Configuration Manual

MSc Research Project
MSc in Artificial Intelligence

Anuj Shashikant Bhogle
Student ID: x23288426

School of Computing
National College of Ireland

Supervisor: Prof. SHERESH ZAHOOR

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. Anuj Shashikant Bhogle ……

Student ID: …… X23288426 ……

Programme: …… MSc in Artificial Intelligence …… **Year:** 2024-25

Module: …… MSc Research Project ……

Lecturer: ……Prof. SHERESH ZAHOOR ……

Submission Due Date: ……11/08/2025……

Project Title: …Use of Artificial Intelligence in cybersecurity threat detection in E-Commerce and Retail…

Word Count: ……1097…… **Page Count:** ……3……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: …… Anuj Shashikant Bhogle ……

Date: ……11/08/2025……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Anuj Shashikant Bhogle
Student ID: x23288426

1 Introduction

This configuration document presents the specific explanation of the setup, implementation, and operational procedure of the fraud detection system that was made to fulfill the MSc research project AI-Driven Fraud Detection in E-Commerce and Retail using LightGBM. The implementation of the project takes advantage of a supervised machine learning model to detect fraud transactions in anonymized e-commerce. The methodology concentrates on the production of a solution that will be in scale, interpretable, and capable of being combined into in real life e-commerce settings. It is not only desired the good predictive performance but also the ability to have the model in a production environment but fulfilling the transparency and regulatory criteria (Rodrigues et al., 2022; Afriyie et al., 2023).

2 System Requirements

The system was implemented to work in a contemporary computing environment that has at least a quad-core processor Intel i7 and at least 16 GB of RAM, to provide potential to deal with large quantities of data. GPUs are an optional but highly recommended acceleration protocol to train models faster especially when repeating hyperparameter attunement. At least 10 GB storage should be available to hold datasets, preprocessed files and model outputs. It is created on the basis of Python 3.10, having an arsenal of specific libraries to build the workflow. These are pandas and numpy when it comes to efficient data manipulation, scikit-learn when it comes to data preprocessing, evaluation and cross-validation tasks as well as lightgbm as the main gradient boosting model, matplotlib and seaborn to easily visualize the data and the results, and shap allow to conduct post-hoc explainability analysis. The data set in this research is the Fraud E-commerce transactions data set in Kaggle consisting of 1,472,952 transactions with 16 features, the amount of the transactions, their product category, device and location of the customer and other demographic features. Its data has a highly skewed distribution, i.e. the case of transactions conducted fraudulently make up an extremely small percentage of the complete cases. Any sensitive data has been made anonymous to meet the rules of data privacy (Xie et al., 2023; Sqalli et al., 2024).

3 Configuration and Implementation Flow

Data acquisition and preprocessing is the starting point of configuration process. After the dataset gets into the working environment their schemas are validated to make sure that the column names, data type and completeness is congruent with the projected structure. The missing numerical values are imputed with Median in order to avoid the bias of outliers, and the missing categorical variables are assigned with the value of Missing to preserve potentially valuable signals related to fraud. Anonymization is done to such personal identifiable information like IP address and residential address but extracted in a way to keep

structural properties The population imbalance between the victims and the attackers is at a severe level in the given dataset; to overcome this, the configuration using the LightGBM class_weight parameter assigns a larger misclassification cost to the fraudulent transactions. This method would make sure that the model would have a focus on remembering the fraud cases without using synthetic over-representation approaches, which potentially can lead to overfitting on the synthetically generated data (Afriyie et al., 2023).which still might hold predictive information. Categorical features are encoded both in terms of one-hot encoding and LightGBM automatic categorical feature handling. Features that are cyclical like the time of the transaction are encoded to achieve cycles of fraud patterns (Murat Golyeri et al., 2023).
The key element to enhance the predictive powers of the model is feature engineering. It creates several derived variables, including transaction velocity metrics that determine a number of transactions that a customer or a device (within a certain period of time). Other aggregate data is also calculated of which the mean, median and maximum transaction level within specific periods per customer. Cross-feature product interaction terms are also produced that are compound variables of the types of products being sold and devices (Damayanti & Adrianto, 2023) as they can identify how the combination of attributes reveals the suspicious purchase patterns when identified at the individual variable level is challenging.
The training procedure of the model starts with the ability to separate the information of the data into a testing and training set with a stratified procedure so as to ensure the original ratio of fraud and non-fraud is not lost. The parameters that should be tuned are done on RandomizedSearchCV to find the best values to use in num_leaves, max_depth, learning_rate, feature_fraction, bagging_fraction, lambda_l1, and lambda_l2. ROC AUC has been considered as the main measure of evaluation during this optimization phase. When it is provided, GPU acceleration is turned on in order to accelerate training (Xu et al., 2023).
After training the model, the performance of the model is measured using some measures such as precision,recall, F1-score, ROC AUC on the test dataset as well as confusion matrix to learn how it is misclassifying. The results of comparative analysis with baseline models, Random Forest and XGBoost, show that LightGBM outperforms in recall (74.17%) and the highest ROC AUC (0.8493), as it was discussed in previous studies also (Rodrigues et al., 2022; Lu et al., 2022).
Explainability is a core component of the configuration and SHAP values are applied to measure the contribution of each feature to individual predictions and model behavior as well. This is essential to develop trust among fraud analysts, as well as to comply with the regulatory framework on explainable AI (Zhu et al., 2022; Sqalli et al., 2024). The associated probability scores exported with the predictions allows dynamic classification threshold capsulizing performance in line with operational requirements.

4 Deployment Considerations

The system, can be deployed both in batch processing and near-real-time settings. At a batch processing environment, daily or hourly transaction batches could be scored and at a near-real-time environment transaction could be scored within seconds of the transaction being initiated. The classification threshold must be precisely adjusted so that it gives priority between false positive and negative criteria based on what the organizationemployment can tolerate operation loss or operational interruption. When the organization is facing a high-risk period, like the seasonal promotions, then the threshold can be reduced in order to cover more potential fraud cases. For sustainable success, the specified model ought to be subjected to constant surveillance and occasional retraining because fraudulent practices are constantly evolving. Upcoming capabilities are to introduce graph-based capabilities to detect

coordinated fraud rings (Lu et al., 2022), as well as the integration of unsupervised anomaly detection methods so that new, and previously unknown fraud patterns, can be detected (Li et al., 2025).

References

Afriyie, J.K., Ma, T., Alhassan, J.K. and Hu, W. (2023) 'A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions', *Decision Analytics Journal*, 6, p.100163. https://doi.org/10.1016/j.dajour.2023.100163

Damayanti, R. and Adrianto, Z. (2023) 'Machine Learning for E-Commerce Fraud Detection', *Jurnal Riset Akuntansi Dan Bisnis Airlangga*, 8(2), pp. 1562–1577. https://doi.org/10.20473/jraba.v8i2.48559

Li, X. et al. (2025) 'Unsupervised Detection of Fraudulent Transactions in E-commerce Using Contrastive Learning'.

Lu, M. et al. (2022) 'BRIGHT — Graph Neural Networks in Real-Time Fraud Detection', *arXiv preprint*, arXiv:2205.13084.

Murat Golyeri, M. et al. (2023) 'Fraud detection on e-commerce transactions using machine learning techniques', *Artificial Intelligence Theory and Applications*.

Rodrigues, V.F. et al. (2022) 'Fraud detection and prevention in e-commerce: A systematic literature review', *Electronic Commerce Research and Applications*, 56, p.101207. https://doi.org/10.1016/j.elerap.2022.101207

Sqalli, M. H., Al-Emran, A. and Shaikh, M. A. (2024) 'A Survey on Cybersecurity in E-Commerce: Threats and AI-Based Countermeasures', *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3351215

Xu, B., Wang, Y., Liao, X. and Wang, K. (2023) 'Efficient Fraud Detection Using Deep Boosting Decision Trees', *Decision Support Systems*, 175, 114037. https://doi.org/10.1016/j.dss.2023.114037

Xie, S., Liu, L., Sun, G., Pan, B., Lang, L. and Guo, P. (2023) 'Enhanced E-commerce Fraud Prediction Based on a Convolutional Neural Network Model', *Computers, Materials & Continua*, 75(1), pp.1107–1117. https://doi.org/10.32604/cmc.2023.034917

Zhu, Y. et al. (2022) 'Modelling Users' Behaviour Sequences with Hierarchical Explainable Network for Cross-domain Fraud Detection'. https://doi.org/10.1145/3366423.3380172