CONFERENCE PAPER
International Multidisciplinary Conference on Innovation, Technology and Sustainability

Accepted: February 24, 2026 | **Published:** March 7, 2026 | **Language:** English

Section of the conference: *Computer science, computing and automation*
Sekcja konferencji: *Informatyka, obliczenia i automatyzacja*

SafeSwipe: A Cloud-Enabled XGBoost Framework for Credit Card Fraud Detection

R. Sree Chaitra[1], M.Hemanth [1], K. Srikanth[1], T. Ravi Kumar[1,*]

[1] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502, Andhra Pradesh, India

✉ ***Corresponding author:** T. Ravi Kumar*

ABSTRACT: The abuse of the credit card systems is a significant cause of financial risks that are subjecting both the customers and the banking institutions to a significant level of risk. Conventional fraud detection systems, which are generally based on a preconfigured set of rules, are unable to adapt fast enough to changing fraud techniques. Consequently, they often produce a significant number of false alarms and decrease the effectiveness of the entire prevention procedure. To overcome these limitations, this paper presents a machine learning-based framework, which combines the use of Amazon SageMaker and XGBoost. With the help of historical transaction data classified as legitimate or malicious, the model is taught the ability to identify the slight changes of behavior that can lead to malice. The proposed approach will enable quick, adaptive evaluation unlike fixed rule engines and can dynamically adapt to new fraud patterns. Such models can be created, modified and stored in Amazon SageMaker, using limited infrastructure, in an easy managed manner. Gradient boosting implementations, such as XGBoost provide greater accuracy and lower false positive detection rates. As a result, this combined usage will strengthen payment security and improve the reliability and convenience of transaction processing for all financial organizations and customers.

KEYWORDS: Credit Card Fraud Prevention, Adaptive Machine Learning, Amazon SageMaker Platform, XGBoost Classifier, Dynamic Fraud Detection, Behavioral Pattern Analysis, Secure Transactions.

How to cite: Sree Chaitra, R., Hemanth, M., Srikanth, K., & Ravi Kumar, T. (2026). SafeSwipe: A Cloud-Enabled XGBoost Framework for Credit Card Fraud Detection. *International Multidisciplinary Conference on Innovation, Technology and Sustainability*. Futurity Research Publishing. https://doi.org/10.5281/zenodo.18974723

I. Introduction

As the number of transactions made electronically is on an upward trend, the problem of credit card fraud has become a burning issue to both individuals and financial organizations. Traditional rule-based systems simply do not keep up with more advanced offenders and their methods of committing fraud, thus they are frequently unable to discover the hidden structure of a fraud. A potential solution is machine learning. As an example, one can refer to the project Fraud Shield, in which the authors state that with the help of cutting-edge analytics and scalable cloud solutions, they can evaluate huge amounts of payment data, increasing the effectiveness of identifying suspicious activity.

Although solutions like Fraud Shield use strong ensemble models such as XGBoost to identify frauds, a more explainable model was used in this project; an implementation of Logistic Regression. Famous due to the ability to estimate the unique aspects that inform a binary classification process, Logistic Regression discloses the Standalone factors that control the classification of a transaction as either legitimate or suspicious.

This not only aids in understanding and explaining the decision-making process but also serves as a solid foundation for developing more complex models in the future.

The aim of the study is to develop an effective system of fraud detection that encompasses both sophisticated learning models with the interpretability of logistic regression that will ensure the flexibility to new methods used in fraud and maintain transparency in the classification outcome.

II. Literature review

Credit card fraud presents substantial financial threats and requires advanced machine learning (ML) and cloud-based detection systems. Conventional techniques are not effective in overcoming the changing patterns of frauds and this necessitates the use of ML models to identify frauds accurately [1], [2].

ML methods such as Random Forest (RF), Logistic Regression (LR), Decision Tree (DT), and XGBoost (XGB) are known to have high interpretations of fraud detection with an accuracy of 98.37 and F1-score of 97.95. The techniques of pre-processing used to improve data quality include feature selection and outlier rejection [3], [4]. Further models such as Hidden Markov Models, Naïve Bayes, and k- Nearest Neighbors are behavioral analysis models that enhance the detection of frauds based on transaction patterns [5].

SMOTE is used in conjunction with ensemble models optimised by Particle Swarm Optimisation (PSO) to address the imbalance between authentic and fraudulent samples in fraud detection. Robust performance is ensured by evaluation metrics like Precision, Recall, F1-score, and Accuracy [7], [8]. Cloud computing provides a means to perform secure, scalable monitoring to minimize data loss and confidentiality problems, however when it comes to fraud detection, systems such as Convolutional Neural Networks (CNN), Support Vector Machines (SVM), and Artificial Neural Networks (ANN) perform much better than traditional ML systems.

During COVID-19, there was a 225% increase in online fraudulent transactions that created more demand for AI-based solutions.ii Therefore, using AWS-based fraud detection systems such as Fraud Detector, A2I, SageMaker, Glue, and Lambda, real-time confirmation of identity and efficient processing of transactions become possible. [9], [10]. On a whole, rule-based methods in fraud detection were the traditional approach, but do not appropriately accommodate the ongoing changes in fraud. iii However, machine learning models are able to predict outcomes based on patterns from previously processed transaction records and therefore have provided increases in accuracy, where as traditional methods were much below what would be considered acceptable [11], [12]. For example, models such as Decision Trees (DT), SVM, and various ensemble methods have demonstrated superior accuracy levels [13], [14].

Sophisticated methods using deep learning techniques, particularly ANNs and CNNs, have been instrumental in advancing fraud detection due to their capabilities for accurately modelling the correlations among many variables (high-

dimensional data) [15],[16]. In addition to those, recent studies explored the usage of autoencoders and GANs for detecting anomalies in credit card transactions; the results showed promise [17],[18].

Cloud-based systems on platforms such as AWS offer both scalability and cost-effective options for deploying fraud detection systems. Real-time detection can be implemented at a lower overall infrastructure cost through serverless computing and services such as AWS Lambda, SageMaker and Fraud Detector [19]. Implementation of tough regulations like GDPR and PCI DSS has created challenges for companies to ensure that customer data maintains its confidentiality, which is a major focus in today's world [20]. Various machine learning algorithms are used in conjunction with these cloud-based solutions to optimize accuracy and dependability in fraud deterrent processes.

To identify fraud, a number of models based on DT, RF, ANN, LR, and SVM are used. Feature selection techniques such as chi- and Pearson correlationTests help identify important characteristics, which improves model effectiveness as digital marketplaces expand quickly and credit cards become more widely used [21], [22]. Logistic regression minimises false positives while achieving nearly 99% accuracy, according to comparative analyses [21].

The rapid expansion of digital marketplaces and the growing prevalence of credit cards have led to a sharp increase in fraud incidents. For effective fraud detection, more sophisticated methods like approximate reasoning, artificial intelligence, and data mining are required because traditional pattern-matching techniques have proven inadequate [21], [22]. According to recent studies, Transformer models outperform traditional machine learning algorithms like RF, SVM, and XGB in detecting fraud. Their robust and consistent performance is supported by metrics such as Precision, Recall, F1 Score, and ROC AUC [23].

The rare instances of fraudulent transactions lead to a significant class imbalance which makes the problem of accurate detection more difficult. Various boosting methods, like XGB, are used to tackle this problem and hence, the detection accuracy is getting better [24], [25]. Besides that, ML models built with TensorFlow have been found to be very helpful in fraud prediction as they take in past transaction data and thus, the output is an efficient and accurate detection system [26].

Majority of Americans faced credit card fraud in 2021 as per the findings published in 2021. This situation had been the cause for an urgent call to automate fraud detection methods. Out of six supervised machine learning models—Naive Bayes, SVM, RF, KNN, LR, and XGB—SVM was found to have the highest accuracy in detecting fraud transactions [27],[28].

Deep learning methods notably CNNs, have similarly demonstrated considerable potential in fraud detection. Using the European card benchmark dataset, experiments unveiled that accuracy, F1-score, and AUC metrics were substantially improved when deep learning was integrated with data balancing techniques [29],[30].

III. METHODOLOGY

The suggested system utilizes Amazon SageMaker to develop and deploy an XGBoost model for the identification of fraudulent credit card transactions through a range of processes including: preprocessing; training; validating; deploying; and monitoring in real-time.

A. Data Collection and Preprocessing

To train the model, an openly available dataset of credit card transactions would be utilized. Prior to the training stage, preprocessing steps would take place, including:

1. **Data Cleaning**: Removing missing values, duplicates, and inconsistencies.

2. **Feature Engineering:** Extracting significant features, including transaction time, amount, merchant category, and user spending behaviors.

3. **Handling Data Imbalance:** Given the scarcity of fraudulent transactions, SMOTE is utilized to balance the data.

4. **Data Normalization:** Standardizing numerical features to improve model convergence.

B. Model Training Using XGB on Amazon SageMaker

The algorithm is selected based on the fact that it implements an optimized version of the traditional gradient boosting algorithm (XGBoost), which is known for its accuracy and is able to be executed in a timely manner when performing the task of identifying fraudulent credit card transactions. As an example, the model would be trained using Amazon SageMaker's managed training environment (the managed training environment is known to support high-performance computing) alongside GPU-based instances for faster processing.

Key training steps:

1. **Hyperparameter Optimization:** SageMaker's auto-tuning optimizes learning rate, tree depth, and estimator count.

2. **K-Fold Cross-Validation:** Adopted to prevent excessive fitting to observed data and maintain robust predictive accuracy.

3. **Parallel Processing:** SageMaker distributes computations across multiple instances to reduce training time.

C. Model Evaluation

The below metrics that would be utilized to evaluate how effectively the model identifies fraudulent transactions.

1. **Accuracy:** Quantifies the total predictive accuracy

2. **Precision & Recall:** Measures how well the model will identify fraudulent transactions.

3. **F1-Score:** composite measure of both precision and recall.

ROC-AUC Score: measure of how well the model can distinguish between fraudulent and non-fraudulent transactions.

Once the training has been completed, hosting services provided by Amazon SageMaker would be used to provide access to the trained XGBoost model through a REST API so that real-time access can be accomplished.

Scalable API Integration: A REST API is provisioned to serve the model for real-time fraud detection.

1. **AWS Lambda & API Gateway:** Enables secure and low-latency model inference.

2. **Auto Scaling:** Adjusts computational resources dynamically based on incoming transaction volume.

D. Continuous Monitoring and Model Improvement

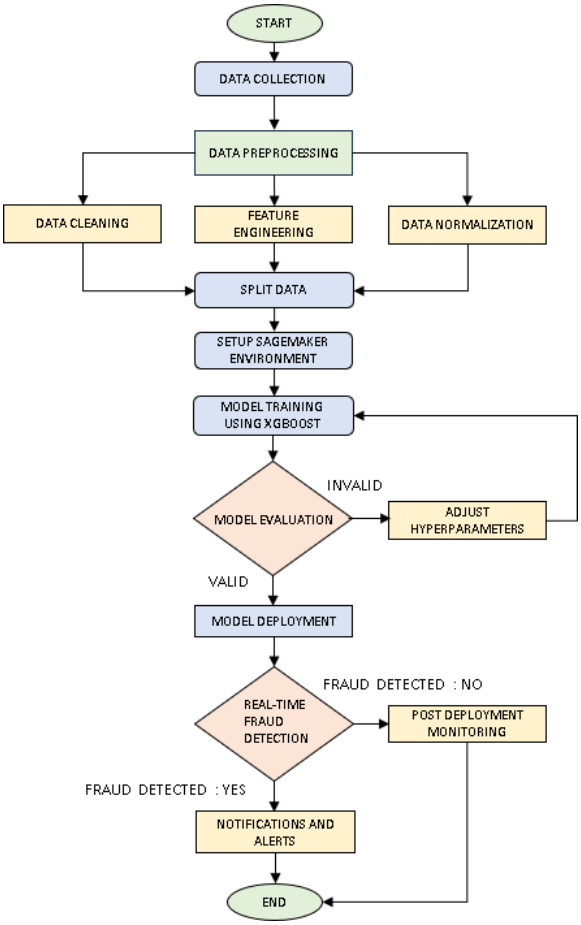
In addition, once the model has been deployed, it would be monitored over-time for accuracy through the use of both Amazon SageMaker Model Monitor and Amazon CloudWatch. Key components that would require monitoring include:

1. **Data Drift Detection:** Identifies changes in transaction patterns.

2. **Automated Retraining:** Triggers model updates when performance degradation is detected.

Figure 1

Methodology Flowchart



RESULTS

The training and validation loss curves for classification models (LR, RF, SVM, GB, KNN, and XGB) are shown in Figures 1-7. The loss function used in all models was Log Loss since it is commonly used to assess performance between two binary classes.

Figure 2

Logistic Regression – Loss Curve

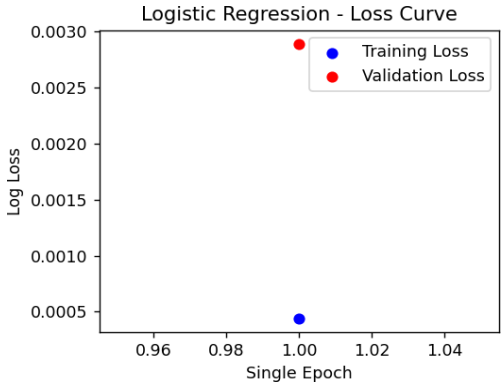
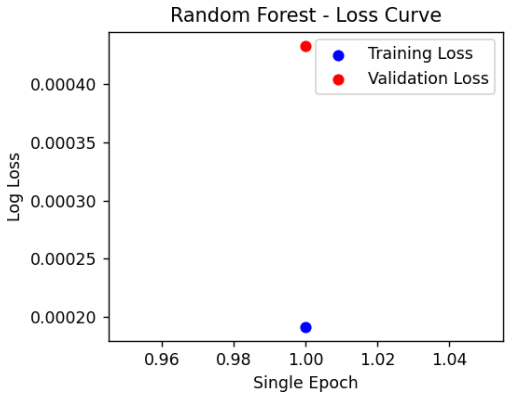


Figure 3

Random Forest – Loss Curve



Analysis of Single-Epoch Trained Models:

For LR, RF, SVM, XGB, and KNN, only one epoch was trained with this model. Therefore, the loss curves for these models only show one point in time, representing the loss after one pass through the training dataset. The loss curves created with only one epoch of training do not give a good indication about how the models are doing with their learning and therefore, any statement made about such points would be nothing more than a guess, and would not be able to be substantiated with much evidence.

Figure 4

SVM – Loss Curve

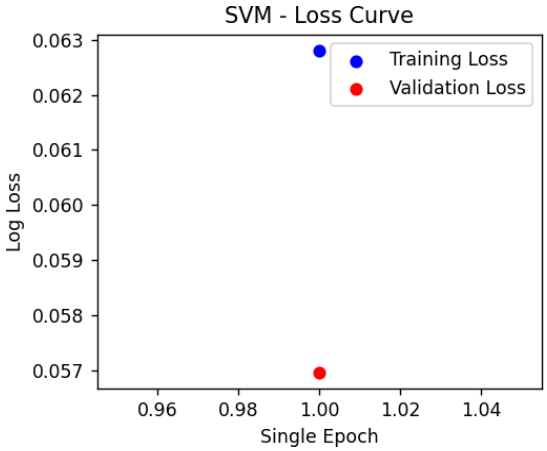
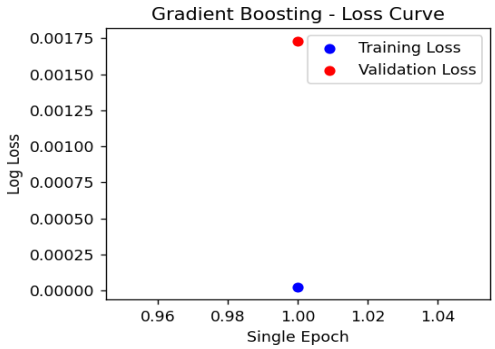


Figure 5

Gradient Boosting – Loss Curve

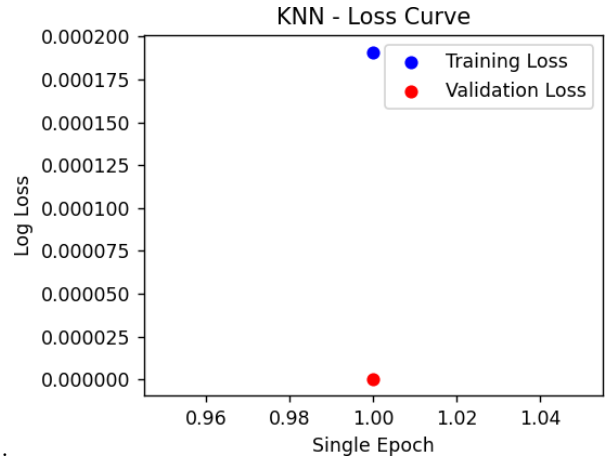


Detailed Analysis of XGBoost Loss Curve:

Since the Model trained with XGBoost has undergone a thorough analysis based on multi-epoch training (Figure 7) the loss journey of the training process is well documented.The training loss was lowered very fast in the first epochs and then it became stable, which means that the model was able to find patterns in the data very efficiently. Validation loss followed the same trend and thus the model can be said to generalize well to the new samples. The steady decrease of the validation loss means that the model's predictive performance on new data kept getting better as the training went on. The fact that the gap between training and validation loss is very small is an indication that the model has not overfitted, as the performance on both sets is still very close. Such a convergence is a sign that the model reached a stable state from which it can be expected that further training will give only very small improvements

Figure 6

KNN – Loss Curve



.

Figure 7

XGBoost – Loss Curve

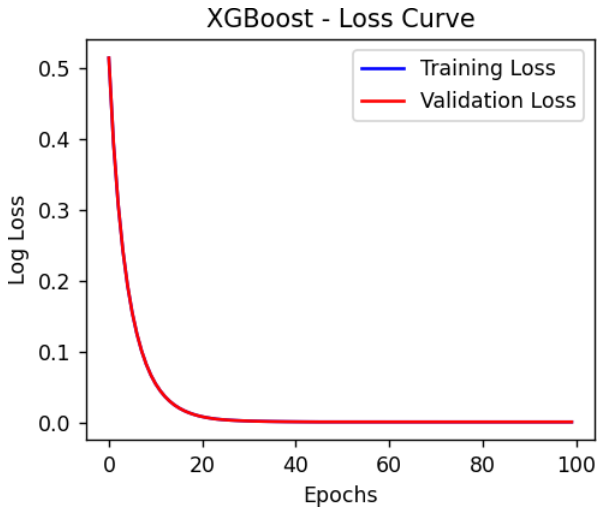
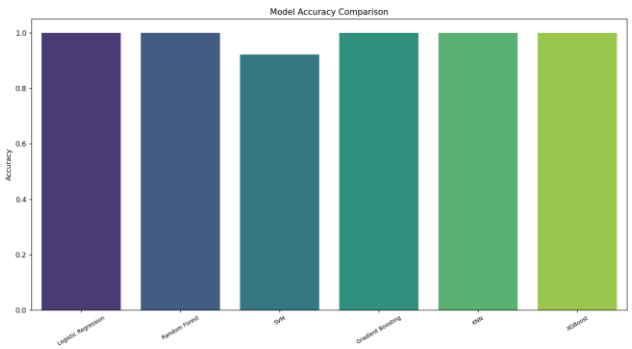


Figure 8 presents a comparative analysis of classification accuracy across six ML models: LR, RF, SVM, GB, KNN, and XGB. The Y-axis quantifies classification accuracy, ranging from 0.0 to 1.0, where 1.0 denotes perfect classification. The X-axis enumerates the respective models.

Figure 8

Model Accuracy Comparision



Observed Performance Trends:

Five models, namely LR, RF, GB, and KNN, demonstrated high classification accuracy, close to or scoring 1.0. This indicates that these models have a strong ability to identify patterns in the dataset.

SVM Performance Deviation:

The SVM model showed a fairly less accurate performance as compared to the other models mentioned above. Although SVM results still point to a decent performance, the difference highlights that the model might have struggled to understand and represent the real distribution of the data in the dataset.

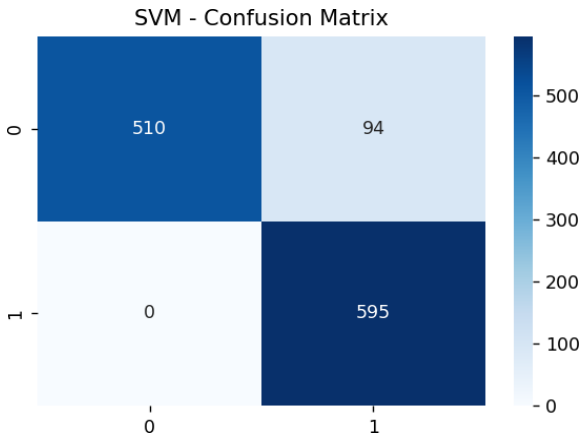
XGBoost Accuracy Anomaly:

A significant difference was noted in the XGB model only that it brought about an accuracy score of 0.492. This result is in conflict with the model's normal performance pattern and thus, it requires further probing to figure out the reasons that are causing it. Possible reasons for this abnormality could be an error in the way the model was implemented, an inconsistency in the data preprocessing, a poor choice of hyperparameters, or even leakage of data, but not necessarily limited to these factors. The next investigation will be directed towards discovering and fixing these possible problems so that the performance evaluation can be accurate and reliable."

Figures 9 to 14 are the confusion matrices for six classification models: LR, RF, SVM, GB, KNN, and XGB. To be specific, XGB, RF, and KNN were able to perform flawless classification. The model made a perfect identification of each instance in the test data set. This outstanding result is the proof of XG's competence in capturing the underlying patterns of the data.

Figure 9

SVM – Confusion Matrix



The SVM model incorrectly labelled 94 real transactions as fake ones, thus it seems that the model has a tendency to be biased towards the positive class. Such a difference reveals the necessity of examining the model setup in detail which comprises changing the values of the hyperparameters, choosing the kernel, and also checking if there is any imbalance in the classes. In addition, the true negative rate (specificity) of the SVM model that is around 84.4% is lower than that of the other models, as well as the precision value of the positive class (fraudulent transactions) and the recall value of the negative class (genuine transactions) of this model.

Model performance (100%) reveals the SVM's inability to identify negative examples flowed from these limitations indicate that when considering this classification task, the SVM does not appear to be the ideal candidate of choice.

Figure 10

Logistic Regression – Confusion Matrix

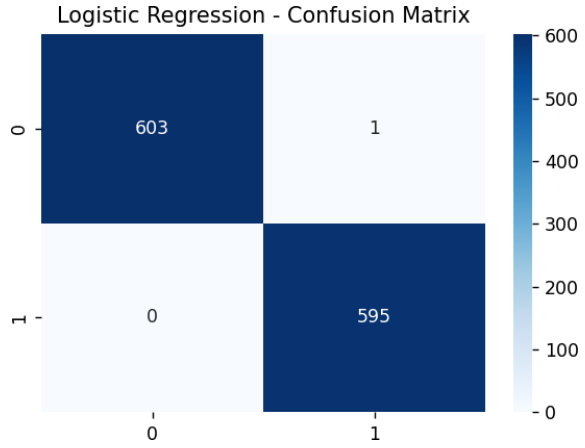
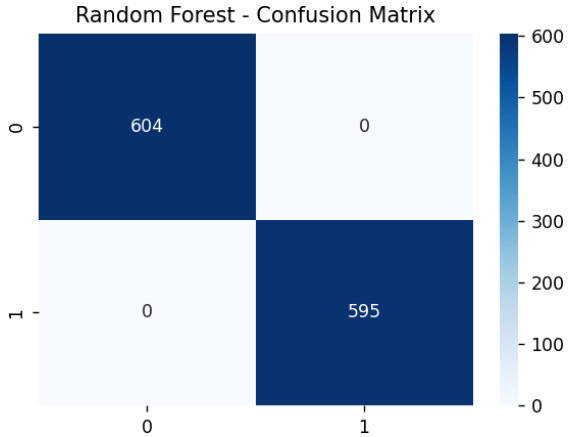


Figure 11

Logistic Regression – Confusion Matrix



The almost perfect performance of RF, KNN, and XGB at the testing phase may suggest that there is an overfitting issue and perhaps some data leakage that causes these models to learn patterns from examples but do not generalize these patterns to new data. To verify the validity of these results, model must use test methods such as k-fold cross-validation and evaluate the performance of the models based on various metrics including accuracy, recall, precision, F1 score, and ROC-AUC. Since the RF, KNN, and XGB models yield almost perfect results, one could conclude that the classification problem is not complicated and that less complex models such as LR would work well; however, the current study is focused on using a more complex method and one that can detect small changes and that is reliable across different situations.

Figure 12

Gradient Boosting – Confusion Matrix

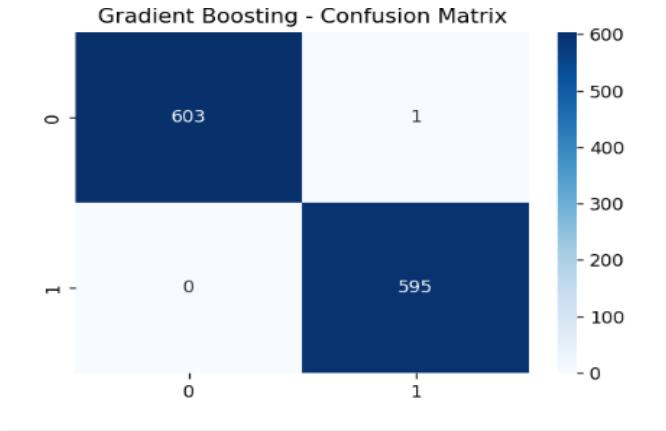
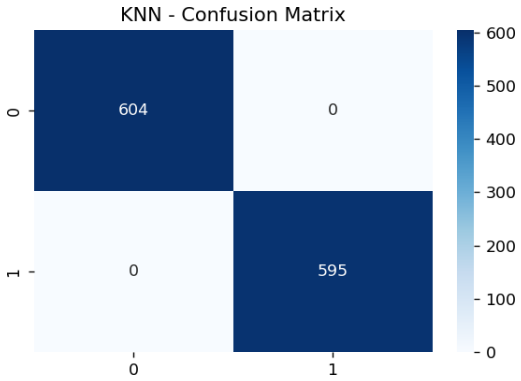


Figure 13.

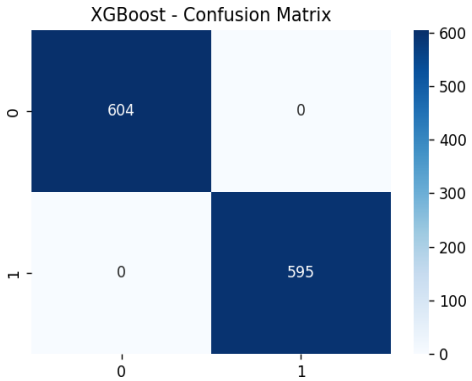
KNN – Confusion Matrix



XGB was used because it is excellent at handling complex relationships and feature interactions, very good at preventing overfitting with efficient regularization techniques and has faster computation speed and scalability with large amounts of data compared to other models such as Random Forest and KNN, which either do not correct errors when making final predictions (Random Forests) or have issues with distance metrics, feature scaling, and irrelevant features (KNN).

Figure 14

XGBoost – Confusion Matrix



In conclusion, XGB provides ideal classification results and has a competitive advantage with its ability to manage complex data, reduce overfitting, and provide an efficient computation time making it the ideal primary model for the current study. The further validation of the model through evaluation can lead to increased confidence in the use of this model for real-world outcomes.

REFERENCES

[1] N. Ahirwar, D. Singh, and K. Maheshwar, "Efficient Credit Card Fraud Detection Based on Multiple ML Algorithms," in *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, Pune, India: IEEE, Apr. 2024, pp. 1–7. doi: 10.1109/I2CT61223.2024.10544195.

[2] Cosma, "DeFraudify4ALL: Prototyping and Validation of a System for Fraud Detection with Big Data and Cloud Technology," in *2024 IEEE 30th International Symposium for Design and Technology in Electronic Packaging (SIITME)*, Sibiu, Romania: IEEE, Oct. 2024,pp. 466–470. doi: 10.1109/SIITME63973.2024.10814887.

[3] H. Rathore and R. Ratnawat, "A Robust and Efficient Machine Learning Approach for Identifying Fraud in Credit Card Transaction," in *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India: IEEE, Sep. 2024, pp. 1486– 1491. doi: 10.1109/ICOSEC61587.2024.10722387.

[4] S. Bonkoungou, N. R. Roy, N. H. A.-E. Ako, and U. Batra, "Credit Card Fraud Detection using ML: A Survey," in *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Bengaluru, India: IEEE, Jan. 2023, pp. 732–738. doi: 10.1109/IITCEE57236.2023.10091035.

[5] M. Devika, S. R. Kishan, L. S. Manohar, and N. Vijaya, "Credit Card Fraud Detection Using Logistic Regression," in 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India: IEEE, Dec. 2022, pp. 1–6. doi: 10.1109/ICATIECE56365.2022.10046976.

[6] B. P. Verma, V. Verma, and A. Badholia, "Hyper-Tuned Ensemble Machine Learning Model for Credit Card Fraud Detection," in *2022 International Conference on Inventive Computation Technologies (ICICT)*, Nepal: IEEE, Jul. 2022, pp. 320–327. doi: 10.1109/ICICT54344.2022.9850940.

[7] S. M. Gopavaram and P. Vinothiyalakshmi, "Cloud Based Credit Card Fraud Detection System in Banking Using Machine Learning and Deep Learning algorithms," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* Delhi, India: IEEE, Jul. 2023, pp. 1–4. doi: 10.1109/ICCCNT56998.2023.10307070.

[8] K. Diwanji, S. Pujari, S. Malegaonkar, S. Shaikh, and Prof. A. Bhosle, "Fraud Detection in Credit Cards System Using ML with AWS Stage Maker," *IJRASET*, vol. 11, no. 3, pp. 2206–2209, Mar. 2023, doi: 10.22214/ijraset.2023.49928.

[9] S. Pujari, K. Diwanji, S. Malegaonkar, S. Shaikh, and Prof. A. Bhosale, "Fraud Detection in Credit Card Automated System using ML with AWS SageMaker," *IJRASET*, vol. 11, no. 5, pp. 1867–1873, May 2023, doi: 10.22214/ijraset.2023.51920.

[10] S. D. S., S. Kuchanur, S. M. P., S. J. M., and K. C., "Credit Card Fraud Detection," *International Journal of Innovative Science and Research Technology (IJISRT)*, pp. 854–860, Mar. 2024, doi: 10.38124/ijisrt/IJISRT24MAR961.

[11] M. K. Kodimenu1, D. S. S2, and D. T. Katoon3, "Credit Card Fraud Detection Using ML & DL," *IJSREM*, vol. 08, no. 07, pp. 1–11, Jul. 2024, doi: 10.55041/IJSREM36686.

[12] Department of Computer Science & Engineering, Raghu Engineering College, Visakhapatnam, India and V. V. Sagar, "CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING," *IJSREM*, vol. 08, no. 04, pp. 1–5, Apr. 2024, doi: 10.55041/IJSREM32382.

[13] K.Kowsalya, Mrs.Vasumathi, and Dr.S.Selvakani, "CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING ALGORITHMS," *EPRA*, pp. 109–116, Mar. 2024, doi: 10.36713/epra16045.

[14] S. Pujari, K. Diwanji, S. Malegaonkar, S. Shaikh, and Prof. A. Bhosale, "Fraud Detection in Credit Card Automated System using ML with AWS SageMaker," *IJRASET*, vol. 11, no. 5, pp. 1867–1873, May 2023,doi: 10.22214/ijraset.2023.51920.

[15] H. Singh, "Credit Card Fraud Detection," *IJRASET*, vol. 12, no. 5, pp. 2238–2244, May 2024, doi: 10.22214/ijraset.2024.62049.

[16] P. Kadam, R. S. Chiparikar, M. A. Kamble, and M. H. Attarde, "Machine Learning Approaches to Credit Card Fraud Detection," *IJRASET*, vol. 12, no. 4, pp. 2802–2807, Apr. 2024, doi: 10.22214/ijraset.2024.60531.

[17] N. J. Nishi, F. Akter Sunny, and S. C. Bakchy, "Fraud Detection of Credit Card using Data Mining Techniques," in *2022 4th International Conference on Sustainable Technologies for Industry 4.0 (STI)*, Dhaka, Bangladesh: IEEE, Dec. 2022, pp. 1–6. doi: 10.1109/STI56238.2022.10103292.

[18] Aditi, A. Dubey, A. Mathur, and P. Garg, "Credit Card Fraud Detection Using Advanced Machine Learning Techniques," in *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, Sonepat, India: IEEE, Jul. 2022, pp. 56–60. doi: 10.1109/CCiCT56684.2022.00022.

[19] Yu, Y. Xu, J. Cao, Y. Zhang, Y. Jin, and M. Zhu, "Credit Card Fraud Detection Using Advanced Transformer Model," in *2024 IEEEInternational Conference on Metaverse Computing, Networking, and Applications (MetaCom)*, Hong Kong, China: IEEE, Aug. 2024, pp. 343–350. doi: 10.1109/MetaCom62920.2024.00064.

[20] H. Feng, "Ensemble Learning in Credit Card Fraud Detection Using Boosting Methods," in *2021 2nd International Conference on Computing and Data Science (CDS)*, Stanford, CA, USA: IEEE, Jan. 2021, pp. 7–11. doi: 10.1109/CDS52072.2021.00009.

[21] Y. Du, "Creating a credit card anti-fraud prediction model using TensorFlow and Machine Learning," in *2022 International Conference on Machine Learning and Intelligent Systems Engineering (MLISE)*, Guangzhou, China: IEEE, Aug. 2022, pp. 334–338. doi: 10.1109/MLISE57402.2022.00073.

[22] N. Ahmed and R. Saini, "Detection of Credit Card Fraudulent Transactions Utilizing Machine Learning Algorithms," in *2023 2nd International Conference for Innovation in Technology (INOCON)*, Bangalore, India: IEEE, Mar. 2023, pp. 1–5. doi: 10.1109/INOCON57975.2023.10101137.

[23] K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[24] P. Chatsuriyawong, S. Toomsawasdi, P. Palangsantikul, and W. Premchaiswadi, "Analyze Credit Card Usage Behavior and Fraud Prevention by Process Mining," in *2022 20th International Conference on ICT and Knowledge Engineering (ICT&KE)*, Bangkok, Thailand: IEEE, Nov. 2022, pp. 1–6. doi: 10.1109/ICTKE55848.2022.9983387.

[25] P. Patil, "Card Defender - Credit Card Fraud Detection System," *IJRASET*, vol. 11, no. 5, pp. 4775–4780, May 2023, doi: 10.22214/ijraset.2023.52748.