**IAES International Journal of Artificial Intelligence (IJ-AI)**
Vol. 15, No. 1, February 2026, pp. 788~797
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i1.pp788-797 

# A novel BERT-long short-term memory hybrid model for effective credit card fraud detection

**Oussama Ndama[1], Safae Ndama[1], Ismail Bensassi[1,2], El Mokhtar En-Naimi[1]**
[1]DSAI2S Research Team, C3S Laboratory, Faculty of Sciences and Techniques of Tangier, Abdelmalek Essaâdi University, Tetouan, Morocco
[2]Department of Computer Science, Faculty of Sciences of Rabat, Mohammed V University, Rabat, Morocco

**Article Info**

***Article history:***

Received Sep 1, 2024
Revised Dec 21, 2025
Accepted Jan 10, 2026

***Keywords:***

BERT-LSTM hybrid
Credit card fraud detection
Financial security
Hybrid models
Natural language processing
Sequence analysis

**ABSTRACT**

In the rapidly evolving landscape of financial transactions, the detection of fraudulent activities remains a critical challenge for financial institutions worldwide. This study introduces a novel bidirectional encoder representation from transformers (BERT)–long short-term memory (LSTM) hybrid model that integrates both textual and numerical data to enhance credit card fraud detection. Leveraging BERT for deep contextual embeddings and LSTM for sequence analysis, the model provides a comprehensive approach that surpasses traditional fraud detection systems primarily based on numerical analysis. On the validation set, the model achieved a recall of 100% and an accuracy of 99.11%, highlighting strong effectiveness in identifying fraudulent transactions under class imbalance. Through rigorous evaluation, the model demonstrated exceptional accuracy and reliability, promising improvements in fraud detection and mitigation. This paper details the development and validation of the hybrid model, emphasizing its use of mixed data types to capture complex patterns in transaction data. The results indicate a new frontier in fraud detection by combining natural language processing (NLP) and sequential data analysis to create a robust solution for real-world applications, supporting the security and integrity of financial systems globally.



***Corresponding Author:***

Oussama Ndama
DSAI2S Research Team, C3S Laboratory, Faculty of Sciences and Techniques of Tangier
Abdelmalek Essaâdi University
Tetouan, Morocco
Email: oussama.ndama@etu.uae.ac.ma

## 1. INTRODUCTION

As the digital age progresses, credit card transactions have increasingly become central to daily commerce, promoting convenience and efficiency across global markets. With millions of transactions occurring every minute, the financial ecosystem heavily depends on the trust and security associated with these interactions [1]. However, this surge in online transactions has also led to a marked increase in fraudulent activities. Credit card fraud not only inflicts substantial financial losses on consumers and financial institutions but also erodes trust in the payment system, presenting a formidable threat to the global economy [2]. Detecting fraudulent transactions is a complex and challenging task due to the dynamic and evolving nature of fraud strategies [3]. Fraudsters continuously adapt and employ sophisticated techniques to bypass traditional security measures [4], [5]. Consequently, there is a pressing need for advanced and adaptive fraud detection systems that can effectively identify and mitigate fraudulent activities in real-time.

Recent advancements in machine learning (ML) and artificial intelligence (AI) have opened new avenues for developisng sophisticated models capable of identifying subtle patterns and anomalies indicative of fraud. These models leverage vast amounts of transactional data to learn and predict fraudulent behavior with high accuracy. However, the availability and quality of real transactional data for training these models are often limited due to privacy concerns, regulatory restrictions, and the inherent sensitivity of financial data [6], [7].

To address these limitations, researchers have turned to simulated datasets, which can mimic the complexity and variability of real-world data without compromising individual privacy. Simulated datasets provide a controlled environment to test and validate ML models, offering valuable insights and enabling the development of more robust fraud detection systems. In this study, a simulated credit-card transaction dataset produced by the Sparkov data generation tool is employed [8]. A hybrid fraud-detection model is proposed that couples bidirectional encoder representation from transformers (BERT) for natural language processing (NLP) with long short-term memory (LSTM) networks for sequence modeling. BERT is used to encode textual fields, specifically merchant names and transaction categories, capturing rich contextual relationships [9], [10], while LSTM captures temporal dependencies present in transaction sequences [11], [12]. By integrating these components, the model leverages complementary textual and sequential signals to better detect complex fraud patterns and curb false positives.

The purpose of this paper is to present the development, implementation, and validation of our hybrid BERT-LSTM model for fraud detection. The model's effectiveness will be demonstrated using the simulated dataset, showcasing its potential to significantly improve fraud detection rates. Additionally, the implications of our findings, the strengths and limitations of our approach, and potential avenues for future research in this critical domain will be discussed.

## 2. RELATED WORKS

### 2.1. Traditional machine learning and imbalance handling

Addressing imbalance remains central to fraud detection. Breskuvienė and Dzemyda [13] propose feature importance–driven (FID) self-organizing maps (SOM), a SOM-based feature selection tailored to skewed data, aligning well with modern tree/boosting pipelines. Chung and Lee [14] emphasize recall via a lightweight k-nearest neighbors (KNN), linear discriminant analysis (LDA)-linear regression ensemble with simple rule logic to favor minority detection. Afriyie *et al.* [15] reaffirm the practicality of classical baselines under undersampling, notably random forest. Our work complements these directions by introducing a unified text–numeric fusion (BERT embeddings plus amount) within a single end-to-end model.

### 2.2. Deep sequence models

Sequence-aware methods capture temporal regularities in transaction streams. Forough and Momtazi [16] cast fraud detection as sequence labeling via LSTM conditional random field (CRF) stack, outperforming LSTM, gated recurrent unit (GRU), and artificial neural network (ANN) baselines and introducing a sequence-aware undersampling method (Seq-US) that preserves pre-fraud context. Complementarily, Boulieris *et al.* [17] integrate explainable AI with LSTM architectures to enhance transparency, while Mienye and Jere [18] survey convolutional neural network (CNN), recurrent neural network (RNN), LSTM, and GRU advances that model complex sequential patterns. Extending beyond purely sequential views, Cherif *et al.* [19] employ an encoder–decoder graph neural network on large Sparkov data to exploit customer–merchant relations, using a graph converter and batch normalization to stabilize training and reporting gains in precision, recall, F1-score, and receiver operating characteristic (ROC); they further underscore geospatial merchant–customer distance as an informative signal for fraud.

### 2.3. Transformer-based and hybrid models

Recent work combines transformer representations with other learners. Ileberi and Sun [20] present a stacking ensemble (CNN, LSTM, Transformer) with an extreme gradient boosting (XGBoost) meta-learner, achieving high sensitivity, specificity, and area under the curve (AUC) on European and Taiwan datasets. Hewapathirana *et al.* [21] investigate TabBERT for transactional dependencies, and NLP-centric lines by [22], [23] leverage language technologies (including chatbots) to detect or mitigate fraud.

Most hybrid systems are compute-heavy and either convert text fields into purely numeric surrogates or fuse modalities only at the score level. Our novelty is a single-branch, representation-level fusion that preserves the NLP signal by using contextual BERT embeddings of merchant and category, and integrates this with the numeric amount in one end-to-end (BERT→fusion→LSTM) architecture rather than flattening everything into numeric. This preserves modality-specific information and avoids heavy stacking, which distinguishes our approach from prior work that homogenizes all inputs into numeric vectors.

## 3. METHOD

This section details the data sources, preprocessing steps, and the methodologies employed in developing the credit card fraud detection model. The dataset is first described, followed by the preprocessing techniques applied to prepare the data for modeling. Subsequently, the implementation details are outlined, including the algorithms used and the architecture of proposed BERT-LSTM hybrid model. Figure 1 illustrates the hybrid model architecture diagram, which visually represents all the steps followed to build the model and provides a framework for the discussions in this section.

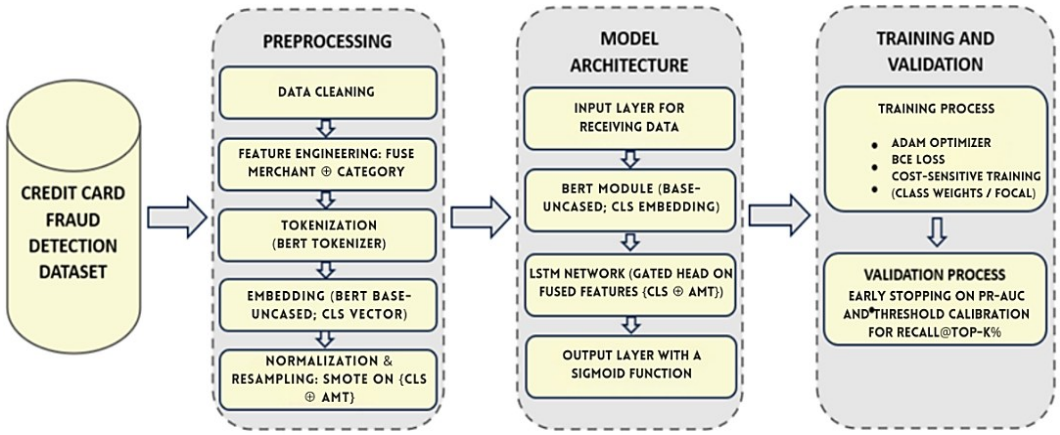



Figure 1. The architecture diagram of the BERT-LSTM hybrid model for credit card fraud detection

### 3.1. Dataset

The dataset used in this study is a simulated credit card transaction dataset generated using the Sparkov Data Generation tool. It contains transactions from 1,000 customers and 800 merchants, spanning the period from January 1, 2019 to December 31, 2020 with a total of 1,296,675 records. The dataset includes both legitimate and fraudulent transactions, with features such as transaction amount, merchant name, category, and a binary fraud label indicating whether a transaction is fraudulent, the features in the dataset are as presented in Table 1.

This diverse set of features provides a rich context for each transaction, capturing not only transactional details but also demographic and spatial information about both cardholders and merchants. By combining textual, categorical, and numeric attributes, the dataset enables interactions that reveal subtle patterns associated with fraud. This richness allows for comprehensive analysis and more robust modeling of fraudulent behavior.

Table 1. Dataset features

| Feature | Description | Type |
|---|---|---|
| trans_date_trans_time | The date and time of the transaction | object |
| cc_num | The credit card number used in the transaction | int64 |
| merchant | The name of the merchant where the transaction occurred | object |
| category | The category of the merchant | object |
| amt | The amount of the transaction | float64 |
| first | The first name of the cardholder | object |
| last | The last name of the cardholder | object |
| gender | The gender of the cardholder | object |
| street | The street address of the cardholder | object |
| city | The city of the cardholder | object |
| state | The state of the cardholder | object |
| zip | The ZIP code of the cardholder | int64 |
| lat | The latitude of the cardholder's location | float64 |
| long | The longitude of the cardholder's location | float64 |
| city_pop | The population of the city where the cardholder resides | int64 |
| job | The occupation of the cardholder | object |
| dob | The date of birth of the cardholder | object |
| trans_num | The transaction number | object |
| unix_time | The transaction time in Unix time format | int64 |
| merch_lat | The latitude of the merchant's location | float64 |
| merch_long | The longitude of the merchant's location | float64 |
| is_fraud | A binary label indicating whether the transaction is fraudulent | int64 |

### 3.2. Preprocessing

Dataset preprocessing is a crucial step in preparing the data for model training. The preprocessing steps for this study include:

i) Data sampling: the original dataset contains 1,296,675 records, which can be computationally intensive to process. To balance computational efficiency with model performance, a random sample of 100,000 records was selected for analysis. This sampling ensures that the subset of data retains the overall characteristics and distribution of the entire dataset, facilitating effective model training and evaluation. From this sampled data, only the relevant columns 'merchant', 'category', 'amt', and 'is_fraud' were selected. This step focused the analysis on the features directly pertinent to detecting fraudulent transactions, simplifying the dataset, and enhancing computational efficiency.

ii) Handling missing values: any missing values in the dataset were handled using appropriate imputation techniques to maintain data integrity [24]. This step ensures that the dataset is complete and suitable for model training without introducing bias or inaccuracies.

iii) Feature engineering: to enhance the model's performance, additional features were engineered from the existing data. The goal of feature engineering is to create new input features that can improve the predictive power of the model [25], [26]. In this study, textual features such as 'merchant' and 'category' were combined to create a single, enriched textual input. This combined feature encapsulates the identity of the merchant and the type of transaction, providing a richer context for the model. By merging these two columns, we aim to capture the relationship between where the transaction took place and what kind of transaction it was, which can be crucial for identifying fraud patterns. This new textual feature was then prepared for further processing and embedding.

iv) Tokenization and embedding: the combined textual features were tokenized and embedded using the BERT tokenizer and model [27]. Tokenization is the process of converting text into smaller units called tokens [28]. The BERT tokenizer breaks down the combined textual input into tokens and maps each token to a unique numerical identifier, creating token IDs. These token IDs are then fed into the BERT model, which generates numerical embeddings for each token. BERT embeddings are contextually rich vector representations that capture the semantic meaning and relationships within the text [29]. This process transforms the textual data into a format that the model can effectively use, allowing it to understand and leverage the contextual nuances of the input text.

v) Combining features: the generated text embeddings were combined with the numerical feature, transaction amount (amt). This step integrates the contextually rich textual information with the quantitative data, forming a comprehensive feature set for each transaction. The combination of textual and numerical data allows the model to consider both the semantic context of the transaction and its monetary value. By merging these diverse features, the model gains a holistic view of each transaction, enhancing its ability to identify fraudulent activities based on both the nature of the transaction and its financial attributes.

vi) Class imbalance handling: the dataset exhibited class imbalance, with fraudulent transactions being significantly fewer than legitimate ones. Fraudulent records represent approximately 0.60% of the entire dataset. Class imbalance can negatively impact the model's performance, as it may become biased towards the majority class (legitimate transactions) and fail to detect fraudulent ones. To address this issue, the synthetic minority over-sampling technique (SMOTE) was applied. SMOTE generates synthetic samples for the minority class (fraudulent transactions) by interpolating between existing minority class samples [30]. This technique ensures a balanced representation of both classes during model training, enabling the model to learn and detect fraudulent transactions more effectively [31]. By addressing class imbalance, the model's sensitivity to fraudulent activities is improved, and the likelihood of false negatives is reduced.

These preprocessing steps prepare the dataset for effective model training. By consolidating relevant features, generating BERT-ready text embeddings, and correcting class imbalance, they improve signal quality and stability. Consequently, the model learns more robustly and detects fraudulent transactions with higher accuracy.

### 3.3. Details of implementation

The implementation of our BERT-LSTM hybrid model for credit card fraud detection was carried out on Google Colab, utilizing the powerful NVIDIA A100 graphics processing unit (GPU) to meet the computational needs of deep learning. Python served as the primary language, supported by libraries such as Pandas and NumPy for data processing, PyTorch for model development, and Hugging Face's transformers library for efficient handling of textual data with BERT. Scikit-learn was used for data splitting and evaluation, while imbalanced-learn and SMOTE addressed class imbalance. This setup ensured efficient, effective model development, leveraging state-of-the-art tools for large-scale data and deep learning.

### 3.4. Algorithms

The development of the credit card fraud detection model employed two main algorithms: BERT and LSTM. Each of these algorithms plays a critical role in handling different aspects of the dataset and modeling challenges. BERT encodes contextual semantics from merchant and category text, whereas LSTM captures temporal dependencies across transactions, allowing the hybrid to address complementary facets of fraud detection.

#### 3.4.1. Bidirectional encoder representations from transformers

The BERT, developed by Google, is a groundbreaking model in the field of NLP. It uses a mechanism known as transformers to understand the context of a word within a text, rather than just the word in isolation [32]. This ability makes BERT extremely effective for tasks that rely on the contextual use of words, such as sentiment analysis, named entity recognition, and in our case, processing and understanding textual data related to transactions [33]. In this project, BERT was utilized to process textual features such as merchant names and transaction categories. By transforming these textual inputs into embedded vectors, BERT provided a nuanced representation of the text, capturing subtle meanings that could indicate fraudulent activity. The embeddings generated by BERT serve as a sophisticated input to the subsequent stages of the model, enhancing its ability to discern patterns indicative of fraud.

#### 3.4.2. Long short-term memory

The LSTM networks are a type of RNN specifically designed to handle sequence prediction problems [34]. LSTMs are capable of learning long-term dependencies in sequence data, which is crucial for applications like time-series analysis, speech recognition, and importantly, transaction sequence analysis [35]. In the context of credit card fraud detection, LSTM networks were employed to analyze the sequences of transactions, considering the temporal relationships and patterns that emerge over time. By integrating LSTM with BERT embeddings, the model could effectively leverage both the contextual and sequential information in the dataset. This integration allows the LSTM to interpret the embedded text in the context of transaction sequences, enhancing its ability to predict fraudulent transactions based on behavioral patterns that unfold over time. Together, BERT and LSTM form a powerful combination for tackling the complexities of fraud detection in transaction data. BERT's deep understanding of textual context, coupled with LSTM's proficiency in sequence modeling, provides a comprehensive approach to identifying fraudulent activities with higher accuracy and efficiency.

## 4. THE PROPOSED BERT-LSTM HYBRID MODEL

In this study, a hybrid model was developed that combines the strengths of BERT and LSTM to enhance credit card fraud detection capabilities. This section details the model architecture and the training and validation methodologies used to construct and deploy the system effectively. It also highlights the design choices that distinguish our approach, preserving token-level BERT representations for LSTM-based sequence modeling and mitigating class imbalance.

### 4.1. Model architecture

The BERT–LSTM hybrid model leverages BERT to produce deep contextual embeddings from textual inputs, while LSTM captures temporal dependencies to analyze transaction patterns over time. These fusion preserves token-level semantics and sequential dynamics, enabling the detector to exploit complementary cues for fraud identification, especially under class imbalance. At a high level, the pipeline proceeds through text feature processing, sequence modeling, and final integration and classification.

#### 4.1.1. Text feature processing

For each transaction, the two textual fields, merchant and category, are concatenated into a single input string. This text is tokenized with the standard BERT tokenizer and passed through the BERT encoder. The [CLS] token embedding is used as a fixed-length representation of the transaction text, capturing contextual information about the merchant and the purchase type in a 768-dimensional vector.

#### 4.1.2. Sequence modeling

The [CLS] embedding is concatenated with the transaction amount (amt), yielding a 769-dimensional feature vector. This vector is presented to an LSTM layer as a single-step sequence (sequence length=1), which functions as a gated projection that can model nonlinear interactions between textual context and amount. Although no temporal sequence across tokens or transactions is used in the current implementation, the LSTM's gating still provides a learnable transformation that can improve

separability relative to a purely linear head. This single-step design is justified by our per-transaction screening objective and the absence of reliable, session-level ordering across transactions, where fabricating windows could introduce spurious dynamics. It also keeps latency and parameter count low, which helps curb overfitting under class imbalance, while leaving a clear path to multi-step sequences when consistent inter-transaction ordering becomes available.

#### 4.1.3. Integration and output

The LSTM outputs a compact representation that integrates contextual meaning with temporal structure, which is subsequently fed to a fully connected classification head. A sigmoid activation maps the output to a probability of fraud, enabling threshold-based decision making aligned with operational risk preferences. This end-to-end design allows the model to combine nuanced text understanding with sequential pattern recognition in a single trainable pipeline.

### 4.2. Model construction and training methodologies

Constructing and training the BERT–LSTM hybrid model involved pragmatic choices to maximize performance under class imbalance while preserving generalization. A pre-trained BERT-base-uncased is fine-tuned to obtain domain-specific text embeddings and model token-level sequences with an LSTM. An imbalance-aware objective and a held-out validation split guide iterative refinements and early stopping.

#### 4.2.1. Pre-training, fine-tuning and sequential data handling

BERT is initialized with publicly available pre-trained weights to encode strong lexical and semantic priors. It is then fine-tuned on transaction text (merchant+category) so the embeddings adapt to domain-specific, fraud-relevant regularities. This two-stage transfer accelerates convergence, adds minimal extra parameters, and yields more discriminative representations for fraud cues.

The LSTM layer is trained on the token-level embeddings to model temporal dependencies within each textual sequence. By learning how meaning unfolds across tokens, the network exposes behaviorally relevant signals that static pooling might overlook. This sequential treatment complements the contextual power of BERT and supports higher recall on minority fraud cases.

#### 4.2.2. Hyperparameters and training settings

For the hybrid model, bert-base-uncased is used as a frozen text encoder, with tokenization configured for padding and truncation at the default maximum length. The fused representation concatenates the BERT [CLS] vector (768 dimensions) with the numeric amount to form a 769-dimensional input. The classifier head is a single-layer LSTM with hidden size 256, batch_first=True, unidirectional, and dropout set to 0, followed by a sigmoid output. Optimization uses Adam with a learning rate of 0.001 and binary cross-entropy loss. Training uses full-batch updates (batch size equal to the number of training examples) for 500 epochs, and evaluation is performed on an 80/20 random train-validation split. To address class imbalance, SMOTE is applied to the combined feature matrix before the split. Unless otherwise noted, metrics are computed at a decision threshold of 0.5.

#### 4.2.3. Validation and iterative improvement

Model development follows a held-out validation scheme to assess generalization to unseen data and guide early stopping. Standard metrics such as accuracy, precision, recall, and F1-score are monitored, and hyperparameters and architectural details are adjusted in response to validation trends. Iterative refinements focus on stabilizing training, improving minority-class sensitivity, and ensuring the pipeline remains robust under class imbalance.

## 5. RESULTS AND DISCUSSION

The BERT-LSTM hybrid model showcased outstanding performance on the validation set, achieving an accuracy of 99.11%. This high level of accuracy highlights the model's robust ability to classify transactions effectively. Precision was notably high at 98.27%, while the model achieved a perfect recall of 100%, indicating its success in identifying all fraudulent transactions within the dataset. The F1-score, balancing precision and recall, stood impressively at 99.13%. The following is a concise summary of the key performance metrics, as illustrated in Table 2.

The model also maintained a low validation loss of 0.0375, further validating its efficiency in fraud detection. This blend of high precision, recall, and accuracy underscores the model’s capabilities in effectively detecting fraud, positioning it as a potent tool in financial security systems. The classification report further details these results in Figure 2, providing a comprehensive breakdown of the model’s

performance across different classes. This visualization enhances understanding of the model's precision and recall by class, illustrating its balanced effectiveness in fraud detection.

Table 2. Performance metrics of the BERT-LSTM hybrid model

| Model | Accuracy |
|---|---|
| Accuracy | 0.9911 |
| Precision | 0.9827 |
| Recall | 1.0000 |
| F1 score | 0.9913 |

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Non-Fraud | 1.00 | 0.98 | 0.99 | 19758 |
| Fraud | 0.98 | 1.00 | 0.99 | 20003 |
| accuracy | | | 0.99 | 39761 |
| macro avg | 0.99 | 0.99 | 0.99 | 39761 |
| weighted avg | 0.99 | 0.99 | 0.99 | 39761 |

Validation Loss: 0.0375

Figure 2. Classification report of the BERT-LSTM hybrid model

The BERT-LSTM hybrid model effectively combines BERT's contextual embeddings with LSTM's sequence analysis capabilities, offering a robust approach to fraud detection. This model not only demonstrates strong statistical performance but also exhibits a deep understanding of complex transaction patterns essential for identifying fraudulent activities. Its high recall rate is crucial in a fraud detection context, ensuring no fraudulent transaction is missed, which could otherwise have severe financial implications. Additionally, the model's impressive precision minimizes false positives, thereby preserving customer trust and operational efficiency.

For external context, Table 3 contrasts our results with representative existing methods evaluated on the same dataset family. Relative to random forest baselines [13], [15], a lightweight classical ensemble [14], and an encoder-decoder GNN [19], the proposed BERT-LSTM fusion attains the highest F1-score and recall while preserving strong precision. These comparisons suggest that unifying textual merchant/category signals with numeric amount inside one model can be advantageous. Protocols and resampling strategies vary across studies, so the numbers are indicative rather than strictly comparable.

However, the model faces challenges, particularly with the adaptability to sophisticated or previously unseen fraud tactics as fraudsters continually evolve their strategies. To enhance its adaptability, future enhancements could include dynamic learning and updating mechanisms to better respond to new fraud patterns. Further research might also explore integrating additional data types such as customer behavior or macroeconomic indicators to boost the model's predictive power. Deploying this model in real-world financial systems would necessitate robust infrastructure for real-time analysis and seamless integration with existing monitoring frameworks, alongside ensuring compliance with stringent data privacy regulations and maintaining high data security standards.

Table 3. Comparison with existing methods (Sparkov dataset family)

| Model | Accuracy | Precision | Recall | F1 score |
|---|---|---|---|---|
| Our model (BERT-LSTM) | 0.9911 | 0.9827 | 1.0000 | 0.9913 |
| Random Forest [13] | - | - | - | 0.8350 |
| KNN, LDA, LR [14] | - | - | 0.9701 | - |
| Random forest [15] | 0.9600 | 0.0900 | 0.9700 | 0.1700 |
| Encoder-decoder GNN [19] | 0.9700 | 0.8200 | 0.9200 | 0.8600 |

## 6. CONCLUSION

The BERT-LSTM hybrid model developed in this study represents a significant step forward in credit card fraud detection by integrating both textual and numerical data. By combining BERT's deep contextual embeddings with LSTM's sequence analysis, the approach outperforms traditional models that only use numerical features, setting a new benchmark for handling heterogeneous data in fraud detection. However, the study is limited by its reliance on synthetic data, absence of true transaction sequences, and a narrow feature set (merchant, category, amount). To advance further, future work should test the model on

real transaction data with privacy safeguards, apply explainable AI methods like Shapley additive explanations (SHAP) and local interpretable model-agnostic explanations (LIME) for decision auditing, and experiment with transformer-based tabular models (e.g., TabTransformer and FT-Transformer) for richer input handling. Additionally, deploying a real-time streaming pipeline with model-drift monitoring will be crucial for maintaining robust and compliant performance as fraud tactics evolve. These directions are key for translating the approach into a reliable fraud detection solution in real-world financial systems.

## FUNDING INFORMATION

Authors state no funding involved.

## AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

| Name of Author | C | M | So | Va | Fo | I | R | D | O | E | Vi | Su | P | Fu |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Oussama Ndama | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Safae Ndama | ✓ | ✓ | | | | ✓ | | | | ✓ | | | | |
| Ismail Bensassi | | | | | | ✓ | | | | ✓ | | | | |
| El Mokhtar En-Naimi | | ✓ | | ✓ | | ✓ | | | | ✓ | | ✓ | ✓ | |

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

## CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

## DATA AVAILABILITY

The dataset used in this study is publicly available and obtained from a well-established repository. The data supporting the credit card fraud detection (CCFD) experiments are openly available on GitHub at: https://github.com/namebrandon/Sparkov_Data_Generation.

## REFERENCES

[1] H. M. Alzoubi, M. T. Alshurideh, B. A. Kurdi, K. M. K. Alhyasat, and T. M. Ghazal, "The effect of e-payment and online shopping on sales growth: evidence from banking industry," *International Journal of Data and Network Scienc*, vol. 6, no. 4, pp. 1369–1380, 2022, doi: 10.5267/j.ijdns.2022.5.014.

[2] M. H. U. Sharif and M. A. Mohammed, "A literature review of financial losses statistics for cyber security and future trend," *World Journal of Advanced Research and Reviews*, vol. 15, no. 1, pp. 138–156, Jul. 2022, doi: 10.30574/wjarr.2022.15.1.0573.

[3] O. A. Bello and K. Olufemi, "Artificial intelligence in fraud prevention: exploring techniques and applications challenges and opportunities," *Computer Science and Information Technology Research Journal*, vol. 5, no. 6, pp. 1505–1520, Jun. 2024, doi: 10.51594/csitrj.v5i6.1252.

[4] S. Cherniavskyi, V. Babanina, I. Vartyletska, and O. Mykytchyk, "Peculiarities of the economic crimes committed with the use of information technologies," *European Journal of Sustainable Development*, vol. 10, no. 1, Feb. 2021, doi: 10.14207/ejsd.2021.v10n1p420.

[5] J. Robinson and M. Edwards, "Fraudsters target the elderly: behavioural evidence from randomised controlled scam-baiting experiments," *Security Journal*, vol. 37, no. 4, pp. 1173–1196, Dec. 2024, doi: 10.1057/s41284-023-00410-4.

[6] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, "Data privacy and cybersecurity challenges in the digital transformation of the banking sector," *Computers & Security*, vol. 147, Dec. 2024, doi: 10.1016/j.cose.2024.104051.

[7] M. Canayaz, I. Kantorovitch, and R. Mihet, "Consumer privacy and value of consumer data," *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3986562.

[8] B. Harris, "GitHub - namebrandon/sparkov_data_generation: synthetic credit card transaction generator used in the sparkov program," *GitHub.* Accessed: Jun. 26, 2024. [Online]. Available: https://github.com/namebrandon/Sparkov_Data_Generation

[9] S. Singla, Priyanshu, A. Thakur, A. Swami, U. Sawarn, and P. Singla, "Advancements in natural language processing: BERT and transformer-based models for text understanding," in *2024 Second International Conference on Advanced Computing & Communication Technologies (ICACCTech)*, IEEE, Nov. 2024, pp. 372–379, doi: 10.1109/ICACCTech65084.2024.00068.

[10] A. Turchin, S. Masharsky, and M. Zitnik, "Comparison of BERT implementations for natural language processing of narrative medical documents," *Informatics in Medicine Unlocked*, vol. 36, 2023, doi: 10.1016/j.imu.2022.101139.

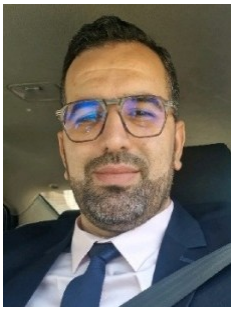
[11] S. Nosouhian, F. Nosouhian, and A. K. Khoshouei, "A review of recurrent neural network architecture for sequence learning: comparison between LSTM and GRU," *Preprints*, 2021, doi: 10.20944/preprints202107.0252.v1.

[12] Y. Chen and M. Du, "Financial fraud transaction prediction approach based on global enhanced GCN and bidirectional LSTM," *Computational Economics*, vol. 66, no. 2, pp. 1747–1766, Aug. 2025, doi: 10.1007/s10614-024-10791-2.
[13] D. Breskuvienė and G. Dzemyda, "Enhancing credit card fraud detection: highly imbalanced data case," *Journal of Big Data*, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-01059-5.
[14] J. Chung and K. Lee, "Credit card fraud detection: an improved strategy for high recall using KNN, LDA, and linear regression," *Sensors*, vol. 23, no. 18, Sep. 2023, doi: 10.3390/s23187788.
[15] J. K. Afriyie *et al.*, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, Mar. 2023, doi: 10.1016/j.dajour.2023.100163.
[16] J. Forough and S. Momtazi, "Sequential credit card fraud detection: a joint deep neural network and probabilistic graphical model approach," *Expert Systems*, vol. 39, no. 1, Jan. 2022, doi: 10.1111/exsy.12795.
[17] P. Boulieris, J. Pavlopoulos, A. Xenos, and V. Vassalos, "Fraud detection with natural language processing," *Machine Learning*, vol. 113, no. 8, pp. 5087–5108, Aug. 2024, doi: 10.1007/s10994-023-06354-5.
[18] I. D. Mienye and N. Jere, "Deep learning for credit card fraud detection: a review of algorithms, challenges, and solutions," *IEEE Access*, vol. 12, pp. 96893–96910, 2024, doi: 10.1109/ACCESS.2024.3426955.
[19] A. Cherif, H. Ammar, M. Kalkatawi, S. Alshehri, and A. Imine, "Encoder–decoder graph neural network for credit card fraud detection," *Journal of King Saud University–Computer and Information Sciences*, vol. 36, no. 3, Mar. 2024, doi: 10.1016/j.jksuci.2024.102003.
[20] E. Ileberi and Y. Sun, "A hybrid deep learning ensemble model for credit card fraud detection," *IEEE Access*, vol. 12, pp. 175829–175838, 2024, doi: 10.1109/ACCESS.2024.3502542.
[21] I. Hewapathirana, N. Kekayan, and D. Diyasena, "A systematic investigation on the effectiveness of the tabbert model for credit card fraud detection," in *2022 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, IEEE, Sep. 2022, pp. 96–101, doi: 10.1109/SCSE56529.2022.9905208.
[22] J. Raval *et al.*, "RaKShA: a trusted explainable LSTM model to classify fraud patterns on credit card transactions," *Mathematics*, vol. 11, no. 8, Apr. 2023, doi: 10.3390/math11081901.
[23] J.-W. Chang, N. Yen, and J. C. Hung, "Design of a NLP-empowered finance fraud awareness model: the anti-fraud chatbot for fraud detection and fraud classification as an instance," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 10, pp. 4663–4679, Oct. 2022, doi: 10.1007/s12652-021-03512-2.
[24] Y. Hanyf and H. Silkan, "A method for missing values imputation of machine learning datasets," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 1, pp. 888-898, Mar. 2024, doi: 10.11591/ijai.v13.i1.pp888-898.
[25] T. Verdonck, B. Baesens, M. Óskarsdóttir, and S. V. Broucke, "Special issue on feature engineering editorial," *Machine Learning*, vol. 113, no. 7, pp. 3917–3928, Jul. 2024, doi: 10.1007/s10994-021-06042-2.
[26] E. Katya, "Exploring feature engineering strategies for improving predictive models in data science," *Research Journal of Computer Systems Engineering*, vol. 4, no. 2, pp. 201–215, Dec. 2023, doi: 10.52710/rjcse.88.
[27] F. C. Souza, R. F. Nogueira, and R. A. Lotufo, "BERT models for brazilian portuguese: pretraining, evaluation and tokenization analysis," *Applied Soft Computing*, vol. 149, Dec. 2023, doi: 10.1016/j.asoc.2023.110901.
[28] A. Nayak, H. Timmapathini, K. Ponnalagu, and V. G. Venkoparao, "Domain adaptation challenges of BERT in tokenization and sub-word representations of Out-of-Vocabulary words," in *First Workshop on Insights from Negative Results in NLP*, Stroudsburg, PA, USA: Association for Computational Linguistics, 2020, pp. 1–5, doi: 10.18653/v1/2020.insights-1.1.
[29] G. Puccetti, A. Miaschi, and F. Dell'Orletta, "How do BERT embeddings organize linguistic knowledge?," in *Proceedings of Deep Learning Inside Out (DeeLIO): The 2nd Workshop on Knowledge Extraction and Integration for Deep Learning Architectures*, Stroudsburg, PA, USA: Association for Computational Linguistics, 2021, pp. 48–57, doi: 10.18653/v1/2021.deelio-1.6.
[30] F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem, and T. Al-Hadhrami, "Ensemble synthesized minority oversampling-based generative adversarial networks and random forest algorithm for credit card fraud detection," *IEEE Access*, vol. 11, pp. 89694–89710, 2023, doi: 10.1109/ACCESS.2023.3306621.
[31] H. Hairani, T. Widiyaningtyas, and D. D. Prasetya, "Addressing class imbalance of health data: a systematic literature review on modified synthetic minority oversampling technique (SMOTE) strategies," *JOIV International Journal of Informatics and Visualization*, vol. 8, no. 3, Sep. 2024, doi: 10.62527/joiv.8.3.2283.
[32] B. Ghojogh and A. Ghodsi, "Attention mechanism, transformers, BERT, and GPT: tutorial and survey," *OSF Preprints*, Dec. 2020, doi: 10.31219/osf.io/m6gcn.
[33] L. Zhao, L. Li, X. Zheng, and J. Zhang, "A BERT based sentiment analysis and key entity detection approach for online financial texts," in *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, IEEE, May 2021, pp. 1233–1238, doi: 10.1109/CSCWD49262.2021.9437616.
[34] R. DiPietro and G. D. Hager, "Deep learning: RNNs and LSTM," in *Handbook of Medical Image Computing and Computer Assisted Intervention*, Elsevier, 2020, pp. 503–519, doi: 10.1016/B978-0-12-816176-0.00026-0.
[35] C. Ubal, G. D.-Giorgi, J. E. C.-Reyes, and R. Salas, "Predicting the long-term dependencies in time series using recurrent artificial neural networks," *Machine Learning and Knowledge Extraction*, vol. 5, no. 4, pp. 1340–1358, Oct. 2023, doi: 10.3390/make5040068.

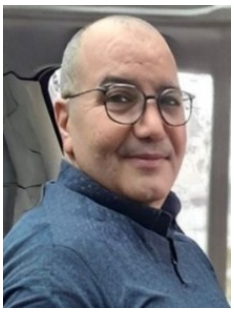
## BIOGRAPHIES OF AUTHORS

**Oussama Ndama** is a doctor Ph.D. in Computer Science and Artificial Intelligence with the DSAI2S (Data Science, Artificial Intelligence and Smart Systems) Research Team, C3S Laboratory, Faculty of Sciences and Technologies, Tangier, Morocco. He is also a business intelligence engineer with more than 6 years of experience in multinational companies. His research interests include smart systems, machine learning, deep learning, natural language processing (NLP), artificial neural networks (ANN), sentiment analysis, and smart cities. He can be contacted at email: oussama.ndama@etu.uae.ac.ma.

**Safae Ndama** is a Ph.D. student in DSAI2S (Data Science, Artificial Intelligence and Smart Systems Research Team), C3S Laboratory, Faculty of Sciences and Technologies (FST), Tangier, Morocco. She earned her master's in Computer Science and Big Data from the FST of Tangier. With two years of experience as a data scientist, her research interests include smart systems, data science, artificial intelligence, sentiment analysis, and smart cities. She can be contacted at email: safae.ndama@etu.uae.ac.ma.



**Ismail Bensassi** is a doctor in DSAI2S (Data Science, Artificial Intelligence and Smart Systems Research Team), C3S Laboratory, Faculty of Sciences and Technologies, Tangier, Morocco. He is an engineer in Computer Science, laureate of FST of Tangier. His research interests include smart connection of user profiles in a big data context, multi-agent systems (MAS), case-based reasoning (CBR), ontology, machine learning, smart cities, and eLearning/MOOC/SPOC. He can be contacted at email: bensassi.ismail@gmail.com.



**Dr. El Mokhtar En-Naimi** is a full professor in the University of Abdelmalek Essaâdi (UAE), Faculty of Sciences and Technologies (FST) of Tangier, Department of Computer Sciences. He was temporary professor from 1999 to 2003 and permanent professor since 2003/2004 until now. He is a Full Professor in UAE, FST of Tangier. He was a head in Department of Computer Sciences, since October 2016 until the end of December 2020. He was responsible for a License of Science and Technology, LST Computer Engineering ("Licence LST-GI"), from January 2012 to October 2016. He is a chief of Data Science, Artificial Intelligence and Smart Systems (DSAI2S) Research Team since the academic year 2022/2023. He is also a founding member of the both laboratories: Laboratoire d'Informatique, Systèmes et Télécommunications (LIST) Laboratory (from 2008 to 2022) and Computer Science and Smart Systems (C3S) Laboratory since the academic year 2022/2023 until now, the University of Abdelmalek Essaâdi, FST of Tangier, Morocco. He is also an expert evaluator with the ANEAQ, since the academic year 2016/2017 until now, that an expert of the private establishments belonging to the territory of the UAE and also an expert of the initial or fundamental formations and formations continuous at the Ministry of Higher Education, Scientific Research and Executive Training and also at the UAE University and the FST Tangier since 2012/2013 until now. He is an author/co-authors of several articles, published in The International Journals in Computer Sciences, in particular, in multi-agent systems (MAS), cases-based reasoning (CBR), artificial intelligent (AI), machine learning (ML), deep learning (DL), eLearning, MOOC/SPOC, big data, data-mining, wireless sensor network, VANet, MANet, and smart city. He was/is also director of several doctoral theses in computer sciences. He has too served as a general chair, technical program chair, technical program committee member, organizing committee member, session chair, and reviewer for many international conferences and workshops. In addition, he is an associate member of the ISCN-Institute of Complex Systems in Normandy, the University of the Havre, France, since 2009 until now. He can be contacted at email: en-naimi@uae.ac.ma.