



RESEARCH ARTICLE

OPEN ACCESS

A REVIEW ON THE OPTIMIZATION OF ENTERPRISE DATA SECURITY USING NEURAL NETWORKS

Nestor Abel Sánchez-Goycochea¹, José Angel Vásquez-Coronel², Miguel Serón³

^{1,2}Centro de Apoyo Logístico para Investigadores, Universidad Tecnológica del Perú, Sede Chiclayo.

³Instituto de Matemáticas, Física y Estadística, Universidad de Las Américas, Concepción, Chile.

¹<http://orcid.org/0000-0002-3235-3113>, ²<http://orcid.org/0000-0001-7121-2623>, ³<http://orcid.org/0009-0005-4222-0014>

E-mail: nsanchezg@utp.edu.pe, C31374@utp.edu.pe, mseron@udla.cl

ARTICLE INFO

Article History

Received: February 25, 2026

Reviewed: March 25, 2026

Accepted: April 01, 2026

Published: May 29, 2026

Keywords:

Frauds,
Data analysis,
Artificial intelligence,
Security attacks,
Monitoring.

ABSTRACT

Technology in business field has helped solve problems that involve card fraud or commercial transactions; however, it has also generated a great need to guarantee the security of customer data. The use of neural networks has emerged as an indispensable tool to address this type of problem. In this study, a systematic review was developed of 64 articles from Scopus and Web of Science, to identify the type of business data, the neural network architecture used, and the influence on a type of analyzed business problem. Search strategies such as PICO and PRISMA2020 were combined for the selection. Based on inclusion and exclusion criteria, this paper seeks to answer the research question: How the neural network models optimize enterprise data security? Four metrics were identified: Accuracy, Precision, Recall, and F-Score, to compare the efficiency of neural network models such as CNN, DNN, LSTM, or their variants. These models outperformed other current techniques in the identification of card or transaction fraud; however, their implementation remains limited in small and medium-sized enterprises due to restrictions in technological infrastructure and computational capacity.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

1. INTRODUCTION

The current financial risk landscape poses a persistent challenge, driven by economic expansion and technological advances [1], [2]. The ongoing digitalization of financial services has increased the incidence of fraudulent activities, adversely affecting financial institutions, regulatory bodies, and end-users [3], [4]. For instance, direct losses from credit card fraud are estimated to amount to billions of dollars annually, excluding indirect losses which are more difficult to quantify [5], [6]. In 2023, global losses reached USD 33.83 billion, slightly exceeding the USD 33.45 billion recorded in 2022. Conventional detection methods, relying primarily on manual scrutiny and rule-based systems, are insufficient to counter the complexity of modern fraud schemes [7], [8]. This situation necessitates the development of more innovative anti-fraud solutions capable of thwarting malicious actors. Various machine learning algorithms as support vector machines, linear and logistic regression, decision trees, random forests, and k-nearest neighbors, have also been employed for fraud detection and corporate data security [9], [10].

However, their accuracy and scalability are often constrained by class imbalance and the need to process large data volumes. Advances in technology and internet accessibility have established deep learning models as significant contributors to optimizing the security and protection of financial, commercial, customer, operational, and human resources data. Architectures such as Convolutional Neural Networks (CNNs), Deep Neural Networks (DNNs), and Dual-Channel Graph Attention Networks (DGANs) achieve superior accuracy compared to traditional approaches. Furthermore, Long Short-Term Memory (LSTM) networks, Recurrent Neural Networks (RNNs), and hybrid structures demonstrate a considerable potential for countering sophisticated attacks in fraud detection. These models learn data representations to identify malicious patterns, anomalous behaviors, or fraud attempts [8], [11]. Other brain-inspired architectures, such as Spiking Neural Networks, Chaotic Coupled Neural Networks, and graph-based approaches, offer additional potential by detecting dynamic and chaotic patterns, thereby adapting to evolving fraudulent behaviors over time [12-16].

Financial institutions face sustained economic risks stemming from inadequate information protection. This challenge has driven the scientific community to design and implement new defensive measures against fraudulent systems [17]. Nevertheless, despite progress in deep learning, comprehensive studies analyzing the capacity of diverse neural network architectures to enhance corporate data security remain scarce. This article presents a comprehensive and up-to-date review of the principal neural network architectures applied to corporate data security. Guided by the PICO strategy and the PRISMA2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework for study search, selection, and analysis, the review systematically categorizes information based on data type, addressed problem, applied neural network architecture, and reported evaluation metrics. This rigorous methodological approach provides a deep understanding of the strengths, limitations, and opportunities for future research in corporate fraud prevention.

II. METHODOLOGY

This study was conducted as a systematic literature review, a methodology characterized by the evaluation and synthesis of relevant information on a specific topic. This review aims to identify neural network models used to analyze corporate data security. To this end, the following research question was formulated: How do neural network models optimize corporate data security?

II.1 PICO STRATEGY

A guided approach based on specific questions from the PICO strategy was employed. Originally applied in medical fields, this tool is now used to identify the Problem (P), Intervention (I), Comparison (C), and Outcomes (O) in any area of study [18], [19]. To address the research question, the comparison component was excluded, allowing for the evaluation of all types of neural networks. Consequently, only three components (P-I-O) were assessed. Table 1 presents the questions and associated keywords for each PIO component. The first question focuses on identifying the types of corporate data analyzed using neural networks; the second addresses the type of neural network used for processing corporate data. Finally, the third question evaluates the influence of neural networks on data analysis. Thus, these three questions determined the research objective.

Table 1: PIO Strategy Components.

Component	Associated Question	Keywords
Problem (P)	What types of corporate data are analyzed using neural networks?	Business Data, Enterprise Data, Company Data, Financial Risk, Fraud Detection
Intervention (I)	What neural network architectures are applied to corporate data?	Neural Networks, Neuronal Networks, NN
Outcomes (O)	How do neural networks influence corporate data security?	Security, Safety, Protection, Confidentiality, Privacy, Analyses

Source: Authors, (2026).

Using the keywords described in Table 1, an exhaustive search was conducted in two high-impact scientific databases: Scopus and Web of Science (WoS) [20], [21]. The search strategy began in Scopus, forming three blocks joined by the logical operator AND. In each block, the *Article title*, *Abstract*, *Keywords* option was selected, and the keywords associated with PIO were entered, connected by OR. As a result, the following search string was obtained (as of May 3, 2025):

(TITLE-ABS-KEY ("business data" OR "enterprise data" OR "company data" OR "financial risk" OR "fraud detection") AND TITLE-ABS-KEY ("neural networks" OR "neuronal networks" OR NN) AND TITLE-ABS-KEY (security OR safety OR protection OR confidentiality OR privacy OR analyses)) AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (OA , "all"))

For the WoS search, the same PIO strategy keywords (see Table.1) were used, placed in three blocks with the *Topic* option, interlinked by the AND connective. The same filters were applied for both Scopus (FS) and WoS (FW). These filters are presented in Table 2.

Table 2: Filters Applied to the Search String.

Filter	Description
FS1: PUBYEAR > 2021 AND PUBYEAR < 2025 FW1: 2022 or 2023 or 2024 (Publication Years)	Limits the search to documents published within a specific date range
FS2: LIMIT-TO (LANGUAGE , "English") FW2: English (Languages)	Selects documents only in the chosen language
FS3: LIMIT-TO (DOCTYPE , "ar") FW3: Article (Document Types)	Restricts results to original articles
FS4: LIMIT-TO (OA , "all") FW4: All Open Access (Open Access)	Filters for open access documents

Source: Authors, (2026).

II.2 PRISMA2020 PROTOCOL

For the selection of documents that formed the basis of this review's results, the PRISMA2020 protocol was applied. This is a widely recognized methodology in the scientific community for conducting bibliometric studies, reviews, and meta-analyses [22]. Specific inclusion and exclusion criteria were applied to minimize bias (see Table 3).

Table 3: Inclusion and Exclusion Criteria.

Filter	Description
CI1: Studies that apply neural networks to the analysis of corporate data in any sector	CE1: Studies not focused on corporate data
CI2: Studies that describe or compare different neural network architectures applied to corporate data	CE2: Studies that do not present clear results on the use of neural networks
CI3: Studies that report performance metrics or impact on business processes or data protection	CE3: Studies that do not provide information on data security through the use of neural networks
CI4: Studies accessible in full text.	CE4: Studies identified as retracted

Source: Authors, (2026).

Figure 1 presents a PRISMA2020 flow diagram to document and visualize the study selection process in a structured manner. This diagram details the stages of search, inclusion, and exclusion of studies, providing a clear framework for the strategy employed in this review. Initially, 221 studies were identified from Scopus (151) and WoS (70). After removing 40 duplicate records, a total of 181 remained. Subsequently, 89 were excluded after analyzing titles and abstracts, reducing the number to 92 articles. All of these were successfully retrieved in full text. During the evaluation phase, 28 articles were excluded based on the exclusion criteria (CE) established in Table 2. Finally, a total of 64 studies were selected for the review analysis.

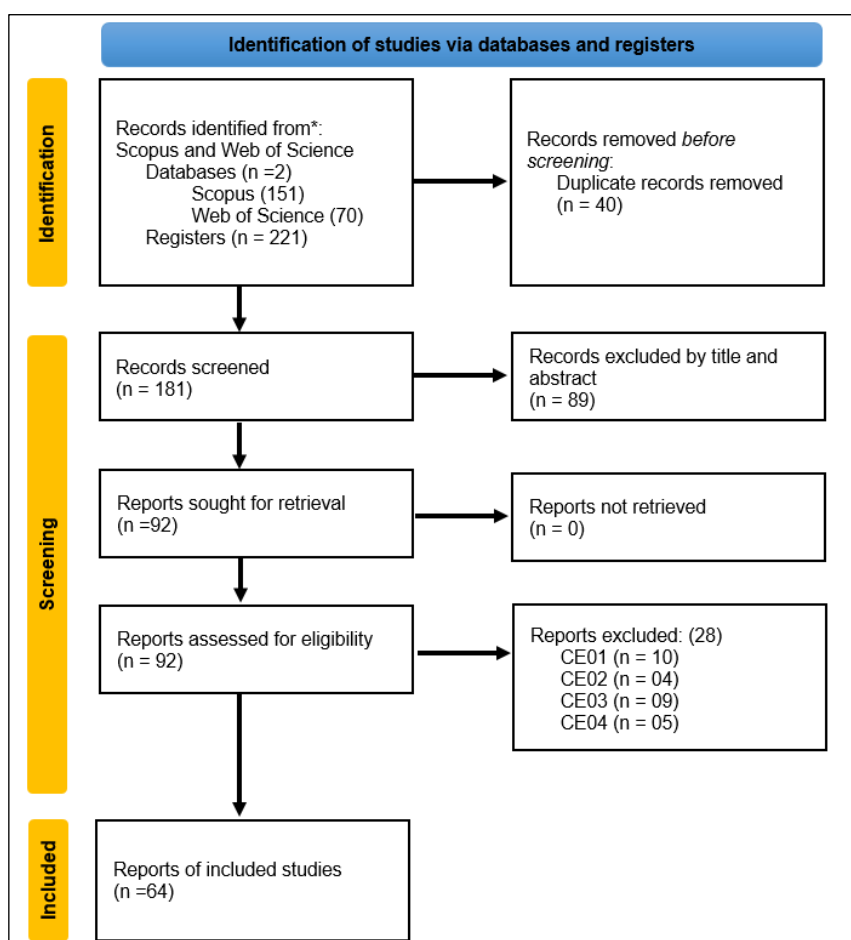


Figure 1: PRISMA Flowchart.

Source: Authors, (2026).

III. RESULTS AND DISCUSSIONS

III.1 BIBLIOMETRIC RESULTS

To present a general report of the articles included in the analysis, journals were classified by quartile type, calculated using the SCImago Journal Rank indicator (SJR 2024). 21 articles correspond to quartile 1 (Q1), 25 to Q2, 15 to Q3, and only 3 articles mention Q4-type journals. Figure 2 describes the percentages associated with each quartile. These results indicate that over 70% of the analyzed studies originate from high-impact Q1 and Q2 journals, demonstrating the editorial quality of the selected studies.

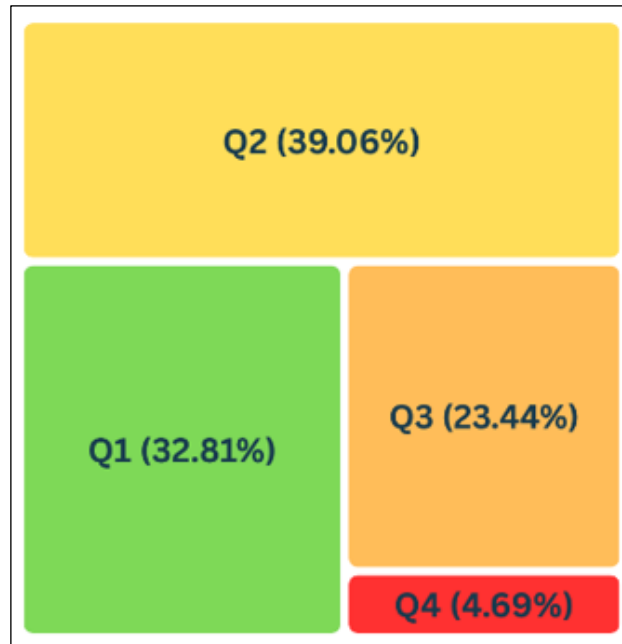


Figure 2: Articles classified by journal quartile.
Source: Authors, (2026).

The most prominent publisher is the Multidisciplinary Digital Publishing Institute (MDPI) with 11 articles, followed by the Institute of Electrical and Electronics Engineers Inc. (IEEE) with 9 articles, whose main journal is IEEE Access (7).

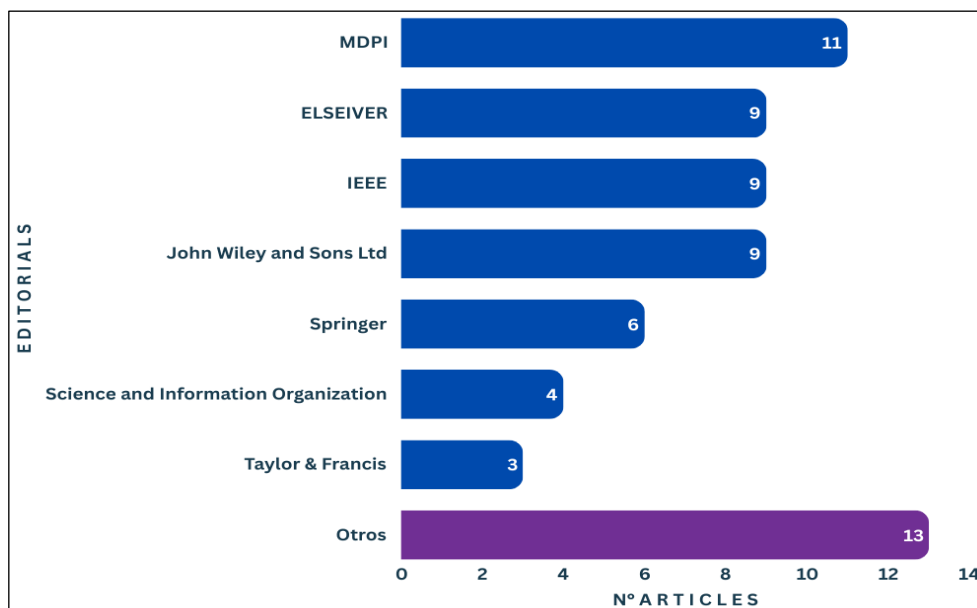


Figure 3: Articles classified by journal publisher.
Source: Authors, (2026).

Studies were also categorized by research field. Computer science stands out in this classification with 69.2%, encompassing artificial intelligence, machine learning, and natural language processing. The information systems area accounts for 12.3%, followed by Finance and Economics with 10.8%. Other represented disciplines are Engineering, with 4.6%, and Mathematics, with 3.1%. This distribution highlights a strong interdisciplinary link in the analyzed works. The following sections will address the questions related to each component of the PIO strategy (see Table 1).

III.2 WHAT TYPES OF CORPORATE DATA ARE ANALYZED USING NEURAL NETWORKS?

One of the main challenges in the corporate sphere is managing the control of large data volumes. Data preparation is one of the initial stages of the process and involves collecting and organizing raw data for efficient analysis [23]. Therefore, using neural networks to analyze such data in real-time has become a necessity to provide timely responses in milliseconds, preventing fraud and increasing customer confidence [24]. Of the 64 selected articles, 87.5% (56 studies) detail some type of corporate data analyzed using neural networks, with commercial transaction data standing out in 25 studies. This type of transaction involves banks processing thousands of transfers per day, which is impossible for a human to supervise, let alone in real time [25].

With the widespread use of credit cards in online and offline transactions, fraud has become a major challenge for the financial sector. Wu et al. in [6], demonstrate that brain-like computing can significantly contribute to improving the security and efficiency of fraud detection systems. On the other hand, with countries like China entering the international market, competition is becoming increasingly complex. Added to this, companies often have gaps in their financial structure, generating significant risks in their international trade [26]. Likewise, financial-type data were identified in 14 studies involving companies that use technological innovation to offer services and products. Liu, T. and Yang L. in [27], used financial data for their analysis, accurately identifying companies with different risk levels, particularly in the low and medium-risk categories. In [28], five financial indicators were identified: (i) interest-bearing debt/total invested capital, (ii) quick ratio, (iii) accounts payable turnover ratio, (iv) proportion of goodwill, and (v) goodwill, demonstrating that these factors have a greater impact on the identification results of many neural network models, reflecting a significant role in identifying financial fraud. Another relevant dataset comprises operational and logistical data (12 articles). This type of data is generated by the various modules of an Operational Management System [29]. Accurately predicting the volatility of financial asset prices has profound theoretical and practical importance, especially for generating early warnings of financial market risks. Identifying the type of data to be analyzed for a problem is fundamental to applying more effective detection methods. If working with imbalanced data, where class distribution is not uniform, it can lead to suboptimal predictive performance, especially for the minority class [30]. Table 4 describes the types of corporate data analyzed using neural networks, detailing the problem studied and the sector of application.

Table 4: Types of corporate data.

Data type	Problem	Sector	Ref.
Commercial Transactions	Anomaly identification in payments, transfer classification	E-commerce	[16], [25], [26], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52].
Financial Data	Fraud detection, credit risk prediction	Microfinance, fintech	[6], [16], [23], [24], [27], [28], [53], [54], [55], [56], [57], [58], [59], [60].
Operational Data	Demand forecasting, quality control	Manufacturing	[15], [29], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70].
Customer Data	Market segmentation	Marketing, e-commerce	[40], [46], [71], [72].
Human Resources Data	Turnover prediction, job performance, absenteeism	Human talent management	[73], [74], [75], [76].

Source: Authors, (2026).

Based on this component, the corporate data analyzed using neural networks correspond mainly to transactional and financial information. This reflects the need to manage data in real-time to prevent fraud or detect anomalies, as noted by previous studies [3],[6]. The literature also makes clear that, with technological advances and the increase in electronic operations, companies seek to implement more robust models to minimize credit risk [4]. Despite the effectiveness demonstrated by neural networks in data analysis, challenges exist related to integrating unstructured sources, such as text or customer behavior. Furthermore, in sectors like manufacturing and logistics, various studies describe the ability of these techniques to improve industrial efficiency through demand forecasting and quality control [61],[63]. However, their adoption in small and medium-sized enterprises remains limited, revealing a technological gap for future research. On the other hand, these models are also applied in customer and human resources management, primarily in marketing and human talent areas [40],[46],[75]. In general, this review shows the frequency of neural network usage in the corporate environment, although their adoption depends on the data type, learning architecture, and interpretability of the implemented models.

III.3 WHAT NEURAL NETWORK ARCHITECTURES ARE APPLIED TO CORPORATE DATA?

Deep learning methods based on artificial intelligence techniques have generated better results for extracting, analyzing, and expressing data compared to traditional methods. Many researchers have gradually applied deep learning technologies to their research, particularly in topics related to corporate financial early warning [34]. 42.19% of the articles selected for this research (27) describe the type of neural network used to analyze a corporate-type problem. Table 5 describes the neural network type, the selected dataset, the corporate problem being solved, the metrics used to measure efficiency, and the reference article. Based on the 27 articles involved for component (I), 26.63% use CNN to solve problems of financial risk, fraud detection, or identification of fraudulent transactions. Unlike other models, CNN methods reflect a significant advantage due to their nonlinear adjustment capability, data processing ability, and generate greater accuracy and discrimination in predictions [34]. According to [31], developed a CNN model to detect and mitigate fraudulent activities in smart contracts. Textual and transactional data from smart contracts from Google BigQuery Ethereum were analyzed.

This dataset includes essential attributes such as sender addresses, recipient addresses, transaction value, and timestamp. On the other hand, inspired by brain-like computing, Wu et al. in [6], implemented an optimized CNN network, known as Continuous Coupled Neural Network (CCNN) for credit card fraud detection, managing to reduce data imbalance through random oversampling techniques. Another type of neural network is the DNN. In [33], establishes that the financial early warning model trained by DNN generates an effective financial early warning for the company. However, due to the hidden layers of these models, uncertainty in their analysis can be generated. For example, fraudsters change their strategies, and consequently, DNNs encounter observations not generated by the same process; another factor is due to the time-consuming process and very few transactions are verified in a timely manner by professional experts to update the DNNs. In [51], three uncertainty quantification (UQ) techniques called "Monte Carlo dropout," "ensemble," and "ensemble Monte Carlo dropout" are proposed, demonstrating that UQ methods provide additional information about point predictions, thereby improving the fraud prevention process.

Other research combines DNN and RNN, resulting in a model called FinAnalytixs [45] for stock performance prediction and fraud detection. This architecture allows DNN to capture complex relationships between various financial indicators, such as the interaction between market trends, company finances, and macroeconomic factors. Other models were identified, such as Graph Neural Networks (GNN), specifically designed to work with graph-structured data [15]. The Backpropagation Neural Network (BPNN), a model built based on blockchain technology for financial data analysis [52]. The NAG (Neural Aggregates Generator) model, which faithfully mimics the structure of state-of-the-art manual function aggregates. This strategy relates any transaction to its recent past by calculating statistics on those transactions similar to the current one [77]. The CRAFTIC (Complex Relationship Analysis for Fraud Identification and Cost management) framework [37] achieves a significant performance improvement in complex fraud detection tasks by combining CNN and LSTM in feature extraction and time series analysis. The analysis of architectures adopted in the corporate sector shows a marked preference for deep and hybrid learning models, capable of optimizing pattern detection and reducing uncertainty in complex financial environments [4], [8].

In particular, CNNs and their composite variants, such as CNN-LSTM and CNN-Transformer-Wavelet, stand out for their robust generalization capability in fraud prevention and financial risk prediction. However, DNNs, BiLSTM, and GRU-LSTM present better performance in handling temporal dependencies, positioning themselves as effective alternatives for financial trend prediction [4], [29], [70]. On the other hand, graph-based approaches stand out for their high potential to capture nonlinear relationships and complex structures between entities and transactions, identifying anomalies that often go unnoticed by conventional methods [15], [16]. The different approaches indicate that there is no universal architecture; rather, its choice depends on the data type and the complexity level of the problem. Although trends point towards hybrid models, challenges still exist related to uncertainty, computational efficiency, and class imbalance in fraud scenarios. Furthermore, their implementation remains limited in small and medium-sized enterprises due to technological infrastructure and computational capacity restrictions.

Table 5: Neural Network Architectures Applied to Corporate Problems.

Neural Network	Dataset and/or Sample	Corporate Problem	Metrics	Ref.
Bi-LSTM	Wind database	Exchange and protection of financial data	Accuracy, AUC	[75]
BP/ARIMA	Not specified	Financial risk prediction	Profitability metric	[26]
BPNN	Shanghai Index and Shenzhen 200 Index (CSI 200)	Commercial transactions with blockchain technology	MAE, MSE, RMSE, Training times	[52]
BPNN	Companies in the financial sector of Shanghai and Shenzhen in the third quarter of 2022	Prediction of financial risks for listed companies	Accuracy, Recall, F1-Score	[27]
CCNN	Kaggle Credit Card Fraud Detection (CCFD)	Security and efficiency of fraud detection in the financial industry	Accuracy, Precision, Recall, F1-Score	[6]
CNN	Google BigQuery Ethereum dataset	Detection and mitigation of fraudulent activities within smart contracts	Accuracy	[31]
CNN	Not specified	Financial risk prediction	Accuracy	[44]
CNN-IKOA	Data from 100 Internet companies	Prediction of risks for Internet companies	MSE, MSPE, MAE, MAPE	[78]
CNN-LSTM	279 companies with net profits of <0 for two consecutive years in Shanghai and Shenzhen A-shares, listed from 2019 to 2023	Corporate financial risk management	Accuracy, Precision, Recall, F1-Score	[34]
CNN-LSTM	Data generated by the Sparkov tool from Brandon Harris, simulating transactions between 01-01-2019 and 31-12-2020	Identification of fraudulent credit card transactions	Accuracy, Precision Recall, F1-score, AUC	[55]
CNN-LSTM	Global supply chain from DataCo and IEEE-CIS fraud detection data	Network transaction security and reduction of socioeconomic problems caused by fraudulent behavior	Accuracy	[37]
CNN-Transformer-Wavelet	Three financial datasets: (i) Standard Poor's 500 Index-SPX500, (ii) West Texas Intermediate-WTI, (iii) London Metal Exchange Gold Price-LGP	Prediction of financial risk in companies	Accuracy, Precision, Recall, F1-Score	[38]
DNN	Kaggle website: Credit card transactions of European cardholders generated over 2 days in 2013	Detection of fraudulent credit card transactions	Accuracy, F1-Score	[73]
DNN	PaySim dataset	Credit card fraud detection	Accuracy, F1 Score, Precision, Recall, AUPRC	[70]
DNN	Vesta Corporation	Credit card fraud detection	UAcc, UPre, USen., USpe	[51]
DNN-DL	Not specified	Analysis of early warning of corporate financial risks	Accuracy	[33]
DNN-RNN	Not specified	Comprehensive analysis of complex financial data	Accuracy, Precision, Recall, F1-score	[45]
FNN	Ninth "TIPDM Cup" financial analysis competition for listed companies	Detection of fraudulent financial data	Accuracy, Precision, Recall, F1-score	[59]
GNN-Autoencoders	Pakistani private banks (Meezan Bank and UBL)	Reduction of fraudulent activities in large organizations	Accuracy, Precision, Recall, F1-Score	[15]

HNN	Mobile advertising platform in China	Identification of fraudulent applications for mobile advertising	Average Precision (AP), AUC	[68]
GRU-LSTM	Three financial datasets: (i) Standard Poor's 500 Index-SPX500, (ii) West Texas Intermediate-WTI, (iii) London Metal Exchange Gold Price-LGP	Prediction of financial asset price volatility	MAE, MSE	[29]
MLP-ANN	Companies listed on the Shenzhen and Shanghai stock exchanges between 2016 and 2020	Stock market forecasting	Accuracy, Z-score	[64]
MOE-DNN-Smote	Kaggle Credit Card Fraud Detection (CCFD)	Improvement of fraud detection performance	Accuracy, TPR, TNR, FPR, MCC	[57]
MS-HGNN	Public data from Amazon and Yelp	Online fraud detection	Recall, AUC	[16]
NAG	Wordline dataset and a public dataset	Credit card fraud detection	Precision-recall curve (AUCPR)	[77]
SVM-FFNN	Kaggle dataset	Detection of fraudulent activities	Accuracy, Precision, Recall	[40]
TH-LSTM	Real-world transactions provided by a Chinese financial institution	Automatic detection of fraudulent transactions	Precision, Recall, F1-Score	[60]

Source: Authors, (2026).

III.4 HOW DO NEURAL NETWORKS INFLUENCE CORPORATE DATA SECURITY?

To address this question, 16 articles (25%) were identified that quantitatively report any of the following 4 metrics: Accuracy, Precision, Recall, F-Score. These metrics provide a comprehensive assessment of the model's classification effectiveness [6], obtained as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F-Score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Where TP: True Positives, TN: True Negatives, FP: False Positives, and FN: False Negatives. Figure 4 shows the metrics recorded for the 16 articles, identifying the type of neural network used. Labels A1-A16 were used for these articles, which are mentioned in Table 6.

Table 6: Articles labeled for component O.

Label	Reference	Label	Reference
A1	[75]	A9	[73]
A2	[27]	A10	[70]
A3	[6]	A11	[33]
A4	[44]	A12	[45]
A5	[34]	A13	[59]
A6	[55]	A14	[15]
A7	[37]	A15	[40]
A8	[38]	A16	[60]

Source: Authors, (2026).

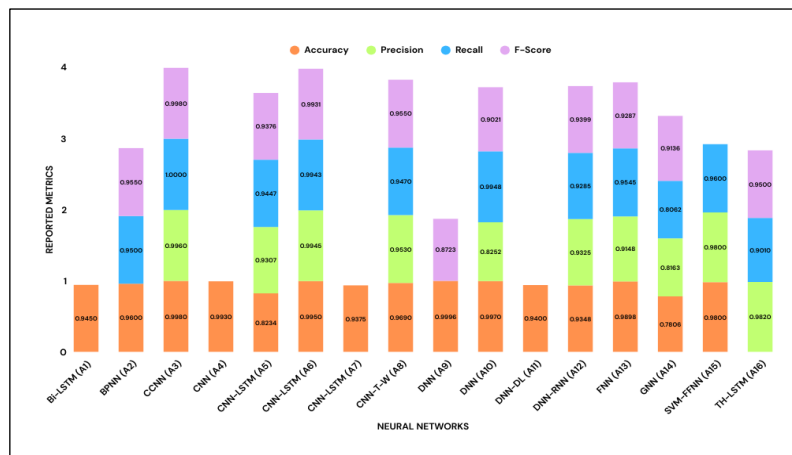


Figure 4: Metrics used by articles employing neural networks.

Source: Authors, (2026).

The results shown in Figure 4 highlight the effectiveness of CCNN in handling the complexity and subtlety of fraud detection, where small and non-obvious patterns often indicate fraudulent behavior [6]. The CNN simulation system based on the scientific node selection method greatly improved the accuracy of financial risk assessment [44]. A CNN model has significant advantages in processing complex financial data; it can perform in-depth mining and feature extraction from massive financial data by simulating the human brain's processing mode [34]. Another suggested approach combining CNN and LSTM outperformed other current techniques and achieved the highest accuracy of 99.5% in identifying credit card fraud [55]. According to [33], demonstrated that the prediction accuracy of the DL network after sample training reached 94%, being superior to other prediction models. The financial early warning model used by Li is based on DL with DNN and can be fully applied to corporate financial risk early warning.

On the other hand, less recurrent models have been of great importance in addressing corporate problems. In [15], they concluded that financial institutions are using deep learning with business intelligence to control money laundering. Their work was based on fraud detection with Graph Neural Networks and anomaly detection using Autoencoders in Credit Cards. Models based on Support Vector Machines (SVM) and Feedforward Neural Networks (FFNN) are used in [40] to distinguish between classes and capture complex patterns and relationships, respectively. The model shows promise in fraud detection with greater accuracy and precision. According to [60] propose a new representation for each transaction record based on users' historical transactions to accurately capture fraudulent patterns. Their proposal is based on an improvement of the LSTM model with a time-aware gate (TH-LSTM), which can capture behavioral changes caused by users' consecutive transactions.

Experimental results demonstrated a clear distinction between legitimate and fraudulent behaviors, achieving better fraud detection performance compared to state-of-the-art methods. In general, models based on neural networks influence corporate data analysis very positively. These statistical indicators show the potential of neural networks in decision-making in corporate contexts, especially for identifying anomalous behaviors and reducing false positives [34],[44]. However, these metrics can be biased by the data type and architecture design, showing limitations against changing scenarios not contemplated in training and testing [15],[40]. Consequently, corporate data security should be evaluated not only by model performance but also by its robustness and adaptability in real-world environments [33],[55].

IV. CONCLUSIONS

This review study organized and systematized the available scientific evidence on the use of neural networks in optimizing and protecting corporate data. The PICO and PRISMA2020 strategies guided the search, selection, and analysis process of information from 64 articles. Specifically, the scientific background was systematized based on answering three specific questions and one general question, which were the focus of the research. The main findings are as follows:

- 87.5% of the studies detail some type of corporate data analyzed using neural networks, with commercial transaction data (25), financial data (14), and operational data (12) being the most prominent.
- 42.19% describe the type of neural network used to analyze a corporate-type problem. In particular, CNNs and their composite variants, such as CNN-LSTM and CNN-Transformer-Wavelet, stand out for their robust generalization capability in fraud prevention and financial risk prediction. Other network types, such as DNNs, BiLSTM, and GRU-LSTM, demonstrate better performance in handling temporal dependencies.
- The different approaches indicate that there is no universal architecture; rather, its selection depends on the type of data and the complexity level of the problem.
- Based on metrics such as Accuracy, Precision, Recall, and F-Score, a positive influence is evidenced in applying neural networks to solve problems involving corporate data. The 25% of articles using these types of metrics mention that models such as CNN or DNN combined with LSTM have significant advantages in processing complex financial data. These models outperformed other current techniques in identifying credit card fraud.

V. AUTHOR'S CONTRIBUTION

Conceptualization: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

Methodology: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

Investigation: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

Discussion of results: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

Writing – Original Draft: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

Writing – Review and Editing: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

Resources: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

Supervision: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

Approval of the final text: N. Sánchez-Goycochea, J. Vásquez-Coronel and M. Serón.

VI. ACKNOWLEDGMENTS

The author Nestor Sánchez-Goycochea express their gratitude to the project: Proyecto de Investigación I+D 2025 UTP-Región Norte, No. P-2025-NOR-26.

VII. REFERENCES

- [1] F. Königstorfer and S. Thalmann, "Applications of Artificial Intelligence in commercial banks—A research agenda for behavioral finance," *J. Behav. Exp. Finance*, vol. 27, p. 100352, 2020.
- [2] A. M. Qatawneh, "The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing," *Int. J. Organ. Anal.*, vol. 33, no. 6, pp. 1391–1409, 2025.

- [3] J. Danielsson, R. Macrae, and A. Uthemann, "Artificial intelligence and systemic risk," *J. Bank. Finance*, vol. 140, p. 106290, 2022.
- [4] F. S. Khan, S. S. Mazhar, K. Mazhar, D. A. AlSaleh, and A. Mazhar, "Model-agnostic explainable artificial intelligence methods in finance: a systematic review, recent developments, limitations, challenges and future directions," *Artif. Intell. Rev.*, vol. 58, no. 8, p. 232, 2025.
- [5] K. J. Barker, J. D'amato, and P. Sheridan, "Credit card fraud: awareness and prevention," *J. Financ. Crime*, vol. 15, no. 4, pp. 398–410, 2008.
- [6] Y. Wu, L. Wang, H. Li, and J. Liu, "A Deep Learning Method of Credit Card Fraud Detection Based on Continuous-Coupled Neural Networks," *Mathematics*, vol. 13, no. 5, p. 819, 2025.
- [7] E. Kurshan and H. Shen, "Graph computing for financial crime and fraud detection: Trends, challenges and outlook," *Int. J. Semantic Comput.*, vol. 14, no. 04, pp. 565–589, 2020.
- [8] J. I.-Z. Chen and K.-L. Lai, "Deep convolution neural network model for credit-card fraud detection and alert," *J. Artif. Intell.*, vol. 3, no. 02, pp. 101–112, 2021.
- [9] L. Hernandez Aros, L. X. Bustamante Molano, F. Gutierrez-Portela, J. J. Moreno Hernandez, and M. S. Rodríguez Barrero, "Financial fraud detection through the application of machine learning techniques: a literature review," *Humanit. Soc. Sci. Commun.*, vol. 11, no. 1, pp. 1–22, 2024.
- [10] A. M. Siam, P. Bhowmik, and M. P. Uddin, "Hybrid feature selection framework for enhanced credit card fraud detection using machine learning models," *PLoS One*, vol. 20, no. 7, p. e0326975, 2025.
- [11] I. Sadgali, N. Sael, and F. Benabbou, "Performance of machine learning techniques in the detection of financial frauds," *Procedia Comput. Sci.*, vol. 148, pp. 45–54, 2019.
- [12] Z. Yi, J. Lian, Q. Liu, H. Zhu, D. Liang, and J. Liu, "Learning rules in spiking neural networks: A survey," *Neurocomputing*, vol. 531, pp. 163–179, 2023.
- [13] T. Ma, J. Mou, A. A. Al-Barakati, H. Jahanshahi, and M. Miao, "Hidden dynamics of memristor-coupled neurons with multi-stability and multi-transient hyperchaotic behavior," *Phys. Scr.*, vol. 98, no. 10, p. 105202, 2023.
- [14] K. Malcolm and J. Casco-Rodriguez, "A comprehensive review of spiking neural networks: Interpretation, optimization, efficiency, and best practices," *ArXiv Prepr. ArXiv230310780*, 2023.
- [15] F. Khaled Alarfaj and S. Shahzadi, "Enhancing Fraud Detection in Banking With Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention," *IEEE Access*, vol. 13, pp. 20633–20646, 2025, doi: 10.1109/ACCESS.2024.3466288.
- [16] J. Long, F. Fang, C. Luo, Y. Wei, and T.-H. Weng, "MS_HGNN: a hybrid online fraud detection model to alleviate graph-based data imbalance," *Connect. Sci.*, vol. 35, no. 1, p. 2191893, Dec. 2023, doi: 10.1080/09540091.2023.2191893.
- [17] E. Parkar, S. Gite, S. Mishra, B. Pradhan, and A. Alamri, "Comparative study of deep learning explainability and causal ai for fraud detection," *Int. J. Smart Sens. Intell. Syst.*, no. 1, 2024.
- [18] A. M. Methley, S. Campbell, C. Chew-Graham, R. McNally, and S. Cheraghi-Sohi, "PICO, PICOS and SPIDER: a comparison study of specificity and sensitivity in three search tools for qualitative systematic reviews," *BMC Health Serv. Res.*, vol. 14, no. 1, pp. 1–10, 2014, doi: 10.1186/s12913-014-0579-0.
- [19] A. Dhrangadhariya and H. Müller, "Not so weak PICO: leveraging weak supervision for participants, interventions, and outcomes recognition for systematic review automation," *JAMIA Open*, vol. 6, no. 1, 2023, doi: 10.1093/jamiaopen/ooac107.
- [20] Y. V. Mokhnacheva, "Document types indexed in WoS and Scopus: Similarities, differences, and their significance in the analysis of publication activity," *Sci. Tech. Inf. Process.*, vol. 50, no. 1, pp. 40–46, 2023, doi: 10.3103/S0147688223010033.
- [21] M. C. Sánchez Gómez, J. L. Cabanillas García, S. Verdugo Castro, and I. D. Brio Alonso, "Métodos de investigación en el área educativa. Análisis bibliométrico: estudio comparativo entre Scopus y WoS," 2025, doi: 10.5944/reec.46.2025.40201.
- [22] M. J. Page et al., "Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas," *Rev. Esp. Cardiol.*, vol. 74, no. 9, pp. 790–799, 2021, doi: 10.1016/j.recesp.2021.06.016.
- [23] T. Bikku, S. Thota, and P. Shanmugasundaram, "A Novel Quantum Neural Network Approach to Combating Fake Reviews," *Int. J. Networked Distrib. Comput.*, vol. 12, no. 2, pp. 195–205, Dec. 2024, doi: 10.1007/s44227-024-00028-x.
- [24] K. Sathupadi, S. Achar, S. V. Bhaskaran, N. Faruqui, and J. Uddin, "BankNet: Real-Time Big Data Analytics for Secure Internet Banking," *Big Data Cogn. Comput.*, vol. 9, no. 2, p. 24, Jan. 2025, doi: 10.3390/bdcc9020024.
- [25] P. M. Preciado Martínez, R. F. Reier Forradellas, L. M. Garay Gallastegui, and S. L. Nández Alonso, "Comparative analysis of machine learning models for the detection of fraudulent banking transactions," *Cogent Bus. Manag.*, vol. 12, no. 1, p. 2474209, Dec. 2025, doi: 10.1080/23311975.2025.2474209.
- [26] L. Xu and G. Dong, "Prediction Model of International Trade Risk Based on Stochastic Time-Series Neural Network," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–9, Jun. 2022, doi: 10.1155/2022/3119535.
- [27] T. Liu and L. Yang, "Financial Risk Early Warning Model for Listed Companies Using BP Neural Network and Rough Set Theory," *IEEE Access*, vol. 12, pp. 27456–27464, 2024, doi: 10.1109/ACCESS.2024.3367228.
- [28] B. Li, J. Yen, and S. Wang, "Uncovering Financial Statement Fraud: A Machine Learning Approach With Key Financial Indicators and Real-World Applications," *IEEE Access*, vol. 12, pp. 194859–194870, 2024, doi: 10.1109/ACCESS.2024.3520249.
- [29] H. Lin and Q. Sun, "Financial Volatility Forecasting: A Sparse Multi-Head Attention Neural Network," *Information*, vol. 12, no. 10, p. 419, Oct. 2021, doi: 10.3390/info12100419.

- [30] I. De Zarzà, J. De Curtò, and C. T. Calafate, "Optimizing Neural Networks for Imbalanced Data," *Electronics*, vol. 12, no. 12, p. 2674, Jun. 2023, doi: 10.3390/electronics12122674.
- [31] 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," *J. Theor. Appl. Electron. Commer. Res.*, vol. 19, no. 3, pp. 2139–2156, Aug. 2024, doi: 10.3390/jtaer19030104.
- [32] S. Gresoi, G. Stamatescu, and I. Făgărășan, "Advanced Methodology for Fraud Detection in Energy Using Machine Learning Algorithms," *Appl. Sci.*, vol. 15, no. 6, p. 3361, Mar. 2025, doi: 10.3390/app15063361.
- [33] J. Li, "An Early Control Algorithm of Corporate Financial Risk Using Artificial Neural Networks," *Mob. Inf. Syst.*, vol. 2022, pp. 1–12, May 2022, doi: 10.1155/2022/4398602.
- [34] Z. Wang, "Application of CNN-based financial risk identification and management convolutional neural networks in financial risk," *Syst. Soft Comput.*, vol. 7, p. 200215, Dec. 2025, doi: 10.1016/j.sasc.2025.200215.
- [35] X. Song, Y. Jing, and X. Qin, "BP neural network-based early warning model for financial risk of internet financial companies," *Cogent Econ. Finance*, vol. 11, no. 1, p. 2210362, Dec. 2023, doi: 10.1080/23322039.2023.2210362.
- [36] S. Wei et al., "Combining intra-risk and contagion risk for enterprise bankruptcy prediction using graph neural networks," *Inf. Sci.*, vol. 659, p. 120081, Feb. 2024, doi: 10.1016/j.ins.2023.120081.
- [37] L. Yangyan and C. Tingting, "CRAFIC Framework: Multi-Account Collaborative Fraud Detection, Efficient Feature Extraction and Relationship Modelling Combined with CNN-LSTM and Graph Attention Network," *IET Commun.*, vol. 19, no. 1, p. e70014, Jan. 2025, doi: 10.1049/cmu2.70014.
- [38] J. Jin and Y. Zhang, "Innovation in Financial Enterprise Risk Prediction Model: A Hybrid Deep Learning Technique Based on CNN-Transformer-WT," *J. Organ. End User Comput.*, vol. 36, no. 1, pp. 1–26, Nov. 2024, doi: 10.4018/JOEUC.361650.
- [39] K. Zhou, "Financial model construction of a cross-border e-commerce platform based on machine learning," *Neural Comput. Appl.*, vol. 35, no. 36, pp. 25189–25199, Dec. 2023, doi: 10.1007/s00521-023-08456-6.
- [40] U. Dr.R., Dr. P. B. K. Chowdary, D. Dr.T., and S. Dr.R., "Integrated SVM-FFNN for Fraud Detection in Banking Financial Transactions," *J. Internet Serv. Inf. Secur.*, vol. 13, no. 4, pp. 12–25, Dec. 2023, doi: 10.58346/JISIS.2023.14.002.
- [41] M. Asmar and A. Tuqan, "Integrating machine learning for sustaining cybersecurity in digital banks," *Heliyon*, vol. 10, no. 17, p. e37571, Sep. 2024, doi: 10.1016/j.heliyon.2024.e37571.
- [42] A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," *IEEE Access*, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.
- [43] ABM. A. Azmee, P. Protim, Md. Aosaful, O. Dutta, and M. Iqbal, "Performance Analysis of Machine Learning Classifiers for Detecting PE Malware," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 1, 2020, doi: 10.14569/IJACSA.2020.0110163.
- [44] R. Wei and D. Ding, "Problems and Countermeasures of Financial Risk in Project Management Based on Convolutional Neural Network," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–7, Mar. 2022, doi: 10.1155/2022/1978415.
- [45] Y. Fan, "Research and Empirical Evidence of Machine Learning based Financial Statement Analysis Methods," *Scalable Comput. Pract. Exp.*, vol. 25, no. 6, Oct. 2024, doi: 10.12694/scpe.v25i6.3284.
- [46] M. Ma, "Research on the Development of Hospital Intelligent Finance Based on Artificial Intelligence," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–6, Aug. 2022, doi: 10.1155/2022/6549766.
- [47] G. Piao and B. Xiao, "Risk Management Analysis of Modern Commercial Banks Using Behavioral Finance Theory and Artificial Neural Networks," *Wirel. Commun. Mob. Comput.*, vol. 2022, no. 1, p. 1161784, Jan. 2022, doi: 10.1155/2022/1161784.
- [48] H. Zhao, "Risk Management of Supply Chain Green Finance Based on Sustainable Ecological Environment," *Sustainability*, vol. 15, no. 9, p. 7707, May 2023, doi: 10.3390/su15097707.
- [49] S. Yang and H. Wu, "The Global Organizational Behavior Analysis for Financial Risk Management Utilizing Artificial Intelligence," *J. Glob. Inf. Manag.*, vol. 30, no. 7, pp. 1–24, Dec. 2021, doi: 10.4018/JGIM.292455.
- [50] O. E. Akinbowale, P. Mashigo, and M. F. Zerihun, "The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry," *Cogent Bus. Manag.*, vol. 10, no. 1, p. 2163560, Dec. 2023, doi: 10.1080/23311975.2022.2163560.
- [51] M. Habibpour et al., "Uncertainty-aware credit card fraud detection using deep learning," *Eng. Appl. Artif. Intell.*, vol. 123, p. 106248, Aug. 2023, doi: 10.1016/j.engappai.2023.106248.
- [52] J. Liu and K. Chen, "Enterprise Financial Risk Prevention and Control and Data Analysis Method Based on Blockchain Technology," *Mob. Inf. Syst.*, vol. 2022, pp. 1–7, Jun. 2022, doi: 10.1155/2022/9452342.
- [53] A. Muaz, M. Jayabalan, and V. Thiruchelvam, "A Comparison of Data Sampling Techniques for Credit Card Fraud Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, 2020, doi: 10.14569/IJACSA.2020.0110660.
- [54] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *J. Big Data*, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.

- [55] A. Taha, "A novel deep learning-based hybrid Harris hawks with sine cosine approach for credit card fraud detection," *AIMS Math.*, vol. 8, no. 10, pp. 23200–23217, 2023, doi: 10.3934/math.20231180.
- [56] S. Wei and S. Lee, "Financial Anti-Fraud Based on Dual-Channel Graph Attention Network," *J. Theor. Appl. Electron. Commer. Res.*, vol. 19, no. 1, pp. 297–314, Feb. 2024, doi: 10.3390/jtaer19010016.
- [57] Z. Yang, Y. Wang, H. Shi, and Q. Qiu, "Leveraging Mixture of Experts and Deep Learning-Based Data Rebalancing to Improve Credit Fraud Detection," *Big Data Cogn. Comput.*, vol. 8, no. 11, p. 151, Nov. 2024, doi: 10.3390/bdcc8110151.
- [58] A. Tiwari, S. Chatterjee, S. Padmakumar, S. Nair, and B. Das, "Statistically inspired discrepancy detection for anomalous spatio-temporal graphs," *Int. J. Data Sci. Anal.*, Oct. 2024, doi: 10.1007/s41060-024-00656-0.
- [59] Y. Tang and Z. Liu, "A Distributed Knowledge Distillation Framework for Financial Fraud Detection Based on Transformer," *IEEE Access*, vol. 12, pp. 62899–62911, 2024, doi: 10.1109/ACCESS.2024.3387841.
- [60] Y. Xie, G. Liu, C. Yan, C. Jiang, M. Zhou, and M. Li, "Learning Transactional Behavioral Representations for Credit Card Fraud Detection," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 4, pp. 5735–5748, Apr. 2024, doi: 10.1109/TNNLS.2022.3208967.
- [61] 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.
- [62] S. Khan, A. Alourani, B. Mishra, A. Ali, and M. Kamal, "Developing a Credit Card Fraud Detection Model using Machine Learning Approaches," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 3, 2022, doi: 10.14569/IJACSA.2022.0130350.
- [63] A. Mutemi and F. Bacao, "E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review," *Big Data Min. Anal.*, vol. 7, no. 2, pp. 419–444, Jun. 2024, doi: 10.26599/BDMA.2023.9020023.
- [64] D. Wu, X. Ma, and D. L. Olson, "Financial distress prediction using integrated Z-score and multilayer perceptron neural networks," *Decis. Support Syst.*, vol. 159, p. 113814, Aug. 2022, doi: 10.1016/j.dss.2022.113814.
- [65] L. Ouyang, "Financial Risk Control of Listed Enterprises Based on Risk Warning Model," *Informatica*, vol. 48, no. 11, Aug. 2024, doi: 10.31449/inf.v48i11.6026.
- [66] Q. Du, "Financial Risk Prediction Model in the Context of Big Data - Corporate Financial Risk Control Based on LSTM Deep Neural Networks," *Appl. Math. Nonlinear Sci.*, vol. 9, no. 1, p. 20231422, Jan. 2024, doi: 10.2478/amns.2023.2.01422.
- [67] C. Zhang and X. Zhou, "Forecasting Credit Risk of SMEs in Supply Chain Finance Using Bayesian Optimization and XGBoost," *Math. Probl. Eng.*, vol. 2023, no. 1, p. 5609996, Jan. 2023, doi: 10.1155/2023/5609996.
- [68] J. Hu, T. Li, Y. Zhuang, S. Huang, and S. Dong, "GFD: A Weighted Heterogeneous Graph Embedding Based Approach for Fraud Detection in Mobile Advertising," *Secur. Commun. Netw.*, vol. 2020, pp. 1–12, Sep. 2020, doi: 10.1155/2020/8810817.
- [69] A. Kjamilji and O. B. Güney, "Highly efficient secure linear algebra for private machine learning classifications over malicious clients in the post-quantum world," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 9, p. 101718, Oct. 2023, doi: 10.1016/j.jksuci.2023.101718.
- [70] M. Alamri and M. Ykhlef, "Hybrid Feature Engineering Based on Customer Spending Behavior for Credit Card Anomaly and Fraud Detection," *Electronics*, vol. 13, no. 20, p. 3978, Oct. 2024, doi: 10.3390/electronics13203978.
- [71] B. Sang, "Application of genetic algorithm and BP neural network in supply chain finance under information sharing," *J. Comput. Appl. Math.*, vol. 384, p. 113170, Mar. 2021, doi: 10.1016/j.cam.2020.113170.
- [72] U. R., J. A., B. S.S., and S. R., "Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification," *J. Internet Serv. Inf. Secur.*, vol. 13, no. 4, pp. 138–157, Dec. 2023, doi: 10.58346/JISIS.2023.14.010.
- [73] C. L. Udeze, I. E. Eteng, and A. E. Ibor, "Application of Machine Learning and Resampling Techniques to Credit Card Fraud Detection," *J. Niger. Soc. Phys. Sci.*, p. 769, Aug. 2022, doi: 10.46481/jnsps.2022.769.
- [74] N. Biswas, A. S. Mondal, A. Kusumastuti, S. Saha, and K. C. Mondal, "Automated credit assessment framework using ETL process and machine learning," *Innov. Syst. Softw. Eng.*, vol. 21, no. 1, pp. 257–270, Mar. 2025, doi: 10.1007/s11334-022-00522-x.
- [75] Y. Wu, "Enterprise financial sharing and risk identification model combining recurrent neural networks with transformer model supported by blockchain," *Heliyon*, vol. 10, no. 12, p. e32639, Jun. 2024, doi: 10.1016/j.heliyon.2024.e32639.
- [76] H. Liao, H. Yue, Y. Lin, D. Li, and L. Zhang, "Enterprise Financing Risk Analysis and Internal Accounting Management Based on BP Neural Network Model," *Math. Probl. Eng.*, vol. 2022, pp. 1–13, May 2022, doi: 10.1155/2022/8627185.
- [77] K. Ghosh Dastidar, J. Jurgovsky, W. Siblini, and M. Granitzer, "NAG: neural feature aggregation framework for credit card fraud detection," *Knowl. Inf. Syst.*, vol. 64, no. 3, pp. 831–858, Mar. 2022, doi: 10.1007/s10115-022-01653-0.
- [78] B. Liu, F. Zhou, H. Jiang, and R. Ma, "A Kepler Optimization Algorithm-Based Convolutional Neural Network Model for Risk Management of Internet Enterprises," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 7, 2024, doi: 10.14569/IJACSA.2024.0150720.