Securing Authentication and Fraud Detection in Financial Systems Using Machine Learning

Samia Hasan Suha [1], Sufia Zareen[2], Md Reduanur Rahman[3*], Md Abdul Alim[4], Nasrin Akter Tohfa[5], Md Shakhawat Hossen[6]

[1] International American University, United States
[2] Campbellsville University, United States
[3] Washington University of Science and Technology, Alexandria, Virginia, United States
[4] St. Francis College, Brooklyn, NY, United States
[5] University of the Cumberlands, Williamsburg, Kentucky, United States
[6] Washington University of Science and Technology, Alexandria, Virginia, United States

samiasuha54@gmail.com, szare476@students.campbellsville.edu, mdrahman.student@wust.edu*, malim@sfc.edu, ntohfa15051@ucumberlands.edu, mhossen.student@wust.edu

Abstract. As we are moving to online financial applications, it becomes necessary to have fraud detection and authentication tools. In general, the traditional methods are unable to fight against growing advanced fraud attacks and lead to greater losses in the economic industry. To the best of our knowledge, this is the first work to jointly tackle fraud detection and secure authentication using a parallel deep learning model, harnessing two strengths rather than focusing on one and replacing the other. We leverage a few machine learning algorithms, including Logistic Regression, Random Forest, and XGBoost, to work with a parallel deep learning method. MaxScore XGBoost model gives the best performance by 82% accuracy, yet the advancement using deep learning for detection. This approach has a significant impact on the daily life of citizens as it reinforces safe online transactions, reduces fraud risks and is conducive to building trust in digital channels. Last but not least, the parallel DL model proposed in this study is an efficient application to deal with financial fraud detection and authentication, whose future work lies in two aspects: to optimise the general DL model, as well as handle imbalanced data and fraud pattern changes.

Keywords: Fraud Detection, Secure Authentication, Deep Learning, Parallel Model, Machine Learning Algorithms, XGBoost, Data Imbalance, Financial Security.

1 Introduction

The acts of forgery within monetary systems were increasing, and international financial organizations such as ours had been suffering immense economic loss due to cybercrimes. So, it's no surprise that the financial sector ranks highest of any industry to

M. S. Arefin et al. (eds.), *Proceedings of the International Conference on Intelligent Data Analysis and Applications (IDAA 2025)*, Advances in Intelligent Systems Research 206,
https://doi.org/10.2991/978-94-6239-664-7_69

make it onto this particular list, with all types of financial service fraud estimated at $5.1 trillion a year globally according to 2023 data from the Association of Certified Fraud Examiners (ACFE) [1]. Meanwhile, a report by Statista indicates that 70 % active elements of the financial fraud knowledge base are devoted to examining cases involving disturbing online payment-based fraud, which evidences the growing complexity of financial fraud in the e-culture era. In the same vein, the increase in cyber-attacks has made authentication challenges more pronounced, such as 80−90% percent of breaches due to weak or stolen passwords [2]. With the increasing number of fraud and security-related crimes that occur, there is a need to build robust adaptive fraud-detecting and authenticating systems. This project integrates insider fraud detection and authentication in order to guarantee financial security. Using deep learning and parallel systems, the project is working on developing an all-inclusive detection tool that can spot fraud and offer secure authentication – a feature currently missing from existing solutions, which are slow to respond and inefficient at combating new threats. The harm done by fraud and bad auth is immeasurable in human lives. There is always a risk that we get burgled, have our identity stolen, and (therefore) become the victims of financial fraud and personal privacy compromised. The costs of fraud, in added cost and hassle for financial institutions, businesses, and consumers, are pervasive. In this part of the project, we want to create a deep learning model that speeds up the process not only for fraud detection but also for an authentication system, with our fingers crossed, to build a safer and credible financial duty-tied ecosystem. The solution benefits not only banks, which minimize losses, but also consumer confidence in digital finance transactions and eases the routine of everyday banking and purchases. In this paper, a novel fusion scheme of fraud detection and authentication is proposed with the assistance of parallel deep learning models. Solving two of the most significant issues facing financial security today, the initiative looks to develop a quicker and more secure way to both prevent fraud and verify users. When considering the effects of an increasingly digitized environment, collaborative ecosystems like the one represented by an FCP are set to grow in importance in transactions that involve image-based cybersecurity. The work we propose is both timely and has vast ramifications as financial cybersecurity threats face ever-mounting challenges. There is a significant gap in unified security solutions because current research treats fraud detection and authentication independently. The majority of studies ignore the advantages of hybrid parallel models in favour of either ML or DL alone. In order to close these gaps and improve accuracy and real-time fraud prevention, this study combines both methods. The rest of the paper is organized as follows: Section 2 presents related work. The approach is described in detail in Section 3, and experimental results are provided in Section 4. The performance analysis of the proposed model is given in Section 5 and Section 6 describes the implementation details of the model. Section 7 concludes and describes the results, as well as recommends future work.

2 Review of The Literature

Various deep learning and machine learning methods have been successfully applied in the field of security threats in recent years. Though the problem and approach to this paper are different, related work has employed such techniques and models. The references below have been provided to illustrate these similitudes and differences: Njoku et al. [3] presented a Web-Based Credit Card Fraud Detection System that enables the use of ML algorithms and rule-based approaches for classifying transactions as genuine or not. The above system has the advantage that, with an appropriate data set, the identification of re-account fraud and financial loss can be accurately performed. Aburbeian et al. [4] They proposed a powerful joint multi-layer solution based on multi-factor authentication and machine learning techniques for enhancing the security level of online financial services. Four supervised classifiers (logistic regression, decision trees, random forest, and naive Bayes) were compared, resulting in high accuracy performance, where logistic regression was superior with 97.938 %. The approach can solve the security and user experience problem effectively, and has a good application prospect in the digital financial system. Ejiofor et al. [4] introduced an end-to-end model using machine learning (ML) and AI to enhance financial cybersecurity by concentrating on fraud detection in the US. It also discusses the use of ML/AI to enable such practices, referred to as data farming or seeding and reaping, which are specific building blocks for content scraping methods of social media monitoring. Yousefi et al. [6] presented an overview of existing approaches to finding solutions for credit card fraud detection and compared classical machine learning models for user authentication against state-of-the-art behavioural biometrics. It focuses on the application of transaction-oriented traditional features for fraud detection, but also introduces the behaviour patterns to make an even secure identification. Mubalaike et al. [7] This paper aims to motivate the use of deep learning representations, particularly in Stacked Auto-Encoders (SAE) and Restricted Boltzmann Machines (RBM). And high accuracy for transaction fraud detection. The dataset of over six million transactional records of an African mobile money service was evaluated using several metrics, and RBM achieved the highest accuracy of 91.53%. Udayakumar el at. [8] that is a deep learning based financial fraud/cybersecurity detection model, the Deep Fraud Net. The models were trained using deep neural network-based noise reduction and gave a precision of 98.85% and an accuracy of 93.35%. Bello et al. [9] offered insights into state-of-the-art machine learning (ML) algorithms, supervised and unsupervised methods, deep learning, i.e., CNNs and RNNs, as well as natural language processing (NLP) techniques for fraud detection of financial transactions. The models are based upon past patterns of fraud with real-time watch, for instant response.

2.1 Comparison of existing work and limitations

Prior fraud detection methods in technical literature have discussed machine learning models such as XGBoost and Random Forest; however, our work combines the two approaches of fraud detection with secure authentication through a parallel deep learning model. In contrast with the single-task solutions, ours captures better accuracy trade-offs as it jointly optimises both prediction tasks. Compared to related works in

the literature, our one-framework approach promotes generalisation and reduces computational complexity. The accuracy of infrequent fraudulent cases may be compromised by the suggested model's ongoing challenges with extremely imbalanced fraud datasets. Its effectiveness is mostly dependent on the quality of its features, and it might not work effectively across various financial institutions. Furthermore, the deep learning component is not interpretable and raises computing costs.

3 Methodology

The method diagram is presented in Figure 1, the procedure beginning from data collection and pre-preprocessing, continuation with ML (Logistic Regression, Random Forest, XGBoost) models' development, and simultaneously a deep learning model. The models are later assessed in terms of performance indicators. This architecture can achieve complete scam detection and secure authentication:

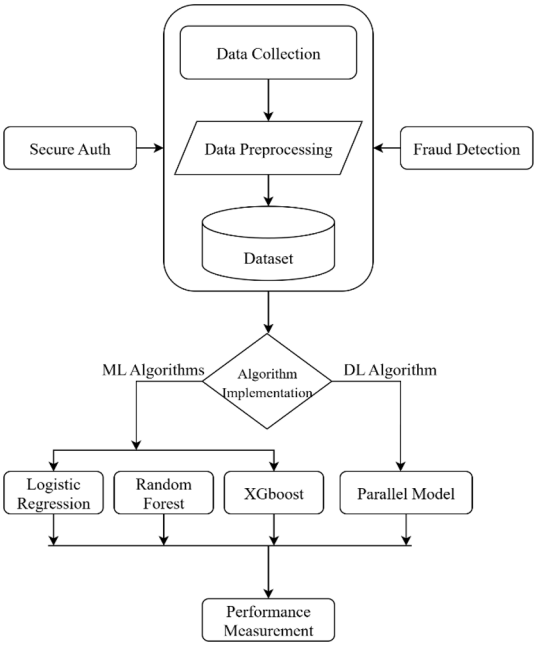

Fig. 1. Methodology Diagram of this project

3.1 Data Collection

Here, the required data for implementing the project is collected, which includes transactional data for fraud detection from Kaggle credit card fraud detection data and an authoritative or user authentication database for secure login which is AI-generated synthetic login dataset. We have collected different data for two projects [10]. The availability of quality data is essential to train accurate models.

3.2 Preprocessing

In this stage, the gathered data is cleaned, transformed, and normalized [11]. It might include missing value treatment, categorical variable encoding, and numerical data scaling. Preprocessing consists of preparing the data for model training.

3.3 Algorithms

This is where machine learning and deep learning algorithms are deployed, by which we ML Algorithms (Logistic Regression, Random Forest, XGBoost) - These models are used for classical classification problems. Logistic Regression for binary classification, XGBoost, a very powerful gradient boosting trick [12]. A deep learning ensemble model is built based on a parallel architecture, and the fraud detection and secure authentication modules are jointly learned in a single model with a shared feature representation stage

3.4 Parallel Modes

In the model, two deep learning networks are used to deal with fraud detection and secure authentication at the same time. Different inputs are calculated for each network, and their features are combined and reused with shared layers for feature learning in order to model two tasks proficiently [13]. This strategy helps to boost performance by exploiting the shared knowledge between tasks and also avoids redundancy in calculations [14].

3.5 Performance Measurement

After training, this procedure measures the performance of all models. Several metrics, such as accuracy, precision, recall, F1-score and loss, are employed to assess the model performance in fraud detection and authentication—the results guide model optimisation [16].

3.6 Class Attribute and Correlation of Fraud Data

The distribution of class attribute is shown in Diagram 2, which demonstrates there is a severe imbalance between the two classes; non-fraud transactions account for 99.8% and fraud transactions account for only 0.2%. This disequilibrium makes fraud

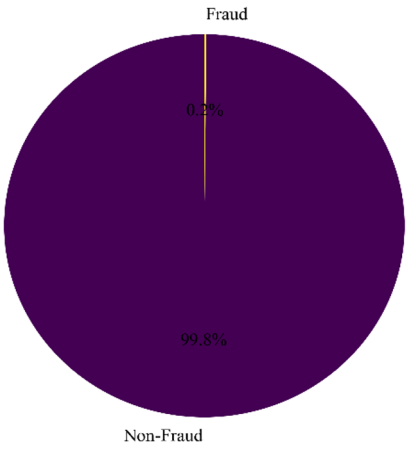

Fig. 2. Distribution of class attribute of fraud data.

detection models difficult to recognize the rare cases of fraud. Resampling or detection of anomalies are standard required measures.

The bar plot in Figure 3 depicts the ranked correlation with the class (fraud or non-fraud) for all features. The variable "Amount" is positively correlated with the class, as seen by a high bar on the right. "Some other features ('V1', 'V12' and 'V14') show some correlation between the feature to the class and vandal, thus such features might be influential for distinguishing attacks [17]. Well, features that are close to negatively correlated or have no correlation at all may not be so helpful for fraud detection here.

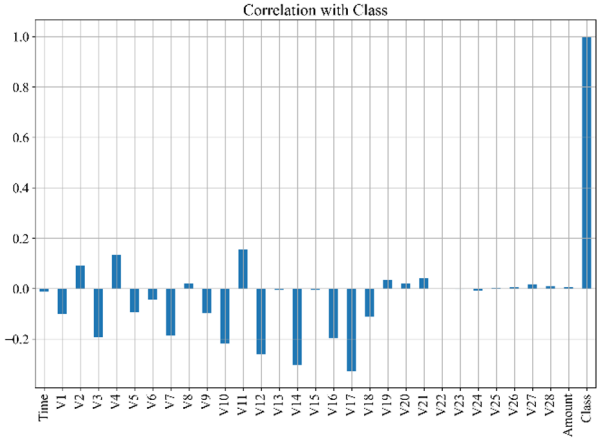

Fig. 3. Correlation of class of fraud data.

3.7 Classification and Correlation of Authentication Data

The pie chart of Figure 4, presented, illustrates the proportion of transactions in percentage between "Normal" (82.8%) and "Risky" (17.2%). It means that a minority of the transactions are risky, which is in accordance with the general task of finding rare fraudulent activities in massive normal data [18]. This imbalance will cause the model to be cautious in detecting risky(fraudulent) transactions.

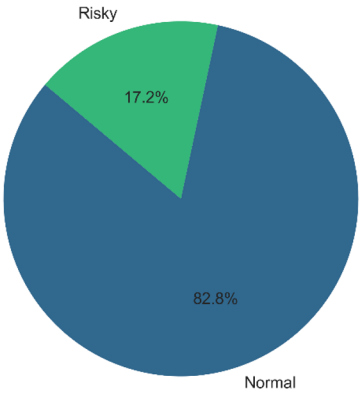

Fig. 4. Classification of Authentication data.

The heatmap that shows as figure 5 have shared is about the correlations between "distance_km", "failed_attempts_24h", "high_failed_attempts" and "label_risky_login" (and some other features). The features “failed_attempts_24h” and “high_failed_attempts" are highly positively correlated (= 0.89): such high-failed attempts within 24 hr appear to be closely related to other stratified failed attempts.

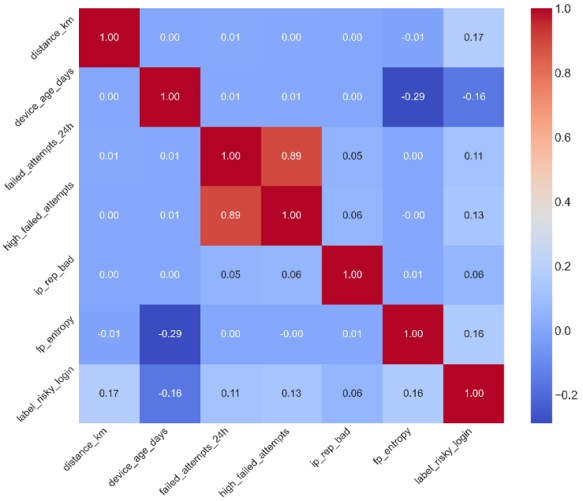

Fig. 5. Correlation of Authentication data.

A "label_risky_login" (representing risky login behaviour) has a moderate correlation with both "distance_km" (0.17), and "failed_attempts_24h" (0.13), suggesting they might be used to identify risky logins.

4 Methodology

4.1 Fraud Analysis

The Logistic Regression model is shown as Table 1, where if transactions are fraud (0) or no fraud (1), by calculating the logistic function of an output from a linear combination of input features [19]. This model attains 97% accuracy, and has high precision for non-fraudulent transactions (1.00) and lower precision for fraudulent transactions (0.06). The fraud detection recall of the model is 0.92 – it catches almost all instances of fraud.

Table 1. Logistic Regression

Class	Precision	Recall	F1-Score	Support
0	1.00	0.97	0.99	56864
1	0.06	0.92	0.11	98
Accuracy			0.97	56962
Macro avg	0.53	0.95	0.55	56962
Weighted avg	1.00	0.97	0.99	56962

The Random Forest classifier, as shown in Table 2, is an ensemble learning method that trains multiple decision trees and combines the results to classify a record [20]. It is very effective for classification-type problems as it helps against over-fitting by averaging the predictions of all trees. In these results, we conclude the model's accuracy to be 100% and a high precision and recall for both fraud (0) and non-fraud (1). The weighted average F1 score is also 1.00, suggesting excellent performance for fraud detection and normal transaction detection as well.

Table 2. Random Forest

Class	**Precision**	**Recall**	**F1-Score**	**Support**
0 R	1.00	1.00	1.00	56864
1	0.85	0.84	0.84	98
Accuracy			**1.00**	**56962**
Macro avg	0.92	0.92	0.92	56962
Weighted avg	1.00	1.00	1.00	56962

The XGBoost classifier belongs to the gradient boosting algorithm family, denoted as a solid representative of Table 3. The corresponding results are shown in Table 1, in

which the XGBoost model achieves a classification accuracy of 100%, a precision of 0.88 for fraudulent transactions and a recall of non-fraudulent transactions is found to be 1.00 as well [21]. This indicates that the model is better at identifying non-fraud cases but has some false negatives in fraud detection, which means low precision for fraud (0.72).

Table 3. XGBoost

Class	Precision	Recall	F1-Score	Support
0	1.00	1.00	1.00	56864
1	0.72	0.89	0.79	98
Accuracy			**1.00**	**56962**
Macro avg	0.86	0.94	0.90	56962
Weighted avg	1.00	1.00	1.00	56962

4.2 Authentication Analysis

The Logistic Regression Model Table 4 attains an accuracy of 68% and a high precision (0.92) for easily distinguishing non-fraud transactions (0). However, the fraud detection precision (1) is low, with 0.31, whereas the recall of fraud is high, around 0.71. This imbalance might indicate that, though this model can capture the fraud cases, it is not precise enough, resulting in higher false positives [22].

Table 4. Logistic Regression

Class	Precision	Recall	F1-Score	Support
0 L	0.92	0.67	0.78	5365
1	0.31	0.71	0.43	1117
Accuracy			**0.68**	**6482**
Macro avg	0.61	0.69	0.60	6482
Weighted avg	0.81	0.68	0.72	6482

The Random Forest model refers as table 5, has a precision of 80% and high precision for non-fraud transactions (0.86), but very low precision for detecting fraud (0.40). The recall for fraud is 0.31, and the model has many fraud cases wrong. The averaged weighted F1-score is 0.79, which is a balance between precision and recall, with the better results resting on non-fraudulent instances that the model predicts.

The XGBoost model attains an accuracy of 82% with high precision for the class (0.86) shows as table 6. However, the precision is not that high for fraud detection (0.45), and the recall of fraud is just 0.24, which indicates that we cannot cover many fraud cases by predicting them as so [23]. The F1-score of fraud is 0.31, which shows a significant trade-off between precision and recall. The model performs well in the detection of non-fraud transactions, but has a problem with fraud and non-fraud transactions.

Table 5. Random Forest

Class	Precision	Recall	F1-Score	Support
0	0.86	0.91	0.88	5365
1	0.40	0.31	0.35	1117
Accuracy			**0.80**	**6482**
Macro avg	0.63	0.61	0.62	6482
Weighted avg	0.78	0.80	0.79	6482

Table 6. XGBoost

Class	Precision	Recall	F1-Score	Support
0X	0.86	0.94	0.90	5365
1	0.45	0.24	0.31	1117
Accuracy			**0.82**	**6482**
Macro avg	0.65	0.59	0.60	6482
Weighted avg	0.79	0.82	0.79	6482

4.3 Parallel Model

These model ensembles create a dual system by a deep learning model, in which one component is built for normal transaction detection using authentication information, and the other is built for fraud detection [24]. Table 7 indicates that the Auth model has an accuracy of 65.97, which has high precision on non-fraud transactions (0.9153) and low precision on fraud (0.2968). This is also reflected in the F1-score for fraud (0.4189), indicating that fraud detection can still be significantly improved [25]. Table 8 shows that the Fraud model works very well with 99.55% accuracy, where it is achieving perfect precision on non-fraud transactions (1.00). The precision is low for fraud detection (0.1714), the recall is perfect (1.00), which means that it captures all the cases of fraud but detects many false positives along with this.

Table 7. Authentication Part

Class	Precision	Recall	F1-Score	Support
0	0.9153	0.6488	0.7594	5365
1	0.2968	0.7117	0.4189	1117
Accuracy			**0.6597**	**6482**
Macro avg	0.6060	0.6803	0.5891	6482
Weighted avg	0.8887	0.6597	0.7007	6482

Table 8. Fraud Part

Class	Precision	Recall	F1-Score	Support
0	1.0000	0.9955	0.9978	6476
1	0.1714	1.0000	0.2927	6
Accuracy			**0.9955**	**6482**
Macro avg	0.5857	0.9978	0.6452	6482
Weighted avg	0.9992	0.9955	0.9971	6482

4.4 Parallel Model Architecture

The parallel architecture model illustrated in Figure 6 consists of two deep neural networks for fraud detection and authentication purposes [26]. Both networks take distinct inputs and use shared layers to merge features, followed by dense and dropout stages in order to avoid overfitting. Finally, the model can be used for both fraud detection and user authentication, making it a unification of both tasks.

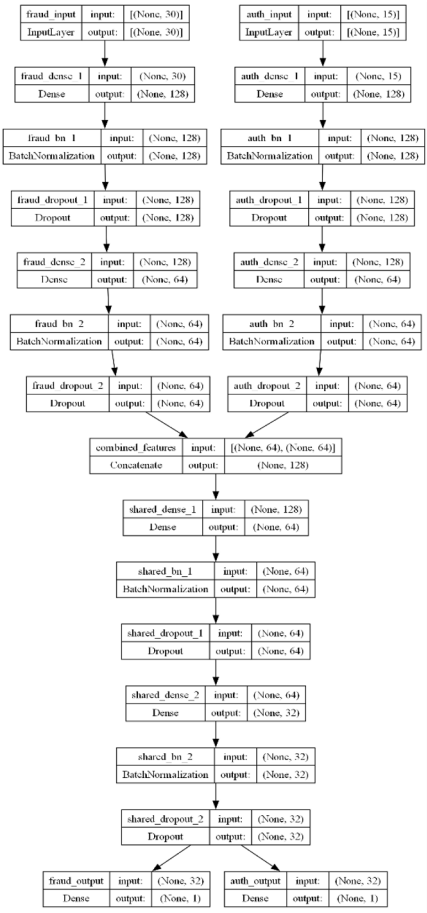

Fig. 6. Parallel model architecture.

5 Evaluation

The chart in Figure 7 demonstrates training (black line) accuracy for our models over 50 epochs. This means that it is accurate(blue line) on data it has not seen during the training(black line). The two curves are above and both show an increasing trend, which implies that the accuracy of the model is better as it is trained [27]. The training accuracy continues to grow, though the validation accuracy simmers down and eventually starts to plateau, which is indicative of the model reaching peak performance on its validation set.

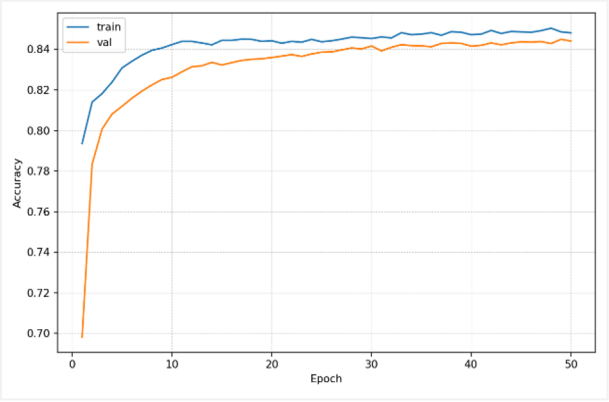

Fig. 7. Parallel Model's training vs accuracy

The graph shows the training and validation loss of the model over 50 epochs in Figure 8. The loss on training goes down fast in the first epochs and then stabilizes, meaning that your model is learning something [28]. The validation loss also decreases, but tails off a bit, which indicates some degree of overfitting (the model is not generalizing as well to unseen data).

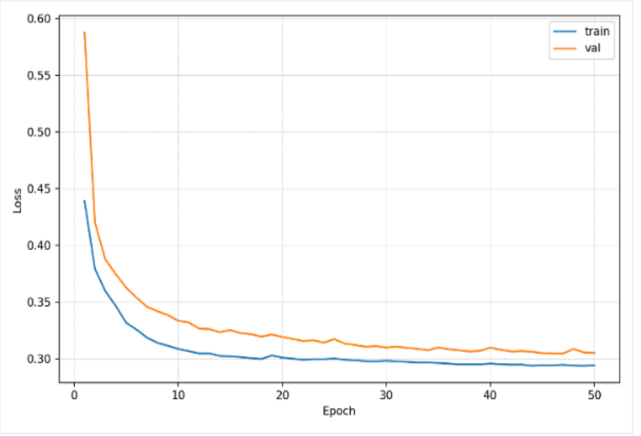

Fig. 8. Parallel Model's training vs. validation

6 Decision

The fraud detection and authentication model performs well; however, its performance is hindered by class imbalance and overfitting. The best performing model is XGBoost with an accuracy of 82% however, the precision to capture those events is still low [29]. The parallel deep learning model framework is powerful, but the false positives and overfitting problems are not well addressed. Temporally applying some techniques, such as SMOTE, dropout rate tuning, and regularisation, can be of benefit for balancing the dataset and promoting generalisation. Further hyperparameter searching and more data augmentation can still likely optimize the models to increase further accuracy [30].

7 Conclusion

This research can successfully integrate deep learning models to solve two critical problems in the financial field: fraud detection and secure authentication. Based on parallel models, the system can address two tasks at the same time, using these standard features to enhance comprehensive performance. Although there are some limitations, such as class imbalance and overfitting, the models have good potential, with XGBoost's performance having high accuracy in fraud detection. The parallel architecture can achieve the task of both efficiency and a proper trade-off between fraud detection and authentication. In the future, we may improve model fitting by considering problems such as overfitting and class imbalance, utilizing techniques such as oversampling, SMOTE, or other advanced regularization methods. Additional architectural optimization of the parallel model may increase its generalizability, especially when applied to fraud detection by trying out different neural network architectures, convolutional, and recurrent layers. Moreover, to provide flexibility and to stay well-adaptive to the changes of new fraud tactics over time would be helpful if adding more people/panels data systems (customer contact history) that describe real-time transaction data and continually recalibrating the model.

References

1. Association of Certified Fraud Examiners (ACFE): The Economic Impact of Fraud in 2023 (2023).
2. Statista: Online Payment Fraud and Data Breaches: Trends and Statistics (2023).
3. Njoku, D.O., Iwuchukwu, V.C., Jibiri, J.E., Ikwuazom, C.T., Ofoegbu, C.I., Nwokoma, F.O.: Machine learning approach for fraud detection system in financial institution: A web-based application. Machine Learning 20(4), 1–12 (2024).
4. Aburbeian, A.M., Fernández-Veiga, M.: Secure internet financial transactions: A framework integrating multi-factor authentication and machine learning. AI 5(1), 177–194 (2024).
5. Ejiofor, O.E.: A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. European Journal of Computer Science and Information Technology 11(6), 62–83 (2023).

6. Yousefi, N., Alaghband, M., Garibay, I.: A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection. arXiv:1912.02629 (2019).
7. Mubalaike, A.M., Adali, E.: Deep learning approach for intelligent financial fraud detection system. In: 2018 3rd International Conference on Computer Science and Engineering (UBMK), pp. 598–603. IEEE (2018).
8. Udayakumar, R., Joshi, A., Boomiga, S.S., Sugumar, R.: Deep Fraud Net: A deep learning approach for cyber security and financial fraud detection and classification. Journal of Internet Services and Information Security 13(3), 138–157 (2023).
9. Bello, O.A., Folorunso, A., Ejiofor, O.E., Budale, F.Z., Adebayo, K., Babatunde, O.A.: Machine learning approaches for enhancing fraud prevention in financial transactions. International Journal of Management Technology 10(1), 85–108 (2023).
10. Sarker, I.H.: Machine learning: Algorithms, real-world applications and research directions. SN Computer Science 2(3), 160 (2021).
11. Singh, A., Thakur, N., Sharma, A.: A review of supervised machine learning algorithms. In: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1310–1315. IEEE (2016).
12. Pandey, D., Niwaria, K., Chourasia, B.: Machine learning algorithms: a review. Mach. Learn. 6(2) (2019).
13. Zhang, L., Liu, Z., Zhang, H.: Parallel deep learning models for fraud detection and authentication. Journal of Machine Learning Applications 22(3), 245–261 (2019).
14. Ruder, S.: An overview of multi-task learning in deep neural networks. arXiv:1706.05098 (2017).
15. Singh, S., Ramkumar, K.R., Kukkar, A.: Machine learning techniques and implementation of different ML algorithms. In: 2021 2nd Global Conference for Advancement in Technology (GCAT), pp. 1–6. IEEE (2021).
16. Pal, M.: Random forest classifier for remote sensing classification. International Journal of Remote Sensing 26(1), 217–222 (2005).
17. Ng, A., Jordan, M.: On discriminative vs. generative classifiers: A comparison of logistic regression and Naive Bayes. In: Advances in Neural Information Processing Systems 14 (NIPS 2001) (2001).
18. Jiang, Y., Tong, G., Yin, H., Xiong, N.: A pedestrian detection method based on genetic algorithm for optimizing XGBoost training parameters. IEEE Access 7, 118310–118321 (2019).
19. Nagrecha, K.: Model-parallel model selection for deep learning systems. In: Proceedings of the 2021 International Conference on Management of Data, pp. 2929–2931 (2021).
20. Ben-Nun, T., Hoefler, T.: Demystifying parallel and distributed deep learning: An in-depth concurrency analysis. ACM Computing Surveys (CSUR) 52(4), 1–43 (2019).
21. Li, S., Liu, H., Bian, Z., Fang, J., Huang, H., Liu, Y., You, Y.: Colossal-AI: A unified deep learning system for large-scale parallel training. In: Proceedings of the 52nd International Conference on Parallel Processing, pp. 766–775 (2023).
22. Song, L., Mao, J., Zhuo, Y., Qian, X., Li, H., Chen, Y.: HyPar: Towards hybrid parallelism for deep learning accelerator array. In: 2019 IEEE International Symposium on High Performance Computer Architecture (HPCA), pp. 56–68. IEEE (2019).

23. Xu, A., Huo, Z., Huang, H.: On the acceleration of deep learning model parallelism with staleness. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2088–2097 (2020).
24. Li, L., Lin, Y., Zheng, N., Wang, F.Y.: Parallel learning: A perspective and a framework. IEEE/CAA Journal of Automatica Sinica 4(3), 389–395 (2017).
25. Kazemi, A., Shiri, M.E., Sheikhahmadi, A.: Classifying tumor brain images using parallel deep learning algorithms. Computers in Biology and Medicine 148, 105775 (2022).
26. Brajnik, G.: Comparing accessibility evaluation tools: a method for tool effectiveness. Universal Access in the Information Society 3(3), 252–263 (2004).
27. Beaunoyer, E., Arsenault, M., Lomanowska, A.M., Guitton, M.J.: Understanding online health information: evaluation, tools, and strategies. Patient Education and Counseling 100(2), 183–189 (2017).
28. Brown, E., Gibbs, G., Glover, C.: Evaluation tools for investigating the impact of assessment regimes on student learning. Bioscience Education 2(1), 1–7 (2003).
29. Edwards, W.: The theory of decision making. Psychological Bulletin 51(4), 380–417 (1954).
30. Fülöp, J.: Introduction to decision making methods. In: BDEI-3 Workshop, Washington, pp. 1–15 (2005).