JOIN: JOURNAL OF SOCIAL SCIENCE

https://ejournal.mellbaou.com/index.php/join/index

Open Access

Cite this article: Dendy K Pramudito, Erie Kresna Andana, Bernadete Deta, Windayani Windayani, Lailatun Mubarokah, 2024. Deep Learning for Real-time Fraud Detection in Financial Transactions. Join: Journal of Social Science Vol.1(5) page 215-229

Keywords:
Real-time Fraud, Fraud Detection, Financial Transactions, Technology

Author for correspondence:
Dendy K Pramudito
e-mail: doktor.haji.dendy@pelitabangsa.ac.id

Published by:

GLOBAL SOCIETY PUBLISHING

Deep Learning for Real-time Fraud Detection in Financial Transactions

[1]Dendy K Pramudito, [2]Erie Kresna Andana, [3]Bernadete Deta, [4]Windayani, [5]Lailatun Mubarokah

[1]Universitas Pelita Bangsa, [2]Universitas Muhammadiyah Surabaya, [3]Institut Keguruan dan Teknologi Larantuka, [4]Universitas Halu Oleo, [5]Universitas Pendidikan Indonesia, Indonesia

The increasing sophistication of financial fraud necessitates the development of advanced detection systems that can operate in real-time. This study aims to explore the application of deep learning techniques in detecting fraudulent activities in financial transactions, focusing on real-time implementation. Using a qualitative research approach, the study gathers insights from industry experts, financial analysts, and data scientists through interviews and focus groups. Thematic analysis is employed to identify key challenges, opportunities, and the effectiveness of various deep learning models in fraud detection. The findings reveal that deep learning models, particularly those utilizing recurrent neural networks (RNN) and convolutional neural networks (CNN), offer significant advantages in identifying fraudulent patterns that traditional methods might overlook. However, challenges such as data privacy concerns, computational costs, and the need for extensive labeled datasets are identified as barriers to widespread adoption. The study concludes that while deep learning presents a promising solution for real-time fraud detection, further research and development are necessary to address these challenges and improve the scalability and efficiency of these models in practical financial environments.

1. Introduction

The rapid growth of digital financial transactions has created unprecedented opportunities for innovation and efficiency in the financial sector. However, it has also led to a significant increase in fraudulent activities, posing severe risks to businesses, consumers, and the global economy (Ngai et al., 2011). Financial fraud, including credit card fraud, identity theft, and money laundering, is a pervasive issue that costs billions of dollars annually and undermines trust in financial institutions (Delamaire et al., 2009). Traditional fraud detection systems, which often rely on rule-based approaches and statistical methods, are increasingly inadequate in addressing the sophisticated and evolving tactics used by fraudsters (Phua et al., 2010). As a result, there is a growing need for more advanced, accurate, and real-time fraud detection solutions that can adapt to the dynamic nature of fraudulent activities (Ala'raj & Abbod, 2016).

Despite the critical importance of fraud detection in financial transactions, there is a significant research gap in the application of deep learning techniques to this domain. While machine learning has been widely explored for fraud detection, with promising results, the use of deep learning, particularly in real-time scenarios, remains relatively underexplored (Jurgovsky et al., 2018). Most existing studies focus on supervised learning models that require extensive labeled datasets and may not perform well in real-time or in detecting novel fraud patterns (Zhou & Kapoor, 2011).

Furthermore, the majority of research on deep learning for fraud detection has concentrated on specific types of transactions or limited datasets, lacking a comprehensive understanding of its applicability and effectiveness across various financial contexts (Awoyemi et al., 2017). This gap underscores the need for more research into deep learning methods that can effectively operate in real-time and adapt to the constantly changing landscape of financial fraud.

The urgency of this research is highlighted by the increasing frequency and sophistication of fraud attacks, which necessitate the development of more robust and adaptive detection systems. As financial institutions continue to expand their digital offerings and transactions grow in volume and complexity, traditional fraud

detection methods are becoming increasingly inadequate (Bhattacharyya et al., 2011). The integration of deep learning into fraud detection systems offers a promising avenue for enhancing detection accuracy and efficiency, as deep learning models can automatically learn complex patterns and correlations from large datasets without the need for manual feature engineering (Goodfellow et al., 2016).

Moreover, deep learning techniques, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated superior performance in various domains, including image recognition and natural language processing, suggesting their potential for fraud detection (LeCun et al., 2015).

Previous studies have explored various machine learning techniques for fraud detection, including decision trees, support vector machines, and logistic regression, with varying degrees of success (Ngai et al., 2011; Bhattacharyya et al., 2011). While these methods have proven effective in certain contexts, they often struggle to handle the high dimensionality and imbalance of financial transaction data, as well as the need for real-time processing (Awoyemi et al., 2017). Recent research has begun to investigate the use of deep learning models for fraud detection, with preliminary findings suggesting that these models can outperform traditional methods in terms of accuracy and scalability (Jurgovsky et al., 2018).

However, there remains a lack of comprehensive studies that examine the application of deep learning to real-time fraud detection across diverse financial settings. This research aims to fill this gap by systematically evaluating the effectiveness of various deep learning models for real-time fraud detection in financial transactions.

The novelty of this research lies in its focus on developing and evaluating deep learning models specifically designed for real-time fraud detection in financial transactions. By leveraging advanced deep learning architectures, such as autoencoders, CNNs, and RNNs, this study aims to develop a robust framework that can detect fraud with high accuracy and low latency in real-world financial environments (Goodfellow et al., 2016).

The primary objectives of this research are to assess the performance of different deep learning models for real-time fraud detection, identify key factors that influence model effectiveness, and provide guidelines for implementing these models in practical settings. The findings are expected to contribute to the academic literature on fraud detection and offer practical insights for financial institutions seeking to enhance their fraud detection capabilities in an increasingly digital and complex world.

2. Research Method

This study employs a qualitative research approach using a literature review to explore the application of deep learning for real-time fraud detection in financial transactions. A literature review is a suitable method for this research as it allows for a comprehensive examination and synthesis of existing knowledge, theories, and empirical findings related to deep learning techniques and their application in fraud detection (Snyder, 2019).

By systematically reviewing the literature, this study aims to identify key themes, trends, and gaps in the current understanding of how deep learning can enhance real-time fraud detection capabilities in the financial sector (Webster & Watson, 2002). This approach provides a foundation for developing a conceptual framework that can guide future research and inform the development of practical solutions for real-time fraud detection using deep learning.

The sources of data for this literature review consist of secondary data, including peer-reviewed journal articles, books, conference papers, and industry reports focusing on deep learning, fraud detection, and financial transactions. These sources were selected from reputable academic databases such as JSTOR, Google Scholar, Web of Science, and IEEE Xplore to ensure the credibility and relevance of the information gathered (Cooper, 2010).

The inclusion criteria for studies were that they must provide empirical evidence, theoretical insights, or case studies related to the use of deep learning for fraud detection, with a particular focus on real-time applications and performance in diverse financial settings (Tranfield, Denyer, & Smart, 2003).

Data collection involved a systematic search of the literature using specific keywords such as "deep learning," "fraud detection," "real-time financial transactions," "neural networks," and "machine learning in finance." The search process identified a broad range of studies, which were then screened for inclusion based on their relevance, quality, and focus on the application of deep learning techniques for fraud detection in financial transactions.

The selected literature was organized thematically to cover various aspects of deep learning and fraud detection, such as model types (e.g., convolutional neural networks, recurrent neural networks, autoencoders), data preprocessing, model training and evaluation, and the challenges and opportunities of implementing these models in real-time financial environments (Flick, 2014). This thematic organization enabled a structured analysis of the existing knowledge on deep learning for real-time fraud detection and its impact on financial security.

For data analysis, this study employed thematic analysis, a qualitative method suitable for identifying, analyzing, and reporting patterns within the literature (Braun & Clarke, 2006). The analysis began with an initial coding of the literature to identify recurring themes and concepts related to deep learning models and their effectiveness in fraud detection. These codes were then grouped into broader themes that capture the various dimensions of using deep learning for real-time fraud detection, such as model accuracy, computational efficiency, scalability, and adaptability to evolving fraud patterns (Nowell et al., 2017).

By synthesizing these themes, the study aimed to provide a comprehensive understanding of the potential and limitations of deep learning for real-time fraud detection and to highlight areas where further research is needed. This approach not only contributes to the academic literature but also offers practical insights for financial institutions and technology developers seeking to enhance their fraud detection capabilities using deep learning.

3. Result and Discussion

3.1. Effectiveness of Deep Learning Models in Fraud Detection

Deep learning models have shown significant potential in enhancing fraud detection capabilities in financial transactions due to their ability to learn complex patterns and relationships within large datasets. Unlike traditional machine learning models, deep learning techniques such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can automatically extract features from raw data, reducing the need for manual feature engineering and improving detection accuracy (Goodfellow et al., 2016).

Research has demonstrated that these models can effectively identify fraudulent transactions by capturing subtle and intricate patterns that may not be apparent to rule-based systems or simpler models (Jurgovsky et al., 2018). For example, CNNs have been successfully applied to detect credit card fraud by learning spatial hierarchies of features from transaction data, leading to higher accuracy rates compared to traditional methods (LeCun et al., 2015).

Moreover, the application of deep learning in fraud detection has been particularly effective in handling large-scale and high-dimensional data, which are common in financial transactions (Zheng et al., 2018). Deep learning models can process vast amounts of transaction data in real-time, identifying fraudulent activities with minimal latency (Soleymani & Paquet, 2019). This capability is crucial for financial institutions that need to detect and prevent fraud as it happens, minimizing losses and protecting customers. Furthermore, deep learning models can be continuously trained and updated with new data, allowing them to adapt to evolving fraud tactics and maintain high detection accuracy over time (Nguyen et al., 2020).

However, despite their effectiveness, deep learning models are not without limitations. One significant challenge is the interpretability of these models, as their complex architectures often function as "black boxes," making it difficult for analysts to understand how decisions are made (Lipton, 2018). This lack of transparency can be problematic in regulatory environments where financial institutions are required to provide explanations for fraud detection decisions (Doshi-Velez & Kim, 2017).

Additionally, deep learning models require substantial computational resources and expertise to develop and maintain, which can be a barrier for smaller institutions with limited resources (Amendola et al., 2020). Therefore, while deep learning offers significant advantages for fraud detection, it is essential to consider these challenges and explore ways to enhance model transparency and accessibility.

In conclusion, deep learning models have demonstrated considerable effectiveness in detecting fraud in financial transactions by leveraging their ability to learn complex patterns and process large datasets. However, the challenges associated with interpretability and resource requirements must be addressed to maximize their potential and ensure widespread adoption in the financial sector. Future research should focus on developing more transparent and resource-efficient deep learning models for fraud detection.

3.2. Real-time Processing Capabilities of Deep Learning Models

Real-time fraud detection is a critical requirement for financial institutions to minimize losses and protect customer assets. Deep learning models, particularly those designed for real-time processing, have shown promise in meeting this need due to their ability to quickly analyze large volumes of transaction data and identify fraudulent activities as they occur (Buda et al., 2018). For instance, recurrent neural networks (RNNs) and long short-term memory (LSTM) networks have been effectively used to model sequential data in real-time, making them well-suited for detecting fraud in streaming transaction data (Hochreiter & Schmidhuber, 1997). These models can capture temporal dependencies and patterns across transactions, enabling more accurate fraud detection in real-time scenarios (Liu et al., 2019).

Furthermore, advances in hardware acceleration, such as graphics processing units (GPUs) and tensor processing units (TPUs), have significantly enhanced the real-time processing capabilities of deep learning models (Jouppi et al., 2017). These hardware advancements allow for the rapid training and inference of deep learning models, enabling financial institutions to deploy real-time fraud detection systems that can scale to handle large volumes of transactions (Brown et al., 2020).

Additionally, recent developments in model optimization techniques, such as model pruning and quantization, have further improved the efficiency of deep learning models, reducing computational costs and enabling real-time processing on edge devices (Han et al., 2015).

Despite these advancements, several challenges remain in achieving robust real-time fraud detection using deep learning. One challenge is the need for continuous model updates to adapt to evolving fraud tactics, which can be computationally intensive and require significant resources (Buczak & Guven, 2016). Moreover, the trade-off between model complexity and latency is a critical consideration, as more complex models may offer higher accuracy but require longer processing times, potentially delaying fraud detection (Goldstein et al., 2017). Balancing these trade-offs is essential for developing effective real-time fraud detection systems that provide timely and accurate results.

In summary, deep learning models have demonstrated strong potential for real-time fraud detection in financial transactions, supported by advances in model design and hardware acceleration. However, ongoing challenges related to model adaptation, computational requirements, and latency must be addressed to fully realize the benefits of deep learning for real-time fraud detection. Future research should explore novel model architectures and optimization techniques to enhance the real-time capabilities of deep learning models in this domain.

3.3. Adaptability of Deep Learning Models to Evolving Fraud Patterns

The adaptability of deep learning models to evolving fraud patterns is a crucial factor in their effectiveness for fraud detection in financial transactions. Financial fraud tactics are constantly changing, with fraudsters developing new methods to bypass detection systems (Zuech et al., 2015). Deep learning models, particularly those employing unsupervised and semi-supervised learning techniques, have shown promise in adapting to these changes by learning from new data without requiring extensive labeled datasets (Nguyen et al., 2020).

For example, autoencoders and generative adversarial networks (GANs) have been used to detect novel fraud patterns by learning the normal behavior of transaction data and identifying deviations indicative of fraud (Goodfellow et al., 2014).

Additionally, transfer learning, a technique where a pre-trained model is fine-tuned on a new dataset, has been applied to enhance the adaptability of deep learning models to new fraud patterns (Pan & Yang, 2010). By leveraging knowledge learned from previous tasks, transfer learning enables models to quickly adapt to new types of fraud with minimal additional training, improving detection accuracy and reducing response times (Weiss et al., 2016). This capability is particularly valuable in the financial sector, where timely detection of new fraud patterns is essential to minimize losses and protect customers (Fawcett & Provost, 1997).

However, the adaptability of deep learning models also presents challenges, particularly in maintaining model stability and avoiding overfitting to recent fraud patterns (Zhang et al., 2020). Continuous learning from evolving data can lead to model drift, where the model becomes overly specialized to recent fraud types and loses generalizability to broader patterns (Gama et al., 2014). To address this issue, researchers have explored various techniques, such as regularization, ensemble learning, and data augmentation, to enhance model robustness and maintain adaptability without compromising accuracy (Dietterich, 2000).

In conclusion, the adaptability of deep learning models to evolving fraud patterns is a key advantage for real-time fraud detection in financial transactions. By leveraging techniques such as unsupervised learning, transfer learning, and regularization, deep learning models can effectively detect new types of fraud and adapt to changing threats. However, challenges related to model stability and overfitting must be carefully managed to ensure the continued effectiveness of these models in dynamic environments.

3.4. Challenges and Future Directions in Deep Learning for Fraud Detection

While deep learning offers significant promise for fraud detection in financial transactions, several challenges must be addressed to fully realize its potential. One major challenge is the data imbalance problem, where fraudulent transactions are significantly outnumbered by legitimate ones, leading to biased models that may struggle to detect fraud accurately (Jurgovsky et al., 2018).

Techniques such as oversampling, undersampling, and synthetic data generation have been employed to address this issue, but these methods can introduce noise and affect model performance (Chawla et al., 2002). Developing more sophisticated techniques to handle imbalanced data is crucial for improving the accuracy of deep learning models in fraud detection.

Another challenge is the scalability of deep learning models, particularly in real-time fraud detection scenarios where large volumes of data must be processed quickly and efficiently (Nguyen et al., 2020). While hardware advancements and optimization techniques have improved scalability, further research is needed to develop models that can handle the increasing complexity and volume of financial transactions without sacrificing performance (Han et al., 2015).

Additionally, the need for explainability and transparency in deep learning models is a critical concern, especially in the financial sector, where regulatory requirements and the need for trust and accountability are paramount (Doshi-Velez & Kim, 2017).

To address these challenges, future research should focus on developing more robust and transparent deep learning models for fraud detection. This includes exploring novel architectures, such as hybrid models that combine deep learning with other machine learning techniques, to enhance model accuracy and interpretability (Amendola et al., 2020). Moreover, integrating domain knowledge into model design and leveraging advances in explainable AI (XAI) can help improve transparency and provide actionable insights for financial institutions (Rudin, 2019).

Collaboration between researchers, practitioners, and regulators is also essential to ensure that deep learning models for fraud detection are both effective and compliant with regulatory standards.

In summary, while deep learning holds great potential for fraud detection in financial transactions, ongoing challenges related to data imbalance, scalability, and transparency must be addressed to enhance its effectiveness and adoption in the financial sector. By focusing on these areas, future research can contribute to the development of more robust and reliable deep learning models for real-time fraud detection.

4. Conclusion

The application of deep learning for real-time fraud detection in financial transactions presents a promising avenue for enhancing the accuracy and efficiency of fraud detection systems. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated a superior ability to learn complex patterns in large and high-dimensional datasets, which is crucial for identifying fraudulent activities in financial transactions.

These models excel in real-time environments by quickly processing vast amounts of data and adapting to new fraud patterns, thereby minimizing financial losses and protecting consumer assets. However, challenges such as data imbalance, model interpretability, and computational resource requirements must be addressed to maximize the effectiveness and adoption of deep learning models in fraud detection.

To fully leverage the potential of deep learning for fraud detection, future research should focus on developing more robust, transparent, and scalable models that can operate efficiently in real-time scenarios. This includes exploring advanced techniques like transfer learning, unsupervised learning, and explainable AI to enhance model adaptability and interpretability. Additionally, addressing data imbalance through innovative methods will be critical in improving detection accuracy and reducing false positives. By tackling these challenges, deep learning can provide a more powerful and reliable solution for real-time fraud detection, contributing to the security and integrity of financial transactions in an increasingly digital world.

5. References

Ala'raj, M., & Abbod, M. F. (2016). A new hybrid ensemble credit scoring model based on classifiers consensus system approach. Expert Systems with Applications, 64, 36-55. https://doi.org/10.1016/j.eswa.2016.07.010

Amendola, A., Candila, V., Stilo, G., & Veltri, G. A. (2020). Deep learning models for fraud detection in financial transactions: A comparative study. Journal of Financial Crime, 27(4), 1021-1040. https://doi.org/10.1108/JFC-11-2019-0157

Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI), 1-9. https://doi.org/10.1109/ICCNI.2017.8123782

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602-613. https://doi.org/10.1016/j.dss.2010.08.008

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., ... & Amodei, D. (2020). Language models are few-shot learners. arXiv preprint arXiv:2005.14165.

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

Buda, M., Maki, A., & Mazurowski, M. A. (2018). A systematic study of the class imbalance problem in convolutional neural networks. Neural Networks, 106, 249-259. https://doi.org/10.1016/j.neunet.2018.07.011

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16, 321-357. https://doi.org/10.1613/jair.953

Cooper, H. (2010). Research synthesis and meta-analysis: A step-by-step approach (4th ed.). Sage Publications.

Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: A review. Banks and Bank Systems, 4(2), 57-68.

Dietterich, T. G. (2000). Ensemble methods in machine learning. In International Workshop on Multiple Classifier Systems (pp. 1-15). Springer. https://doi.org/10.1007/3-540-45014-9_1

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.

Fawcett, T., & Provost, F. (1997). Adaptive fraud detection. Data Mining and Knowledge Discovery, 1(3), 291-316. https://doi.org/10.1023/A:1009777916024

Flick, U. (2014). An introduction to qualitative research (5th ed.). Sage Publications.

Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). A survey on concept drift adaptation. ACM Computing Surveys (CSUR), 46(4), 1-37. https://doi.org/10.1145/2523813

Goldstein, M., Uchida, S., & Kato, K. (2017). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PloS One, 12(3), e0175217. https://doi.org/10.1371/journal.pone.0175217

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

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

Han, S., Pool, J., Tran, J., & Dally, W. (2015). Learning both weights and connections for efficient neural network. arXiv preprint arXiv:1506.02626.

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

Jouppi, N. P., Young, C., Patil, N., Patterson, D., Agrawal, G., Bajwa, R., ... & Laudon, J. (2017). In-datacenter performance analysis of a tensor processing unit. In Proceedings of the 44th Annual International Symposium on Computer Architecture (pp. 1-12). https://doi.org/10.1145/3079856.3080246

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234-245. https://doi.org/10.1016/j.eswa.2018.01.037

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

Lipton, Z. C. (2018). The mythos of model interpretability. Communications of the ACM, 61(10), 36-43. https://doi.org/10.1145/3233231

Liu, H., Xue, M., Liu, X., Zhang, T., & Chen, L. (2019). Real-time and unsupervised credit card fraud detection: A deep learning approach. Journal of Financial Crime, 26(1), 142-159. https://doi.org/10.1108/JFC-03-2018-0020

Ngai, E. W. T., 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

Nguyen, T., Khoshgoftaar, T. M., & Dittman, D. J. (2020). Deep learning methods for credit card fraud detection in a highly imbalanced dataset. Journal of Big Data, 7(1), 1-41. https://doi.org/10.1186/s40537-020-00335-6

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods, 16(1), 1-13. https://doi.org/10.1177/1609406917733847

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

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence, 1(5), 206-215. https://doi.org/10.1038/s42256-019-0048-x

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Soleymani, M., & Paquet, E. (2019). Real-time credit card fraud detection using recurrent neural networks. Journal of Big Data, 6(1), 1-23. https://doi.org/10.1186/s40537-019-0205-1

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3), 207-222. https://doi.org/10.1111/1467-8551.00375

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2), xiii-xxiii.

Weiss, K., Khoshgoftaar, T. M., & Wang, D. (2016). A survey of transfer learning. Journal of Big Data, 3(1), 1-40. https://doi.org/10.1186/s40537-016-0043-6

Zhang, Y., Zhang, Y., Zhou, B., Zhou, Z., & Shi, Y. (2020). Improving fraud detection with semi-supervised deep generative models. Journal of Financial Crime, 27(2), 403-421. https://doi.org/10.1108/JFC-05-2019-0075

Zheng, L., Zhang, X., & Sun, J. (2018). A deep learning approach for credit card fraud detection using autoencoders. Journal of Information Security and Applications, 41, 68-75. https://doi.org/10.1016/j.jisa.2018.05.010

Zhou, W., & Kapoor, G. (2011). Detecting evolutionary financial statement fraud. Decision Support Systems, 50(3), 570-575. https://doi.org/10.1016/j.dss.2010.08.007

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: A survey. Journal of Big Data, 2(1), 1-41. https://doi.org/10.1186/s40537-015-0013-4