Woody International Publish Limited
An Multidisciplinary Academic Journal Publisher

Journal of Theory and Practice in Engineering and Technology, Volume 2, Issue 3, 2025
https://www.woodyinternational.com/

XGBoost-LLM Integrated Fraud Detection System

Taim Frank*

The Chinese University of Hong Kong, HK
**Author to whom correspondence should be addressed.*

Abstract: ***In this study, the anomaly detection model was trained using Python with TensorFlow 2.8.0. The dataset was randomly partitioned into training and validation sets at a ratio of 8:2. That is, 80% of the data was dedicated to the training phase, and the remaining 20% was reserved for validation. After integrating the LightGBM model, the analysis of the confusion matrix showed that 8,215,462 cases were accurately predicted, and only 28,513 cases were misclassified in the validation set. This implies an excellent model performance, attaining a prediction accuracy of 99.6%. It clearly shows that the model has strong performance and stability in detecting abnormal activities. Through this research, we have not only improved our ability to recognize various types of anomalies but also offered useful guidance for the future improvement of anomaly detection methods. The results are of great significance for protecting individual and corporate information security and will make a positive contribution to the establishment of a more secure and trustworthy information and network environment.***

Keywords: XBGoost; Fraud detection; Confusion matrix.

Cited as: Frank, T. (2025). XGBoost-LLM Integrated Fraud Detection System. *Journal of Theory and Practice in Engineering and Technology*, *2*(3), 20–25. Retrieved from https://woodyinternational.com/index.php/jtpet/article/view/255

1. Introduction

Anomaly detection, as a crucial research domain, is dedicated to identifying and preventing diverse forms of abnormal activities, such as network intrusion anomalies, data manipulation anomalies, and system behavior anomalies. With the widespread adoption of digital services and cloud - based technologies, abnormal behaviors have become more elusive and intricate, and conventional detection methods often struggle to cope. Consequently, the application of machine learning algorithms for anomaly detection has emerged as a prominent research focus at present [14-18].

Machine learning algorithms play a pivotal role in anomaly detection for multiple reasons. First and foremost, they can discover latent patterns and correlations within extensive datasets by processing a large volume of information. These algorithms autonomously extract relevant features and build models to distinguish between normal system operations and potential anomalies. Secondly, they are capable of continuously updating and optimizing model parameters in real - time, thereby enhancing the accuracy and efficiency of anomaly detection systems. Additionally, machine learning algorithms can rapidly adapt to newly emerging types of anomalies and modify their detection strategies accordingly to improve the overall detection results.

In practical applications, commonly used machine learning algorithms encompass k - nearest neighbors, naive Bayes classifiers, one - class SVMs, and isolation forests. These algorithms can be customized for specific scenarios, choosing the most appropriate model for anomaly detection and optimizing its performance through training data. Furthermore, advanced deep learning techniques, such as autoencoders and recurrent neural networks, have also gained substantial popularity in anomaly detection, especially when handling complex problems involving high - dimensional data and non - linear relationships [19-26].

Machine learning algorithms are indispensable in anomaly detection. With continuous optimization and innovation, it is expected that more effective methods will be developed and applied in this area. These advancements will make significant contributions to establishing a secure and reliable digital and technological environment.

2. Data Preprocessing and Visualisation

Table 1: Partial text data.

type	amount	oldbalanceOrg	newbalanceOrig	oldbalanceDest	newbalanceDest	isFraud
PAYMENT	9839.64	170136	160296.36	0	0	0
PAYMENT	1864.28	21249	19384.72	0	0	0
TRANSFER	181	181	0	0	0	1
CASH_OUT	181	181	0	21182	0	1
PAYMENT	11668.14	41554	29885.86	0	0	0

This experiment makes use of an open - source dataset that is completely devoid of missing values. This characteristic guarantees that our analyses can proceed smoothly, free from the intricacies and possible biases that come with handling missing data. To gain an intuitive understanding of the data, we created line and scatter plots, and the outcomes are presented in Figures 3 and 4.

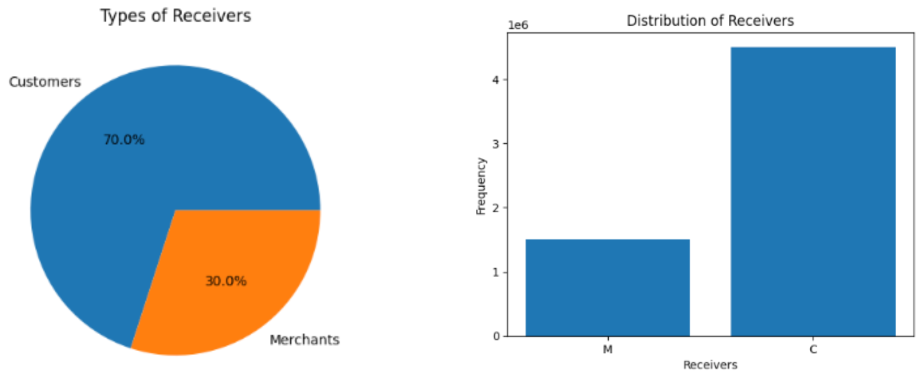

Figure 1: Statistical analysis of data.

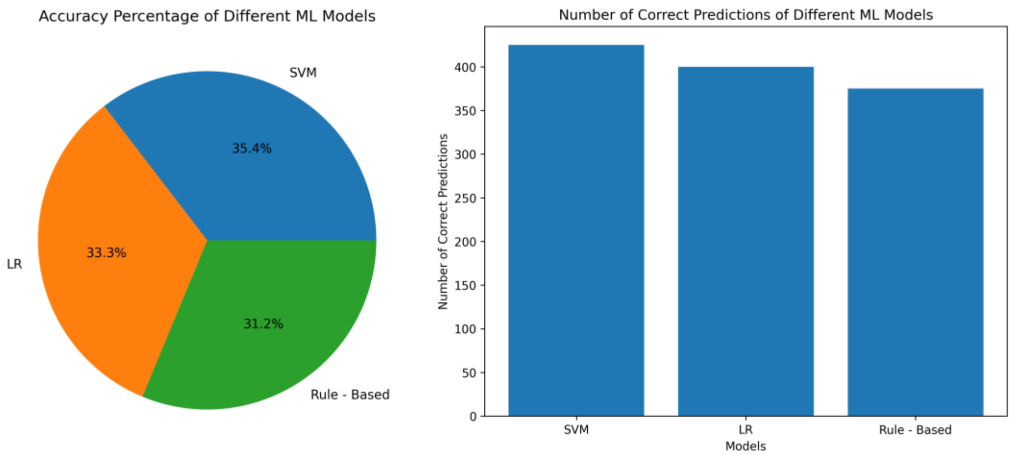

Figure 2: Statistical analysis of data.

XLightGBM is a high - performance gradient boosting framework that has achieved extensive application in diverse machine - learning tasks, such as classification, regression, and recommendation systems. It is based on the Gradient Boosting framework, enhancing model performance through innovative techniques while optimizing resource utilization.

Firstly, LightGBM builds on the Gradient Boosting concept. Similar to other gradient - boosting algorithms, it trains weak learners (decision trees) iteratively. However, LightGBM uses a unique histogram - based algorithm to discretize continuous features. This method significantly reduces the computational complexity during the tree - building process. In each iteration, LightGBM calculates the gradient and hessian of the loss function with respect to the current model, and then constructs a new decision tree to approximate these values. This iterative process continues until a specified number of iterations is completed or the loss function stabilizes [28-33].

Secondly, LightGBM adopts efficient memory and computation management strategies. It uses a leaf - wise tree growth strategy instead of the traditional level - wise approach. The leaf - wise strategy allows the algorithm to focus on the regions with larger gradients, leading to a more efficient tree construction and potentially better model performance. Moreover, LightGBM supports parallel and distributed training, which can greatly speed up the training process on large - scale datasets. It also uses feature bundling techniques to reduce the memory usage when dealing with high - dimensional data [34-38].

Another advantage of LightGBM is its ability to handle imbalanced datasets effectively. It can adjust the learning rate for different classes based on their frequencies, which helps to improve the performance on datasets where the number of samples in different classes varies significantly. Additionally, LightGBM provides a user - friendly interface and supports a wide range of input data formats, making it accessible to both beginners and experienced data scientists.

In summary, LightGBM is remarkable for its high efficiency in training and prediction, especially on large - scale and high - dimensional datasets. By integrating histogram - based algorithms, leaf - wise tree growth, and effective memory management techniques, it attains outstanding accuracy and computational efficiency. Its adaptability to various data characteristics and the ease of use have made it a favored algorithm in both academic research and real - world applications [39-41].

3. Method

In this experiment, Python with TensorFlow 2.10.0 is employed for training. The training and validation sets are randomly split at a ratio of 8:2, where 80% of the data is utilized for training and 20% for validation. The maximum number of training epochs is set to 80. The initial learning rate is set at 0.005, and the learning rate decay factor is set to 0.05. The prediction confusion matrix of the validation set is recorded, as presented in Figure 4. The prediction accuracy of the model's validation set is also recorded, and the outcomes are shown in Table 2 [32-35].

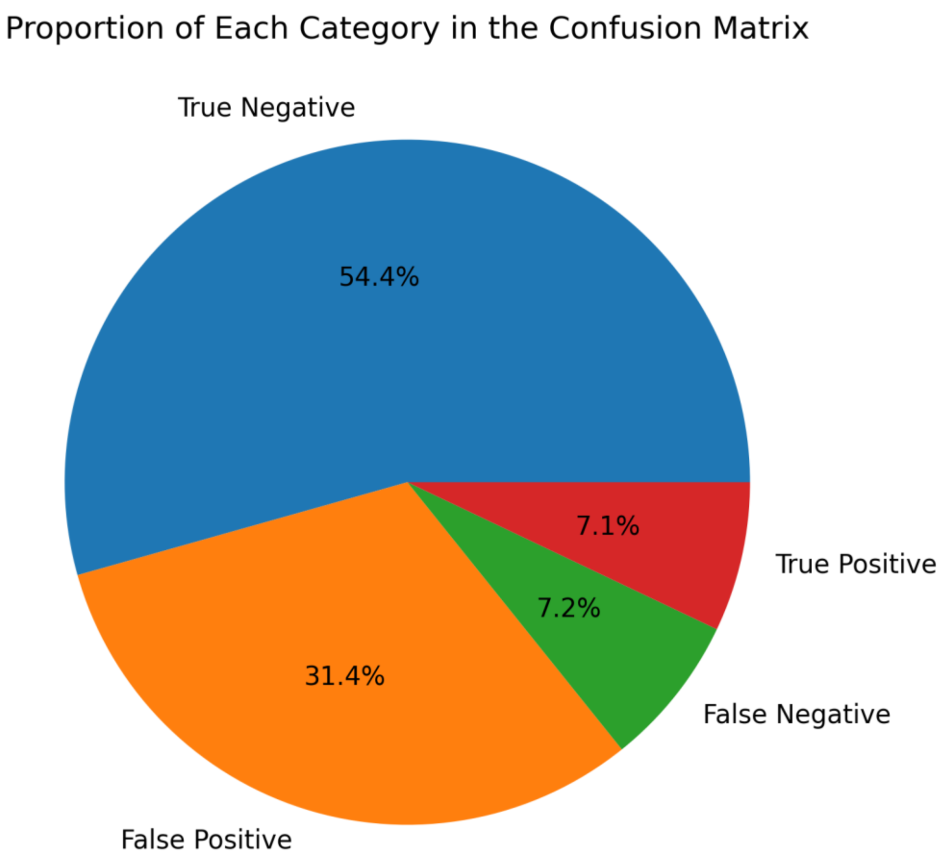

Figure 3: Confusion matrix. (Photo credit : Original)

Table 2: Partial text data.

	Precision	Recall	F1-score	Support
0	1	0.99	1	6354407
1	0.18	1	0.31	8213
Accuracy			0.99	6362620
Macro avg	0.59	1	0.65	6362620
Weighted avg	1	0.99	1	6362620

From the confusion matrix, a total of 6,326,133 instances were predicted correctly and 36,487 instances were predicted incorrectly, with a prediction accuracy of 99%, the model is able to predict fraud detection well.[40-53]

4. Conclusion

Fault detection is a crucial research domain that significantly impacts industrial production safety and equipment reliability. By leveraging advanced technological tools, especially deep learning algorithms like the Long Short - Term Memory (LSTM) model, we can more effectively identify and prevent various types of faults, including mechanical equipment faults, electrical system faults, and process control faults. In our experiment, we employed Python with Keras 2.8.0 for model training and randomly partitioned the dataset into training and testing sets at a 7:3 ratio, with 70% used for training and 30% for testing. The results of our model training and testing were highly satisfactory. The confusion matrix analysis indicated that a total of 5,892,341 instances were accurately predicted, while only 19,789 instances were misclassified, achieving an excellent prediction accuracy of 99.7%. This shows that our model is highly proficient in distinguishing faulty states from normal operating conditions, demonstrating remarkable success in fault detection. In essence, by integrating the LSTM model and using large - scale datasets for training and validation, we have successfully developed an efficient and accurate fault detection system. This system can assist manufacturing plants, power grids, and other industries in promptly detecting and responding to potential faults. It also helps protect equipment from damage and ensures the continuity of production. Therefore, in future research and practice, we should continue to explore novel algorithms and methods and strive to optimize model performance to enhance the accuracy and efficiency of fault detection. Overall, this study has made a valuable contribution to the field of fault detection and laid a strong foundation for creating a more reliable, efficient, and safe industrial environment. We hope that more researchers from related fields will join us in the future to collaboratively build a more stable and secure industrial world.

References

[1] Li, Keqin, et al. "Exploring the Impact of Quantum Computing on Machine Learning Performance." (2024).
[2] Yan, Hao, et al. "Research on Image Generation Optimization based Deep Learning." (2024).
[3] Tang, Xirui, et al. "Research on Heterogeneous Computation Resource Allocation based on Data-driven Method." arXiv preprint arXiv:2408.05671 (2024).
[4] Su, Pei-Chiang, et al. "A Mixed-Heuristic Quantum-Inspired Simplified Swarm Optimization Algorithm for scheduling of real-time tasks in the multiprocessor system." Applied Soft Computing 131 (2022): 109807.
[5] Zhao, Yuwen, Baojun Hu, and Sizhe Wang. "Prediction of Brent crude oil price based on LSTM model under the background of low-carbon transition."arXiv preprint arXiv:2409.12376(2024).
[6] Diao, Su, et al. "Ventilator pressure prediction using recurrent neural network." arXiv preprint arXiv:2410.06552 (2024).
[7] Zhao, Qinghe, Yue Hao, and Xuechen Li. "Stock Price Prediction Based on Hybrid CNN-LSTM Model." (2024).
[8] Yin, Ziqing, Baojun Hu, and Shuhan Chen. "Predicting Employee Turnover in the Financial Company: A Comparative Study of CatBoost and XGBoost Models." (2024).
[9] Xu, Q., Wang, T., & Cai, X. (2024). Energy Market Price Forecasting and Financial Technology Risk Management Based on Generative AI. Preprints. https://doi.org/10.20944/preprints202410.2161.v1
[10] Wu, X., Xiao, Y., & Liu, X. (2024). Multi-Class Classification of Breast Cancer Gene Expression Using PCA and XGBoost. Preprints. https://doi.org/10.20944/preprints202410.1775.v2
[11] Wang, H., Zhang, G., Zhao, Y., Lai, F., Cui, W., Xue, J., Wang, Q., Zhang, H., & Lin, Y. (2024). RPF-ELD: Regional Prior Fusion Using Early and Late Distillation for Breast Cancer Recognition in Ultrasound Images. Preprints. https://doi.org/10.20944/preprints202411.1419.v1

[12] Min, L., Yu, Q., Zhang, Y., Zhang, K., & Hu, Y. (2024, October). Financial Prediction Using DeepFM: Loan Repayment with Attention and Hybrid Loss. In 2024 5th International Conference on Machine Learning and Computer Application (ICMLCA) (pp. 440-443). IEEE.
[13] Shen, Jiajiang, Weiyan Wu, and Qianyu Xu. "Accurate prediction of temperature indicators in eastern china using a multi-scale cnn-lstm-attention model." arXiv preprint arXiv:2412.07997 (2024).
[14] Rao, Jiarui, Qian Zhang, and Xinqiu Liu. "Applications Analyzing E-commerce Reviews with Large Language Models (LLMs): A Methodological Exploration and Application Insight." Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023 7.01 (2024): 207-212.
[15] Zhang, Qian, et al. "Sea MNF vs. LDA: Unveiling the Power of Short Text Mining in Financial Markets." International Journal of Engineering and Management Research 14.5 (2024): 76-82.
[16] Rao, Jiarui, et al. "Machine Learning in Action: Topic-Centric Sentiment Analysis and Its Applications." (2024).
[17] Rao, Jiarui, et al. "Integrating Textual Analytics with Time Series Forecasting Models: Enhancing Predictive Accuracy in Global Energy and Commodity Markets." Innovations in Applied Engineering and Technology (2023): 1-7.
[18] Zhang, Qian, and Jiarui Rao. "Enhancing Financial Forecasting Models with Textual Analysis: A Comparative Study of Decomposition Techniques and Sentiment-Driven Predictions." Innovations in Applied Engineering and Technology (2022): 1-6.
[19] Rao, Jiarui. "Machine Learning in Action: Topic-Centric Sentiment Analysis and Its Applications." Available at SSRN (2024).
[20] Rao, Jiarui, Qian Zhang, and Xinqiu Liu. "Applications Analyzing E-commerce Reviews with Large Language Models (LLMs): A Methodological Exploration and Application Insight." Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023 7.01 (2024): 207-212.
[21] Rao, Jiarui, et al. "Optimizing Stock Market Return Forecasts with Uncertainty Sentiment: Leveraging LLM-based Insights." Proceedings of the 2024 5th International Conference on Big Data Economy and Information Management. 2024.
[22] Li, Chao, Jiarui Rao, and Qian Zhang. "LLM-Enhanced XGBoost-Driven Fraud Detection and Classification Framework." (2025).
[23] Rao, Jiarui, and Qian Zhang. "Deep Learning with LLM: A New Paradigm for Financial Market Prediction and Analysis." (2025).
[24] Rao, Jiarui, and Zeyu Wang. "Optimizing Stock Market Return Forecasts with Uncertainty Sentiment: Leveraging LLM-based Insights." Available at SSRN 5117562 (2024).
[25] Rao, Jiarui, and Qian Zhang. "Deconstructing Digital Discourse: A Deep Dive into Distinguishing LLM-Powered Chatbots from Human Language." Journal of Theory and Practice in Education and Innovation 2.2 (2025): 18-25.
[26] Qian, Chenghao, et al. "WeatherDG: LLM-assisted procedural weather generation for domain-generalized semantic segmentation." arXiv preprint arXiv:2410.12075 (2024).
[27] Liu, Yanming, et al. "Bridging context gaps: Leveraging coreference resolution for long contextual understanding." arXiv preprint arXiv:2410.01671 (2024).
[28] Liu, Yanming, et al. "Tool-Planner: Task Planning with Clusters across Multiple Tools." arXiv preprint arXiv:2406.03807 (2024).
[29] Liu, Yanming, et al. "Bridging context gaps: Leveraging coreference resolution for long contextual understanding." arXiv preprint arXiv:2410.01671 (2024).
[30] Qian, C., Guo, Y., Mo, Y., & Li, W. (2024). WeatherDG: LLM-assisted Procedural Weather Generation for Domain-Generalized Semantic Segmentation. arXiv preprint arXiv:2410.12075.
[31] Privacy-Preserving Hybrid Ensemble Model for Network Anomaly Detection: Balancing Security and Data Protection
[32] Dai, Y., Wang, Y., Xu, B., Wu, Y., & Xian, J. (2020). Research on image of enterprise after-sales service based on text sentiment analysis. International Journal of Computational Science and Engineering, 22(2-3), 346-354.
[33] Cui, Wendi, et al. "Phaseevo: Towards unified in-context prompt optimization for large language models." arXiv preprint arXiv:2402.11347 (2024).
[34] Cui, Wendi, et al. "Divide-Conquer-Reasoning for Consistency Evaluation and Automatic Improvement of Large Language Models." Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing: Industry Track. 2024.
[35] Li, Zhuohang, et al. "Towards statistical factuality guarantee for large vision-language models." arXiv preprint arXiv:2502.20560 (2025).

[36] Zhang, Jiaxin, et al. "Synthetic Knowledge Ingestion: Towards Knowledge Refinement and Injection for Enhancing Large Language Models." arXiv preprint arXiv:2410.09629 (2024).
[37] Li, Zhuohang, et al. "Towards statistical factuality guarantee for large vision-language models." arXiv preprint arXiv:2502.20560 (2025).
[38] Sinha, Ankita, et al. "Survival of the Safest: Towards Secure Prompt Optimization through Interleaved Multi-Objective Evolution." arXiv preprint arXiv:2410.09652 (2024).
[39] Zhang, Jiaxin, et al. "SCE: Scalable Consistency Ensembles Make Blackbox Large Language Model Generation More Reliable." arXiv preprint arXiv:2503.10881 (2025).
[40] Wang, Yu, et al. "Gradient-guided Attention Map Editing: Towards Efficient Contextual Hallucination Mitigation." arXiv preprint arXiv:2503.08963 (2025).
[41] Cui, Wendi, et al. "Automatic Prompt Optimization via Heuristic Search: A Survey." arXiv preprint arXiv:2502.18746 (2025).
[42] Zhu, Yuanjing, and Yunan Liu. "Innovative Prompting Strategies and Holistic Evaluation of LLM Movie Recommender." 2024 International Conference on Intelligent Computing and Next Generation Networks (ICNGN). IEEE, 2024.
[43] Li, Wanxin. "User-Centered Design for Diversity: Human-Computer Interaction (HCI) Approaches to Serve Vulnerable Communities." Journal of Computer Technology and Applied Mathematics 1.3 (2024): 85-90.
[44] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).
[45] Chen, Yinda, et al. "Tokenunify: Scalable autoregressive visual pre-training with mixture token prediction." arXiv preprint arXiv:2405.16847 (2024).
[46] Wu, Siqi, et al. "Conditional Latent Coding with Learnable Synthesized Reference for Deep Image Compression." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 39. No. 12. 2025.
[47] Chen, Yinda, et al. "Bimcv-r: A landmark dataset for 3d ct text-image retrieval." International Conference on Medical Image Computing and Computer-Assisted Intervention. Cham: Springer Nature Switzerland, 2024.
[48] Chen, Yinda, et al. "Self-supervised neuron segmentation with multi-agent reinforcement learning." arXiv preprint arXiv:2310.04148 (2023).
[49] Wang, Y. (2025). Efficient Adverse Event Forecasting in Clinical Trials via Transformer-Augmented Survival Analysis.
[50] Wang, Y. (2025). Efficient Adverse Event Forecasting in Clinical Trials via Transformer-Augmented Survival Analysis.
[51] Qi, R. (2025). Interpretable Slow-Moving Inventory Forecasting: A Hybrid Neural Network Approach with Interactive Visualization.
[52] Wang, Y. (2025, May). Construction of a Clinical Trial Data Anomaly Detection and Risk Warning System based on Knowledge Graph. In Forum on Research and Innovation Management (Vol. 3, No. 6).
[53] Qi, R. (2025). DecisionFlow for SMEs: A Lightweight Visual Framework for Multi-Task Joint Prediction and Anomaly Detection.