International Journal of Advanced and Applied Sciences, 12(12) 2025, Pages: 174-202

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.ijaas.in

FCNN-DMOGM: Credit Card Fraudulent Detection System using Dynamic Multi-Object Optimization Technique and Full Convolution Method in Cloud

L. Vetrivendan [1*], Dr. T. Ganesh Kumar [2], Dr. Ajeet Singh [3]

[1] *Research Scholar, Department of Computer Science and Engineering, Galgotias University, India*
[2] *Professor, Department of Computer Science and Engineering, Galgotias University, India*
[3] *Professor, Department of Computer Science and Engineering, Galgotias University, India*

ARTICLE INFO

Article history:
Received: 10-07-2025
Received in revised form: 19-08-2025
Accepted: 05-09-2025

Keywords:

Convolutional Neural Network, Optimization, Machine Learning, Fraud Detection, Cloud.

ABSTRACT

Internet and mobile computing have significantly improved performance in various applications, including digital payments, storage, and confidential information access. However, 44% of frauds were identified in various fields from 1998 to 2022, making security and confidentiality crucial. To address this issue, researchers have developed and implemented cloud-based security systems using deep and machine learning optimization methods. These systems achieve high performance, making them a major requirement in cloud computing design. For credit card fraud identification, fully convolution neural networks (FCCN) and Dynamic Multi-Object based Optimization for Gradient Boosting algorithm (DMOGB) technologies are implemented. These technologies enable real-time fraud identification, classification, and feature extraction. The approach operates on clouds, with a central decision and privacy-preserving mechanism, making fraud identification easier. To decrease the fraud ratio, a real and accurate fraud detection system is needed. This research uses deep and machine learning optimization methods to detect credit card fraud. Existing works have limited accuracy, F-score, recall, and precession. To address these limitations, the research introduces deep learning mechanisms like fully convolution neural networks, convolution neural networks, and machine learning mechanisms like SVM, neural network, and LR methods. The experiment is performed on Amazon Web Services Cloud, and performance measures such as accuracy, recall, and true positive rate are calculated. The implementation results in improvements in accuracy, decision rate, and false alarm rate.

INTRODUCTION

Cloud computing is a network, and it is used to run various applications and services for different platforms, such as financing, banking, and IT sector applications. Using cloud computing, users can easily and securely access files and records. At the time of digital payments cloud computing faces many problems, therefore security are necessary. Various frauds are identified, at the instance of payment processing. Digital payments have been utilized since 1970, and different techniques have been implemented for gateway

payments. When the internet came, various applications are incorporate for different applications in several areas, as frauds also occur. In this work, cloud-based scams are identified for secure transactions.

Cloud computing is the server setup in the database, it is an interdisciplinary field of computer science, and this has been a process of computational pattern discovery in huge data sets consisting of different AI (Artificial Intelligence) and ML (Machine learning) models [1]. The main agenda of cloud computing with fraud detection is an understandable model with further utilization. Cloud servers have been attracting the entrepreneur with promise, offering speed of demand, and highly available pricing models. In this real-time scenario, different hackers have been adopting cloud servers and services. When hacking occurred, this can be a chance of attaining accounts of customers, and authorized credentials, and therefore decreases the scalable of cloud servers. Cloud services are providing different applications like banking, trading, E-commerce, debit cards, and credit card services. Using clouds authorized companies to accept all incoming services like credit cards without any need for a physical amount [2].

All various advantages of the cloud are utilized by entrepreneurs but different hackers, and fraudsters take benefit from cloud servers for hacking. International guide of "ISACA" –Spivey Jeff explains Cloud Security Alliance (CSA) and scales the attractiveness of fraudsters' behavior [3]. Cybercriminals practice cloud-based frauds and these may be rehearsal prevention. These threats shall expose legal activities like criminal liabilities, loss, profit, blocking of transactions, etc. Cloud computing is an event in which legitimate business, phenomenal of business, the fraudulent operation is performed. The substantial market agency's discussion related to the security of the cloud has been a focus on consumer side relations even a cloud providing various resources, but data security cannot look into the fact, numerous other customers have moved to the threat. The utilization of credit cards had become a standard function in every person in daily life. The advantage of CC (credit card) is the transactions that are processed straightforwardly. Therefore, it is

flexible, and payments can perform easily. The identifications of credit card frauds conducted in the deadly process, so consumers interested to involve, flexible, careful operations have committed. This is an excellent critical study in cashless transactions like digital payments using credit cards [4]. Even though this model is high significance in handling frauds in an efficient consumer involvement now a days, financial transactions and medical transactions drastically increase; for a better experience, many vendors deploy their applications on the cloud. Since 2019 many professional surveys are analyzing that 80% of industries and micro-organizations use their application in cloud computing so, we necessary to provide security to those applications, these are identified and the safety of the fraud of servers is possible only by deep and machine learning techniques. Microsoft, Google, and Oracle were offering cloud services for many IT applications. The usual methods do not satisfy the present features. Therefore, cloud computing with advanced technologies effectively provides many advanced functions. Clouds regularly maintain the most important datasets, but the servers, barrier this overhead. The cloud environment supports the many devices that handle significant volumes, different formats, and big data [2]. Clouds are a combination of a pool of applications and provide the resources; thus, they service economic applications, network applications, and big data technologies. The clouds are prominently functioning the sufficient effects to the MSME companies.

Machine learning (ML) and deep learning (DL) mechanisms can solve many cloud computing problems. This platform is offering many applications for easy access and maintenance. Big data, mobile computing, and cloud computing technologies have many more advantages in the software industry. Bank applications, finance applications, and software applications require a flexible environment for their operations. The previous methods are mostly accepting applications in the server. But the server maintenance is very complex and economical. Therefore, a flexible platform for deploying applications is necessary; in this

research work, the server-based applications have to be exchanged to the cloud environment. In these clouds, many frauds have been identified, and these have to be automated for CC fraud detection. ML and DL models help credit card fraud detections (CCFD) at any time-varying nature of the cloud server.

LITERATURE REVIEW

Cloud computing is an advanced technology to improve the efficiency of the application from a service and security point of view. In this section, various implemented methods and surveys have been performed briefly. The cloud-based frauds regarding credit cards are one of the significant threats to applications and services. [6] The shrouded significance of Cloud Computing is coming into or placing away otherwise sharing the facts on the net. In an acclimated plot, dispensed calculating is distribution in addition to developing step by step also emerges as the greatest huge aspect in firms both government and non-public businesses. A wonderful fear in distributed computing worldview is the appropriate burden of adjusting over the possible property. Grouped Load adjusting calculation and system has stood created to create gifted consumption of viable property and also enhance the complete execution.

Financial Frauds

Considering a decade's findings, the financial fraud areas can be categorized into insurance loans, automobile insurance, financial statement, and credit card. The data mining classification algorithms that have been used in these areas are Naïve Bayes, Logistic regression, KNN, SVM, NN, Decision tree, Genetic algorithm, Fuzzy Logic, and Random Forest. From 2008 to 2022, it was seen that Logistic Regression is best, especially in financial statement frauds and insurance frauds. Random Forest came into existence only after 2015.

The clustering techniques like K-Means clustering and stream clustering, the Artificial Immune system, and SOM are also methods used in this decade. The study highlights that both supervised and unsupervised learning were used and noted that more frequently supervised learning is used which leads to conclude that its performance is valuable and efficient [7]. The brief framework of classification algorithms that are used in the area of

financial fraud is summarized in Table 1 which had discussed the article percentage published in each year from 2008-2022.

Table 1: Publication Articles on Various Classification models and Frauds (2008-22)

Fraud Type	Description	Article percentage
Financial Statement Frauds	This mainly focuses on the challenges for the managers and investors due to the action irresponsible behavior, purposeful leading to fra statements.	30-40%
Bank Frauds	Credit card fraud, Money Laundering, Fraud bank accounts. Stealing others' funds.	50-60%
Insurance Frauds	Health care insurance, automobile insurance Auto insurance, etc. mainly assurance misuse.	30-40%
Other Financial frauds	Tax frauds, fund transactions, financial reporting.	20%

In this broadsheet, our point is to analyze organized calculations to find out the association of burden adjusting in distributed calculating and subsequently observe them on one-of-a-kind parameters. Additionally, communicate about the legitimacy and faults of the calculations.

Prevailing Data Mining Techniques

[8] highlighted the false financial statements (FFS) encountered in Asian countries and developed a statistical technique -two FFS detection models using Classification and Regression Tree (CART) both for industry benchmarked and non-industry benchmarked and compared with the logistic regression achieved high accuracy. The CART industry benchmark is found better at predicting the false financial statement. It also captured the indicators and their combination to detect the FFS in China. [9] Proposed a detection approach using detection measures for money laundering applied simultaneously thus minimizing circumvention with a consolidative index. Trade deviations, their frequency, typical trade partner receipts, or illegal payments were

detected by using the three measures. Ben ford's Law is used to find fraud in finance by counting the number of occurrences of a certain digit at a place in a number. It was successful in discovering the possible frauds that are planted in the simulated data.

While evaluating the life insurance claims, small clusters are flagged such that the claims have similar patterns and there exists a large cluster that contains claims with large interest payments and lagging in their payments. This helps auditors in detecting fraud automatically. The clustering that was used is K-Means clustering performing an anomaly detection method implemented in the WEKA platform. [11] proposed financial cyber-crime detection system combining rule-based filtering, data mining, Bayes theorem, and artificial intelligence. A model considering the time of the transaction, on which day, based on the history of transactions was built with five components DBSCAN, Data ware house, linear equations, Bayes theorem, and rules are developed and named transaction risk score generation model (TRSGM).it is implemented to detect online frauds and can be used for new incoming transactions too based on the transaction amount.

[12] Proposed a quantitative approach to textual data named Computational Fraud Detection Model (CFDM). They were a success in developing automated detection for potential fraud. [13] structured a Meta framework for the detection of financial frauds with legitimate and fraud recall that was over 80% effective in stakeholder's cost settings and had more performance than the existing semi-supervised learning methods and also the existing financial detection models. Thus, outperforms over Adaptive semi-supervised learning model. [14], has done review the fraud detection techniques to detect fraud in credit cards. The various supervised and unsupervised learning have been compared with different datasets. This research work also highlights the number of skewed distribution concepts and the performance of the learning algorithm deeply considering different journal studies. [15][22] have done a comparative study analysis of decision trees. The analysis done is survival analysis which is compared with discriminant analysis and log it analysis which is

always stable with time. The survival analysis is a longitudinal insurance fraud data that can cooperate with time series that is it can predict the fraud claims both at time and before. The automobile insurance claim that was fraudulent is predicted based on three different case studies, combining the decision tree to form a hybrid model. The performance of the Artificial Neural Network which is a back propagation model is done separately with the bootstrap dataset. [16] Developed a model using self - an organizing map and neural clustering to characterize the users likely to generate fraud invoices in the year based on the payment of their tax having similar behavioral styles. Followed by the data mining classifiers Bayesian networks, decision trees, and neural networks to determine associated behavioral frauds and non-frauds to help the audit team of the tax department [17] implemented an outlier detection model for an audit log for application systems. The work mainly concentrated on existing various outlier detection algorithms are used such as C4.5, DBSCAN, and Bayesian networks that could use to detect an anomaly from the given data set. Generated a tool for the system auditors that use the alpha-numeric features of the audit logs within an information system

CLOUD INFRASTRUCTURE

Every application needed the flexibility of allowing the resources; it is possible by cloud computing. Big data and cloud computing can maintain many companies' profiles with less economy along with this offering efficient performance. Rapid technology is allowing the applications enormous demand; automatically some of the applications handle the problems faced by users. The advanced software analytics and processing power make the application efficient. The cloud correctly uses deep and machine learning everywhere for solving statistical computations. Deep learning requires many resources for increasing application performance; the machine learning in the cloud utilizes the massive environment storage in the available space. Artificial intelligence-based datasets are collected for cloud-based fraud detection. The example datasets are MNIST, NIST, and CIFAR10. The advanced learning models give efficient solutions to clouds.

Financial organizations and IT applications mainly offer the cloud environment for ease of access and security. Different optimization models designed for cloud computing such as SVM, CNN, RFO, and X-boost. The implemented methods do not improve the CCFD rate. Therefore, fraud is done by fraudsters easily, in this research work combination of deep learning and machine learning techniques are proposed. This method is named fully convolution neural networks and gradient boosting machine learning.

Figure 1: Relationship Model of Fraud Prevention Model and Cloud

Fraud prevention is possible through advanced machine learning models such as those operated by auto-machine techniques. By 2023 zero fraud detections are attacking the cloud means we achieve good improvement. But, nowadays, this fraud rate is more for prevention, encouraging the advancements of technologies.

FCNN (FULLY CONVOLUTION NEURAL NETWORK)

The name itself reflects its architecture, which is a locally connected threshold layer model. The various layers test and train the problems in cloud computing. The significant layers called convolution, hidden, and pooling is performed in their operation to help the architecture. In this any density layer does not disturb the cloud architecture and performance, this FCNN analyzes the dynamic cloud nature and continuously updates the frauds in the cloud. The reduction of various parameters in the dataset resembles the response time, accuracy, and cloud performance. FCNN network takes the input from a dataset with original information and requires fixed parameters and stages.

Without any variable parameters FCNN operated easily, it is a special nature of deep neural networks. The datasets are segmented by networks, usually in three parts [18][19].

- Sampling path: Capture the dataset information.
- Un sampling path: Recover the information
- Up or down-sampling: Decided by a fitness function

The sampling and un-sampling parameters are the information analyzers which are continuously graded the samples. This sampling analysis was done by spatial information technique. When the cloud requires more information, up-sampling is performed else down; sampling comes into the picture.

Dataset

The MNIST dataset is collected for the cloud-based fraud detection system. In the MNIST, especially credit card fraud (CCF) data and medical records are taken as references.

- Training set: 1050000 records
- Testing set: 25000 records
- The validation set: 1025000 records

Above mentioned different dataset parameters which are collected from MNIST credit card fraud-oriented transactions.

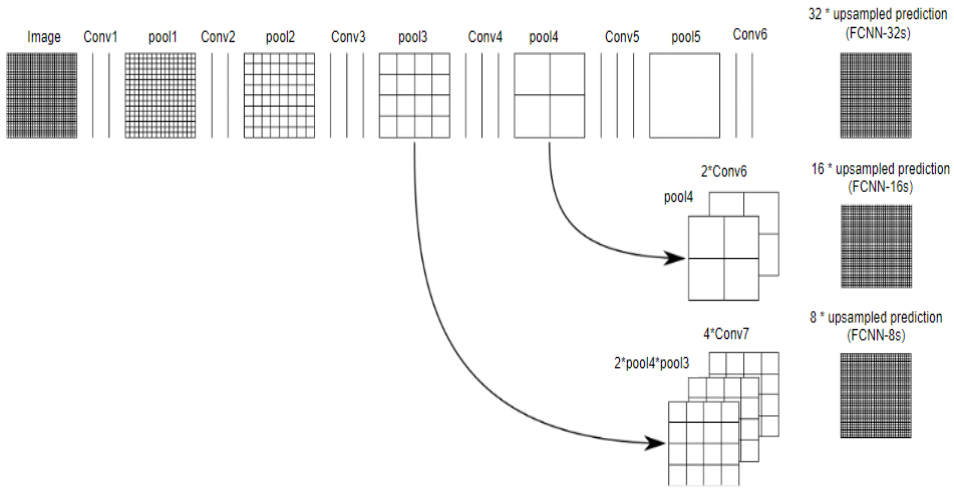

Figure 2: Fully Convolutional Neural Network Architecture

The FCNN architecture is clearly explained in Figure 2. It is a combination of hidden layers, pooling layers, and convolution neural networks. Using all parameters can easily find out the frauds in the

cloud. Credit cards are more and more popular in economic transactions in the same way frauds also increase. The combination of convolution neural networks and machine learning methods to detect fraud behavior expertly the negligence diverse the cloud to imbalance the negative and positive transactions The FCNN-based fraud identification is used as a pre-processor and extractor and DMOGB utilizes it as a classifier. An abundant transaction caused the fraud quickly, and a full convolution neural network was to apply on this situation to detect the patterns of fraud behaviors [23]. This experiment over-imposed on the significant real-world transaction and identify the CC fraud performance.

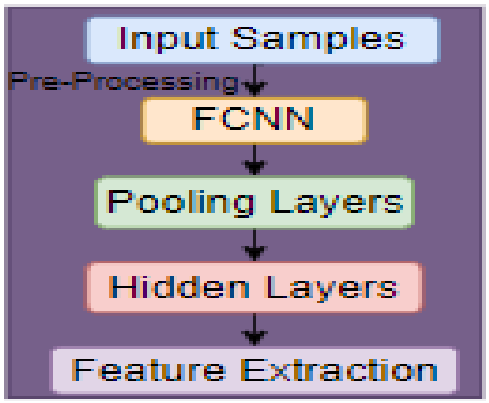

Figure 3: FCNN contributions to real-world credit card data

Figure 3 is an explanation of detailed steps in the FCNN model; in this model, sample records are collected from the MNIST credit card database. In the first phase, pre-processing steps are applied, i.e., FCNN modeling. Various layers are involved in this FCNN named as pooling layer, hidden layer, and feature extraction stage. After completion of all these steps, a clear picture of cloud behavior is identified.

The detailed contribution of the FCNN model is explained below the flow chart with a detailed description. At the primary stage, FCNN is used for pre-processing and feature extraction purposes. The credit card transactions are applied to the FCNN pre-processor using mining latent fraud patterns. In the second stage,

matrix feature extraction is applied to original the time series of transactions.

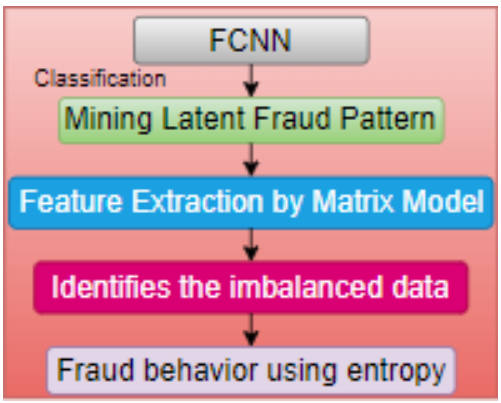

Figure 4: FCNN Classification and Feature Extractions Deep Analysis.

In the third phase sampling method was applied to calculate the entropy value, finally when this entropy feature attains less value decide that fraud behavior is observed on a cloud in above figure 4.

Fully Convolutional Neural Network Methodology

The fraud detection system is designed for the reorganization of cloud behavior in a dynamic nature. FCNN-related fraud detection system calculates the entropy value using feature extraction and classification steps.

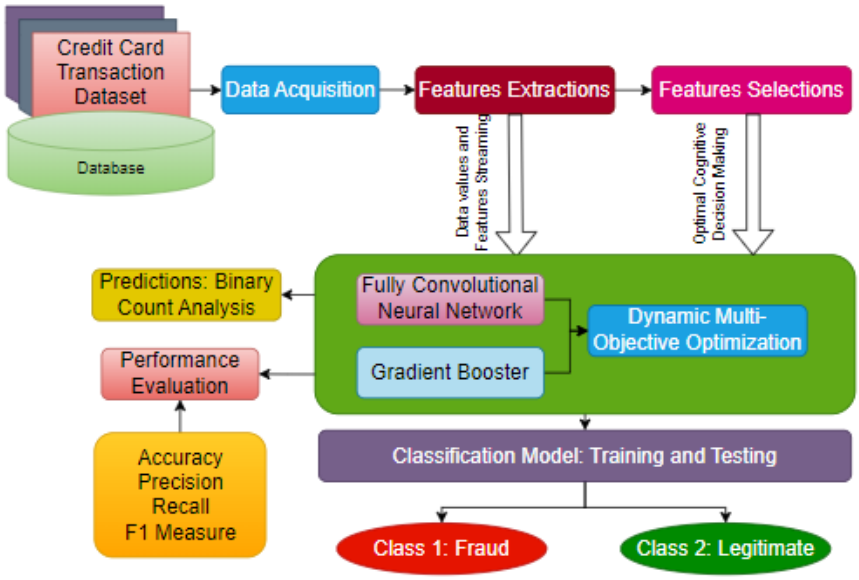

Figure 5: Overall FCNN.

This fraud detection model framework is shown in Figure 5; it consists of training computations and testing methods based on entropy measurement. The training model mainly divides into four-part:

- Feature dataset collection
- Sampling methods
- FCNN transformation
- Training procedure

The testing part comes offline, and the training part is online when a transaction comes into a cloud computing environment the FCNN starts the prediction process and compares the online information. The feature extraction consists of transforming the variables in the datasets and aligning the elements in a format. For feature extraction, the FCNN starts the aggregation procedure and mathematical entropy computations. These steps make the system efficient.

$$p_i = \frac{Amount * T_i}{Total\ Amount} \quad (1)$$

$$EntT = -\sum_i^k p_i \log p_i \quad (2)$$

$$TradingEntropyT = EntT - NewEntT \quad (3)$$

Equation 2 calculates the transaction from the merchant, T is the total amount, i is the number of transactions, and entropy is calculated by using equation 3. The trading entropy is calculated for the behavior of CC fraud if this value is more confirms that fraud had done. The sampling technique is applied for the observation of neighbor probabilities when this probability rate is more down sampling or up sampling is adjusted and identifies the fraud.

Table 2 clearly explains parameter types in the dataset; these are basic requirements of the FCNN model. We apply the FCNN model on clouds to detect the fraud of a credit card; the FCNN model is most suitable for a large type of dataset, and also this mechanism overcomes the overfitting limitation. The FCNN is applied to clouds for feature extraction of fraud behavior [20].

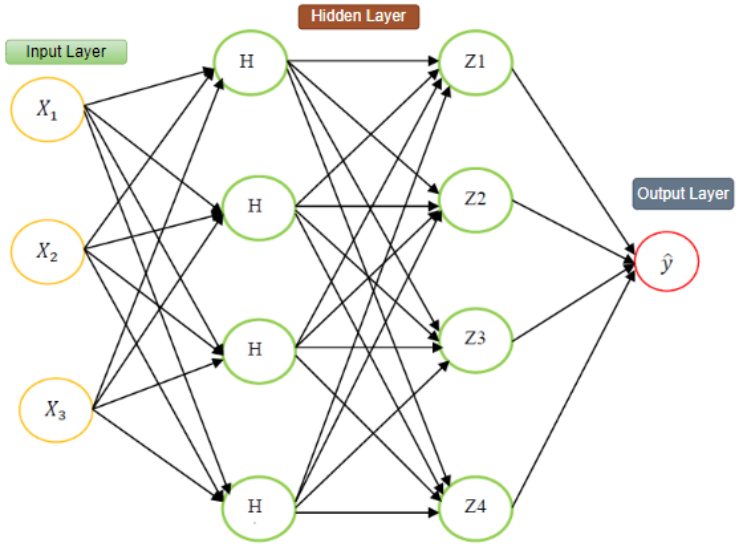

Figure 6: FCNN multi-layer models

This FCNN model calculates fraud on clouds and network issues using the ReLU function. In this investigation, N=56, and CON = two datasets are used to calculate the fraud behavior on clouds. This design is implemented on the Keras package, which is available in the Python library F_t+▲.

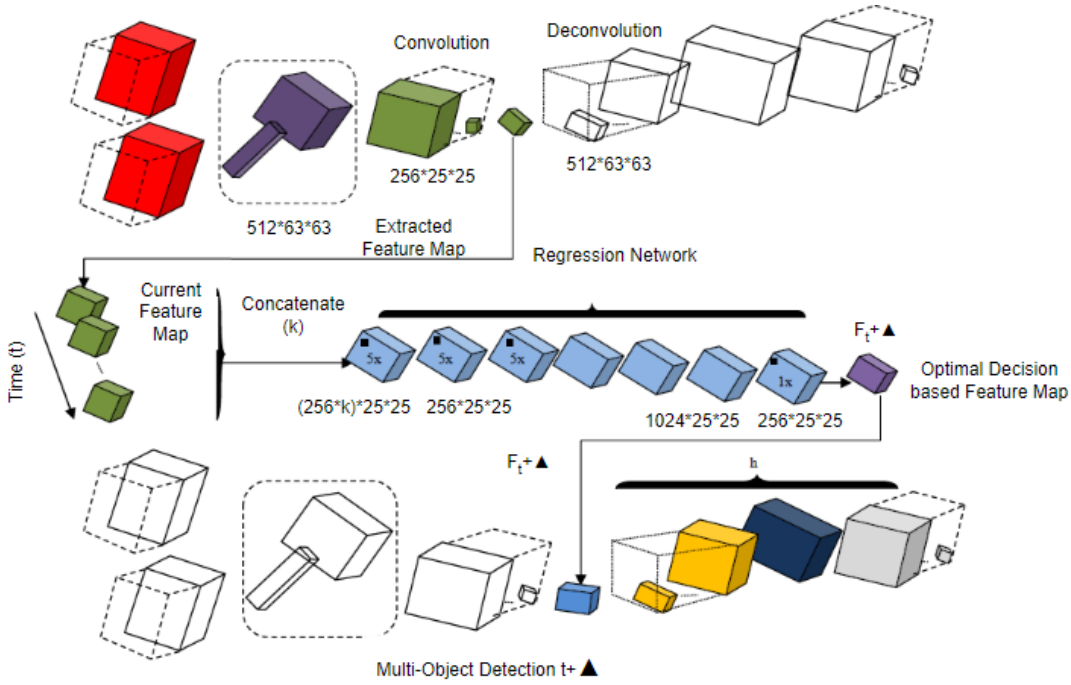

Figure 7: Multilayer FCNN Various Feature Mapping Architecture

Multilayer FCNN is a normalized deep learning model; this can use to identify cloud behavior. In this network cloud, dynamic nature is

detected by hidden layers, the pooling layers responsible for fraud in the cloud. The ReLU function in the above block diagram is handling the summation of weights from available node inputs. The activation function in the rectified linear unit becomes a default active function; it is a link of neural networks that can be used to train and test the operations [24]. The convolution and de-convolution layers in the FCNN handle the frauds in cloud computing in a tactical manner. The convolution process extracts the dataset features and gives further process to the current feature map in the FCNN network. The de-convolution network is a regression process; its handover the fraud objects in cloud computing. The $t + \Delta$ is the information about the fraud target and time of the fraud. These parameters test the entire cloud network to identify fraud in the system [25].

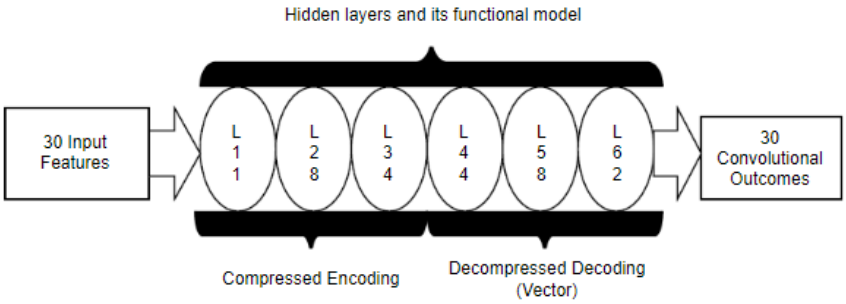

Figure 8: Auto Encoding Decoding Model (30 Convolutional Outcomes)

The attributes in the FCNN network have been functioning depending on several layers for the encoder and the number of layers at the decoder. In this L1, L2, and L3 are used for encoders and L4, L5, and L6 are decoding the attributes. Figure 8 deals with 30 attributes using the 3x3 ReLU deep learning model. Compared to CNN, the FCNN achieves the best residual performance for auto encoding and decoding of fraud transactions in cloud computing [21][26].

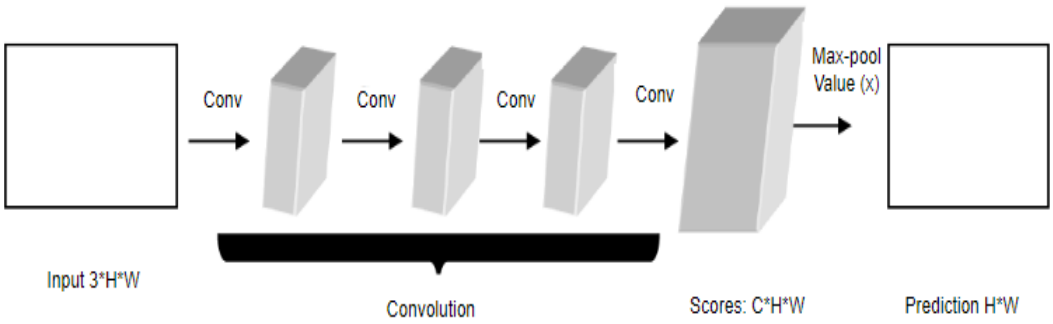

Figure 9: Prediction of Average Convolution

The encoding and decoding of cloud network is a state of art framework; in these convolution neural networks performs the prediction of frauds at the time of dynamic operation of the application. At the input stage, 3xHxw problems are given as input, and an average of pooling layers predict the problem and identify the frauds in the transaction.

$$Z_i^{[l]} = W_i^T . a^{[l-1]} + b_i a_i^{[l]} = g^{[l]}\left(Z_i^{[l]}\right)$$

(4)

Equation 4 briefly explains weight balancing and average score generation network. Here $Z_i^{[l]}$ = average score from FCNN, $g^{[l]}$= the number of layers involved, and a and b are the average number of rows and columns in the predicted ReLU matrix.

$$Weight\_Bal\_Score_1^{[2]} = W_1^T . a^{[l-1]} + b_1 a_1^{[2]} = g^{[l]}\left(Z_1^{[2]}\right)$$

(5)

$$Weight\_Bal\_Score_2^{[2]} = W_2^T . a^{[l-1]} + b_2 a_2^{[2]} = g^{[l]}\left(Z_2^{[2]}\right)$$

(6)

$$Weight\_Bal\_Score_3^{[2]} = W_3^T . a^{[l-1]} + b_3 a_3^{[3]} = g^{[l]}\left(Z_3^{[2]}\right)$$

(7)

Equations 5 to 7 deal with the encoder section of the FCNN network, which can handle the attributes of layer 1 to layer 3 [27]. The hidden layers and pooling layers can continuously encode the available data. The weights, attributes, and layers handle the FCNN model for encoding the network of cloud computing along with its frauds in a dynamic time.

$$Weight\_Bal\_Score_4^{[2]} = W_4^T . a^{[l-1]} + b_4 a_4^{[2]} = g^{[l]}\left(Z_4^{[2]}\right)$$

(8)

$$Weight\_Bal\_Score_5^{[2]} =$$

$$W_5^T . a^{[l-1]} + b_5 a_5^{[2]} = g^{[l]}\left(Z_5^{[2]}\right)$$

(9)

$$Weight\_Bal\_Score_6^{[2]} =$$

$$W_6^T . a^{[l-1]} + b_6 a_6^{[3]} = g^{[l]}\left(Z_6^{[2]}\right)$$

(10)

The mathematical computations from equations 8 to 10 clearly explain the decoding section of the FCNN deep learning model [27]. It is decoding the transaction details related to fraud identified or not. If any fraud is identified the feedback path presented in the FCNN handles it and is smoothly operated by various layers in the network. After the identification of every fraud, the ReLU function once confirms whether the weather fraud happened or not.

$$ReLU\ (x) = \begin{cases} 0\ if\ x < 0 \\ x\ if\ x \geq 0 \end{cases}$$

(11)

The ReLU function estimates the rank of the matrix; the selected confusion matrix performs the operations if the rank is zero; there are no frauds identified in the cloud Else fraud is detected. After the deep learning process feature extraction stage is completed, further for classification we are moving to dynamic multi-objective optimization for gradient boosting machine learning algorithm (DMOGB).

DMOGB CLASSIFICATION SYSTEM

Various machine learning methods efficiently classify the problem, and different classifiers already discussed classification models such as RBF, privacy-preserving, and SVM, etc. but further investigation on clouds can solve the many hidden issues in cloud computing. At this stage gradient boosting mechanism shootout on screen, it is a powerful and popular machine learning technique to solve ever end the problem.

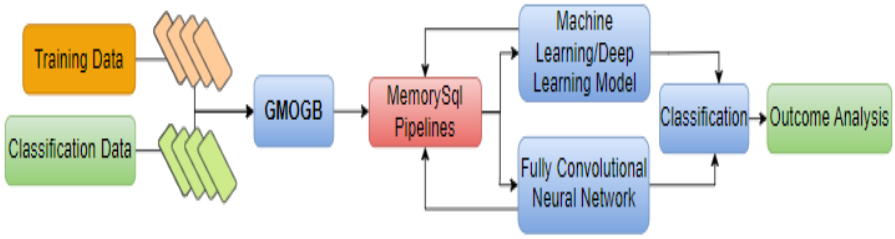

Figure 10: Fraud classifier- GMOGM with Classification Process

In this diagram, a clear picture of the DMOGB technique is briefly

explained. The training and testing of data samples and real-time transactions filtered by the FCNN model. After the pre-processing classifier, DMOGB handles the fraud transaction based on weights and tree structure. In dynamic multi-objective optimization for gradient boosting classification algorithm, each tree is balanced with its weights based on the valid transaction, if any invalid transaction occurred in the cloud, then this tree is un- balanced to particular weights. At that time, the argument finalizes the transaction type. The evaluation process started from tree 1…. tree N, when the weights of residuals are identified from inputs. The real-time clouds extracted the available information and compared the transactions with an available dataset. The main motivation of this DMOGB classifier is to classify the medical records and credit card fraud identification system efficiently.

Dynamic Multi Object based Optimization for Gradient Booster Terminology

The DMOGB technique is a useful problem identifier for regression and classification when the prediction is identified on weaker transactions than decision trees typically predict the disorders of frauds using booster algorithm, $h1$is the response of generalized operation. Using these parameters identifies the fall transaction in the cloud easily.

$$r_{2m} = \frac{-\partial L}{\partial f(x_i)}\left(y_i, f(x_i)\right) \quad (12)$$

$$\alpha = argmin_{\alpha} L(y_i, f_{m-1}(x) + \alpha h_m(x)) \quad (13)$$

The differentiation of equation 13 gives the rank of the matrix; if the level is 0, then the transaction is true. Else, fraud had occurred. $\alpha$is the trained argument for dataset feature extraction.

$$Loss = \sum_{i=1}^{n} L\left(y_i, f_{m-1}(x_i) + \alpha h_m(x_i)\right) + \sum_{j=1}^{T} \Omega\left(h_m(x_j)\right) \quad (14)$$

The loss function can give the particular fraud that happened in cloud computing when this equation is applied to selected parameters then automatically trees, weights, and faults are easily identified. Here h_m = impulse train function Ω.

$$Loss = -\frac{1}{2}\sum_{j=1}^{T}\left[\frac{G_j^2}{x_j+\lambda}\right] + \text{ET} \quad (15)$$

$$Gain = Loss\ Before -$$

$$Loss\ a\ filter\ split$$

(16)

$$Loss = -E + \frac{1}{2}\left[\frac{G_L^2}{H_L+\lambda} + \frac{G_R^2}{H_R+\lambda} - \frac{(G_L+G_R)^2}{H_R+H_L+\lambda}\right]$$

(17)

equation 17 explains about gain fitness function, which is observed from the DMOGB classifier. Using this equation, we can find out the gain of the transaction based on a loss before the variance and loss filter by a split. The DMOGB model training and testing components can variant the transaction score based on the DMOGB model. The prevention of busy states and identification of fraud transactions can be solved by the DMOGB classifier easily.

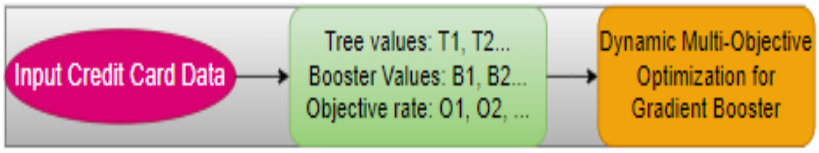

Figure 11: DMOGB tree allocations.

Figure 11 clearly explains the DMOGB tree classification and prediction of fraud transactions in cloud computing. The fitness function and gain function can estimate the trees and weights related to DMOGB. This classifier differentiates real-time transactions and available dataset transactions. If any false alarm is observed in the fitness function, then automatically fraud is identified dynamically.

CCFD DATASET

This proposed FCNN-DMOGB method utilizes the MNIST and DN-CN2 datasets. These are filtered and features are extracted by FCNN deep learning method. DMOGB classifier can enhance the operations based on dynamic current transaction history.

```
##from keras import layers
##from keras import modelsmodel = models.Sequential()
##model.add(layers.Conv2D(32,(5,5),activation='relu',
                                 input_shape=(28, 28,1)))
##model.add(layers.MaxPooling2D((2,
##2)))model.summary()_____
_____
##Layer (type)                 Output Shape              Param #
=================================================================
=====
##conv2d_1 (Conv2D)            (None, 24, 24, 32)    832
_________________________________________________________________
_____
##max_pooling2d_1 (MaxPooling2 (None, 12, 12, 32)    0
=================================================================
=====
##Total params: 832
##Trainable params: 832
##Non-trainable params: 0
```

Python software with packages is used to implement the deep learning and machine learning model. The packages play an important role such as Keras, pandas, and NumPy. These mathematical and theoretical results can solve the issues of cloud computing fraud on health records and credit cards. The dataset, iterations, and variables in the cloud computing system help the transactions whether they are fraud or not. In this investigation, the health records and credit card fraud data instances are selected, i.e., 284997 related 40 attributes are shootout the problem.

Dataset Features

The MNIST, DN-CON1, and DN-CON2 datasets and their features are illustrated below in Table 3.

Table 3: Dataset Features

S. No	Data set	Multivariate
1.	Attributes	Categorical, Integer
2.	Associated functio	Classification
3.	No. of instances	284997
4.	No. of Attributes	40
5.	Missing	N/A

The number of attributes, associated functions, and instances can strengthen end the dataset. The table itself clearly explains 285000 and 40 instances, attributes selected, respectively.

```
#Layer (type) Output Shape Param #
=================================================================
#conv2d_1 (Conv2D) (None, 24, 24, 32) 832
_________________________________________________________________
#max_pooling2d_1 (MaxPooling2 (None, 12, 12, 32) 0
_________________________________________________________________
#conv2d_2 (Conv2D) (None, 8, 8, 64) 51264
_________________________________________________________________
#max_pooling2d_2 (MaxPooling2 (None, 4, 4, 64) 0
_________________________________________________________________
#flatten_1 (Flatten) (None, 1024) 0
_________________________________________________________________
#dense_1 (Dense) (None, 10) 10250
=================================================================
#Total params: 62,346
#Trainable params: 62,346
#Non-trainable params: 0

#model =
#models.Sequential()model.add(layers.Conv2D(32,(5,5),activation
='relu',
                                    input_shape=(28,28,1)))
#model.add(layers.MaxPooling2D((2,
#2)))model.add(layers.Conv2D(64, (5, 5), activation='relu'))
#model.add(layers.MaxPooling2D((2,
#2)))model.add(layers.Flatten())
#model.add(layers.Dense(10, activation='softmax'))
```

The max-pooling layer, hidden layer, and output layers enhance the dynamic problem of clouds. The above Python code mentions the different packages like conv2, max pool, and hidden. These packages can help the system make efficient.

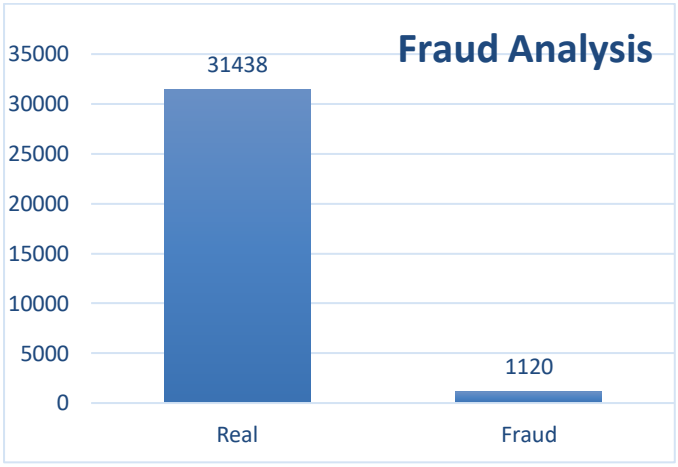

Figure 12: Data Set Distributions

Figure 12 describes the graphical analysis of the dataset, time, and oversampling frauds mentioned with attributes. It is identified that 3.12% of transactions are frauds, and the remaining are recognized as genuine transactions. This type of case study can handle the problem solution and proper remedy.

PERFORMANCE MEASURES

The real-time medical records and credit card records are trained with MNIST, DAN- CON-1,2 datasets. It is recognized that if any fraud transaction is identified then automatically shootout the problem. This FCNN-DMOGB technique distributes the balanced classes and gives the training and testing set. The combination of machine learning and deep learning can increase performance improvement compared

to existing methods.

Comparison of Algorithms: Different optimization mechanisms have already been implemented for cloud-based fraud detection systems. But improvement is needed for challenging the present models. This research work presented FCNN and DMOGB machine learning optimization techniques, it gives more improvement compared to the present model.

The four models are run on CCF data and concerning real-time values. After the training and testing, we evaluated TPR, TNR, FPR, and FNR. These four parameters can easily estimate the accuracy, precision, false alarm rate, false discovery rate, and negative prediction rate. These all give the performance measures of the system, such as sensitivity, recall, F1 score, and specificity. The entire mathematical computations and an example are clearly described in the following methods.

Mathematical computations of performance measures

The classification model is evaluated by accuracy, it is the prediction of the model in the right way. When these parameters are to be good, the application performance is more. In this workaround, 285000 transactions are identified as non-frauds and achieve 99.8% accuracy which is shown in below equation 18.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (18)$$

The recall is a parameter that identifies the fraudulent transactions out of current transactions. Our model achieves a 93.78% recall measure, which is an improved version compared to existing methods which is shown in equation 19.

$$Recall = \frac{TP}{TP+FN} \quad (19)$$

Precision is the calculation of all transactions estimated to be fraudulent, our proposed model enhances the previous methods and achieves 98.9% precision. This is a good improvement, which is shown in Equation 20.

$$Precision = \frac{TP}{TP+FP} \quad (20)$$

The F1 measure is the combination of $\frac{TP}{TP+FN}$ and $\frac{TP}{TP+FP}$ into a single metric. The calculation recall and precision give the individual F1 scores based on falls positive rate and false-negative rate. If the imbalance has occurred in the cloud computing network, then automatically F1 score

has to be reduced which is shown in equation 21

$$F1_{Score} = 2 * \frac{Recall * Precision}{Recall + Precision} \quad (21)$$

RESULTS AND DISCUSSION

In this section, the various outcome and their comparison models are discussed briefly. The advanced methods like SVM, LR, NN, and proposed FCNN-DMOGB are compared with each other and identify the best-improved algorithm.

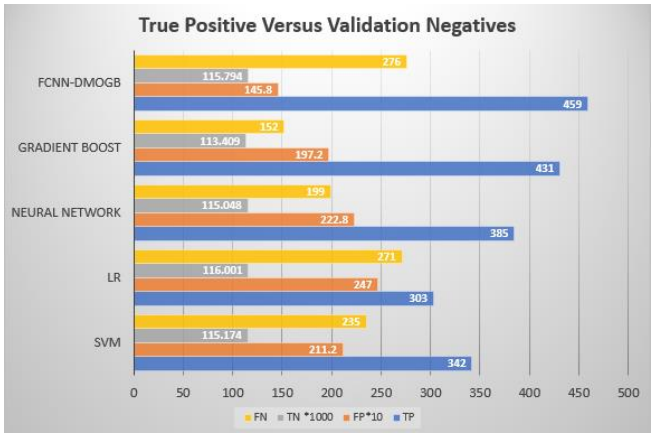

Figure 13: T_p vs T_n

The above table 4 & Figure 13 demonstrate the performance measures of TP, TN, FP, and FN elements. These are the key factors that can decide the accuracy and sensitivity.

Table 4: Various Classification F1 Score Values

Classifications	F1 score
SVM	0.226601
LR	0.270546
Neural Network	0.241546
Gradient Booster	0.177568
FCNN-DMOGB	0.299456

Figure 14: F1 Score Comparison with Different Detection Method.

Table 5 and Figure 14 give a discussion of the F1 score measure, which can decide the designed application performance. It is identified that the proposed FCNN-DMOGB attains more enhancement equated to LR, SVM, neural networks, and gradient booster.

Table 5: Accuracy of FCNN-DMOGB

Classification	**Accuracy**
SVM	98.1%
LR	98.2%
Neural Networks	97.8%
Gradient Booster	96.5%
FCNN-DMOGB	99%

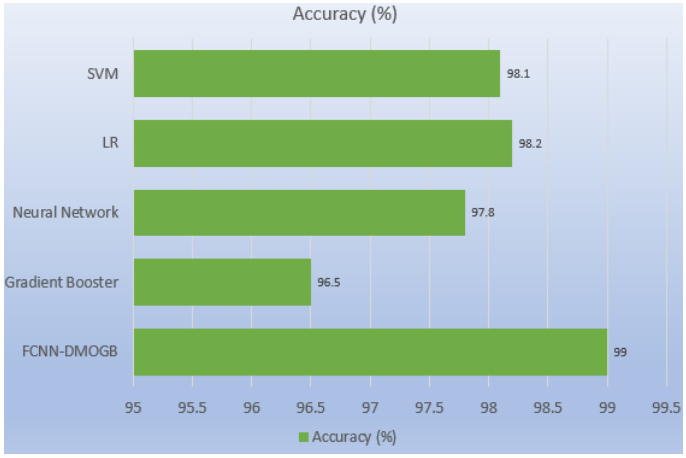

Figure 15: Compared Proposed Model with Existing Classification Analysis of Prediction Accuracy

Figure 15 clearly describe the accuracy analysis of the FCNN-

DMOGB technique. It is identified that our designed FCNN-DMOGB attains more enhancement compared to SVM and LR.

CONCLUSION AND FUTURE ENHANCEMENT

This research work defined the three objectives, i.e., Cloud-based credit card frauds and medical records fraud estimation models. The unstructured credit card dataset has been analyzed through a software-defined approach. This mechanism sorts out the problems of cloud-based CC frauds with dynamic control access. The FCNN-DMOGB method is a combination of deep and machine learning models and also gives accurate simulation results Deep and Machine learning techniques achieve noticeable results in different areas like data analysis, processing, and classification, which make the possibility of constructing fast and real-time intelligent models. This work proposes a live cloud-based fraud detection system depending on fully convolution neural networks and machine learning technology. Our implementation model has based on auto-encoder FCNN and DMOGB technology. It permits to process and classification the real-time financial transactions, promising results for our proposed model are higher than existing solutions in terms of accuracy, recall, and precision. At final, propose a robust machine and deep learning method, i.e., FCNN-DMOGB method for credit card frauds and medical record frauds identification system on a dynamic cloud environment. This work identifies transaction fraud or not. The entire investigation achieves an accuracy of 98%, an F1 score of 0.299, and a true positive rate is 379 has been completed. Which is an excellent improvement for handling real-time This is an excellent improvement for handling the real-time CC fraud identification system, this work is helpful for researchers at feature technologies like cloud computing environments.

The implemented credit card-based fraud identification system gives more robust simulation outcomes. The help of artificial intelligence and deep learning techniques makes this application efficient. If using auto stack encoder-based deep learning algorithm handles the imbalance datasets and unsupervised applications efficiently. Therefore, in the future, there may be artificial

intelligence, machine learning, and deep learning combination to classify credit card frauds with less response time and more accuracy.

REFERENCES

1. Dang, T.K.; Tran, T.C.; Tuan, L.M.; Tiep, M.V. Machine Learning Based on Resampling Approaches and Deep Reinforcement Learning for Credit Card Fraud Detection Systems. Appl. Sci. 2021, 11, 10004. https://doi.org/10.3390/app112110004.
2. Anuruddha, Thennakoon., Chee, Bhagyani., et al., (2019), "Real-time Credit Card Fraud Detection Using Machine Learning." 9th International Conference on Cloud Computing, Data Science & Engineering, IEEE. DOI: 10.1109/CONFLUENCE.2019.8776942 JULY, pp488-493.
3. J. Luna, A. Taha, R. Trapero and N. Suri, "Quantitative Reasoning about Cloud Security Using Service Level Agreements," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 457-471, 1 July-Sept. 2017, doi: 10.1109/TCC.2015.2469659.
4. Bai, B., Yen, J., Yang, X. (2008), "False Financial Statements: Characteristics of China's Listed Companies and CART Detecting Approach." International Journal of Information Technology & Decision Making 2008; 7: 339–359.
5. S. K. Hashemi, S. L. Mirtaheri and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," in IEEE Access, vol. 11, pp. 3034-3043, 2023, doi: 10.1109/ACCESS.2022.3232287.
6. Z. Xiao, D. He, Y. Guo and J. Du, "Request Balancing Among Users in Multiple Autonomous Cloud Provider Environments," in IEEE Transactions on Industrial Informatics, vol. 16, no. 2, pp. 1140-1148, Feb. 2020, doi: 10.1109/TII.2019.2928314.
7. S. S. Velicheti, A. S. H. Pavan, B. T. Reddy, N. V. Srikala, R. Pranay and S. K. Kannaiah, "The Hustlee Credit Card Fraud Detection using Machine Learning," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 139-144, doi: 10.1109/ICCMC56507.2023.100

84063.

8. C. Lin, M. Luo, X. Huang, K. -K. R. Choo and D. He, "An Efficient Privacy-Preserving Credit Score System Based on Noninteractive Zero-Knowledge Proof," in IEEE Systems Journal, vol. 16, no. 1, pp. 1592-1601, March 2022, doi: 10.1109/JSYST.2020.3045076.
9. Yang, S., Wei, L., (2010), "Detecting Money Laundering using Filtering Techniques: A Multiple Criteria Index." Journal of Economic Policy Reform 2010; 13: 159–178.
10. Thiprungsri, S., Vasarhelyi, M.A., (2011), "Cluster Analysis for Anomaly Detection in Accounting Data: An Audit Approach." The International Journal of Digital Accounting Research; 11: 69-84.
11. J. Cui, C. Yan and C. Wang, "ReMEMBeR: Ranking Metric Embedding-Based Multi-contextual Behavior Profiling for Online Banking Fraud Detection," in IEEE Transactions on Computational Social Systems, vol. 8, no. 3, pp. 643-654, June 2021, doi: 10.1109/TCSS.2021.3052950.
12. Glancy, F.H., Yadav, S.B., (2011), "A Computational Model for Financial Reporting Fraud Detection." Decision Support Systems 2011; 50: 595–601.
13. Abbasi, A., Albrecht, C., Vance, A., Hansen, J., (2012), "Meta-fraud: A Meta-Learning Framework for Detecting Financial Fraud." MIS Quarterly 2012; 36: 1293-1327.
14. Razaque, A.; Frej, M.B.H.; Bektemyssova, G.; Amsaad, F.; Almiani, M.; Alotaibi, A.; Jhanjhi, N.Z.; Amanzholova, S.; Alshammari, M. Credit Card-Not-Present Fraud Detection and Prevention Using Big Data Analytics Algorithms. Appl. Sci. 2023, 13, 57 https://doi.org/10.3390/app13010057.
15. Gepp, A, Wilson, J.H., Kumar, K., Bhattacharya, S. A., (2012), "Comparative Analysis of Decision Trees Vis-a-vis Other Computational Data Mining Techniques in Automotive Insurance Fraud Detection." Journal of Data Science 2012; 10: 537-561.
16. Gonzalez, P.C., Velasquez, J.D., (2013), "Characterization and Detection of Taxpayers with

False Invoices Using Data Mining Techniques." Expert Systems with Applications 2013; 40: 1427–1436.

17. Carneiro, E.M.; Forster, C.H.Q.; Mialaret, L.F.S.; Dias, L.A.V.; da Cunha, A.M. High-Cardinality Categorical Attributes and Credit Card Fraud Detection. Mathematics 2022, 10 3808. https://doi.org/10.3390/math10203808.

18. S. Jose, D. Devassy and A. M. Antony, "Detection of Credit Card Fraud Using Resampling and Boosting Technique," 2023 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA), Ernakulam, India, 2023, pp. 1-8, doi: 10.1109/ACCTHPA57160.2023.10083376.

19. Chaudhary, K., Yadav, J., Mallick, B., (2012), "A Review of Fraud Detection Techniques: Credit Card.", International Journal of Computer Applications, 45(1), 39- 44.

20. S. Han, K. Zhu, M. Zhou and X. Cai, "Information-Utilization-Method-Assisted Multimodal Multiobjective Optimization and Application to Credit Card Fraud Detection," in IEEE Transactions on Computational Social Systems, vol. 8, no. 4, pp. 856-869, Aug. 2021, doi: 10.1109/TCSS.2021.3061439.

21. Honlam Li. 2023. Credit Card Fraud Detection Based on Combination of Sparse Autoencoder and Support Vector Machine. In Proceedings of the 2022 6th International Conference on Electronic Information Technology and Computer Engineering (EITCE '22). Association for Computing Machinery, New York, NY, USA, 1252–1255 https://doi.org/10.1145/3573428.3573650.

22. Dharwa, J. N., Patel, A.R., (2011), "A Data Mining with Hybrid Approach Based Transaction Risk Score Generation Model (TRSGM) for Fraud Detection of Online Financial Transaction." International Journal of Computer Applications 2011; 16: 18- 25.

23. Raval, J.; Bhattacharya, P.; Jadav, N.K.; Tanwar, S.; Sharma, G.; Bokoro, P.N.; Elmorsy, M.; Tolba, A.; Raboaca, M.S.

RaKShA: A Trusted Explainable LSTM Model to Classify Fraud Patterns on Credit Card Transactions. Mathematics 2023, 11, 1901 https://doi.org/10.3390/math11081901.

24. Beyazit Bestami Yuksel, Serif Bahtiyar, and Ayse Yilmazer. 2021. Credit Card Fraud Detection with NCA Dimensionality Reduction. In 13th International Conference on Security of Information and Networks (SIN 2020) Association for Computing Machinery, New York, NY, USA, Article 18, 1–7 https://doi.org/10.1145/3433174.3433178.

25. H.D., Kuna, et al., (2014), "Outlier Detection in Audit Logs for Application Systems.", Information Systems, Volume (44) Aug-2014, pp-22-33.

26. H. Wang, W. Wang, Y. Liu and B. Alidaee, "Integrating Machine Learning Algorithms with Quantum Annealing Solvers for Online Fraud Detection," in IEEE Access, vol. 10, pp. 75908-75917, 2022, doi: 10.1109/ACCESS.2022.3190897.

27. Yuxin Gao, Shuoming Zhang, and Jiapeng Lu. 2021. Machine Learning for Credit Card Fraud Detection In Proceedings of the 2021 1st International Conference on Control and Intelligent Robotics (ICCIR '21) Association for Computing Machinery, New York, NY, USA, 213–219 https://doi.org/10.1145/3473714.3473749.

28. Ran Xia and Faleh Alshameri. 2020. Credit card fraud detection: an evaluation of SMOTE resampling and machine learning model performance. J. Comput. Sci. Coll. 36, 3 (October 2020), 165.

29. Wenxuan Shi. 2021. A Comparison between Classifiers on Credit Card Fraud Detection Problem. In 2020 2nd International Conference on E-Business and E-commerce Engineering (EBEE 2020) Association for Computing Machinery, New York, NY, USA, 13–16 https://doi.org/10.1145/3446922.3446925.

30. Ge Zhang, Zhao Li, Jiaming Huang, Jia Wu, Chuan Zhou, Jian Yang, and Jianliang Gao. 2022. EFraudCom: An E-commerce

Fraud Detection System via Competitive Graph Neural Networks. ACM Trans. Inf. Syst. 40, 3, Article 47 (July 2022), 29 pages https://doi.org/10.1145/3474379.

31. Moschini, G.; Houssou, R.; Bovay, J.; Robert-Nicoud, S. Anomaly and Fraud Detection in Credit Card Transactions Using the ARIMA Model. Eng. Proc. 2021, 5, 56. https://doi.org/10.3390/engproc2021005056.

32. Muyuan Chen. 2023. Credit Card Fraud Detection Based on Multiple Machine Learning Models. In Proceedings of the 2022 6th International Conference on Electronic Information Technology and Computer Engineering (EITCE '22). Association for Computing Machinery, New York, NY, USA, 1801–1805 https://doi.org/10.1145/3573428.3573745.

33. Wei Zhou, Xiaorui Xue, and Yizhen Xu. 2022. Credit card fraud detection based on self-paced ensemble neural network. In Proceedings of the 4th International Conference on Information Technology and Computer Communications (ITCC '22) Association for Computing Machinery, New York, NY, USA, 92–98 https://doi.org/10.1145/3548636.3548650.

34. Strelcenia, E.; Prakoonwit, S. A Survey on GAN Techniques for Data Augmentation to Address the Imbalanced Data Issues in Credit Card Fraud Detection. Mach. Learn. Knowl. Extr. 2023, 5, 304-329. https://doi.org/10.3390/make5010019.

35. N. Nguyen et al., "A Proposed Model for Card Fraud Detection Based on CatBoost and Deep Neural Network," in IEEE Access, vol. 10, pp. 96852-96861, 2022, doi: 10.1109/ACCESS.2022.3205416.