Service based credit card fraud detection using Oracle SOA suite

Shubham Ingole[1 2], Abhishek Kumar[1 3], Debachudamani prusti[1 4] *, Santanu Kumar Rath[1 5]

[1] Department of CSE
[1] National Institute of Technology, Rourkela
[2] 219CS3469@nitrkl.ac.in, [3] 219CS3466@nitrkl.ac.in, [4] debaprusti@gmail.com,[5] skrath@nitrkl.ac.in

*** Corresponding author:**
Debachudamani Prusti
debaprusti@gmail.com
Mobile no. +91 9853636785

Abstract

Credit card fraud detection techniques help to capture fraudulent transactions carried out by illegitimate users and thus prevent any misuse of the credit card. Due to the technological advancement, credit card usage has been on the rise of financial transactions keeping aside the risk of increase in number of fraudulent transactions. Thus, some sort of improved strategies are desired to be implemented in order to curb and avoid such fraudulent transactions. This study intends to propose a fraud detection technique by implementing various machine learning techniques on cloud platform which itself is based on service oriented architecture (SOA). SOA helps to create applications by making use of services available over the network. Further, this credit card fraud detection technique, focuses on orchestration of various services using Oracle SOA suite mingled with different machine learning models such as support vector machine (SVM), isolation forest, random forest regressor, local outlier factor (LOF) and different neural networks such as multilayer perceptron (MLP), autoencoder and convolutional neural network (CNN). The outputs of all the machine learning models are integrated with Oracle SOA suite in order to provide proper agility and efficiency. And this Oracle SOA suite model has been deployed on Google cloud platform (GCP) for providing reliable solution in an online mode. A comparative analysis on performance of different machine learning algorithms has been presented for their critical assessment.

Keywords: SOA, Machine learning algorithms, CNN, Oracle SOA suite, GCP

1. Introduction

Over the last decade the use of electronic money has seen an upsurge and people are preferring using this type of currency instead of carrying hard cash. Credit cards are one of the easier means for carrying out transactions online. But the inflation of credit cards usage has resulted in increase in number of cases of fraudulent trasactions. So it has become a very much necessity for the financial institutions to block such fraudulent transactions [1]. It is observed that financial institutions have to face a good number of challenges as the number of transaction happening everyday are quite large in number. For example, in the month of June 2020 there were about 125 million number of point of sale transactions made by using the credit cards in India (https://www.statista.com/statistics/631396/). As the number of fraudulent transactions are quite less compared to overall transactions, it becomes a quite onerous task to capture such fraudulent transactions in real time.

Credit card fraud detection process can be considered as a two classs classification problem to classify the fraudulent and normal transactions. Where the objective is to classify the transaction into the fradulent one or genuine one. Various techinques have been proposed by several researchers and applicationists to detect such fraudulent trasactions. It has been observed that several machine learning techinques (both spuervised and unsupervised methods) such as SVM, random forest, isolation forest, local outlier factor, autoencoder etc. have been applied to obtain competitive results for prediction of the fraudulent transaction [3, 8, 9].

In this study, both supervised as well as unsupervised learning techniques have been considered for performance comparison and analysis. The methodologies such as Support vector machine (SVM), Multilayer perceptron (MLP), Random forest regressor are considered as supervised learning and methodologies such as Isolation forest (IF), Local outlier factor (LOF), Autoencoder are considered under the unsupervised learning techniques. Convolutional neural network (CNN) is a deep learning technique, which is also considered along with the other two techniques.

Under the supervised technique category, fraudulent transactions are classifed based on the previous data to predit the class label. Based on the prior knowledge about the class label of data samples, supervised learning technique predits the transaction as fraudulent or not. Whereas, when unsupervised learning technique is being considered the transactions are classified based on behavioural fraud. In the absence of any prior knowledge, the behavioural features are extracted to detect a traction as fraudulent or not [18, 19].

The credit card fraud detection system has been proposed by considering it as a service associated with service oriented architecture, consisting of a group of services in a network communicating with each other. A service has characteristics such as: it is self-contained, well defined and provides distinct functionality. A service can be Entity service, Task Service, Utility Service, Proxy Service, Device service, Process service and Business service. To build such a service oriented architecture, Oracle SOA suite has been considered which helps to remodel a complex application integration into an agile and reusable service-based application.

There are various cloud platforms available for users to deliver various computing services. Development in the cloud technology has allowed practitioners to use services provided by this cloud vendors in reliable and real time mode.

2. Related Works

A good number of research works have already been carried out on credit card fraud detection by different researchers as well as applicationist [2, 6-8]. Numerous techinques have been proposed to classify the fraudulent transactions and to achieve the degree of success. Still it is observed that more research need to be carried out to capture fraudulent transactions since the fraudsters adopt various changeable techniques frequently. Previous works have been done on credit card fraud detection using various machine learning techniques. But Instead of proposing fraud detection using some machine learning model, an ensemble of machine learning models can be applied, where decision is taken based on majority voting technique. Improved results have been obtained by different parameter settings for any particular algorithm [21]. Some related works have been considered and their application methodologies are discussed below.

And when it comes to service based applications, one doesn't find much standard work on providing fraud detection as a service based on SOA architecture. Of course, in the literature few research works are available on development of software to detect fraudulent transactions, but still it is observed that more thrust needs to be applied to make the cloud based software, focused on SOA architecture.

Masoumeh Zareapoor et al., have proposed bagging ensemble classifier based on decision tree algorithm which is novel technique in area of credit card fraud detection system [2]. The bagging ensemble classifier based on decision tree works well attributes values which are independent. The ability of this method to handle highly unbalanced data is found to be stable and also it takes very less time.

Kuldeep Randhawa et al., have proposed machine learning algorithms to detect credit card fraud and further AdaBoost and majority voting methods have been applied [7]. The performance measure used is MCC and the best MCC score achieved is 0.823 using majority voting. Noise has also been added to the data samples to check the robustness of the the model and the MCC score achieved after introducing nose is 0.942.

John et al.,   have worked on credit card fraud detection with local outlier factor and isolation forest to classify fraudulent transaction and genuine one [11]. A comparison between these two algorithms has been provided. Local outlier factor provided 97% accuracy and isolation forest provided 76% accuracy while classifying fraudulent and genuine transaction.

Amruta Pawar et al., have proposed a novel outlier detection system to detect credit card fraud detection [5]. Five outlier detection technique: supervised outlier detection, semi-supervised outlier detection, unsupervised outlier detection, neural network based, rule based and clustering based have been proposed. Principal component analysis (PCA) is used to reduce the initial 20 attributes of the dataset and then the proposed outlier detection system has been applied on it.

3. Dataset

The dataset used for this study is that of the European cardholder (https://www.kaggle.com/mlg-ulb/creditcardfraud). The dataset contains transaction made by credit cards over a period of two day in September 2013. The total number of samples in the dataset are 284807. The dataset is highly unbalanced. As the number of fraudulent transaction are very less in number as compared to genuine transaction. The number of genuine transacion counts to 284315. And the number of fraudulent transaction counts to 492 only. The fraudulent transaction accouts for a mere 0.172%.

Due to confedentiality of the data, the original feature and other background information is not provided directly. Instead PCA transformation of the values is provided in numerical form. The dataset contains a total of 30 feature attribute and one classification attribute ‘Class‘. Out of 30 features, 28 features named as V_1, V_2, V_3......V_{28} are numeric values obtained from PCA transformation and remainig two features are *Time* and *Amount*. And the *class* attribute has two possible values such as *0* and *1* for genuine transactions and fraudulent transactions respectively.

3.1 Preprocessing of data

Preprocessing activity is carried out on the dataset to remove redundant features from the dataset. If the dataset is unbalanced that is, it contains large number of samples belonging to one class and very few of other. It needs to be balanced using some resampling techinque.

3.1.1 Redundant Feature

Out of total 30 attributes, attribute ‘Time‘ has very little or no effect on the final result, whether a transaction is fraudulent or not. So ‘Time‘ attribute is dropped from the dataset. Total 29 attributes are being cosidered for classification purpose.

3.1.2 Resampling

Resampling is an efficient methodology for sorting out inconsistencies associated with class-imbalance problems [20]. It is observed that the credit card dataset is a highly imbalanced dataset where there is presence of few fraudulent transactions that occur very rarely; hence it becomes difficult to identify fraudulent data. Only 0.172% of transactions that represent only 492 transactions out of 284807 (approx. Ratio is 1:579) are obeserved to be fraudulent in this dataset as shown in Figure 1. The dataset is resampled to make it a balanced one by increasing the number of fraudulent transaction data. The resampling techinque used is 'sklearn.util.resample' [12]. The number of fraudulent transactions before resampling was 492 and after resampling, it is increased to 20000. The performance parameters are calculated with varying sample sizes (such as 5000 samples, 20000 samples, 60000 samples and so on) of fraudulent transactions. The credit card dataset is oversampled to 20000 to hit the optimal accuracy value, since oversampling helps to change the performance values produced by different classifcation models. But finding the exact sampling rate in advance to hit the optimal rate is an arduous task.

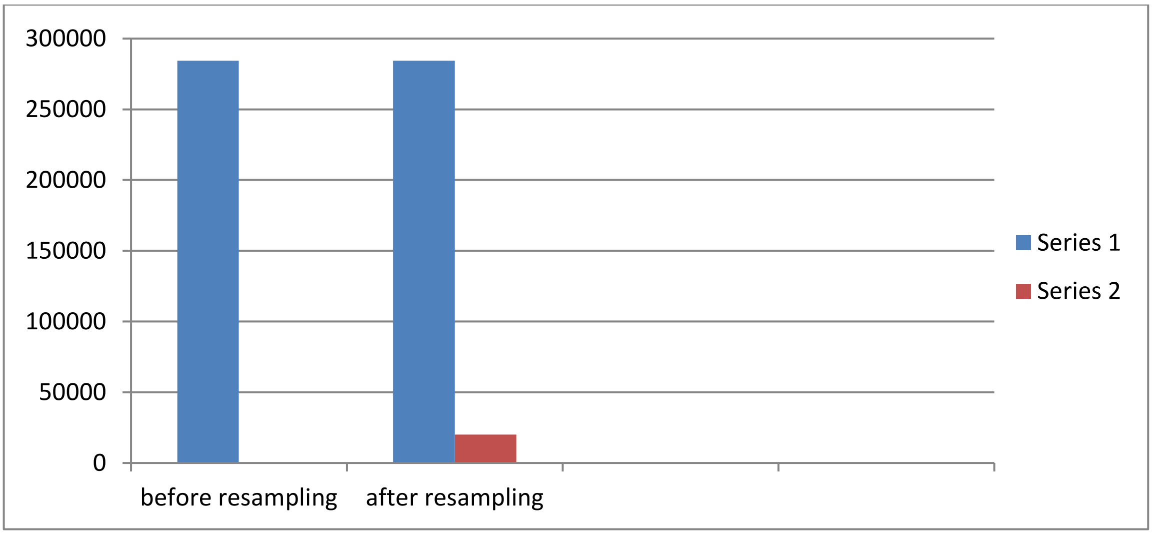


Fig. 1. Dataset before and after resampling

4. Machine learning classification models

Various machine learning algorithms have been considered to carry out the proposed research work and and their conceptual models with explanation have been presented. The details of the model in the following table guarantee the reproducibility of the models. The table also contains the machine learning library used to implement the respective models. Different parameter structures for each specific model have been shown in Table 1.

Table 1. Parameter structures for each specific classification model

Sl. no.	Model	Important Parameter	Library
1	CNN	First three layers are Conv1D (filters = 32, kernel_size = 3, activation = "ReLU"), Maxpool1D (pool size=2) and Dropout (0.2). The same three layers are repeated again with filters =64 for Conv1D and Dropout = 0.2. The next layer is Conv1D followed by "Flatten" layer. Then "Dense" layer is added followed by "Dropout (0.5)" layer and again "Dense" layer (activation = "sigmoid") with 1 output node is added. The model is then compiled (optimizer = "Adam", loss = "binary cross entropy)	Tensorflow
2	Feed forward neural network	Activation = "ReLU", loss= binary cross-entropy hidden layers = 4	Keras.model, keras.layers
3	Autoencoder	Activation = "ReLU", loss= mean squared error	Keras.model, keras.layers
4	SVM	kernel = "RBF"	sklearn
5	Isolation forest	Max_samples=100 , random_state = 42	sklearn.ensemble
6	Random forest regressor	Default values	sklearn.ensemble
7	Local Outlier factor	N neighbors = 2	sklearn.neighbors

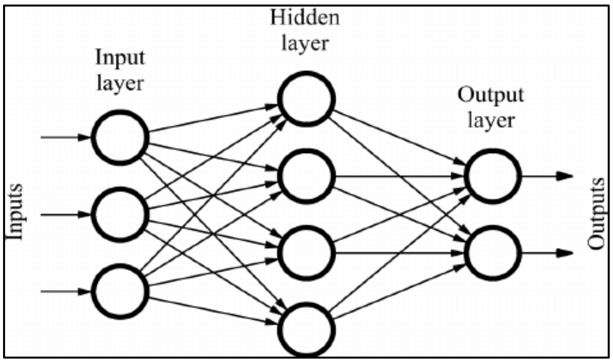
*ReLU (Rectified Linear Unit) is the activation function.

4.1 Feedforward Neural Network

Feedforward Neural Network is a type of neural network were data flows in one direction [14]. It is a supervised learning model. In this type of network, connections between the nodes does form a cycle. A Feedforward neural network has basically three types of layer first one is input layer , one or more hidden layer and one output layer. Each perceptron in one layer is connected to every perceptron on the next layer as shown in the Figure 2. Each perceptron accepts a input and passes through a activation function(relu, tanh, sigmoid). Generally, neural network has six stages of learning. Feeding the values, Forwad propogation, Error Function, Backpropogation, updating weight, convergence.

4.2 Autoencoder

Autoencoder are type of neural network where input and output is same as shown in Figure 3. They reduces the input into lower dimensional code and then remodel the output from this lower state [17].They are mostly use for anomaly detection. Hence fit good for credit card fraud detection. Autoencoder consists of three component :encoder, code and decoder. Here the autoencoder is train with genuine transaction and when fraudulent transaction are feed into the network it fails to regenerate at the output layer.Thus classifying the fraudulent from the genuine transaction.



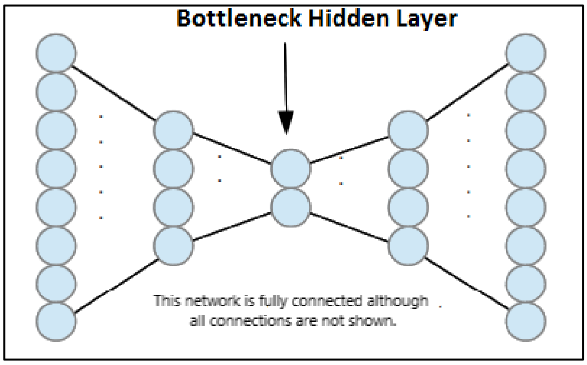

Bottleneck Hidden Layer
This network is fully connected although all connections are not shown.

Fig. 2. Neural network with one hidden layer

Fig. 3. Autoencoder with hidden layer

4.3 Convolutional neural network

A convolutional neural network is applied with an unsupervised model using deep learning algorithm [13]. This network consist of a sequence of layers as shown in Figure 4. The different layers in the CNN model are mentioned in Table 1. There are mainly three types of layers knowns as convolutional layer, pooling layer and fully connected layer. CNN are used for image recognition but applying CNN on credit card data gives good results.

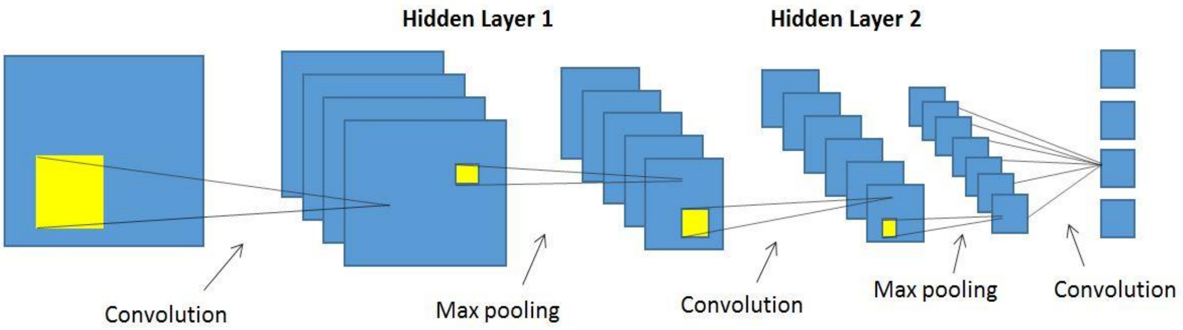


Fig. 4. Convolutional Neural Network with sequence of layers

4.4 Support Vector Machine

Support Vector Machine is supervised learning model which is use for two class classification problem [8]. SVM divides the data into two sets with the help of a hyperplane as shown in Figure 5. This hyperplane is called as decision boundary. But there is a possibility of more than two hyperplane separating the data. Thus hyperplane with maximun margin is choosen. The data is plot in n demensianl space. To work with problems where they cannot be separated linearly, SVM has a method called as kernel trick. SVM kernel function transforms lower dimensional space into higher dimensinal space. It converts non separable problems into linearly separable problems.

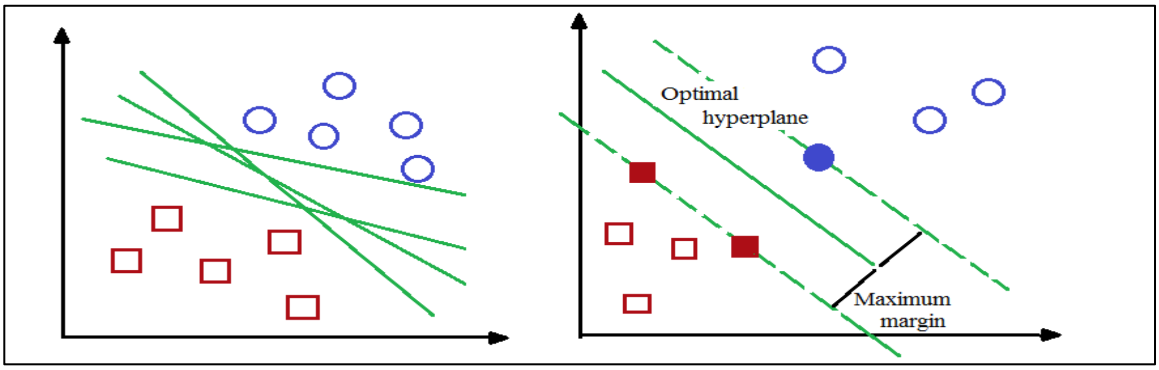


Fig. 5. Support vector machine representation with maximizing the hyperplane

4.5 Random forest regressor

Random Forest Regressor is a supervised learning technique [8]. It uses ensemble learning method for regression. Ensemble learning technique merges predictions from different machine learning algorithms to make more accurate predictions than just using one model. Random Forest Regressor is powerful and accurate model. It works well with many problem. Problems where features have non linear relationship. Random Forest has multiple decision trees as base learning models. We randomly perform row sampling and feature sampling from the dataset forming sample datasets for every model, which is a part of bootstrap methodology mainly used for random sampling with replacement.

4.6 Isolation forest

Isolation forest is alike random forest and is built using decision tree but unlike reandom forest isolation forest identifies anomalies and outliers [3]. It is best suited for anomaly detection. It isolates the outliers by randomly selecting a feature from the given set of features and then randomly selecting a split value between the max and min values of that feature as shown in Figure 6. This random partitioning of features will produce shorter paths in trees for the anomalous data points, thus it helps in distinguishing the data instances from the rest of the available data.

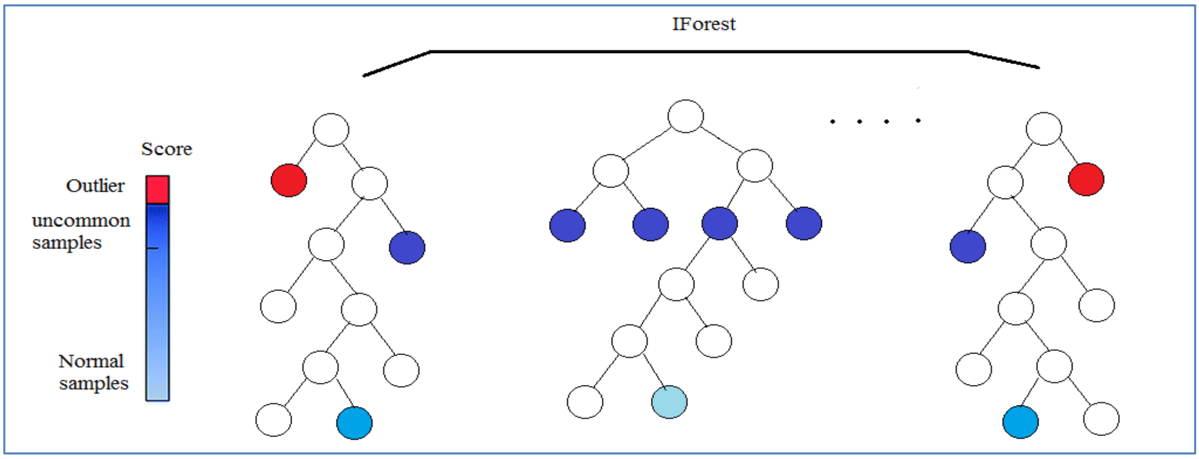


Fig. 6. Isolation forest with min amd max split value of features

4.7 Local outlier factor

Another unsupervised machine learning algorithm is Local outlier factor [3]. In this, each sample has some anomaly score known as local outlier factor. In local outlier factor local deviation is measure with reference to its neighbors. It is based on local density of the samples. The anomaly score of a sample means how isolated that smaple is from its neigbouring sample. Local density of a sample can be measured and compared to local densities of its neighbors and thus is used to identify the data samples with lower density than their neighbors.

5. Service Oriented Architecture

Service Oriented Architecture is basically a collection of services considered for cloud based software development [10, 15]. This services can communicate with each other which involves data passing or it involves two or more servies coordinating some activity. Service Oriented architecture leads to reusability of software components. The services are exposed using protocols such as simple object access protocol (SOAP) or Javascript Object Notation (JSON) / Hypertext Transfer Protocol (HTTP) to send and recieve data. This architecture leads to loose coupling between services. Two of the important roles in service oriented architecture is service provider and service consumer. Service provider maintains the services and make them available to service consumer. Services consumer can use this services. Figure 7 shows the interaction between service consumer and service provider.

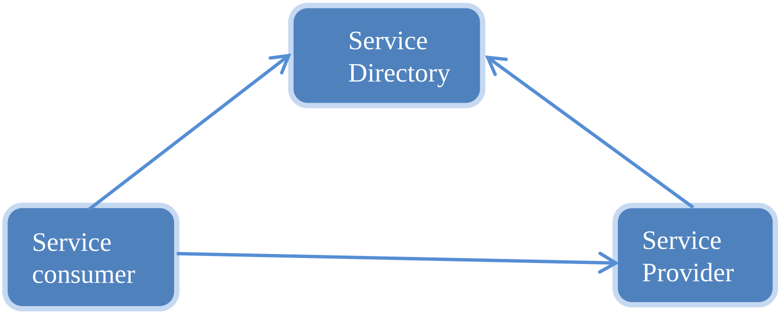


Fig. 7. Interaction between service consumer and service provider

5.1 Oracle SOA Suite

Oracle SOA Suite is a component of the Oracle Fusion Middleware . Oracle SOA Suite is a large, hot-pluggable software suite that allows you tobuild, deploy, and manage combinations using service-oriented architecture. It allows you to modify multiple application compounds into flexible and reusable service-based applications to decrease the time to sell, respond quicker to marketing obligations, and lower costs.

Oracle SOA Suite enables the developers to build the services and manage them. The services can then be applied to the business processes and composite applications. Organizations can easily extend and evolve the architectures with the hot-pluggable components from Oracle SOA Suite. Replacing existing investments would not be required. The product strategy, product details, and customer experience relating to the SOA Suite are shared by Oracle Corporation.

5.2 Business Process Execution Language (BPEL)

BPEL is applied to build service oriented architecutre . It is use to define and execute for business process using web service. BPEL allows allows top-down realization through composition, orchestration and coordination of web services. Orchestration and Choreography is used to combine web services. Orchestration is a more flexible way and has advantages over choreography.

BPEL process defines the order in which services are invoked. That is whether sequentially or parallelly. BPEL provides loops construction, variable declaration, copy and assign variable, defining fault handlers and so on. This helps in defining complex business process. In a given scenario, the BPEL process receives a request. The respective web services are invoked and the responds back to the caller.

6. Proposed Architecture

In this study, an effective architecture has been proposed for credit card fraud detection and is being developed by exposing Respresentational Stats Transfrom (REST) API service. This service oriented architecture is modeled in Oracle SOA suite which provide different functionalities to build such architecture [15]. Oracle BPEL Process Manager provides support for convence in design, deployment, monitoring, and administering processes based on BPEL standards.

Seven classification models (both supervised and unsupervised) have been considered such as SVM, Random Forest Regressor, Isolation Forest, Local outlier factor, Feedforward neural network, Autoencoder and Convolutional neural network as shown in the Figure 8. These models cover both supervised machine learning algorithm as well as unsupervised learning algorithm. The supervised learning algorithm used are SVM, Random Forest regressor, Feedforward neural network and convolution neural network. The unsupervised algorithm used are Isolation forest, Autoencoder and Local outlier factor. These algorithms cater to services for providing classification of transaction into fraudulent and genuine ones.

Invoke service activity is considered in BPEL model for invoking the classifier services. A port is opened by the invoke activity to send and receive data. This port is used to feed required data and receive a response. The responses from all the seven classifier services are used to identify the class that provides majority. The majority class decides the fraudulent or genuine transaction. The data of the transaction is feed through the exposed REST API service.

One of the limitations of using REST API service is that REST services are less secured in comparison with SOAP services. Of course, there is an overhead of validating each and every SOAP message by the SOAP engine that takes longer time. But SOAP based services are more secured since they support message level security. As of now, this study presents web services based on REST API. However, research work can be extended to provide it with SOAP based web services. The proposed architectural model can also be implemented on cloud platform like AWS, Microsoft-Azure, IBM-Bluemix, GCS etc. to make it more easily accessible and reliable.

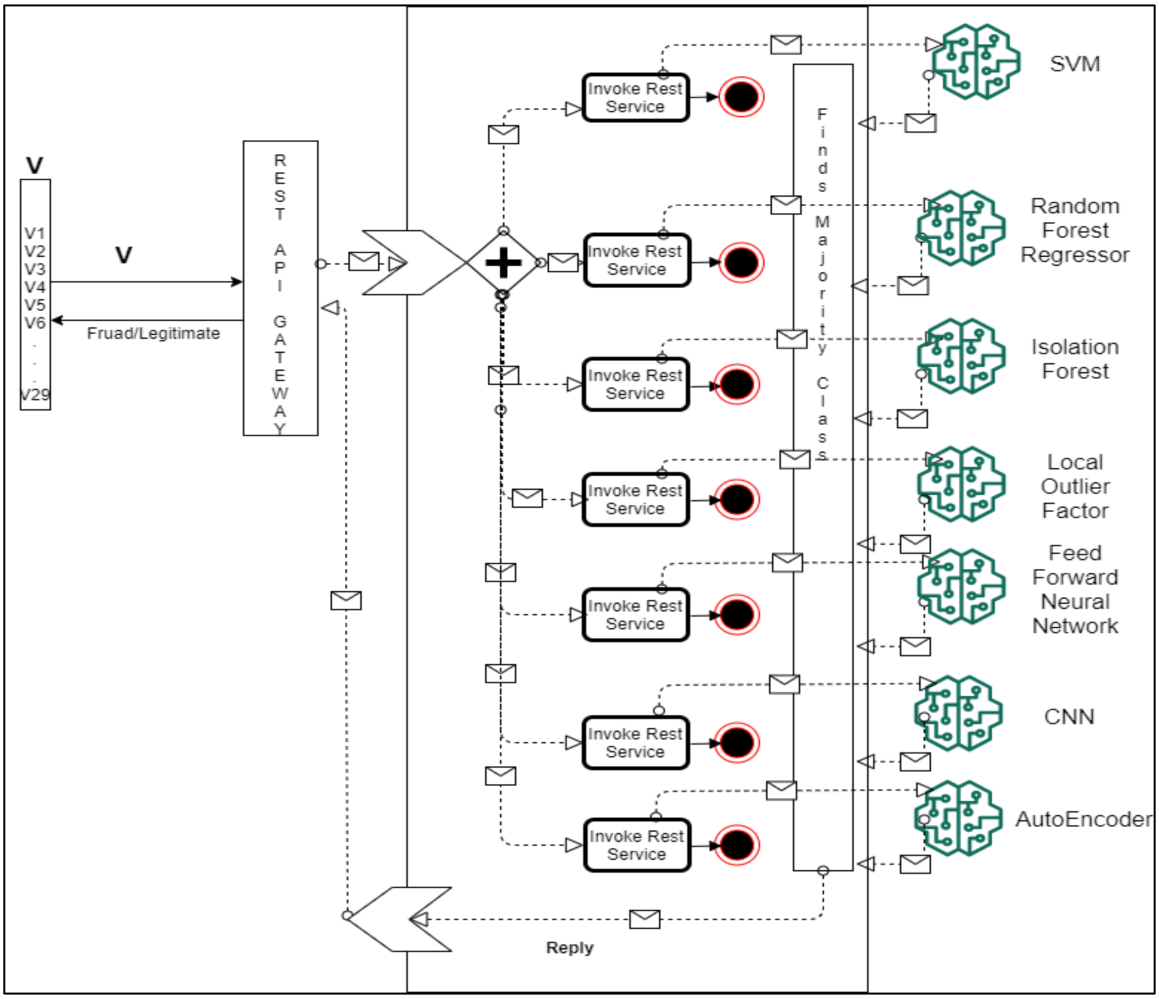


Fig. 8. Proposed SOA architecture model based on REST API with different machine learning algorithms

7. Experimental Results

Total seven classification models such as Feedforward Neural Network, Autoencoder, convolutional Neural Network, Support Vector Machine, Random Forest Regressor, Isolation Forest and Local Outlier factor have been implemented in this study. Each model provides varying degree of results. Various performance parameters have been calculated and compared for the purpose of critical assessment.

The performance parameters of the machine learning models include Accuracy, Precision, Sensitivity, Specificity and F1-score [16]. Accuracy is one of the most commonly used parameter. It is defined as ratio of number correct predictions to all the predictions made. Precision informs us about the positive data point recognized by the model. Sensitivity, also known as recall, measures as to how much the model has predicted true data points. Specificity informs us about negative data points predicted by the model. Harmonic mean of precision and sensitivity is called as F1-score. In Table 2, True positive, True negative, False positive and False negative are represented by TP, TN, FP, FN respectively. Various evaluation metrices are represented in Table 3 for comparative analysis among various machine learning techniques.

Table 2. Various performance parameter evaluation with formula

Sl. no.	**Performance parameter**	**Formula**
1	Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$
2	Precision	$\frac{TP}{TP + FP}$
3	Sensitivity	$\frac{TP}{TP + FN}$
4	Specificity	$\frac{TN}{TN + FP}$
5	F1-score	$\frac{2TP}{2TP + FP + FN}$

Table 3. Performance comparison of various classification models for credit card fraud detection

Classification model	**Sample**		**Accuracy**	**Precision**	**Sensitivity**	**Specificity**	**F1-score**
	Training	**Testing**					
FeedForwad Neural Network	304315	60863	99.13	99.72	99.36	95.84	99.54
Autoencoder	243452	60863	97.09	98.45	98.49	77.91	98.47
Convolutional Neural Network	107134	26789	**99.51**	99.52	100.00	97.37	99.76
Support Vector Machine	95138	23785	98.65	99.99	98.91	99.60	99.45
Random Forest Regressor	243452	60863	98.97	99.7	100.00	99.56	99.8
Isolation Forest	289315	57863	95.65	95.97	99.59	24.90	97.75
Local Outlier Factor	243452	60863	82.37	89.09	91.95	12.43	90.50

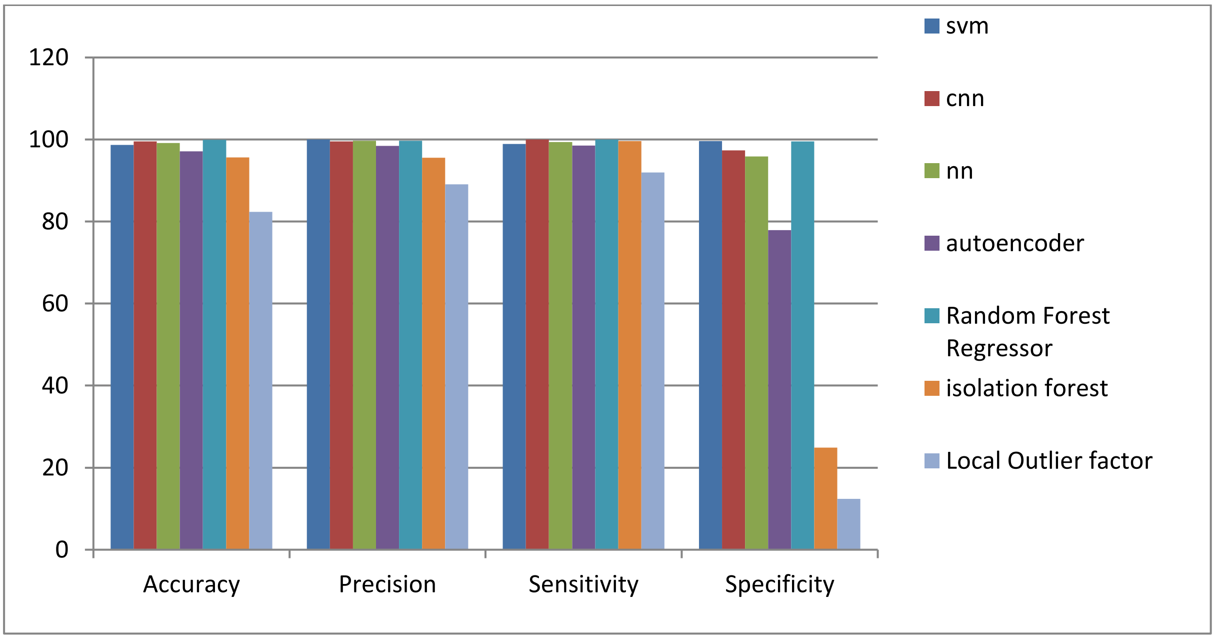


Fig. 9. Performance comparison of various classification models

8. Conclusion

In this study we have presented credit card fraud detection as service with the help of Oracle SOA suite, Oracle‘s BPEL process manager helps to realize the service oriented architecture through composition, orchestration and coordination of web services. Seven number of mahcine learning models have been implemented for classification purpose. which includes both supervised learning alogrithm as well as unsupervised learning algorithm. We have achieved competitive accuracy in CNN model while predicting the fraudulent transaction.

It is hereby proposed to extend this work by deploying the service on various cloud platforms and predict fraudulent transactions in a real time fraud detection. As of now, this study presents web services as REST API. Research work can be carried out with SOAP based web services. The proposed architecture can be implemented on cloud platform like AWS, MS-Azure, IBM-Bluemix, GCS etc. to make it easily accessible and reliable.

Compliance with Ethical Standards

In this study, the original research has been carried out by following the ethical principles.

Funding: No funding source

Conflict of interest: Authors have declared that no conflict of interest exists.

References

1. Linda Delamaire, Hussein Abdou, John Pointon (2009) Credit card fraud and detection techniques: a review. Banks and Banks System 4(2).
2. Masoumeh Zareapoora, Pourya Shamsolmoalia (2015) Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. Procedia Computer Science 48: 679-685.
3. K.Ratna Sree Valli , P.Jyothi , G.Varun Sai , R.Rohith Sai Subash (2020) Credit card fruad detection using machine learning algorithm. Journal of Research in Humanities and Social Science 8(2):04-11.
4. Mehak Mahajan, Sandeep Sharma (2019) Detects Frauds in Credit Card using Data Mining Techiques. International Journal of Innovative Technology and Exploring Engineering (IJITEE) 9(2): 4891-4895.
5. Amruta Pawar,Prakash Kalavadekar,Swapnali Tambe (2014) A Survey on Outlier Detection Techniques for Credit Card Fraud Detection. IOSR Journal of Computer Engineering (IOSR-JCE) 16(2):44-48.
6. Ishu Trivedi, Monika, Mrigya Mridushi (2016) “Credit Card Fraud Detection“. International Journal of Advanced Research in Computer and Communication Engineering 5(1).
7. Randhawa, Kuldeep, Chu Kiong Loo, Manjeevan Seera, Chee Peng Lim, and Asoke K. Nandi (2018) Credit card fraud detection using AdaBoost and majority voting. IEEE access 6:14277-14284
8. Navanshu Khare and Saad Yunus Sait (2018) Credit Card Fraud Detection Using Machine Learning Models and Collating Machine Learning Models. International Journal of Pure and Applied Mathematics 118(20): 825-838.
9. Mr.Manohar, Arvind Bedi, Shashank kumar, Shounak kr Singh (2020) Fraud Detection in Credit Card using Machine Learning Techniques. International Research Journal of Engineering and Technology 7(4): 1786-1791.
10. I. Jerstad, S. Dustdar and D. V. Thanh (2005) A service oriented architecture framework for collaborative services. 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05), Linkoping pp. 121-125. doi: 10.1109/WETICE.2005.11.
11. John, Hyder, and Sameena Naaz (2019) Credit card fraud detection using local outlier factor and isolation forest. Int. J. Computer Science Engg 7: 1060-1064.
12. Pedregosa et al., (2011) Scikit-learn: Machine Learning in Python. General of Machine Learning Research 12(85): 2825-2830.
13. Zhaohui Zhang, Xinxin Zhou, Xiaobo Zhang, Lizhi Wang, Pengwei Wang (2018) A Model Based on Convolutional Neural Network for Online Transaction Fraud Detection. Security and Communication Networks 2018.

14. Georgieva, Sevdalina & Markova, Maya & Pavlov, Velisar (2019). Using neural network for credit card fraud detection. AIP Conference Proceedings 2159: 030013. doi:10.1063/1.5127478.
15. Chiu Chuang-Cheng and Chieh-Yuan Tsai (2004) A web services-based collaborative scheme for credit card fraud detection. In IEEE International Conference on eTechnology, e-Commerce and e-Service 2004:177-181.
16. Debachudamani Prusti & Santanu Kumar Rath (2019, October). Web service based credit card fraud detection by applying machine learning techniques. In *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*, IEEE, 2019:492-497.
17. Pumsirirat, A., & Yan, L. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. *International Journal of advanced computer science and applications*, *9*(1), 18-25.
18. Aswathy M S, Liji Sameul(2018). Survey on credit card fraud detection. *International Research Journal of Engineering and Technology,* 5(11):1291-1294.
19. Samaneh Sorournejad, Zahra Zojaji, Reza Ebrahimi Atani, Amir Hassan Monadjemi (2016). A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective. *CoRR* abs/1611.06439.
20. Andrew Estabrooks, Taeho Jo and Nathalie Japkowicz (2004). A Multiple Resampling Method for Learning from Imbalanced Data Sets. *Computational Intelligence,* 20(1): 18-36.
21. David H. Wolpert and William G. Macready (1997). No Free Lunch Theorems for Optimization. *IEEE Transactions on Evolutionary Computation,* 1(1): 67-83.