data.

LSTM Model Performance: The study introduces a LSTM model and compares it to Isolation Forest, RRCF, and RNN models. The LSTM model showed superior prediction performance with lower error metrics on the same dataset. This is attributed to the model responsive to the data, giving it better adaptability for varied data distributions.

5. Conclusions

This study successfully demonstrated the effectiveness of an unsupervised, LSTM-based anomaly detection model in identifying financial crimes within time-series transaction data. By leveraging the unique capabilities of LSTM networks, the proposed model efficiently learned normal behavioural patterns from unlabelled data, addressing a significant challenge in financial fraud detection, especially in the post-COVID-19 era. Our approach, which involves setting an error threshold based on the 95th percentile of prediction errors, proved to be a robust and adaptable method for flagging anomalous

transactions that deviate from the established norm. Our experimental findings demonstrate the LSTM-based system's superior performance over the other anomaly detection models used in the experiments, including RNN-based models, One-Class SVM, and Isolation Forest. While some alternatives might show slightly higher precision, our model's notable lead in recall and F1-score—the most critical metrics for imbalanced datasets like those found in financial fraud—confirms its enhanced ability to detect a higher percentage of actual fraud cases without excessive false negatives. The model's low error metrics further underscore its accuracy and reliability.

The research also reaffirms the dual nature of AI in the financial sector, where it is used by both criminals to perpetrate sophisticated fraud schemes (e.g., deepfakes and automated phishing) and by financial institutions to build a robust defence. According to these findings, a proactive, AI-driven approach is necessary to keep a competitive edge in this ongoing "arms race." While the proposed method is effective, future research could explore integrating other data types, such as unstructured text data from transaction descriptions, into the model to improve its contextual understanding. Additionally, investigating the integration of Explainable AI (XAI) techniques with our LSTM model would be beneficial. This would not only enhance trust in the system but also provide clear, justifiable reasons for flagging specific transactions, which is crucial for regulatory compliance and dispute resolution. Continued research on federated learning could also address data privacy concerns by allowing collaborative model training across institutions without direct data sharing.

Funding source

Authors are funded by UKRI Grant EP/W020408/1 and Grant RS718 through Doctoral Training Centre at Swansea University.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] D.B. Sholademi,"FINANCIAL CRIME IN THE AGE OF AI: DEEP FAKES AND IDENTITY THEFT RISKS". International Research Journal of Modernization in Engineering Technology and Science, Volume: 06/Issue: 12/December-2024 Impact Factor- 8.187 www.irjmets.com

[2] S. Liao, C. Liu, Y. Xia, H. Tu,"Similaritycheck-Time series anomaly detection based on GAN-VAE, Data Science and Informetrics" (2025), doi: https://doi.org/10.1016/j.dsim.2025.02.002

[3] K. Bukovski,J. Cooper,D.Basu,S. Steria,"Enhancing Financial Crime Detection By Implementing End-to-end AI Frameworks". ISSN: 3033-4136. 2024. DOI: https://doi.org/10.17868/strath.00091081

[4] Stop Scams UK (2023), "Impact of Artificial intelligence on Fraud and scams", https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf

[5] N. M. Hussien, and Y.M. Mohialden,"An Overview of Fraud Applications and Software on Social Media," in A. J. Obaid,G. H. Abdul-Majeed,A. Burlea-Schiopoiu,P. Aggarwal, (editors) advanced practical approaches to Deepfake Detection and Applications.Published in the United States of America by IGI Global (an imprint of IGIGlobal) 701 E. Chocolate Avenue Hershey PA 17033 Tel: 717-533-8845Fax: 717-533-8661 E-mail: cust@igi-global.com Web site: http://www.igiglobal.com/reference. Published 2023.

[6] R. PATIL, S. BOIT, V. GUDIVADA, J. NANDIGAM,"A Survey of Text Representation and Embedding Techniques in NLP". Digital Object Identifier 10.1109/ACCESS.2023.3266377

[7] R. B. Marqas, A. Mousa, and F. ¨Ozyurt, “Innovative hybrid deep learning models for financial sentiment analysis,” Acadlore Trans. Mach. Learn., vol. 3, no. 4, pp. 225–236, 2024. https://doi.org/10.56578/ataiml030404.

[8] Z. Miao,"Financial Fraud Detection and Prevention: Automated Approach Based on Deep Learning”. Journal of Organizational and End User Computing Volume 36 • Issue 1 • January-December 2024

[9] S.K. Adari, and S. Alla,"Beginning Anomaly Detection Using Python-Based Deep Learning: Implement Anomaly Detection Applications with Keras and PyTorch, Second Edition". ISBN-13 (pbk): 979-8-8688-0007-8 ISBN-13 (electronic): 979-8-8688-0008-5 https://doi.org/10.1007/979-8-8688-0008-5. Published 2024.

[10] B. V. Vishwas and A. Patel, "Hands-on Time Series Analysis with Python: From Basics to Bleeding Edge Techniques".ISBN-13 (pbk): 978-1-4842-5991-7 ISBN-13 (electronic): 978-1-4842-5992-4 https://doi.org/10.1007/978-1-4842-5992-4

[11] A. Bl´azquez-Garc´ıa,A. Conde,U. Mori,J. A.Lozano,(2020),"A review on outlier/anomaly detection in time series data". Tue, 11 Feb 2020 07:25:45 UTC. https://arxiv.org/abs/2002.04236

[12] Z. Zulfiqar,S.U.R. Malik ,S.A. Moqurrab,Z. Zulfiqar,U. Yaseen,G. Srivastava, "DeepDetect: An innovative hybrid deep learning framework for anomaly detection in IoT networks". Elsevier, Journal of Computational Science,https://doi.org/10.1016/j.jocs.2024.102426

[13] G. Verze,"Anomaly Detection in Multivariate Time Series: Comparison of Selected Inference Models and Threshold Definition Methods". 2022. Politecnico ilano 1863. https://www.politesi.polimi.it/retrieve/d8b79654-d4b2-49f1-9137-c27811effdac/2023_05_Verze_01.pdf

[14] G. Lee,Y. Yoon, K.Lee, "Anomaly Detection Using an Ensemble of Multi-Point LSTMs".Entropy 2023, 25, 1480. https://doi.org/10.3390/e25111480

[15] Y. Lu , X. Jin,D. Liu,X. Zhang,G. Geng, "Anomaly Detection Using Multiscale C-LSTM for Univariate Time-Series". Hindawi Security and Communication Networks Volume 2023, Article ID 6597623, 12 pages https://doi.org/10.1155/2023/6597623

[16] M.H. Qais, S. Kewat, K.H. Loo, C.-M. Lai, A. Leung, "LSTM-Based Stacked Autoencodersfor Early Anomaly Detection in Induction Heating Systems". Mathematics 2023, 11, 3319. https://doi.org/10.3390/math11153319

[17] Z. Zhao, C. Xu, B. Li, “A LSTM-Based Anomaly Detection Model for Log Analysis".https://doi.org/10.1007/s11265-021-01644-4/ Published online: 5 February 2021.Journal of Signal Processing Systems (2021) 93:745-751

[18] S. Aggarwal, "LSTM based Anomaly Detection in Time Series for United States exports and imports" ,Online at https://mpra.ub.uni-muenchen.de/117149/MPRA Paper No. 117149, posted 26 Apr 2023 00:12 UTC

[19] M. A. Bashar, R. Nayak, "ALGAN: Time Series Anomaly Detection with Adjusted-LSTM GAN", International Journal of Data Science and Analytics.https://doi.org/10.1007/s41060-025-00810-2 .2025

[20] Y. Lu, X. Jin, J. Chen, D. Liu, G. Geng, "F-SE-LSTM: A Time Series Anomaly Detection Method with Frequency Domain Information".arXiv:2412.02474v1 [cs.AI] 3 Dec 2024

[21] Y. Wang, X. Du, Z. Lu, Q. Duan and J. Wu, "Improved LSTM-Based Time-Series Anomaly Detection in Rail Transit Operation Environments," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9027-9036, Dec. 2022, doi: 10.1109/TII.2022.3164087.

[22] O. Ndama, I. Bensassi, E. M. En-Naimi,"Innovative credit card fraud detection: a hybrid model combining artificial neural networks and support vector machines".IAES International Journal of Artificial Intelligence (IJ-AI). Vol. 13, No. 3, September 2024, pp. 2674~2682. ISSN: 2252-8938, DOI: 10.11591/ijai.v13.i3.pp2674-2682

[23] K. CHOI, J. YI, C. PARK, S. YOON,"Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines". DOI 10.1109/ACCESS.2021.3107975,IEEE Access

[24] Z. Niu, K. Yu, X. Wu, "LSTM-Based VAE-GAN for Time-Series Anomaly Detection". 2020. https://doi.org/10.3390/s20133738

[25] V. M. Sudhakar, "LLM for Financial Services: Risk Analysis and Fraud Detection".Appl. Sci. Eng. J. Adv.Res.2025; 4(1):65-70.

[26] D. Vallarino,"AI-Powered Fraud Detection in Financial Services: GNN, Compliance Challenges, and Risk Mitigation" (March 07, 2025). Available at SSRN: https://ssrn.com/abstract=5170054 or http://dx.doi.org/10.2139/ssrn.5170054

[27] S. Jena, D. Rajput, T. Pathak, "Fraud Detection – A Hybrid Machine Learning Approach". International Journal of Scientific Research in Computer Science, Engineering and Information Technology.2025. 11. 3463-3470. 10.32628/CSEIT25112825.

[28] H. Kumar and V. Saxena,"Software Defect Prediction Using Hybrid Machine Learning Techniques: A Comparative Study". Journal of Software Engineering and Applications, 17, 155-171. Doi: 10.4236/jsea.2024.174009.

[29] O. A. Bello, A. Folorunso, O.E.Ejiofor, F.Z.Budale, K. Adebayo, and O.A.Babatunde , "Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions", International Journal of Management Technology, Vol.10, No 1, pp.85-109. 2023. Doi: https://doi.org/10.37745/ijmt.2013/vol10n185109.

[30] L.H. Aros, L. X. B. Molano, F. Gutierrez-Portela, J.J.M. Hernandez, M.B.R Barrero,"Financial fraud detection through the application of machine learning techniques": a literature review. Humanities and Social Sciences Communications, 2024. https://doi.org/10.1057/s41599-024-03606-0

[31] ISMG, "Fighting Fraud and Financial Crime - Assessing the impact of AI and other change Agents",902 Carnegie Centre • Princeton, NJ • 08540 • www.ismg.io. 2023

[32] Y. N. FENTAHUN,"DETECTION OF SUSPICIOUS CUSTOMERS ALGORITHM ON ANTI-MONEY LAUNDERING (AML) IN ETHIOPIAN BANKS". ST. MARY'S UNIVERSITY SCHOOL OF GRADUATE STUDIES. http://repository.smuc.edu.et/handle/123456789/6918. (2021),

[33] D.K. Snehansh Devera Konda,"The Integration of Large Language Models in Financial Services: From Fraud Detection to Generative AI Applications". International Journal of Scientific Research in Computer Science, Engineering and Information Technology ISSN: 2456-3307. Available Online at: www.ijsrcseit.com. doi: https://doi.org/10.32628/CSEIT241061208 Volume 10, Issue 6, November-December-2024 | http://ijsrcseit.com

[34] V. K. Parimala, "Anomaly Detection – Recent Advances, AI and ML Perspectives and Applications" in V. K. Parimala, and A. Engelbrecht(2024), Anomaly Detection - Recent Advances, AI and ML perspectives and Applications. Published 2023.

[35] B. Mohanty, M.S. Aashima, "Role of artificial intelligence in financial fraud detection". Academy of Marketing Studies Journal, 27(S4), 1-15, 2023

[36] D. Senegal, "The reign of botnets - Defending against Abuses, bots and fraud on the internet", published by John Wiley & Sons, Inc., Hoboken, New Jersey.2024. ISBNs: 9781394262410 paperback), 9781394262427 (ePDF), 9781394262434 (ePub)

[37] K. MISHEV, A. GJORGJEVIKJ, I. VODENSKA, L.T. CHITKUSHEV D. TRAJANOV, "Evaluation of Sentiment Analysis in Finance: From Lexicons to Transformers". IEEE Access. Digital Object Identifier 10.1109/ACCESS.2020.3009626

[38] A. J. Obaid, B. Bhushan, M. S. PdI, S. S. Rajest, "Advanced Applications of Generative AI and Natural Language Processing Models". IGI Global book series Advances in Computational Intelligence and Robotics (ACIR) (ISSN: 2327-0411; eISSN: 2327-042X). Published 2024.

[39] K. Raza, N. Ahmad, D. Singh (eds.), Generative AI: Current Trends and Applications, Studies in Computational Intelligence 1177, https://doi.org/10.1007/978-981-97-8460-8_2. https://link.springer.com/book/10.1007/978-981-97-8460-8

[40] A. Zaremba, and E. Demir, "ChatGPT: Unlocking the future of NLP in finance". Modern Finance, 2023, Vol 1, No. 1, pp. 93-98. https://doi.org/10.61351/mf.v1i1.43

[41] G. Saporta, and S. Maraney, "Practical Fraud Prevention - Fraud and AML Analytics for Fintech and eCommerce, Using SQL and Python", Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. 2022

[42] C. Wang, "Overview of Digital Finance Anti-fraud in Anti-Fraud Engineering for Digital Finance Cheng Wang Behavioural Modelling Paradigm" 2023. .ISBN 978-981-99-5256-4 ISBN 978-981-99- 5257-1 (eBook) https://doi.org/10.1007/978-981-99-5257-1

[43] A. Churchill, and J. Jee, "Data sharing to prevent Economic Crime: Why you can now share data with confidence". 2024. The payment association, www.thepaymentsassociation.org

[44] J. Jee,"Financial Crime, Payment Fraud and the Role of Digital Identity", Emerging Payments Association.2021. https://www.emergingpayments.org/portfolio/project-financial-crime/

[45] T. Tanchangya, K. Naher, M.B. Mia, S. Chowdhury, N. Islam, "Assessing the impact of financial technology: Is it a curse or blessing for financial crimes in financial institutions?" Financial Risk and Management Reviews 2025 Vol. 11, No. 1, pp. 1-36,ISSN(e): 2411-6408,ISSN(p): 2412-3404' DOI: 10.18488/ 89.v11i1.4075

[46] INTERPOL, https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf

[47] E.G. Dada,T.Mapayi, O.M Ilaifa,P. A. Owolabi, "Credit Card Fraud Detection using k-star Machine Learning Algorithm",3rd Biennial Conference on Transition From Observation To Knowledge To Intelligence (TOKI 2019),held from August 15 to 16 in University of Lagos, Nigeria.

[48] A. B. NASSIF, M. A. TALIB, Q.D. NASIR, M. FATIMA, "Machine Learning for Anomaly Detection: A Systematic Review". IEEE Access, Digital Object Identifier 10.1109/ACCESS.2021.3083060. (2021)

[49] S. Lazarus, O. Olaigbe, A. Adeduntan,E.T. Dibiana,U. O. Geoffrey, "Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps".Journal of Economic Criminology journal homepage: www.journals.elsevier.com/journal-of-economic-criminology. 2023

[50] G. Boskou,E. Chatzipetrou,E. Tiakas,E.Kirkos,C. Spathis,"Exploring the Boundaries of Financial Statement Fraud Detection with Large Language Models", (May 27, 2024). Available at SSRN: https://ssrn.com/abstract=4842962 or http://dx.doi.org/10.2139/ssrn.4842962

[51] G.S.N. Malleswari,P. Manikanta,R. V. Lavanya,A. Avinash,U.G. Tarak,"TIME SERIES ANALYSIS USING PYTHON".International Journal of Techno-Engineering, ISSN: 2057-5688. 2024

[52] M. Azib, B. Renard,P.Garnier,V. Génot, N. André,M. Bouchemit, Myriam, "A Python Package for Time Series Event Detection". https://indico.cern.ch/event/1283970/contributions/5554338/attachments/2722833/4730953/Menouar%20Azib%20-%20EventDetector%20A%20Python%20Package%20for%20Time%20Series%20Event%20Detection.pdf

[53] D. Perera, M. Rajaratne, Maneesha, D. Sandaruwan, and N. Kodikara, "Fraud Detection in a Financial Payment System". 10.1007/978-3-030-55307-4_79. Published 2021.