

COPY RIGHT



ELSEVIER

SSRN

2024 IJIEMR. Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 15th Dec 2023. Link

[:http://www.ijiemr.org/downloads.php?vol=Volume-13&issue=Issue4](http://www.ijiemr.org/downloads.php?vol=Volume-13&issue=Issue4)

10.48047/IJIEMR/V13/ISSUE 04/18

TITLE: A DEEP LEARNING ENSEMBLE WITH DATA RESAMPLING FOR CREDIT CARD FRAUD DETECTION

Volume 13, ISSUE 04, Pages: 137-150

Paper Authors Dr Medidia Jayapal, Yerragudi Sai Bharath Reddy, Kothapalli Churnika Priya, Madireddy Harsha Vardhan Reddy, Khethavath Sai Prashanth



USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per **UGC Guidelines** We Are Providing A Electronic Bar Code

A DEEP LEARNING ENSEMBLE WITH DATA RESAMPLING FOR CREDIT CARD FRAUD DETECTION

Dr Medidia Jayapal, Yerragudi Sai Bharath Reddy, Kothapalli Churnika Priya, Madireddy Harsha Vardhan Reddy, Khethavath Sai Prashanth

Assistant Professor, Department of CSE, GITAM University (Deemed to be University), Telangana, India.
jayapalmedida@gmail.com

Department of CSE, GITAM University (Deemed to be University), Telangana, India. y.s.bharathreddy@gmail.com

Department of CSE, GITAM University (Deemed to be University), Telangana, India.
churnikapriyakothapalli@gmail.com

Department of CSE, GITAM University (Deemed to be University) Telangana, India.
harshamadireddy7@gmail.com

Department of CSE, GITAM University (Deemed to be University), Telangana, India.
rathodprashanth18@gmail.com

Abstract: Credit cards are crucial in the digital economy. Credit card fraud is rising due to their use. ML detects credit card fraud. Credit card models are complicated by controversy and shifting user behavior. Our study reveals that deep learning is strong. LSTM and GRU neural networks were base learners while MLP was meta learner in the combined research. SMOTE-ENN balances dataset classes. The deep learning method was tested using SMOTE-ENN with a sensitivity of 1.000 and a specificity of 0.997. This outperforms other machine learning models and methods in the literature. We then introduce various integration methods, such as sharding and voting, and test them on the original data and SMOTE-ENN. The Flask system used with SQLite also allows users to register, log in, and test, increasing project efficiency and user engagement.

Index terms - Credit card, deep learning, ensemble learning, fraud detection, machine learning, neural network.

1. INTRODUCTION

Electronic business (e-commerce) solutions are popular because information technology affects financial transactions. The COVID-19 epidemic has emphasized the digital world and boosted e-commerce [1, 2]. Online commerce is plagued by credit card fraud [3]. Credit card fraud has grown, causing banks problems[4]. Credit card fraud rises with internet buying. To maximize profits, banks require credit card fraud detection (CCFD).

Artificial intelligence and machine learning may boost financial institution efficiency, cost, and client satisfaction[5]. Many machine learning approaches detect credit cards. Malik et al. [6] examined the

CCFD hybrid model. Make a hybrid model using XGBoost, Random Forest, AdaBoost, and LGBM. Our experiments suggest that the AdaBoost-LGBM model performs well. Alfaiz and Fati [7] examined credit card detection using machine learning and profile resampling. This research uses Naive Bayes, LGBM, XGBoost, Random Forest, CatBoost, and Logistic Regression. The k-nearest neighbor undersampling CatBoost algorithm works best.

For some reasons, machine learning based on the CCFD model is still unreliable. First of all, for quality products, only variable data such as currency, country and product are taken into account. They do not review customer orders, which could reveal patterns of fraud [8, 9]. Second, the theft of credit card information is suspicious because the number of real transactions exceeds the number of fraudulent transactions [10]. Unequal distribution occurs when the data of classes are not equal in prediction models [11].

Subsets form a smaller portion of the data set than clusters. Most machine learning methods assume that classes are evenly distributed, resulting in unequal distributions. Incorrect information (such as credit card information settings) can create misclassification patterns, especially in some criminal cases. Patterns of exposure to ethnic minorities are important for employment inequality [12]. Deep learning (DL) and integrated learning dominate machine learning (ML) [13], [14], [15], [16]. They are good at anticipating difficult situations and can assist with credit card searches. Deep learning uses multilayer neural networks [17]. Recurrent neural network (RNN) deep learning models have been used to solve machine

learning problems based on network models [18, 19, 20]. Shen et al. RNN models outperform ML models. [21]. Simple RNN-based models commonly have the gradient vanishing issue, which prohibits the RNN from conveying gradient information to neighboring sensors [22]. In sequential task classification, LSTM and GRU-based RNNs perform well and have been suggested to tackle the incomplete issue [8, 23, 24].

LITERATURE SURVEY

Various studies have shown the use of deep neural networks (DNN) in credit card fraud. Different network topologies or learning models have been used to improve content prediction and eliminate bias [1]. Using predictive values to measure uncertainty can reduce model bias and help developers develop reliable systems that do not make wrong decisions when confidence is low. In the real world of card fraud, DNN prediction is inaccurate because (a) fraudsters change their strategies all the time, so DNN finds observations that differ from the normal distribution, and (b) experts need to examine various changes. The new state of the DNN needs to be maintained, which takes time [8, 23, 24]. Therefore, this article introduces Monte Carlo loss, joint Monte Carlo loss and joint Monte Carlo uncertainty (UQ). These can detect card fraud on business profiles. These predictions were measured by the uncertainty of UQ and other performance measures. Tests show that aggregated data can better predict errors. We also show that the University of Queensland's scheme improves fraud prevention by adding more information to make predictions.

Credit card fraud has become increasingly common as a result of new technologies and communications, such as wireless payments. We analyzed the latest research on researching and forecasting the credit card market from 2015 to 2021. After reviewing 40 relevant projects, they were classified as machine learning (modeling, deep learning, problem solving, etc.) and details. There is currently little research on deep learning. This means that more research is needed to use big data analytics, big machine learning [13], [14], [15] and cloud computing to improve credit cards. Our study addresses current research questions and suggests future research directions. Researchers and businesses can use it to identify financial fraud processes and develop effective solutions.

Due to the popularity of e-commerce, theft has become one of the biggest problems. [3] Fraud harms e-commerce website rankings and results in poor business performance. Detecting e-commerce fraud is very important in real life. This job is difficult because scammers are trying to deceive you. Because e-commerce fraud devices use known scams to detect other vulnerabilities, they quickly become ineffective and cannot keep up with new scams. We propose a fraud detection system (eFraudCom) based on a competitive graph neural network (CGNN) for a large online shopping site "Taobao". The eFraudCom system's Competitive Graph Neural Network (CGNN) can directly classify user activities by modeling the classification of malicious and fraudulent behavior. Weak monitoring of certain routines can help CGNNs establish stable patterns of behavior rather than fraud [31,32]. (3) Sharing information can help CGNN distinguish good

behavior from fraud, making it more efficient. eFraudCom is a versatile experiment. The deep CGNN scheme outperforms other models in detecting fraud on Taobao and two public certificates. Taobao's case study shows that CGNN was still active when the scam was updated.

Misinformation is a major issue when developing credit card fraud (CCF) detection software. We evaluate novel machine learning (ML) and deep learning (DRL) algorithms for CCF's fraud and anti-fraud detection. Resampling the skewed CCF dataset using SMOTE and ADASYN. [4] This data equation was used to create the CCF detection ML tool. DRL then creates an unbiased CCF data call. Evaluate the performance of ML and DRL models using different metrics. Based on the actual experiment, we use the iterative method and DRL model to determine the most stable ML model to find the CCF. SMOTE and ADASYN compare CCF data before training/testing respectively. The accuracy of the ML model reaches 99%, which is a very good figure. This ML model [4] performed poorly when simulating the CCF dataset, especially logistic regression, achieving an accuracy of 1.81% and an F1 score of 3.55% when ADASYN was applied. Our research shows that the DRL method is only 34.8% effective.

As time went on, these crimes became increasingly serious, causing financial institutions to lose business. Various single and combined machine learning algorithms have been used to identify credit cards. These methods are limited because they do not consider other combinations for the same data set. According to this study [6], seven hybrid machine learning models can detect fraud using real-world

data. The new hybrid model consists of two parts. First, advanced machine learning algorithms detect credit card theft. The best algorithm from the first part is used to create the hybrid approach. Our data shows that Adaboost + LGBM works best. Future credit card research should examine hybrid systems and methods.

2. METHODOLOGY

i) Proposed Work:

This solution leverages a deep team to improve credit card search. Stacked integration uses LSTM and GRU neural networks as base learners. Everything is learned from MLP. This solution changes the gap between purchasing behavior and credit card fraud across all categories. The system uses the difference between minority and neighbor (SMOTE-ENN) to distribute cells evenly. Testing showed that this method is more sensitive and accurate than other machine learning methods; This makes it the best choice for instant fraud detection. Compare this to models such as AdaBoost, Random Forest, MLP, LSTM, and GRU [8, 23, 24]. We then use a variety of methods such as Random Forests and MLPs combined with individual objects, as well as AdaBoost and Random Voters combining Random Forests. Both the original dataset and the SMOTE-ENN enhanced dataset were used to test this model. The Flask model is also designed for use with SQLite; This simplifies user registration, login, and testing. This update allows you to try and test different products, add usability tests and interactions, making the project more stable.

ii) System Architecture:

The process begins with collecting information about credit card transactions, including details of legal and criminal activity. There should be a work plan that includes cleaning the data, removing missing codes, modifying the data to ensure it is good. A profile selection procedure was used to extract different groups. This may mean using limited classes (financial fraud) and possibly undersampling most classes using methods such as SMOTE-ENN [27], [28], [29], or dummy models can be created to illustrate additional processes. Specific options are used to find the functions or features that are most useful in detecting fraud. This reduces the number of dimensions and focuses on the profile features that are most useful in exporting. ML and DL algorithms use certain options as input. The model uses prior and selective data to show how to distinguish truth from deception. There are evaluation steps in the system to check how well the learning algorithm works. Different validation models are often used to test the model's ability to adapt to new situations. Some of the metrics used to determine model success include recall, sensitivity, specificity, F1 score, ROC curve, AUC, and accuracy. This test is done to understand the functioning of the system and to prevent fraud and scams. The system uses this analysis to determine whether the new credit card is real or possibly fake.

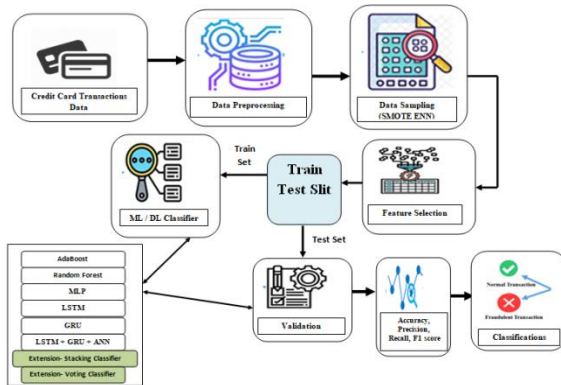


Fig 1 System Architecture

iii) Dataset collection:

We use the Kaggle dataset and data support method to solve the problem of using cards to steal data. We also use data analytics and social analytics to better understand the data. This process helps discover anomalies, data patterns, and connections between events, making data processing and design easier. Kaggle's credit card fraud detection dataset is used to train machine learning [17]. Initially, the configuration file contains different properties related to "Value", "Time" and change from "V1" to "V28". Information regarding previous studies is kept confidential in order to protect personal information.

V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	...	V28	V
-0.611712	-0.769705	-0.149759	-0.224877	2.028577	-2.019887	0.292491	-0.523020	0.356468	0.070050	...	0.380739	0.0234
-0.814682	1.319219	1.329415	0.027273	-0.284871	-0.653985	0.321552	0.455875	-0.704298	-0.600684	...	0.090680	0.4011
-0.318193	1.118618	0.969884	-0.127052	0.569563	-0.532484	0.706252	-0.064986	-0.463271	-0.528357	...	-0.123884	-0.4956
-1.328271	1.018378	1.775426	-1.574193	-0.117866	-0.457733	0.681867	-0.031641	0.383872	0.334853	...	-0.229197	0.0099
1.276712	0.617120	-0.578014	0.879173	0.061706	-1.472002	0.373682	-0.287204	-0.084482	-0.696578	...	-0.076738	0.2587

† 32 columns

Fig 2 Dataset

iv) Data Processing:

Data processing is the process of converting redundant data into information that businesses can use. Generally speaking, data scientists work with data; This means they collect data, organize it, clean it, analyze it, analyze it, and place it into a readable document, such as an image or text. There are three ways to process information: manual, mechanical or electronic. The goal is to make the experience better and the decision easier. This helps companies run their business better and make informed decisions faster. This is largely done through the use of information processing tools such as computers. It can help transform big data and other types of big data into useful information for decision making and quality control.

v) Feature selection:

Custom selection is the process of selecting the most reliable, effective and unobtrusive design elements. As the number and type of data increases, it is important to reduce the data size as planned. One of the main goals of feature selection is to make the prediction model work better and use less power.

One of the most important aspects of architecture is feature selection, which is the process of selecting the most important features that will feed a machine learning algorithm. Feature selection removes redundant or useless features and preserves only the most important features for machine learning models. This reduces the number of input devices. If you choose which features are most important first instead of letting the machine learning model do this, the main results are as follows.

vi) Algorithms:

AdaBoost, also known as Adaptive Boosting, is a machine learning method that improves the accuracy of classification by mixing several simple models. It starts with a simple model, like a one-level decision tree, and trains new models over and over again, giving more weight to the data points that the old models got wrong. By putting these models together, AdaBoost makes a strong group that can make accurate predictions. This makes it useful for your project because it can improve credit card fraud detection by learning from past models' mistakes and making the whole thing run better [36].

```
from sklearn.ensemble import AdaBoostClassifier

# instantiate the model
ada = AdaBoostClassifier(n_estimators=100, random_state=0)

ada.fit(X_train, y_train)

y_pred = ada.predict(X_test)
```

Fig 3 Adaboost

Random Forest is a type of ensemble learning that uses more than one decision tree to make predictions. It works by teaching a group of decision trees on random parts of the data and then taking the average of what they said. This ensemble method improves accuracy, lowers overfitting, and gives stable results for both regression and classification tasks.

```
from sklearn.ensemble import RandomForestClassifier

# instantiate the model
forest = RandomForestClassifier(max_depth=2, random_state=0)

forest.fit(X_train, y_train)

y_pred = forest.predict(X_test)
```

Fig 4 Random forest

A false neural network called **Multilayer Perceptron (MLP)** is used in this project to find credit card scams. Multiple levels of neurons that are linked to each other process information and learn complicated patterns. The MLP changes its internal settings to reduce forecast mistakes while it is being trained. The MLP can change to different situations and find non-linear connections in data. This makes it a useful tool for finding fake credit card transactions.

```
from sklearn.neural_network import MLPClassifier

# instantiate the model
mlp = MLPClassifier(random_state=1, max_iter=30)

mlp.fit(X_train, y_train)

y_pred = mlp.predict(X_test)
```

Fig 5 MLP

The goal of **LSTMs** is to get around the problems that regular RNNs have when dealing with sequential data. Because they can learn and remember long strings of information, they are good at many things, such as natural language processing, speech recognition, time series analysis, and more. [9] It is possible for LSTMs to describe complex relationships and patterns in sequential data well because they use a system of cells, gates, and states to store and send information over time.

```
inputs1=Input((1,11))
att_in=LSTM(50,return_sequences=True,dropout=0.3,recurrent_dropout=0.2)(inputs1)
att_in_1=LSTM(50,return_sequences=True,dropout=0.3,recurrent_dropout=0.2)(att_in)
att_out=attention()(att_in_1)
outputs1=Dense(1,activation='sigmoid',trainable=True)(att_out)
model1=Model(inputs1,outputs1)
```

Fig 6 LSTN

The **Stacking Classifier** is a machine learning method that takes the best features of several base classifiers and combines them to make a stronger and more accurate model. Random Forest and Multilayer Perceptron (MLP) are the two main classifiers used in the Stacking Classifier system in the code you gave me. This is what the Light Gradient Boosting Machine (LGBM) algorithm says will happen. The Stacking Classifier tries to make predictions better by using the different powers of these classifiers. The information from different base models can be combined in this ensemble method, which can be useful for dealing with large datasets and difficult classification problems.

```
estimators = [('rf', RandomForestClassifier(n_estimators=10)),('mlp', MLPClassifier(random_state=1, ma
clf1 = StackingClassifier(estimators=estimators, final_estimator=LGBMClassifier(n_estimators=10))

clf1.fit(X_train,y_train)

y_pred = clf1.predict(X_test)
```

Fig 7 Stacking classifier

A recurrent neural network (RNN) design called the **Gated Recurrent Unit (GRU)** is very good at handling sequential data. The Long Short-Term Memory (LSTM) type is similar to this one, but this one is made to work faster. [8] The best thing about GRU is that it can find relationships and patterns in sequences while using less computing power. It does this with the help of a blocking system that controls the flow of data, letting it keep important features and get rid of less important ones. GRU is used a lot in areas where it's important to work with sequential

data, like natural language processing, time series analysis, and speech recognition. It's often used for machine learning jobs because it's easy to use and works well.

```
inputs1=Input((1,11))
att_in=GRU(50,return_sequences=True,dropout=0.3,recurrent_dropout=0.2)(inputs1)
att_in_1=GRU(50,return_sequences=True,dropout=0.3,recurrent_dropout=0.2)(att_in)
att_out=attention()(att_in_1)
outputs1=Dense(1,activation='sigmoid',trainable=True)(att_out)
model1=Model(inputs1,outputs1)
```

Fig 8 GRU

This project combines long-term memory (LSTM), gated recurrent unit (GRU), and artificial neural network (ANN) multilayer perceptron (MLP) into a powerful integrated model. LSTM and GRU are two types of convolutional neural networks (RNNs) that are very good at understanding sequences and how they are connected to each other. LSTM is especially good at long-term connections, while GRU is good at increasing computational speed [8, 23, 24]. Adding MLP as a meta learner makes it easier for teams to find complex topics in credit card data. This combination is known for its ability to capture both short-term and long-term relationships, making fraud in the workplace increasingly profitable.

```
inputs1=Input((1,11))
att_in=LSTM(50,return_sequences=True,dropout=0.3,recurrent_dropout=0.2)(inputs1)
att_in_1=GRU(50,return_sequences=True,dropout=0.3,recurrent_dropout=0.2)(att_in)
att_out=attention()(att_in_1)
outputs = Dense(8, activation='relu')(att_out)
outputs = Dense(6, activation='relu')(att_out)
outputs1=Dense(1,activation='sigmoid',trainable=True)(att_out)
model1=Model(inputs1,outputs1)
```

Fig 9 LSTM + GRU + ANN

In machine learning, the Soft Voting Classifier method is a part of ensemble learning. In this method, the results from several separate algorithms are put together to make a single forecast. It doesn't give each classifier the same amount of weight; instead, it looks at the chance values that each classifier gave

for each class. The program then adds up these estimates of the odds, giving more weight to the models that are more sure of their results. This leads to a final prediction that is more detailed and correct. When looking for credit card fraud, using a Soft Voting Classifier with different base classifiers, such as AdaBoost and Random Forest, can make the system work better by using the best parts of each model.

```
eclf2 = VotingClassifier(estimators=[('ad', clf1), ('rf', clf2)], voting='soft')
eclf2.fit(X_train, y_train)
y_pred = eclf2.predict(X_test)
```

Fig 10 Voting classifier

3. EXPERIMENTAL RESULTS

Precision: Precision is the percentage of correctly classified cases or samples compared to those that were correctly classified as hits. So, here is the method to figure out the precision:

$$\text{Precision} = \frac{\text{True positives}}{\text{True positives} + \text{False positives}} = \frac{TP}{TP + FP}$$

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

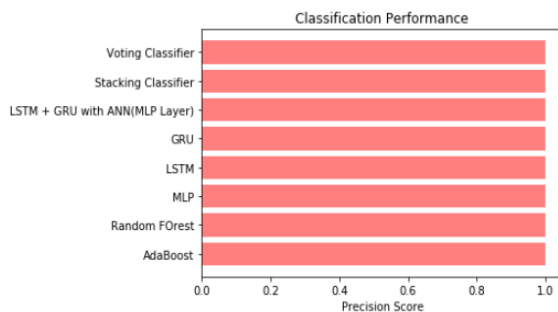


Fig 11 Precision comparison graph

Recall: In machine learning, recall is a parameter that shows how well a model can find all the important cases of a certain class. It indicates the model's ability to capture a particular class of events. It is calculated by dividing the number of correct predictions by the total number of positive predictions.

$$\text{Recall} = \frac{TP}{TP + FN}$$

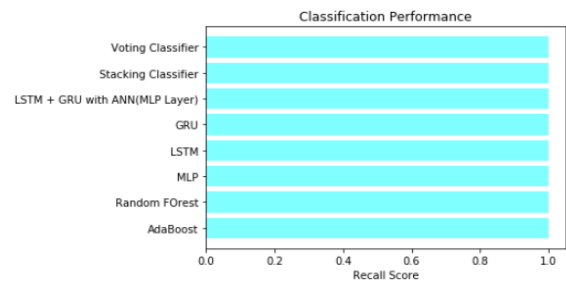


Fig 12 Recall comparison graph

Accuracy: Accuracy is the percentage of right guesses in a classification job. It shows how accurate a model's forecasts are generally.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN}$$

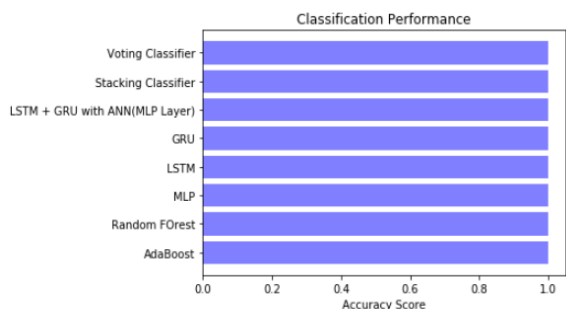


Fig 13 Accuracy graph

F1 Score: F1 score is a compromise between accuracy and return. This is a fair measure that takes both positive and negative into account, so it can be used with inconsistent data.

$$F1\ Score = 2 * \frac{Recall \times Precision}{Recall + Precision} * 100$$

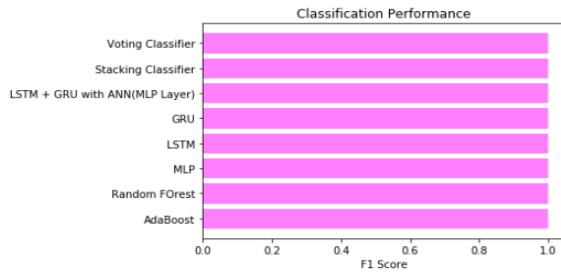


Fig 14 F1Score

	ML Model	Accuracy	Precision	Recall	F1-Score
0	AdaBoost	0.999	0.999	0.999	0.999
1	Random Forest	0.999	0.999	0.999	0.999
2	MLP	0.999	0.999	0.999	0.999
3	LSTM	0.998	1.000	0.998	0.999
4	GRU	0.998	1.000	0.998	0.999
5	LSTM + GRU with ANN(MLP Layer)	0.998	1.000	0.998	0.999
6	Extension- Stacking Classifier	1.000	0.999	0.999	0.999
7	Extension- Voting Classifier	1.000	1.000	1.000	1.000

Fig 11 Performance Evaluation original dataset

	ML Model	Accuracy	Precision	Recall	F1-Score
0	AdaBoost	0.952	0.953	0.952	0.952
1	Random Forest	0.931	0.938	0.931	0.931
2	MLP	0.999	0.999	0.999	0.999
3	LSTM	0.499	1.000	0.499	0.666
4	GRU	0.499	1.000	0.499	0.666
5	LSTM + GRU with ANN(MLP Layer)	0.499	1.000	0.499	0.666
6	Extension- Stacking Classifier	1.000	1.000	1.000	1.000
7	Extension- Voting Classifier	1.000	1.000	1.000	1.000

Fig 12 Performance Evaluation SMOTE-ENN dataset

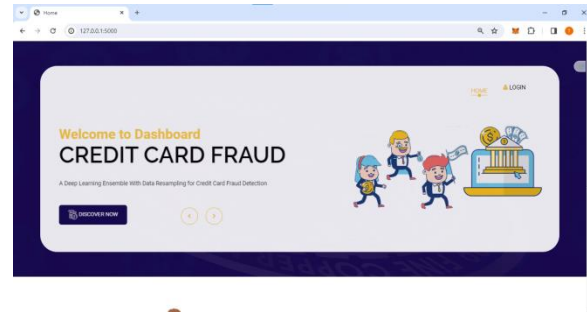


Fig 13 Home page

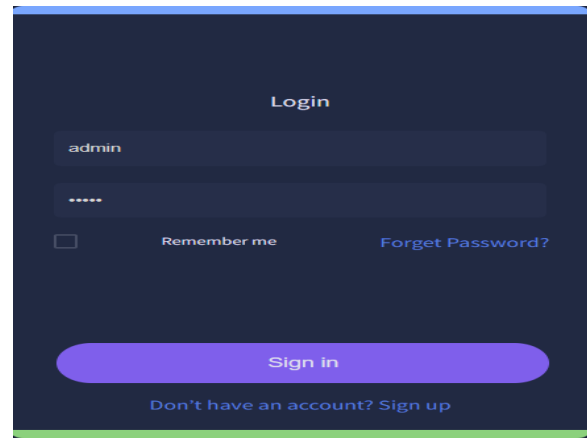


Fig 14 Login page

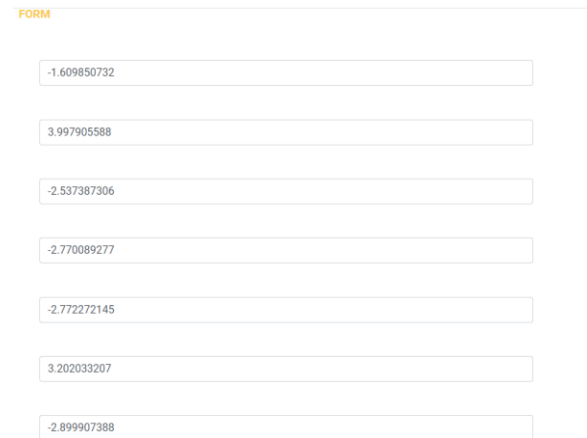


Fig 15 User input



Fraudlent Transaction Happened based on the ML for the Given Input!

Fig 16 Predict result for given input

4. CONCLUSION

The project successfully solves the problem of finding credit card scams in the digital age, which is becoming more and more important as the world's reliance on digital transfers grows. Using different data sampling and scaling methods, the project makes sure that the dataset is in the best possible shape for machine learning models. This shows how important it is to carefully organize data in order to improve model performance. It was shown that different models, such as AdaBoost, Random Forest, MLP, LSTM, GRU, and LSTM + GRU + MLP, work well by building and testing them [8, 23, 24]. As an add-on to the project, voting and stacked classifiers were added. The Voting Classifier performed better than the others, showing better accuracy. The scam detection system became much more accurate and reliable after ensemble methods were added. The project had great results because it encouraged different models to work together. This shows that the field has room for more progress. The project's dedication to accessibility and ease of use is shown by the addition of a user-friendly front-end interface built on the Flask framework and user registration. This method makes sure that the system is useful for users by making it easy for them to enter information and sort fake transactions [10].

5. FUTURE SCOPE

In the future, researchers can look into making models more diverse by mixing LSTM with different predictors, such as random forest, logistic regression, or SVM, to make credit card fraud detection even more accurate [34]. Using feature importance analysis in future research can help figure out the most important factors in finding credit card fraud, which can lead to the creation of better and faster ways to find it. Researchers in the future might look into risk factor analysis to find out what causes credit card scams in the first place. This knowledge can help people come up with better ways to find things. To make the suggested deep learning ensemble approach better, it might be worth looking into different model designs, optimization techniques, and hyperparameter setting methods that make the system work better. The suggested method can be used to find fraud in areas other than credit card fraud, like insurance fraud or online transaction fraud. This makes the proposed method useful for a wider range of fraud prevention options. Also, looking into the development and distribution options for real-time can help find and stop scams right away in banking activities.

REFERENCES

- [1] M. Habibpour, H. Gharoun, M. Mehdipour, A. Tajally, H. Asgharnezhad, A. Shamsi, A. Khosravi, M. Shafie-Khah, S. Nahavandi, and J. P. S. Catalao, "Uncertainty-aware credit card fraud detection using deep learning," 2021, arXiv:2107.13508.
- [2] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud

detection in the era of disruptive technologies: A systematic review,” *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 1, pp. 145–174, Jan. 2023, doi: 10.1016/j.jksuci.2022.11.008.

[3] G. Zhang, Z. Li, J. Huang, J. Wu, C. Zhou, and J. Yang, “eFraudCom: An e-commerce fraud detection system via competitive graph neural networks,” *ACM Trans. Inf. Syst.*, vol. 40, no. 3, pp. 1–27, Mar. 2022, doi: 10.1145/3474379.

[4] T. K. Dang, T. C. Tran, L. M. Tuan, and M. V. Tiep, “Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems,” *Appl. Sci.*, vol. 11, no. 21, p. 10004, Oct. 2021, doi: 10.3390/app112110004.

[5] J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. MuñozRomero, and J.-L. Rojo-Álvarez, “On the black-box challenge for fraud detection using machine learning (I): Linear models and informative feature selection,” *Appl. Sci.*, vol. 12, no. 7, p. 3328, Mar. 2022, doi: 10.3390/app12073328.

[6] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, “Credit card fraud detection using a new hybrid machine learning architecture,” *Mathematics*, vol. 10, no. 9, p. 1480, Apr. 2022, doi: 10.3390/math10091480.

[7] N. S. Alfaiz and S. M. Fati, “Enhanced credit card fraud detection model using machine learning,” *Electronics*, vol. 11, no. 4, p. 662, Feb. 2022, doi: 10.3390/electronics11040662.

[8] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, “Enhanced credit card fraud detection based on attention mechanism and LSTM deep model,” *J. Big Data*, vol. 8, no. 1, p. 151, Dec. 2021, doi: 10.1186/s40537-021-00541-8.

[9] E. Ezenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, “A neural network ensemble with feature engineering for improved credit card fraud detection,” *IEEE Access*, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[10] E. Btoush, X. Zhou, R. Gururaian, K. Chan, and X. Tao, “A survey on credit card fraud detection techniques in banking industry for cyber security,” in *Proc. 8th Int. Conf. Behav. Social Comput. (BESC)*, Oct. 2021, pp. 1–7, doi: 10.1109/BESC53957.2021.9635559.

[11] I. D. Mienye and Y. Sun, “Performance analysis of cost-sensitive learning methods with application to imbalanced medical data,” *Inform. Med. Unlocked*, vol. 25, Jan. 2021, Art. no. 100690, doi: 10.1016/j.imu.2021.100690.

[12] S. A. Ebiaredoh-Mienye, T. G. Swart, E. Ezenogho, and I. D. Mienye, “A machine learning method with filter-based feature selection for improved prediction of chronic kidney disease,” *Bioengineering*, vol. 9, no. 8, p. 350, Jul. 2022, doi: 10.3390/bioengineering9080350.

[13] C. Ho, Z. Zhao, X. F. Chen, J. Sauer, S. A. Saraf, R. Jialdasani, K. Taghipour, A. Sathe, L.-Y. Khor, K.-H. Lim, and W.-Q. Leow, “A promising deep learning-assistive algorithm for

histopathological screening of colorectal cancer,” *Sci. Rep.*, vol. 12, no. 1, pp. 1–9, Feb. 2022, doi: 10.1038/s41598-022-06264-x.

[14] P. Goel, R. Jain, A. Nayyar, S. Singhal, and M. Srivastava, “Sarcasm detection using deep learning and ensemble learning,” *Multimedia Tools Appl.*, vol. 81, no. 30, pp. 43229–43252, Dec. 2022, doi: 10.1007/s11042-022-12930-z.

[15] I. D. Mienye, P. Kenneth Aina, I. D. Emmanuel, and E. Esenogho, “Sparse noise minimization in image classification using genetic algorithm and DenseNet,” in *Proc. Conf. Inf. Commun. Technol. Soc. (ICTAS)*, Mar. 2021, pp. 103–108, doi: 10.1109/ICTAS50802.2021.9395014

[16] R. T. Aruleba, T. A. Adekiya, N. Ayawei, G. Obaido, K. Aruleba, I. D. Mienye, I. Aruleba, and B. Ogbuokiri, “COVID-19 diagnosis: A review of rapid antigen, RT-PCR and artificial intelligence methods,” *Bioengineering*, vol. 9, no. 4, p. 153, Apr. 2022, doi: 10.3390/bioengineering9040153.

[17] G. Nguyen, S. Dlugolinsky, M. Bobák, V. Tran, L. L. García, I. Heredia, P. Malík, and L. Hluchý, “Machine learning and deep learning frameworks and libraries for large-scale data mining: A survey,” *Artif. Intell. Rev.*, vol. 52, no. 1, pp. 77–124, Jun. 2019. [Online]. Available: <http://link.springer.com/10.1007/s10462-018-09679-z>

[18] S. O. Alhumoud and A. A. Al Wazrah, “Arabic sentiment analysis using recurrent neural networks: A review,” *Artif. Intell. Rev.*, vol. 55, no. 1, pp. 707–748, Jan. 2022, doi: 10.1007/s10462-021-09989-9.

[19] Z. Zhong, Y. Gao, Y. Zheng, B. Zheng, and I. Sato, “Real-world video deblurring: A benchmark dataset and an efficient recurrent neural network,” *Int. J. Comput. Vis.*, vol. 131, no. 1, pp. 284–301, Jan. 2023, doi: 10.1007/s11263-022-01705-6.

[20] J. Van Gompel, D. Spina, and C. Develder, “Satellite based fault diagnosis of photovoltaic systems using recurrent neural networks,” *Appl. Energy*, vol. 305, Jan. 2022, Art. no. 117874, doi: 10.1016/j.apenergy.2021.117874.

[21] F. Shen, X. Zhao, G. Kou, and F. E. Alsaadi, “A new deep learning ensemble credit risk evaluation model with an improved synthetic minority oversampling technique,” *Appl. Soft Comput.*, vol. 98, Jan. 2021, Art. no. 106852, doi: 10.1016/j.asoc.2020.106852.

[22] A. Tsantekidis, N. Passalis, and A. Tefas, “Chapter 5—Recurrent neural networks,” in *Deep Learning for Robot Perception and Cognition*, A. Iosifidis and A. Tefas, Eds. New York, NY, USA: Academic, 2022, pp. 101–115, doi: 10.1016/B978-0-32-385787-1.00010-5.

[23] Y. Xie, G. Liu, C. Yan, C. Jiang, M. Zhou, and M. Li, “Learning transactional behavioral representations for credit card fraud detection,” *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Oct. 5, 2022, doi: 10.1109/TNNLS.2022.3208967.

[24] Y.-C. Wei, Y.-X. Lai, and M.-E. Wu, “An evaluation of deep learning models for chargeback fraud detection in online games,” *Cluster Comput.*, vol. 26, pp. 927–943, Jul. 2022, doi: 10.1007/s10586-022-03674-4.

- [25] S. Mishra, K. Shaw, D. Mishra, S. Patil, K. Kotecha, S. Kumar, and S. Bajaj, "Improving the accuracy of ensemble machine learning classification models using a novel bit-fusion algorithm for healthcare AI systems," *Frontiers Public Health*, vol. 10, May 2022, Art. no. 858282. [Online]. Available: <https://www.frontiersin.org/articles/10.3389/fpubh.2022.858282>
- [26] I. D. Mienye, G. Obaido, K. Aruleba, and O. A. Dada, "Enhanced prediction of chronic kidney disease using feature selection and boosted classifiers," in *Intelligent Systems Design and Applications*. Cham, Switzerland: Springer, 2022, pp. 527–537, doi: 10.1007/978-3-030-96308-8_49.
- [27] N. L. Fitriyani, M. Syafrudin, G. Alfian, C.-K. Yang, J. Rhee, and S. M. Ulyah, "Chronic disease prediction model using integration of DBSCAN, SMOTE-ENN, and random forest," in *Proc. ASU Int. Conf. Emerg. Technol. Sustainability Intell. Syst. (ICETISIS)*, Jun. 2022, pp. 289–294, doi: 10.1109/ICETISIS55481.2022.9888806.
- [28] J. Yang and J. Guan, "A heart disease prediction model based on feature optimization and smote-Xgboost algorithm," *Information*, vol. 13, no. 10, p. 475, Oct. 2022, doi: 10.3390/info13100475.
- [29] D. S. Sisodia, N. K. Reddy, and S. Bhandari, "Performance evaluation of class balancing techniques for credit card fraud detection," in *Proc. IEEE Int. Conf. Power, Control, Signals Instrum. Eng. (ICPCSI)*, Sep. 2017, pp. 2747–2752, doi: 10.1109/ICPCSI.2017.8392219.
- [30] H. Guan, Y. Zhang, M. Xian, H. D. Cheng, and X. Tang, "SMOTE-WENN: Solving class imbalance and small sample problems by oversampling and distance scaling," *Int. J. Speech Technol.*, vol. 51, no. 3, pp. 1394–1409, Mar. 2021, doi: 10.1007/s10489-020-01852-8.
- [31] L. Ni, J. Li, H. Xu, X. Wang, and J. Zhang, "Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection," *IEEE Trans. Computat. Social Syst.*, early access, Feb. 13, 2023, doi: 10.1109/TCSS.2023.3242149.
- [32] H. Fanai and H. Abbasimehr, "A novel combined approach based on deep autoencoder and deep classifiers for credit card fraud detection," *Exp. Syst. Appl.*, vol. 217, May 2023, Art. no. 119562, doi: 10.1016/j.eswa.2023.119562.
- [33] F. Itoo, Meenakshi, and S. Singh, "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection," *Int. J. Inf. Technol.*, vol. 13, no. 4, pp. 1503–1511, Aug. 2021, doi: 10.1007/s41870-020-00430-y.
- [34] S. K. Saddam Hussain, E. Sai Charan Reddy, K. G. Akshay, and T. Akanksha, "Fraud detection in credit card transactions using SVM and random forest algorithms," in *Proc. 5th Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Nov. 2021, pp. 1013–1017, doi: 10.1109/I-SMAC52330.2021.9640631.
- [35] I. D. Mienye, Y. Sun, Z. Wang, "Prediction performance of improved decision tree-based



algorithms: A review,” *Proc. Manuf.*, vol. 35, pp. 698–703, Jan. 2019, doi: 10.1016/j.promfg.2019.06.011.

[36] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, “Credit card fraud detection using AdaBoost and majority voting,” *IEEE Access*, vol. 6, pp. 14277–14284, 2018, doi: 10.1109/ACCESS.2018.2806420.

[37] T.-H. Lin and J.-R. Jiang, “Credit card fraud detection with autoencoder and probabilistic random forest,” *Mathematics*, vol. 9, no. 21, p. 2683, Oct. 2021, doi: 10.3390/math9212683.

[38] A. Rb and S. K. Kr, “Credit card fraud detection using artificial neural network,” *Global Transitions Proc.*, vol. 2, no. 1, pp. 35–41, Jun. 2021, doi: 10.1016/j.gltip.2021.01.006.

[39] S. C. Dubey, K. S. Mundhe, and A. A. Kadam, “Credit card fraud detection using artificial neural network and BackPropagation,” in *Proc. 4th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, May 2020, pp. 268–273, doi: 10.1109/ICICCS48265.2020.9120957.

[40] O. N. Akande, S. Misra, H. B. Akande, J. Oluranti, and R. Damasevicius, “A supervised approach to credit card fraud detection using an artificial neural network,” in *Applied Informatics*. Cham, Switzerland: Springer, 2021, pp. 13–25, doi: 10.1007/978-3-030-89654-6_2.