EFFECTIVE ANOMALY DETECTION OF E-WALLET TRANSACTIONS USING DEEP LEARNING AND SPATIO-TEMPORAL ANALYSIS

THESIS

Submitted to Fulfill One of the Requirements in Obtaining a Master of Informatics (S2) Degree

IMAM FAISAL
20220130012

MASTER OF COMPUTER SCIENCE PROGRAM
SCHOOL OF COMPUTER SCIENCE

AUGUST 2024

AUTHOR'S STATEMENT

THESIS TITLE	: EFFECTIVE ANOMALY DETECTION OF E-WALLET TRANSACTIONS USING DEEP LEARNING AND SPATIO-TEMPORAL ANALYSIS
NAME	: IMAM FAISAL
NIM	20220130012

"I declare and be responsible for the fact that this Thesis is my own work except for the snippets and summaries each of which I have explained the source of. If in the future there is another party who claims that this thesis is his work, which is accompanied by sufficient evidence, then I am willing to cancel my Master's degree in Computer Science along with all the rights and obligations attached to the title"

Sukabumi, August 2024

IMAM FAISAL

THESIS APPROVAL

THESIS TITLE	: EFFECTIVE ANOMALY DETECTION OF E-WALLET TRANSACTIONS USING DEEP LEARNING AND SPATIO-TEMPORAL ANALYSIS
NAME	: IMAM FAISAL
NIM	20220130012

This script has been checked and approved

Sukabumi, August 2024

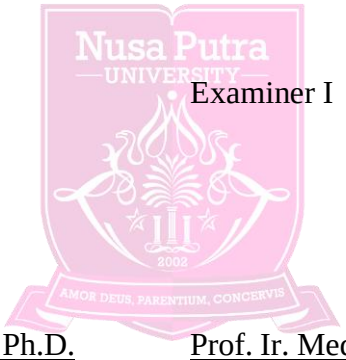
Head of Study Program,	Supervisor,
Prof. Ir. Teddy Mantoro, M.Sc., Ph.D.	Umar Aditiawarman, M.Sc., Ph.D.
NIDN.	NIDN.

THESIS VALIDATION

THESIS TITLE	: EFFECTIVE ANOMALY DETECTION OF E-WALLET TRANSACTIONS USING DEEP LEARNING AND SPATIO-TEMPORAL ANALYSIS
NAME	: IMAM FAISAL
NIM	20220130012

This Thesis has been tested and defended in front of the Board of Examiners in Thesis session on 4 Agustus 2024. In our review, this Thesis adequate in terms of quality for the purpose of awarding the Master of Computer Degree (M.Sc.).

Sukabumi, August 2024



Supervisor I	Examiner I
Umar Aditiawarman, M.Sc., Ph.D.	Prof. Ir. Media Anugerah Ayu, M.Sc., Ph.D.
NIP.	NIP.
Supervisor II	Examiner II
Haris Al Qodri Maarif, S.T., M.Sc., Ph.D.	Deshinta Arrova Dewi, S.Kom., M.Si., Ph.D.
NIP.	NIP.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDIXS

This thesis is dedicated to my beloved family.

To my spouse, for your endless support, patience, and encouragement, which have been my guiding light throughout this journey.

To my childrens, for filling my life with joy and reminding me of the importance of perseverance and love.

To my parents, whose unwavering belief in me has been the foundation of my success.

And to the company that provided the financial support and resources necessary to make this research possible. Your investment in my education has been invaluable.

Thank you all for your love and sacrifices. This work is as much yours as it is mine.

FOREWORD

Praise and gratitude the author prays to God Almighty, because only with His blessings and grace can the author complete this thesis. Writing this thesis is one of the requirements to achieve a Master's degree in Computers at Nusa Putra University. I realize that, without the help and guidance of various parties, from the lecture period to the preparation of this thesis, it is very difficult for the author to complete this thesis. Therefore, I would like to thank:

1. Dr. H. Kurniawan, ST., M.Si., MM. as Chancellor of Nusa Putra Sukabumi University;
2. Prof. Ir. Teddy Mantoro, M.Sc., Ph.D. as Head of School Computer Science Nusa Putra Sukabumi University;
3. Umar Aditiawarman, M.sC., Ph.D. and Haris Al Qodri Maarif, S.T., M.Sc., Ph.D. as Supervisors;
4. All Master Of Computer Science Lecturers who have provided very usefull knowledge during lectures;
5. Parents and my family for their supports, patience, prayers and never getting tired of educating and giving, bothmaterial and non-material;
6. Fellow comrades in Master of Computer Science 2022 who always give encouragement and always accompany from the beginning of the lecture until now;
7. All parties who have helped the author in writing this thesis;

For further improvement, suggestions and constructive criticism will be gladly accepted. Finally, only to Allah SWT the author submits everything, hopefully it can be useful especially for writers in general for all of us.

Sukabumi, August 2024

Writer

ABSTRACT

Electronic wallet transactions are increasingly popular and becoming a part of everyday life. However, as the number of transactions increases, the risk of anomalies and fraud also increases. This study aims to develop an anomaly detection model in e-wallet transactions using the Recurrent Neural Network (RNN) model, Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU) and spatio-temporal analysis.

The transaction data used in this study comes from the Mony platform and includes various information such as transaction IDs, timestamps, transaction amounts, geographical coordinates (latitude and longitude), as well as sender and recipient account information. The steps in the data processing process include: first, data pre-processing to correct and fill in the missing values; second, the extraction of spatio-temporal features to calculate the distance, time difference, speed of movement between transactions, and calculate the habit of the number of transactions; and third, data labeling to identify normal and anomalous transactions.

The built Deep Learning model consists of two layers with 256 and 128 units respectively, equipped with a dropout layer to prevent overfitting. The data were trained using the SMOTE oversampling technique to handle data imbalances and then divided into training, validation, and testing sets. Model evaluation was carried out using accuracy, precision, recall, and F1-score metrics.

The evaluation results show that this LSTM model has the best performance with a test accuracy of 94.64%, precision of 94.81%, recall of 94.64%, and F1-score of 94.62%. The GRU model showed a test accuracy of 94.46%, precision of 94.86%, recall of 94.46%, and F1-score of 94.39%. The RNN model has lower performance with a test accuracy of 91.78%, precision of 91.74%, recall of 91.78%, and F1-score of 91.76%. This shows that the LSTM model developed has excellent ability to detect anomalies in e-wallet transactions.

Keywords: anomaly detection, e-wallet transactions, Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), spatial-temporal analysis, deep learning.

CHAPTER I
INTRODUCTION

1.1. Research Background

In the rapidly advancing digital era, e-wallet transactions have become an integral aspect of daily life, providing significant convenience and efficiency for both personal and business-related financial activities. However, this surge in transaction volume and frequency has introduced new challenges, particularly the rise of suspicious transaction patterns. These anomalies include transactions conducted in multiple locations within an unreasonably short timeframe, which would be physically impossible without some form of manipulation. Additionally, transactions occurring in rapid succession and those involving unusually large amounts far exceeding the user's average transaction size are indicative of potential fraudulent activity.

This concern is critical because suspicious transactions not only result in financial losses but also dangerous the reputation of financial institutions. Therefore, early detection of such anomalies is vital to maintaining the security and integrity of the digital financial system. The primary challenge lies in efficiently and accurately identifying abnormal transaction patterns within the vast amounts of data, given the complexity and variability of transaction behaviors. Recent advancements in Machine Learning (ML) and Deep Learning (DL) have shown promise in addressing these challenges. Specifically, models such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRUs) have demonstrated superior capabilities in processing sequential and spatio-temporal data, making them particularly suitable for analyzing transaction sequences and identifying suspicious patterns.

This study proposes an approach that leverages three deep learning models RNN, LSTM, and GRU independently to enhance the anomaly detection system for e-wallet transactions. Unlike traditional methods that typically treat transactions as isolated events, this approach emphasizes the temporal context, recognizing that suspicious transactions often exhibit unique patterns distinct from legitimate transactions when analyzed over time. By harnessing the sequential learning

capabilities of RNNs, LSTMs, and GRUs, the study aims to develop a robust and precise anomaly detection system.

Theoretically, a key challenge in this research is the effective integration of spatio-temporal features into the RNN, LSTM, and GRU frameworks, enabling these models to capture and leverage patterns that differentiate between legitimate and suspicious transactions. Spatio-temporal analysis provides critical insights into the context of a transaction—specifically, when and where it occurred—both of which are essential for detecting anomalies. Transactions occurring at unusual times or locations often signal potential fraud. On a practical level, challenges include data pre-processing, feature extraction, and model optimization. The model must be capable of processing large volumes of transaction data in real-time while maintaining high detection accuracy to minimize false positives and false negatives.

The growing complexity of fraud schemes necessitates continuous advancements in anomaly detection methodologies. Traditional rule-based systems frequently fall short in detecting increasingly sophisticated fraud tactics. Consequently, financial institutions face ongoing pressure to enhance their anomaly detection capabilities to safeguard consumers and uphold trust. This research responds to this need by developing an optimized anomaly detection system utilizing RNN, LSTM, and GRU models independently. This approach not only enhances detection accuracy but also offers a scalable and adaptive solution to the dynamic nature of fraudulent activities.

The distinctiveness of this study lies in its exploration of three deep learning models RNN, LSTM, and GRU each independently applied with spatio-temporal analysis for detecting anomalies in e-wallet transactions. By focusing on the sequential and contextual patterns within transaction data, this study aims to extend the boundaries of existing anomaly detection methodologies, offering a more comprehensive and effective solution through the integration of spatio-temporal features. This research not only advances the development of a more effective anomaly detection system but also provides valuable insights into the application of deep learning techniques in digital finance.

Overall, the study aims to push the state of the art in anomaly detection by introducing an optimized system that leverages RNNs, LSTMs, and GRUs

independently. This innovative approach addresses a range of theoretical and practical challenges, delivering a robust solution for detecting and mitigating anomalous activity in e-wallet transactions. The optimization performed on this anomaly detection system is expected to serve as a benchmark for future developments in similar technologies. Moreover, the research opens avenues for further exploration into the development of more sophisticated anomaly detection algorithms and their integration with broader financial monitoring systems, ultimately enhancing security and trust in the digital financial ecosystem.

1.2. Problem Statement

Building on the research background presented, the following research questions have been identified:

1. How can an effective and efficient system be developed to detect anomalies in e-wallet transactions, particularly those occurring across multiple locations at abnormal times?
2. To what extent can Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU) accurately detect suspicious transactions using spatio-temporal analysis?
3. What are the most effective methods for integrating spatio-temporal analysis into deep learning models to enhance the accuracy of anomaly detection in e-wallet transactions?

1.3. Research Objectives

Building on the formulated problem statement, the objectives of this research are as follows:

1. To develop and evaluate a system capable of effectively and efficiently detecting anomalies in e-wallet transactions, particularly those occurring across multiple locations at unusual times, within short intervals, or involving sudden large transaction volumes.
1. To assess and compare the accuracy of LSTM and CNN models in detecting suspicious transactions through spatio-temporal analysis.
2. To effectively integrate spatio-temporal features into RNN, LSTM, and GRU models to enhance the accuracy of anomaly detection in e-wallet transactions.

1.4. Research Significance

This research offers several significant theoretical and practical contributions:

1. This study provides valuable insights into the detection of anomalies in e-wallet transactions through the application of RNN, LSTM, GRU models, and spatio-temporal analysis. The findings from this research can serve as a foundation for further academic inquiry and development in the field of digital financial security.
2. By developing a more effective detection system, financial institutions can mitigate the risk of fraud and enhance transaction security, thereby increasing user confidence and trust in the digital financial ecosystem.
3. The implementation of Deep Learning techniques such as RNNs, LSTMs, and GRUs in anomaly detection automates traditionally manual processes, leading to significant time and resource savings while increasing operational efficiency for financial institutions.
4. A more rapid and precise detection system will enable financial institutions to more effectively identify and address suspicious transactions, significantly reducing the potential for financial losses due to fraudulent activities.

1.5. Problem Limitations and Research Assumptions

This research focuses on the development and optimization of an anomaly detection system specifically for electronic wallet transactions, utilizing RNN, LSTM, GRU models, and spatio-temporal analysis. The scope of this study is defined by the following limitations:

1. The research is confined to the development and optimization of an anomaly detection system based solely on RNN, LSTM, GRU models, and spatio-temporal analysis. Alternative anomaly detection methods are beyond the scope of this study.
2. The dataset employed in this study includes location information (latitude and longitude), timestamps, and the number of transactions from the last ten transactions conducted by users. Other forms of transactions, including physical transactions outside of e-wallets, are not considered in this research.

3. This study exclusively utilizes RNN, LSTM, and GRU models for anomaly detection. No other Machine Learning or Deep Learning models are incorporated or analyzed within this research.

The research is grounded in several key assumptions that underpin and limit the scope of the study. These assumptions are as follows:

1. The transaction data used in this study is assumed to be accurate and representative of actual e-wallet transaction patterns, ensuring the generalizability of the analysis results.
2. Anomalies in e-wallet transactions are presumed to be identifiable through spatio-temporal patterns that can be effectively detected by RNN, LSTM, and GRU models. This assumption justifies the use of these models in this study.
3. It is assumed that e-wallet users exhibit relatively consistent transaction patterns, allowing anomalies to be detected through the analysis of significant deviations from these patterns.
4. The RNN, LSTM, and GRU models are assumed to be capable of processing and analyzing transaction data across temporal and spatial sequences with a high degree of accuracy, supporting their selection as the primary models for this research.
5. The data used has undergone appropriate pre-processing, including normalization, sorting by timestamp, and handling of missing values, to ensure that data quality does not negatively impact model performance.

Nusa Putra
UNIVERSITY
2002
AMOR DEUS, PARENTIUM, CONCERVIS

CHAPTER V
CONCLUSIONS AND RECOMMENDATIONS

5.1. Conclusion

This study aims to develop and test an anomaly detection system in electronic wallet transactions using deep learning models, namely Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU) with spatio-temporal analysis. Based on the results of the research and discussions that have been carried out.

While spatio-temporal features such as the distance between transactions, time differences between transactions, and movement speed were key elements of the model, it is important to note that the study did not include a comparative analysis against models without these features. Therefore, the effectiveness of spatio-temporal analysis in improving anomaly detection accuracy is observed within the context of the models tested, without a baseline for comparison to non-spatio-temporal approaches. Of the three models tested, LSTM showed the best performance in detecting anomalies in e-wallet transactions. Although GRU and RNN also show good results, LSTM has an advantage in terms of accuracy, precision, recall, and F1-score. LSTMs are superior in handling the complexity and variation of spatio-temporal data, making them more suitable for anomaly detection applications in financial transactions.

A comparative table of training results between RNNs, LSTMs, and GRUs also supports these findings. LSTM showed the best performance with a training accuracy of 93.46%, a training loss of 16.64%, a validation accuracy of 94.64%, and a validation loss of 13.49% with a training time of 15 minutes and 36 seconds. GRU also showed excellent performance with a training accuracy of 92.76%, a training loss of 17.22%, a validation accuracy of 94.46%, and a validation loss of 15.45% with a training time of 12 minutes and 15 seconds. Meanwhile, RNN showed lower performance with a training accuracy of 90.94%, a training loss of 22.07%, a validation accuracy of 91.78%, and a validation loss of 17.28% with a training time of 6 minutes and 1 second.

Model	Train Accuracy	Train Loss	Val Accuracy	Val Loss	Time
RNN	90.94%	22.07%	91.78%	17.28%	361.511s
LSTM	93.46%	16.64%	94.64%	13.49%	936.353s
GRU	92.76%	17.22%	94.46%	15.45%	735.209s

Table 22: Comparison of Training Results of RNN, LSTM, and GRU Models

The comparison graph of training accuracy shows that LSTM and GRU achieve higher accuracy than RNN as the epoch increases. LSTMs have a steady and consistent increase in accuracy, while RNNs show more volatile performance and do not achieve as high accuracy as LSTMs and GRUs. The validation accuracy comparison graph also shows that the LSTM maintains the highest accuracy among the three models, with the GRU following behind, and the RNN at the lowest. This shows that LSTM is not only superior in training but also in generalization to new data.

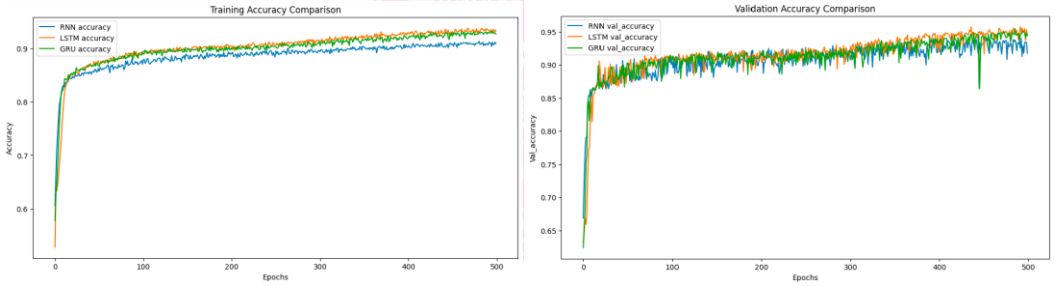


Figure 28:Comparison Chart of Training Accuracy and Validation of RNN, LSTM, and GRU Models

The comparison graph of training losses shows that the LSTM and GRU models experienced a more significant loss reduction and achieved a lower loss level compared to RNN. This shows that LSTM and GRU are more efficient at studying patterns in data and reducing prediction errors. The validation loss comparison graph reinforces these findings, with LSTM and GRU showing lower and stable losses than RNNs, which have higher and volatile loss values.

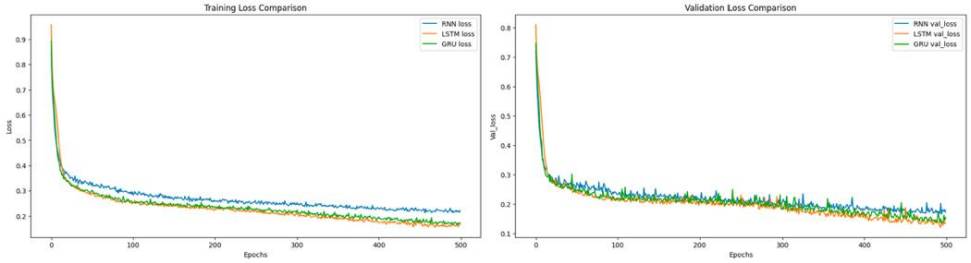


Figure 29: Comparison Chart of Training Loss and Validation of RNN, LSTM, and GRU Models

The RNN model is able to recognize temporal patterns in transaction data, but it has limitations in handling long-term dependencies due to the vanishing gradient problem. The RNN model showed a test accuracy of 91.78%, precision of 91.74%, recall of 91.78%, and F1-score of 91.76%.

LSTM successfully solves the problem of vanishing gradient and is able to retain long-term information in sequential data. The evaluation results show that the LSTM model has the best performance with a test accuracy of 94.64%, precision of 94.81%, recall of 94.64%, and F1-score of 94.62%. This shows that LSTM is effective in detecting anomalies in e-wallet transactions.

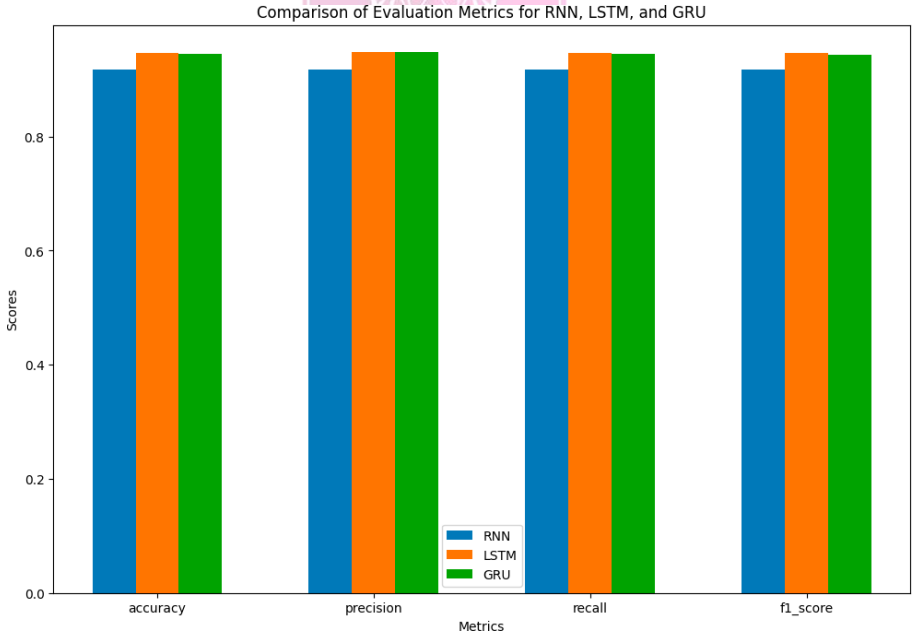


Figure 30: Comparison Chart of Evaluation Metrics Results of RNN, LSTM, and GRU Models

GRUs have a simpler architecture than LSTMs, but are still effective in overcoming vanishing gradients and handling long-term dependencies. The GRU model showed a test accuracy of 94.46%, precision of 94.86%, recall of 94.46%, and F1-score of 94.39%.

Model	True Normal	True Anomaly	False Normal	False Anomaly
RNN	345	716	44	51
LSTM	349	745	15	47
GRU	337	755	5	59

Table 23: Comparison of Prediction Results of RNN, LSTM, and GRU Models

The results indicate that the LSTM model, when used with spatio-temporal analysis, is a highly effective approach for detecting anomalies in e-wallet transactions within the context of this study. This research contributes to the ongoing development of more sophisticated and efficient anomaly detection systems and highlights opportunities for further research in applying machine learning technology to fraud detection in the financial sector. The evaluation metrics comparison between RNN, LSTM, and GRU models indicates that LSTM outperforms the other models across all measured metrics, including accuracy, precision, recall, and F1-score. This concludes that LSTM is the most suitable model to be applied in the context of detecting anomalies in e-wallet transactions.

5.2. Recommendations

Based on the results of this study, there are several recommendations that can be given for further development in the detection of anomalies in e-wallet transactions. First, it is recommended to explore other machine learning models for comparison. In addition to RNN, LSTM, and GRU, models such as Transformer, Random Forest, Gradient Boosting, and Support Vector Machine (SVM) should be evaluated. This exploration may help identify models that offer different or complementary strengths in detecting anomalies. Performance evaluation of each model is carried out using metrics such as accuracy, precision, recall, and F1-score to understand the strengths and weaknesses of each.

Second, the spatio-temporal features can be further explored and potentially enriched. Additional features such as the type of transaction location (e.g., ATM, retail store, online), specific transaction times (e.g., during business hours, on

weekends), and user mobility patterns may provide deeper insights. These enhanced features could help in identifying suspicious transactions more accurately. These features can provide additional context that is useful for identifying suspicious transactions. It is also important to study the transaction patterns of users from a spatial-temporal perspective to understand their habits. With this information, we can develop a model that is more adaptive to the user's normal habits, so that it is more accurate in detecting anomalies. In addition, it is also necessary to analyze the pattern of transaction recipients. Understanding the recipient's habits can help detect anomalies that may occur due to behavioral changes from both the sender and receiver.

Third, conduct real-time testing to test the model's performance under real-world conditions. This test can be done with real-time transaction simulations to see how the model detects anomalies in real time. In real-time situations, we can measure model performance with metrics such as response time, detection accuracy, and system reliability. This testing is important to ensure that the model can function properly in a dynamic operational environment. After successfully passing the simulation test, the next step is to implement the anomaly detection system in a real operational environment. This involves integrating with existing transaction systems and ensuring the model can process data efficiently and effectively in real-time.

By implementing these recommendations, it is hoped that the anomaly detection system can become more sophisticated, responsive, and accurate in identifying suspicious transactions. This implementation is also expected to be widely adopted in the financial industry, make a significant contribution to improving the security of electronic wallet transactions, and provide practical benefits for the financial industry in an effort to prevent fraud and transaction anomalies.

REFERENCES

Airlangga, G. (2024). Evaluating the Efficacy of Machine Learning Models in Credit Card Fraud Detection. *Journal of Computer Networks Architecture and High Performance Computing*, *6*(2), 829–837. https://doi.org/10.47709/cnahpc.v6i2.3814

Kamuangu, P. (2024). A Review on Financial Fraud Detection using AI and Machine Learning. *Journal of Economics Finance and Accounting Studies*, *6*(1), 67–77. https://doi.org/10.32996/jefas.2024.6.1.7

Tian, Y., & Liu, G. (2021). Transaction Fraud Detection via Spatial-Temporal-Aware Graph Transformer. *JOURNAL OF LATEX CLASS FILES*, *14*(8), 1–2. https://doi.org/10.0000/0000

Li, Q. (2023). Textual Data Mining for Financial Fraud Detection: A Deep Learning Approach. In *Preprint Submitted to Journal Name* (p. 5). https://arxiv.org/abs/2308.03800v1

Gopichander Ravichander, A., K. Leboulluec, A., & L. Leboulluec, P. (2023). Financial Fraud Detection using Machine Learning and Deep Learning Models. *International Journal of Computer Applications*, 32–33.

Huang, M., & Li, W. (2023). *Financial Fraud Detection Using Deep Learning Based on Modified Tabular Learning*. Proceedings of the 2022 3rd International Conference on E-commerce and Internet Technology (ECIT 2022). https://doi.org/10.2991/978-94-6463-005-3

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. a. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Appl. Sci.*, *12*, 9637. https://doi.org/10.3390/app12199637

Amini, M., & Rabiei, M. (2022). Ensemble Learning for Fraud Detection in E-commerce Transactions: A Comparative Study. In *Journal of Applied Intelligent Systems & Information Sciences* (Vols. 2–2, pp. 65–73). https://doi.org/10.22034/JAISIS.2022.377265.1057

Amran, A., Islami, M. I., Jaya, A. K., & Bakri, B. (2020). Spatio-Temporal Model of Rainfall Data Using Kalman Filter and Expectation-Maximization

Algorithm. *Jurnal Matematika Statistika Dan Komputasi*, *17*(2), 304–313. https://doi.org/10.20956/jmsk.v17i2.11918

Salih, T. A., & Younis, N. K. (2021). Designing an Intelligent Real-Time Public Transportation Monitoring System Based on IoT. *OALib*, *08*(10), 1–14. https://doi.org/10.4236/oalib.1107985

Pang, G., Shen, C., Cao, L., & Van Den Hengel, A. (2021). Deep Learning for Anomaly Detection: A Review. *ACM Computing Surveys*, 38. https://doi.org/10.1145/3439950

Owolafe, O., Ogunrinde, O. B., & Thompson, A. F. B. (2021). A Long Short Term Memory Model for Credit Card Fraud Detection. In *Studies in computational intelligence* (pp. 369–391). https://doi.org/10.1007/978-3-030-72236-4_15

Pei, Y., Lyu, F., Van Ipenburg, W., & Pechenizkiy, M. (2020). *Subgraph anomaly detection in financial transaction networks*. https://doi.org/10.1145/3383455.3422548

Cheng, D., Xiang, S., Shang, C., Zhang, Y., Yang, F., & Zhang, L. (2020a). Spatio-Temporal Attention-Based Neural Network for Credit Card Fraud Detection. In *The Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI-20)*.

Karadayı, Y., Aydin, M. N., & Öğrenci, A. S. (2020). A Hybrid Deep Learning Framework for Unsupervised Anomaly Detection in Multivariate Spatio-Temporal Data. In *Applied Sciences*. https://doi.org/10.3390/app10155191

Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, A. (2021). Deep Learning Methods for Credit Card Fraud Detection. *Journal of Credit Card Fraud Detection*.

Mamun, S. M. a. A., & Beyaz, M. (2019). LSTM Recurrent Neural Network (RNN) for Anomaly Detection in Cellular Mobile Networks. In *Lecture notes in computer science* (pp. 222–237). https://doi.org/10.1007/978-3-030-19945-6_15

Gunavathi, C., Priya, R. M. S., & Aarthy, S. L. (2018). Big Data Analysis for Anomaly Detection in Telecommunication Using Clustering Techniques. In

Advances in intelligent systems and computing (pp. 111–121). https://doi.org/10.1007/978-981-13-3329-3_11

Unsupervised Anomaly Detection in Multivariate Spatio-Temporal Data using Deep Learning: Early Detection of COVID-19 Outbreak in Italy. (2017). *IEEE Access, XX*. https://doi.org/10.1109/ACCESS.2017.Doi

Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). *Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis*.

Syeda, M., Zbang, Y. Q., & Pan, Y. (2002). Parallel Granular Neural Networks for Fast Credit Card Fraud Detection. In *Department of Computer Science*.

Cheng, D., Xiang, S., Shang, C., Zhang, Y., Yang, F., & Zhang, L. (2020b). Spatio-Temporal Attention-Based Neural Network for Credit Card Fraud Detection. *Proceedings of the AAAI Conference on Artificial Intelligence*, *34*(01), 362–369. https://doi.org/10.1609/aaai.v34i01.5371

Karthikeyan, T., Govindarajan, M., & Vijayakumar, V. (2023). An effective fraud detection using competitive swarm optimization based deep neural network. *Measurement Sensors*, *27*, 100793. https://doi.org/10.1016/j.measen.2023.100793

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. *ACM Computing Surveys*, *41–41*(3), 15–15. https://doi.org/10.1145/1541880.1541882

Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In *Proceedings of NAACL-HLT 2019* (pp. 4171–4186). Association for Computational Linguistics. Retrieved August 15, 2024, from https://aclanthology.org/N19-1423.pdf

Chalapathy, R., & Chawla, S. (2019). *DEEP LEARNING FOR ANOMALY DETECTION: A SURVEY*.

Pang, G., Shen, C., Cao, L., & Van Den Hengel, A. (2020). Deep Learning for Anomaly Detection: A Review. *ACM Comput. Surv.*, 1–36. https://doi.org/10.1145/3439950

Bandyopadhyay, S. K. (2020). Detection of Fraud Transactions Using Recurrent Neural Network during COVID-19. *Journal of Advanced Research in*

Medical Science & Technology, *07*(03), 16–21. https://doi.org/10.24321/2394.6539.202012

Bian, W., Cong, L. W., & Ji, Y. (2023). *THE RISE OF E-WALLETS AND BUY-NOW-PAY-LATER: PAYMENT COMPETITION, CREDIT EXPANSION, AND CONSUMER BEHAVIOR*. NATIONAL BUREAU OF ECONOMIC RESEARCH. http://www.nber.org/papers/w31202