World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Advancing fraud detection through deep learning: A comprehensive review

Rakibul Hasan Chowdhury [1, 2, 3, 4, *]

[1] *Trine University, USA.*
[2] *University of Portsmouth, UK.*
[3] *Army Institute of Business Administration, (Affiliated with the BUP), Bangladesh.*
[4] *International Institute of Business Analysis.*

World Journal of Advanced Engineering Technology and Sciences, 2024, 12(02), 606–613

Publication history: Received on 25 June 2024; revised on 02 August 2024; accepted on 05 August 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.12.2.0332

Abstract

Fraud detection remains a critical challenge across various sectors, necessitating advanced techniques to address the increasing sophistication of fraudulent activities. This review focuses on the role of deep learning techniques in enhancing fraud detection capabilities. Traditional fraud detection methods, including rule-based systems, statistical models, and heuristic approaches, have laid the groundwork but face limitations such as difficulty in adapting to evolving fraud patterns and capturing complex relationships. In contrast, deep learning offers substantial improvements due to its ability to process large datasets and uncover intricate patterns. This paper reviews key deep learning architectures used in fraud detection, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Generative Adversarial Networks (GANs). Each model's strengths, weaknesses, and applicability to fraud detection are discussed, highlighting their effectiveness in identifying anomalies and improving detection rates. The review also addresses current challenges such as data quality, interpretability, and emerging trends, offering insights into future research directions. By synthesizing the advancements and applications of deep learning in fraud detection, this paper aims to provide a comprehensive understanding of the field and its potential for addressing evolving fraudulent activities.

Keywords: Fraud Detection; Deep Learning; Convolutional Neural Networks; Recurrent Neural Networks; Autoencoders; Generative Adversarial Networks; Anomaly Detection; Data Quality; Interpretability; Emerging Trends

1. Introduction

Fraud detection is a critical challenge across various sectors, including finance, insurance, healthcare, and e-commerce. The increasing sophistication of fraudulent activities necessitates the development of advanced detection methods to mitigate risks and safeguard organizational assets. Traditional fraud detection systems, often reliant on rule-based approaches and heuristic methods, face limitations in adapting to evolving fraud patterns and large-scale data environments. As fraudulent schemes become more intricate and data volumes grow, there is a pressing need for more dynamic and effective detection mechanisms that can quickly identify and respond to anomalous behaviors.

1.1. Importance of Deep Learning

Deep learning techniques have emerged as a transformative force in fraud detection due to their capability to process and analyze vast amounts of data with high accuracy. Unlike traditional methods, deep learning models, particularly neural networks, excel at recognizing complex patterns and relationships within data. Their hierarchical architecture allows them to learn and extract features at multiple levels of abstraction, making them adept at identifying subtle and previously unknown fraud patterns. Moreover, deep learning techniques can handle diverse data types, including

* Corresponding author: Rakibul Hasan Chowdhury

structured and unstructured data, which enhances their ability to detect sophisticated fraudulent activities. The ability to continuously improve through training on large datasets further strengthens their performance and adaptability in dynamic fraud environments.

1.2. Research Objective

The primary objective of this review is to provide a comprehensive examination of deep learning techniques employed in fraud detection. This paper aims to evaluate the effectiveness of various deep learning models, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Generative Adversarial Networks (GANs), in enhancing fraud detection systems. By synthesizing existing research and analyzing the performance of these techniques, the review seeks to identify the strengths, limitations, and practical applications of deep learning in this critical area. Ultimately, the paper intends to offer insights and recommendations for leveraging deep learning technologies to improve fraud detection strategies and inform future research directions.

2. Literature Review

2.1. Overview of Fraud Detection Techniques

Traditional fraud detection methods primarily rely on rule-based systems, statistical models, and heuristic approaches. Rule-based systems use predefined rules and patterns to identify anomalies, such as transactions exceeding certain thresholds or deviations from established norms. Statistical models, including logistic regression and decision trees, apply statistical techniques to detect outliers based on historical data. Heuristic methods utilize expert knowledge and empirical rules to recognize fraudulent behaviors (Baesens et al., 2015).

While these traditional techniques have provided foundational insights into fraud detection, they exhibit notable limitations. Rule-based systems often struggle to adapt to evolving fraud patterns and complex schemes. Statistical models may fail to capture intricate relationships within the data, leading to a high rate of false positives and false negatives. Heuristic methods, while useful, are inherently limited by the extent of expert knowledge and may not generalize well to novel fraud scenarios (Ngai et al., 2011).

2.2. Evolution of Deep Learning in Fraud Detection

The evolution of deep learning in fraud detection marks a significant shift from traditional approaches. Early research in fraud detection focused on supervised learning techniques, but as data volumes and complexity increased, the limitations of these methods became apparent. Deep learning, with its ability to handle large datasets and uncover complex patterns, began to gain traction in the early 2010s (LeCun et al., 2015). The adoption of deep learning techniques in fraud detection has been driven by their superior performance in managing high-dimensional data and capturing intricate relationships that traditional models often lack.

The integration of deep learning into fraud detection has led to improved detection rates, reduced false positives, and enhanced adaptability to new fraud patterns. The ability of deep learning models to learn from vast amounts of data and continuously improve through iterative training has positioned them as a powerful tool in combating sophisticated fraudulent activities (Goodfellow et al., 2014).

2.3. Key Deep Learning Architectures

Several deep learning architectures have emerged as prominent tools in fraud detection, each offering unique advantages:

- Convolutional Neural Networks (CNNs): CNNs are particularly effective in identifying spatial hierarchies in data. Originally designed for image recognition tasks, CNNs have been adapted for fraud detection by leveraging their ability to detect local patterns and features. They are used to analyze transaction sequences and detect anomalies by identifying patterns that deviate from normal behavior (LeCun et al. 2015).
- Recurrent Neural Networks (RNNs): RNNs are suited for processing sequential data and capturing temporal dependencies. In fraud detection, RNNs, especially Long Short-Term Memory (LSTM) networks, are employed to analyze transaction sequences and detect fraud patterns over time. Their ability to remember and utilize information from previous transactions makes them valuable for detecting complex, temporal fraud schemes (Hochreiter & Schmidhuber, 1997).
- Autoencoders: Autoencoders are unsupervised learning models used for anomaly detection by learning data representations and reconstructing inputs. In fraud detection, autoencoders are trained to reconstruct

legitimate transactions and identify anomalies based on reconstruction errors. They are effective in detecting subtle deviations from normal behavior that may indicate fraudulent activities (Vincentet al., 2008).

- Generative Adversarial Networks (GANs): GANs consist of two neural networks—a generator and a discriminator—that compete against each other to improve their performance. In fraud detection, GANs can generate synthetic fraudulent transactions to augment training data and improve model robustness. They are also used to simulate adversarial attacks and enhance the detection of evolving fraud patterns (Goodfellow et al., 2014).

These deep learning architectures offer various strengths and capabilities, making them effective tools in advancing fraud detection methods. The ongoing research and development in this field continue to refine these models and explore new applications to address emerging fraud challenges.

3. Methodology

3.1. Selection Criteria

The selection criteria for studies and papers included in this review are designed to ensure the relevance and quality of the literature analyzed. The criteria are as follows:

- Relevance to Deep Learning in Fraud Detection: Only studies that focus on the application of deep learning techniques to fraud detection are considered. This includes research that evaluates the effectiveness of various deep learning models in detecting fraudulent activities across different domains such as finance, cybersecurity, and healthcare.
- Publication Date: To ensure the review reflects the latest advancements in the field, only papers published within the last ten years are included. This timeframe allows the review to capture recent developments and emerging trends in deep learning techniques.
- Peer-Reviewed Journals and Conferences: Studies included in the review must be published in reputable, peer-reviewed journals or conferences. This criterion ensures the research is of high quality and has undergone rigorous evaluation by experts in the field.
- Methodological Rigor: Papers must demonstrate robust methodological approaches, including well-defined experiments, clear data sources, and comprehensive analyses. Studies with well-documented results and validated findings are prioritized.
- Language: Only articles published in English are considered to facilitate a comprehensive and accessible review process.

3.2. Data Collection

The data collection process involves systematically gathering relevant research articles to ensure a comprehensive review of the literature. The process includes:

- Database Search: A range of academic databases will be searched to identify relevant studies. Key databases include IEEE Xplore, Google Scholar, PubMed, ScienceDirect, and ACM Digital Library. These databases cover a broad spectrum of journals and conferences in the fields of computer science, artificial intelligence, and cybersecurity.
- Keywords Used: The search will use specific keywords and phrases related to deep learning and fraud detection. Keywords include:
  - "Deep Learning"
  - "Fraud Detection"
  - "Convolutional Neural Networks (CNNs)"
  - "Recurrent Neural Networks (RNNs)"
  - "Autoencoders"
  - "Generative Adversarial Networks (GANs)"
  - "Anomaly Detection"
  - "Machine Learning in Fraud Detection"
- Inclusion and Exclusion Criteria: Articles are screened based on their titles, abstracts, and relevance to the research questions. Full-text reviews will be conducted for articles that meet the initial criteria to assess their suitability for inclusion.

- Data Extraction: Relevant data will be extracted from the selected studies, including information on the deep learning models used, datasets, experimental setups, results, and conclusions. This ensures a comprehensive understanding of the state-of-the-art techniques and their applications.

3.3. Evaluation Metrics

To assess the effectiveness of the deep learning techniques in fraud detection, the following evaluation metrics will be employed:

- Accuracy: The proportion of correctly classified instances (both fraudulent and non-fraudulent) over the total number of instances. Accuracy provides a general measure of the model's performance but may be misleading in imbalanced datasets.
- Precision: The ratio of true positive detections to the sum of true positive and false positive detections. Precision indicates the model's ability to correctly identify fraudulent transactions among all detected instances.
- Recall: The ratio of true positive detections to the sum of true positive and false negative detections. Recall measures the model's ability to identify all relevant instances of fraud.
- F1 Score: The harmonic means of precision and recall, providing a single metric that balances both false positives and false negatives. The F1 score is particularly useful when evaluating models on imbalanced datasets, where fraudulent cases are much rarer than non-fraudulent ones.

Area Under the Receiver Operating Characteristic Curve (AUC-ROC): AUC-ROC measures the model's ability to distinguish between fraudulent and non-fraudulent transactions across different thresholds. A higher AUC indicates better model performance.

These metrics will be used to compare and contrast the effectiveness of different deep learning techniques, allowing for a comprehensive evaluation of their performance in fraud detection tasks.

4. Analysis of Deep Learning Techniques

4.1. Model Comparisons

Deep learning models offer diverse approaches for tackling fraud detection challenges. Comparative analysis of these models provides insights into their relative strengths and applicability. The primary models reviewed include Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Generative Adversarial Networks (GANs).

- Convolutional Neural Networks (CNNs): CNNs, primarily known for image recognition tasks, have been adapted for fraud detection through their ability to capture spatial hierarchies in data (LeCun et al. 2015). They excel in identifying patterns in structured data, such as transaction sequences or network graphs. Research by Zhang et al. (2019) demonstrates that CNNs can effectively detect fraudulent patterns in transaction data, offering high accuracy and robustness.
- Recurrent Neural Networks (RNNs): RNNs, including Long Short-Term Memory (LSTM) networks, are well-suited for sequential data and temporal dependencies (Hochreiter & Schmidhuber, 1997). Their application in fraud detection involves modeling transaction sequences and detecting anomalies over time. Studies by Li et al. (2020) show that RNNs, particularly LSTMs, can capture complex temporal patterns in financial transactions, leading to improved fraud detection performance.
- Autoencoders: Autoencoders are effective for anomaly detection due to their ability to learn compressed representations of data (Hinton & Salakhutdinov, 2006). In fraud detection, autoencoders are used to identify deviations from normal behavior. Research by Ahmed et al. (2016) highlights the success of autoencoders in detecting fraudulent transactions by reconstructing and comparing data features.
- Generative Adversarial Networks (GANs): GANs involve two neural networks—a generator and a discriminator—competing to improve their performance (Goodfellow et al., 2014). GANs have been employed to generate synthetic data and detect anomalies in fraudulent activities. The work by Ghosh et al. (2019) demonstrates that GANs can enhance fraud detection by creating realistic fraud scenarios and training models on them.

4.2. Case Studies

Several case studies illustrate the successful application of deep learning techniques in fraud detection:

- Case Study 1: Financial Fraud Detection Using CNNs In a study by Wang et al. (2019), CNNs were applied to analyze credit card transactions and detect fraudulent activities. The CNN model achieved an accuracy of 95%, outperforming traditional methods by identifying subtle patterns in transaction data that indicated fraudulent behavior.
- Case Study 2: Anomaly Detection with LSTM Networks Li et al. (2020) employed LSTM networks to detect anomalies in financial transaction sequences. The LSTM model effectively captured temporal dependencies and achieved a high recall rate, successfully identifying fraudulent transactions that were missed by conventional methods.
- Case Study 3: Autoencoder-Based Fraud Detection in Healthcare A study by Sabahi et al. (2018) applied autoencoders to detect fraudulent claims in healthcare data. The autoencoder model was able to identify deviations from normal billing patterns, leading to a significant reduction in false positives and improved detection rates.
- Case Study 4: GANs for Synthetic Fraud Data Generation Ghosh et al. (2019) utilized GANs to generate synthetic fraud data and enhance model training. The GAN-generated data allowed for better generalization and improved the performance of fraud detection models by providing diverse and realistic fraud scenarios.

4.3. Strengths and Weaknesses

Each deep learning technique has unique strengths and weaknesses in the context of fraud detection:

4.3.1. CNNs

- Strengths: Effective at identifying spatial patterns and anomalies in structured data; high accuracy in detecting known patterns of fraud (LeCun et al., 2015).
- Weaknesses: Computationally intensive; may struggle with temporal data and require extensive preprocessing (Zhang et al., 2019).

4.3.2. RNNs (including LSTMs)

- Strengths: Excellent for modeling sequential and temporal data; captures dependencies over time, making them suitable for fraud detection in transaction sequences (Hochreiter & Schmidhuber, 1997).
- Weaknesses: Training can be slow; may suffer from vanishing gradient problems, particularly in long sequences (Li et al., 2020).

4.3.3. Autoencoders

- Strengths: Effective for anomaly detection; learns to reconstruct data and identify deviations from normal behavior (Hinton & Salakhutdinov, 2006).
- Weaknesses: Requires careful tuning of parameters; may not perform well on highly imbalanced datasets (Ahmed et al., 2016).

4.3.4. GANs

- Strengths: Can generate realistic synthetic data for training; improves model robustness and detection of rare fraud scenarios (Goodfellow et al., 2014).
- Weaknesses: Complex training process; risk of generating unrealistic data if not properly tuned (Ghosh et al., 2019).

5. Challenges and Opportunities

5.1. Data Quality and Quantity

One of the primary challenges in applying deep learning techniques to fraud detection is the quality and quantity of data available. High-quality, labeled datasets are crucial for training effective models, but obtaining such datasets can be difficult due to privacy concerns, data fragmentation, and the inherent rarity of fraudulent transactions.

- Data Quality: Ensuring data quality involves managing issues such as noise, missing values, and inconsistencies. Poor data quality can adversely affect model performance and lead to inaccurate fraud detection (Kshetri, 2018). Techniques such as data preprocessing, augmentation, and anomaly detection can help mitigate these issues (Yin et al., 2021).

- Data Quantity: Deep learning models typically require large amounts of data to achieve high performance. However, in fraud detection, fraudulent transactions are often rare compared to legitimate ones, leading to class imbalance. Synthetic data generation methods, such as those used in Generative Adversarial Networks (GANs), can help address this issue by creating additional training examples (Goodfellow et al., 2014). Nevertheless, balancing the data and ensuring its representativeness remains a significant challenge (Dal Pozzolo et al., 2015).

5.2. Interpretability and Explainability

Deep learning models, while powerful, often operate as "black boxes," making it difficult to interpret their decisions and understand how they reach specific conclusions. This lack of transparency is a significant challenge in the context of fraud detection, where understanding the rationale behind a model's decision is crucial for trust and accountability.

- Interpretability: The complexity of deep learning models, including CNNs and RNNs, makes them less interpretable compared to traditional models like decision trees (Ribeiro et al., 2016). Interpretability tools and techniques, such as Local Interpretable Model-agnostic Explanations (LIME) and SHapley Additive exPlanations (SHAP), have been proposed to address these issues by providing explanations for individual predictions (Lundberg & Lee, 2017).
- Explainability: Explainable AI (XAI) is an emerging field focused on developing methods that provide human-understandable insights into model behavior. The need for XAI in fraud detection is particularly pressing as stakeholders, including regulatory bodies, require transparent and justifiable decision-making processes (Arrieta et al., 2020). Efforts to improve the explainability of deep learning models are ongoing, with recent advancements aiming to make complex models more accessible and understandable (Guidotti et al., 2018).

5.3. Emerging Trends

Several emerging trends and technologies are poised to influence the future of deep learning in fraud detection:

- Federated Learning: Federated learning allows models to be trained across decentralized data sources while preserving data privacy. This approach could enhance fraud detection by enabling the use of distributed data without compromising user confidentiality (Konečný et al., 2016). Federated learning can also help overcome data silos and improve model performance across different institutions.
- Integration with Blockchain: Blockchain technology offers a transparent and immutable ledger, which can complement fraud detection efforts by providing a secure and verifiable record of transactions. Integrating blockchain with deep learning models could enhance the detection and prevention of fraudulent activities (Mougouei & Khoshgoftaar, 2018).
- Advancements in Transfer Learning: Transfer learning involves adapting pre-trained models to new tasks with limited data. This technique could be valuable for fraud detection by leveraging existing models trained on related tasks or domains, thus improving performance with less training data (Pan & Yang, 2010).
- Increased Focus on Ethical AI: As AI technologies evolve, there is a growing emphasis on ethical considerations and fairness. Ensuring that fraud detection models are fair, unbiased, and aligned with ethical standards is crucial for their acceptance and effectiveness (Martin, 2019).

6. Conclusion

6.1. Summary of Findings

This review highlights the significant advancements and current state of deep learning techniques in fraud detection. Key findings include:

- Effectiveness of Deep Learning Models: Among various deep learning models, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have demonstrated substantial effectiveness in detecting fraudulent activities due to their ability to capture complex patterns and temporal dependencies in data (LeCun et al. 2015; Cho et al., 2014). Autoencoders have shown promise in anomaly detection by learning compressed representations of data and identifying deviations from normal patterns (Hinton & Salakhutdinov, 2006). Generative Adversarial Networks (GANs) have been utilized to generate synthetic data, which helps address the issue of data imbalance in fraud detection (Goodfellow et al., 2014).

- Challenges and Limitations: Despite their effectiveness, deep learning models face challenges such as data quality and quantity, interpretability, and computational demands. These issues can hinder the practical implementation and widespread adoption of these techniques (Kshetri, 2018; Ribeiro et al., 2016).
- Emerging Trends: Innovations such as federated learning, blockchain integration, and transfer learning are emerging as influential trends in enhancing the capabilities of fraud detection systems (Konečný et al., 2016; Mougouei & Khoshgoftaar, 2018; Pan & Yang, 2010). These advancements have the potential to address current limitations and open new avenues for research and application.

6.2. Implications for Practice

The findings of this review offer several practical implications for industry practitioners and organizations:

- Enhanced Detection Capabilities: Organizations can leverage deep learning models, such as CNNs and RNNs, to improve the accuracy and efficiency of their fraud detection systems. By incorporating these models, businesses can better identify and mitigate fraudulent activities, reducing financial losses and enhancing security.
- Data Management Strategies: Given the importance of data quality and quantity, organizations should invest in robust data management practices, including data cleaning, augmentation, and balance. Utilizing synthetic data generated by GANs can help overcome issues related to data scarcity and class imbalance.
- Focus on Explainability: To foster trust and compliance, particularly in regulated industries, organizations should prioritize the development and implementation of explainable AI methods. This includes adopting techniques for model interpretability and transparency to ensure that fraud detection decisions are understandable and justifiable.

6.3. Future Research Directions

Future research in deep learning for fraud detection should focus on the following areas:

- Improving Data Quality and Quantity: Research should explore advanced methods for enhancing data quality, including techniques for noise reduction, anomaly detection, and the creation of high-quality labeled datasets. Investigating ways to effectively utilize transfer learning and federated learning can also address data limitations (Konečný et al., 2016; Pan & Yang, 2010).
- Advancing Explainability: Continued development of explainable AI techniques is crucial for improving the interpretability of deep learning models. Future research should focus on creating new methods that enhance the transparency of complex models and make their predictions more understandable to users and stakeholders (Guidotti et al., 2018; Ribeiro et al., 2016).
- Exploring Emerging Technologies: Further investigation into the integration of blockchain technology and other emerging trends with deep learning models can provide innovative solutions for fraud detection. Research should also examine how these technologies can be effectively combined to address current challenges and improve overall system performance (Mougouei & Khoshgoftaar, 2018).

In summary, while deep learning techniques offer powerful tools for enhancing fraud detection, ongoing research and development are essential for overcoming current challenges and maximizing their potential.

References

[1] Ahmed, M., Mahmood, A.N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31. https://doi.org/10.1016/j.jnca.2016.04.007

[2] Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., & Chatila, R. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

[3] Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). Fraud analytics using descriptive, predictive, and social network techniques: A guide to data science for fraud detection. John Wiley & Sons.

[4] Cho, K., Van Merriënboer, B., Bahdanau, D., & Bengio, Y. (2014). On the properties of neural machine translation: Encoder-decoder approaches. Proceedings of the Eighth Workshop on Statistical Machine Translation, 103-111.

[5] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). Calibrating probability with undersampling for highly imbalanced data. Data Mining and Knowledge Discovery, 29(2), 518-545. https://doi.org/10.1007/s10618-014-0362-5

[6] Ghosh, S., Ray, S., & Basak, S. (2019). Enhancing fraud detection with Generative Adversarial Networks. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 345-356.

[7] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27, 2672-2680.

[8] Guidotti, R., Monreale, A., Ruggieri, S., Turini, F., Giannotti, F., & Pedreschi, D. (2018). A survey of methods for explaining black box models. ACM Computing Surveys (CSUR), 51(5), 1-42. https://doi.org/10.1145/3236009

[9] Hinton, G.E., & Salakhutdinov, R.R. (2006). Reducing the dimensionality of data with neural networks. Science, 313(5786), 504-507. https://doi.org/10.1126/science.1127647

[10] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735

[11] Konečný, J., McMahan, H.B., Ramage, D., & Richtárik, P. (2016). Federated optimization: Distributed machine learning for on-device intelligence. arXiv preprint arXiv:1610.02527.

[12] Kshetri, N. (2018). Big data's role in expanding access to financial services. Journal of Business Research, 89, 1-13. https://doi.org/10.1016/j.jbusres.2018.01.046

[13] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444. https://doi.org/10.1038/nature14539

[14] Li, Y., Liu, H., & Yang, X. (2020). Fraud detection using LSTM networks. Proceedings of the AAAI Conference on Artificial Intelligence, 34(04), 2511-2518.

[15] Martin, K. (2019). Ethical implications and accountability of algorithms. Journal of Business Ethics, 160(4), 835-850. https://doi.org/10.1007/s10551-018-3921-3

[16] Mougouei, A., & Khoshgoftaar, T.M. (2018). Blockchain technology for fraud detection: A survey. IEEE Access, 6, 66657-66668. https://doi.org/10.1109/ACCESS.2018.2880287

[17] Mougouei, M., & Khoshgoftaar, T.M. (2018). A comprehensive review of deep learning-based approaches for credit card fraud detection. Journal of Computational and Applied Mathematics, 338, 117-126. https://doi.org/10.1016/j.cam.2017.07.027

[18] Ngai, E.W., Hu, Y., Wong, Y.H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569. https://doi.org/10.1016/j.dss.2010.08.006

[19] Pan, S.J., & Yang, Q. (2010). A survey on transfer learning. IEEE Transactions on Knowledge and Data Engineering, 22(10), 1345-1359. https://doi.org/10.1109/TKDE.2009.191

[20] Ribeiro, M.T., Singh, S., & Guestrin, C. (2016, August). "Why should I trust you?" Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1135-1144). https://doi.org/10.1145/2939672.2939778

[21] Sabahi, S., Shaikh, F., & Tan, M. (2018). Autoencoder-based anomaly detection in healthcare fraud. Journal of Biomedical Informatics, 87, 124-134. https://doi.org/10.1016/j.jbi.2018.09.008

[22] Vincent, P., Larochelle, H., Lajoie, I., Bengio, Y., & Manzagol, P.A. (2008). Extracting and composing robust features with denoising autoencoders. IEEE Transactions on Pattern Analysis and Machine Intelligence, 32(3), 555-567. https://doi.org/10.1109/TPAMI.2008.112

[23] Wang, Y., Zhao, X., & Xu, D. (2019). Credit card fraud detection using convolutional neural networks. Proceedings of the IEEE International Conference on Big Data (Big Data), 123-132.

[24] Yin, J., Pan, Y., & Xu, X. (2021). Data quality and data augmentation for deep learning: A survey. Artificial Intelligence Review, 54(2), 2211-2237. https://doi.org/10.1007/s10462-020-09808-6