International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 11, Issue 10, October 2020, pp.51-66, Article ID: IJARET_11_10_006
Available online at http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=10
ISSN Print: 0976-6480 and ISSN Online: 0976-6499
DOI: 10.34218/IJARET.11.10.2020.006

AN IMPLEMENTATION OF REAL AND ACCURATE CLOUD BASED FRAUD DETECTION SYSTEM BY USING DEEP AND MACHINE LEARNING TECHNIQUES

Prasanthi Gottumukkala
Department of Information Technology CMR Engineering College, Hyderabad, India.

Dr .G. Srinivasa Rao
Department of Information Technology, GITAM University, Visakhapatnam, India.

ABSTRACT

From the last decades deep and machine learning techniques are achieves prominent outcomes in various areas like data analytics, big data processing and cloud classifications. Which makes the real time intelligent models, in this investigation proposes a cloud based fraud detection system by using Fully Convolution Neural Networks (FCNN). Along this deep learning, Gradient Boosting Machine Learning (GBML) technology is incorporated, it permits the real time frauds classification and regression on clouds. Our proposed methodology FCNN and GBML compete with existing models in terms of accuracy, recall, true positive rate and precision.

Keywords: Cloud Frauds, GBML, FCNN, Credit Card Frauds.

Cite this Article: Prasanthi Gottumukkala and Dr .G. Srinivasa Rao, An Implementation of Real and Accurate Cloud Based Fraud Detection System by Using Deep and Machine Learning Techniques, *International Journal of Advanced Research in Engineering and Technology (IJARET),* 11(10), 2020, pp.51-66
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=10

1. INTRODUCTION

The number of financial transactions via credit card increases drastically and with it various frauds has occurred. From 2019 financial association and professionals survey the payment frauds observed clearly. This survey of records analyzes the frauds around 80% of all organizations. As rise of online payments billions of frauds can occur on clouds. Because of this reason banks and financial organizations challenge to construct an effective fraud detection system. Deep learning presenting a many applications with active solutions, this can helps the management traders, risk analyzers and fraud detectors. In digital landscape, for example, deep learning is used to build an intelligence software that can directly interact with people and gives

quires. In trading, trade analyze system is utilized to made fast decisions. More over the general usage of deep learning in banking sectors is the security against frauds. With the help of deep learning and machine learning techniques identify the suspicious fraud activities with an easy way.

Depending upon ID's of transaction history, deep learning shows the behaviors of customers and machine learning detects fraudster data with efficient classification, if there is a fraud or not. In this research, the main objective is cloud based frauds detection system design using modern techniques.

Deep learning presents a very significant solution to deal with fraud transactions on clouds, making to accurate use of "financial organizations-big data". In deep learning many methods are there, in this fully convolution neural networks (FCNN) are utilized for preprocessing stage. At final stage, classification purpose gradient boosting machine learning technique is to be used. FCNN currently has given that accurate precisions and throughputs to many problems.

In this data investigation, clouds related fraud detection with binary categorization trouble are investigated, this FCNN predict the binary fields with efficient manner. So clouds-frauds can easily identified by the FCNN and classify the "legitimate" or "fraudulent". The binary classification is an easiest classification, where a compilation of information is classified into 2 classes, depending upon features available.

Based upon transaction history machine learning optimization technique with new methods analyze the fraud detection ratios and identifies the transaction is fraud or not [15]. MCKNSAY [5] explains that an important solution to deal the frauds at big data related heavy transactional traffic. In FCNN multi-level pooling layers and hidden layers learning model is discussed in [7].

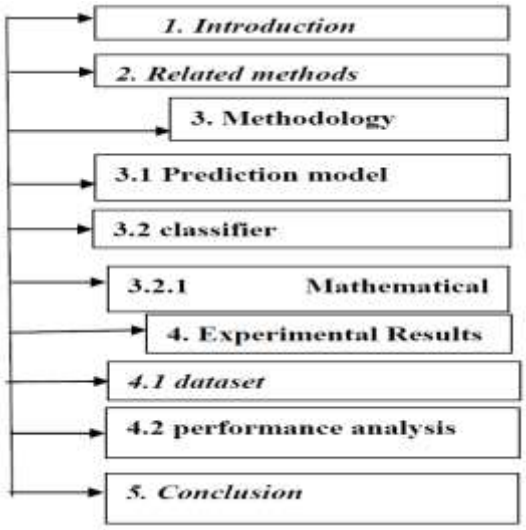
The best precision and efficiency generating system promising the results in many fields at binary classification. In big data analysis cloud based fraud detection system with binary classification is analyzed and classified for specific outcomes. There are many numerical models for binary learning classifications such as DT- Decision trees, NN- Neural networks, SVM- Support vector machine, KNN- K-nearest neighbors and logistic regression [8].

Figure 1 Fraud prevention system.

The real time information which has been collected from john a stanko dataset, this dataset consist of various control actions on receiving data, processing data and returning data at the time of transaction[11]. Our proposed model is a novel work, it is useful for real time applications at the time of cloud based fraud classification. The deep learning networks utilizing the auto encoder, classifies the transactions and real time decision, resulting that fraudulent

identification data is the output. Gradient boosting machine learning model is used for testing and classification. Along this, support vector machines are also used for binary classification of cloud based frauds but not efficient [17]. The present work performed based on gradient boosting machine learning model and compare with SVM, LR and KNN etc.[6]. The SVM's drawn a major attention in current studies because of its major performance depending on classification action. However in some of conditions ANN had given efficient results compare with nonlinear models [18]. As for datasets one example exercise is performed on European cards transaction history. This work gives two key points, which are illustrated below.

- A real time full convolution neural networks (FCNN) approach on credit card fraud detection problem for clouds based on auto encoder.
- Comparison of different classification methods for observation of auto encoder functionality.



This discussion and implemented design compete with current technology and achieves better improvement. The rest of the work is organized as like in section 2 discuss a short review on related methods. In section 3 describes FCNN architecture and GBML classification. In section 4 explains testing environment, then analyze the test out comes. Finally in section 5 we gives a future work and conclusion.

2. RELATED METHODS

From few years back many alternate solutions are proposed for clouds fraud detection system. The significant methods are statistical or artificial intelligence [10] has been used based on illustrated examples such as

- Regression model
- SVM
- Multiple discriminant analysis [23].

2.1. Literature Survey

The logistic regression optimization method utilized for binary classification [24], compare various modern models for fraud detection [15] improves the accuracy. Like various methods were used for cloud based problem detection system. The brief discussion on various multi model features explained below table 1 clearly.

Table 1 literature survey

ARTICLE NO	SURVEY ARTICLE METHODOLOGY OF COMMUNICATION	TECHNIQUE	KEY POINTS
[1]	Fraud Control	Machine learning	EC 2 layer problems State of art framework Cloud security
[2]	Global payments group	Data mining encoder approach	Fraud identification Fraud classification Real time database analysis
[3]	Business data mining	Machine learning	Classification Regression Analysis
[4]	Binary classification	Big data and cloud computing classification	Financial market analysis Cloud computing techniques
[5]	Fraud analysis	Quick estimation Account Take over method	Knowledge based authentication Fraud landscape shifting EVM security on clouds
ARTICLE NO	SURVEY ARTICLE METHODOLOGY OF COMMUNICATION	TECHNIQUE	KEY POINTS
[6]	Statistical theory	Machine learning	Productive function statistical learning algorithm
[7]	MIT press	Deep learning	Cloud data fraud analysis EC2 layer estimation efficiency, accuracy
[8]	Survey of data mining	Deep learning	Tensor flow calculation Accuracy, True positive rate
[9]	Statistical fraud detection	Statistics and machine learning effective technologies data analytics method.	Fraud detection Digital cloud audit mechanism. Transactions history analysis.
[10]	Data mining related fraud detection	Rank based fraud detection	Matec web content dataset Credit score Fraud or not?
[11]	Real time computing	MISCONCEPTION	Cloud efficiency EC2 server Sensitivity
[12]	Credit card frauds	Conventional SVM method	Fraud identification Server boosting real time efficiency
[13]	Credit card computer system	Auto encoder	Cloud based frauds analysis EC2 cloud fraud identification
[14]	Fraud detection technique	Analysis of credit card fraud using deep learning	Efficiency Accuracy Throughput
[15]	Data mining for credit card	Neural networks	Credit card fraud detection Linear discriminant analysis Recall and F1 score

The mobile computing and cloud computing technologies are facing many issues at the time of business transactions. The machine learning models with random forest optimization solves the many issues in the cloud computing. But, this is a traditional search process, therefore the delay of operations takes more time [26]. The mechanism of business analysis and service possible with cloud and mobile computing technologies. Such that an advanced cloud computing and security tools are necessary to analyze the frauds. The block chain and big data technologies mainly facing security issues, without data securities these technologies are going to be affordances. The decision making and application computing May takes more time with less accuracy. These type of partial results degrade the cloud usage. The data computing and cloud security management is a major driven approach at data mining. Now a days the major IT business depending on cloud based applications, if this services are cannot give the assurance then automatically fraudsters are attacking cloud applications. The theoretical and experimental models deal the current issues of cloud security and gives the better decision making [27]. The data security and network issues are major challenges in cloud system, if fraudsters hack clouds then applications getting trouble. Therefore an advanced technology is necessary to implement the security to clouds [28]. With exponential growth in IoT and edge computing technologies helps the clouds and its applications. The generalized cloud environment can deals the moderate security issues, but real time monitoring is necessary. For these applications purpose we can design the accurate cloud security model with low latency time [29].

In this study [30] cloud computing and its services are explained clearly, the layers security and cryptography protection concepts are discussed. Various cloud services and related security issues managed by computing features concept. The challenges like security, computing and platform economy features are major roles in cloud computing technology.

3. METHODOLOGY

3.1. Prediction model-FCNN

In this section our proposed classification method using FCNN is designed based on pooling layer and hidden layer.

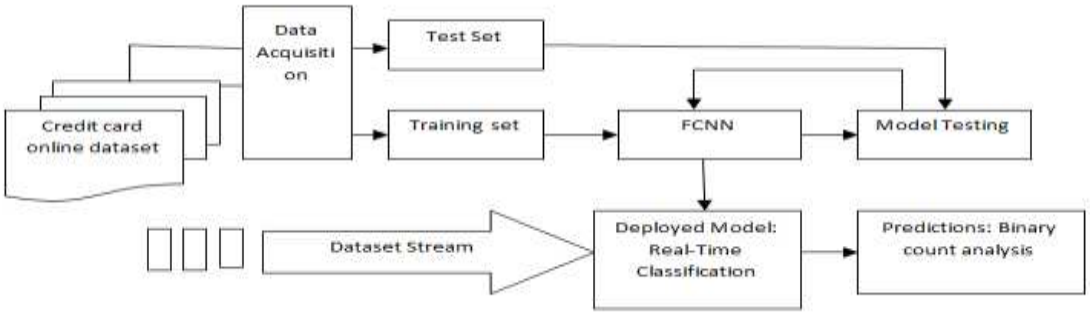


Figure 2 FCNN for fraud detection.

A periodical online credit card fraud training dataset is given to input of our design and predict the frauds based on FCNN mathematical computations. The deep learning is a user friendly mechanism it can help any type of platforms like clouds, data mining and big data analytics. FCNN network can normalize the dropouts by using rectified linear units (ReLU) function. This function helps for various layers in the FCNN network, in all convolutional network the final layer is 3*3 sigmoid activation layer.

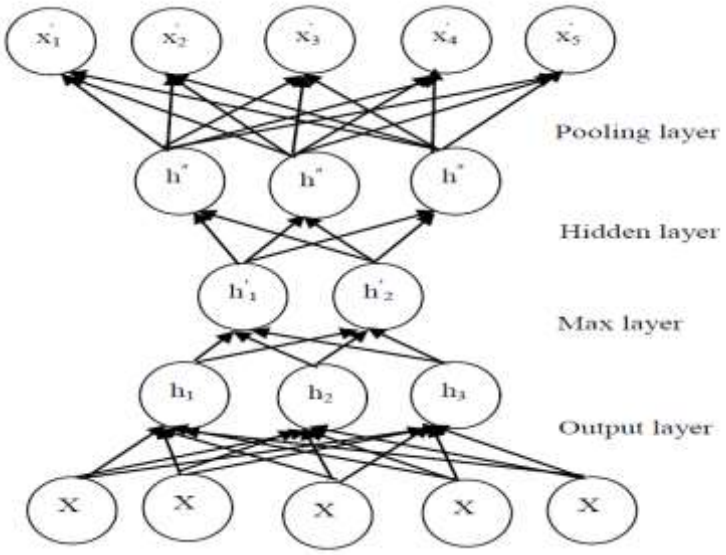


Figure 3 FCNN layer analysis.

This mechanism very helpful for cloud based dropdown network issues at every time, all FCNN filters searching the ReLU activated sub layers for fraud detection. In this N=56 FCNN CON 2 dataset is used to identify the computed frauds in the clouds, which is shown in fig2 clearly. Fig 3 describes about general architecture of layer information which can operated using 300*300*56 confuse matrix. More than 500 trained weights are predicted using FCNN keras library, FCNN processed the ReLU activation function and convolute the filter layers which is shown in above figure.

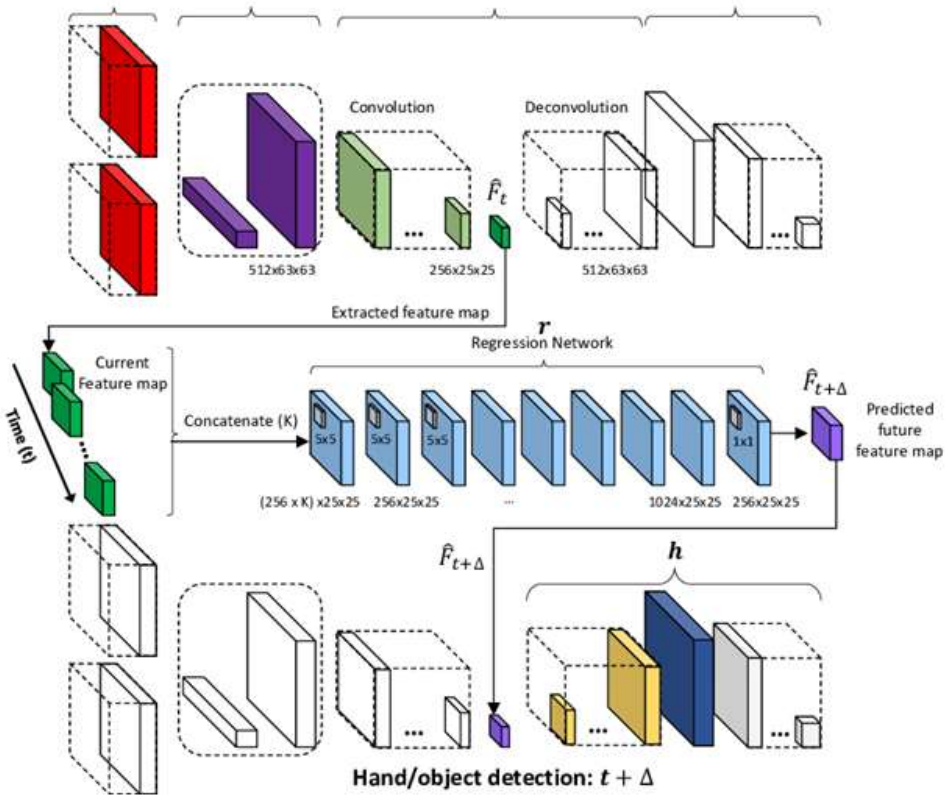


Figure 4 FCNN complete architecture.

The FCNN is process the normalized ReLU functions using 32 to 64 CNN layers, our design classified into three residuals which are illustrated below. 1. A regular depth of cloud computing key parameters and normalized dropout layers has described. 2. Replace the last convolutional layer with altered layers such as 1, 2, 4, 8, 16 etc.. 3. The entire architecture is combination of second and 3rd layers. Using FCNN CON 2 dataset is input to our training model and validate the target test data.

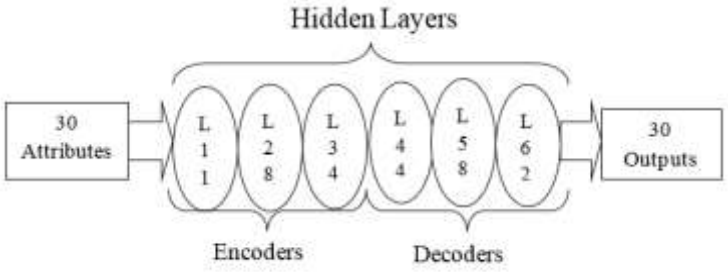


Figure 5 Auto encoder method.

We also compare the FCNN with CNN, results that FCNN residuals got best performance. In this FCNN deep learning is used as auto encoder, it is a neural network and equalize the input and output functions. Which is shown in above figure4.

Fig 5 explains that auto encoder and decoder model, which consist of two parts 1. Encoder: Identify the more number of frames at maximum point operations. At this point clouds may be loose their security issues, therefore chance of frauds may occur on original inputs. 2. Decoder: The input data is able to decode with reconstructed data and it is fed back to encoder stage. The entire operations are shown in below equations 1to 3.

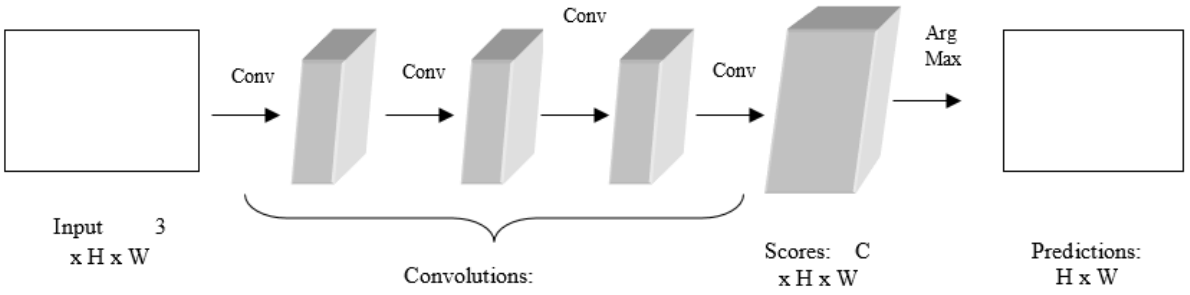


Figure 6 average convolution prediction.

We can write the same for all m neurons in layer

$$Z_i^{[l]} = W_i^T \cdot a^{[l-1]} + b_i \qquad a_i^{[l]} = g^{[I]}(Z_i^{[l]}) \tag{1}$$

Fig 6 explains that tangent function analysis at automatic convolution and data computations. The fraud information is predicted easily by using the average nature of gradient FCNN realization.

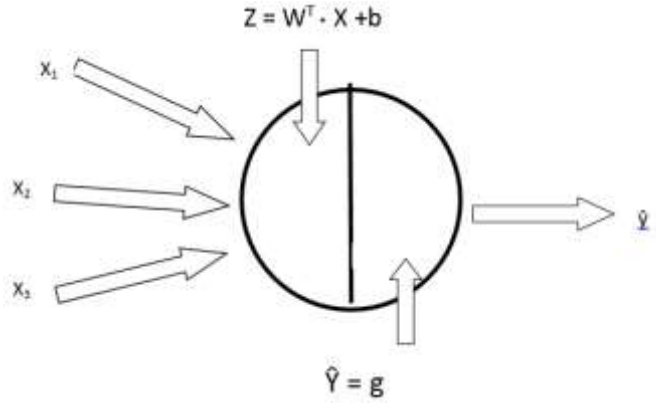


Figure: 7. Deep Learning analysis.

$$Z_1^{[1]} = W_1^T \cdot a^{[0]} + b_1 \qquad a_1^{[1]} = g^{[1]}(Z_1^{[1]}) \tag{2}$$

$$Z_2^{[2]} = W_2^T \cdot a^{[1]} + b_2 \qquad a_2^{[2]} = g^{[2]}(Z_2^{[2]}) \tag{3}$$

Equation 1 to 3 are major equations, these are used to find out the Impulse response of first connected layer in Convolutional neural network. Here Z is impulse function, W is weight of particular tree, a & b are co-expression knowledge in FCNN. Fig 7 explains that over all deep learning analysis of FCNN model, this model can implement on python 3.6, keras GPU, GPX 660, Memory of 16GB. In this y represents of output of cloud based fraud count. In this overall information of fraud has detailed like date, time, location and platform. By the help of following equations which are shown in above equations 4

$$Z_n^{[N]} = W_3^T \cdot a^{[n]} + b_3 \qquad a_3^{[n]} = g^{[n]}(Z_3^{[n]}) \tag{4}$$

$$\text{RELU}(x) = \begin{cases} 0 \; if \; x < 0 \\ x \; if \; x >= 0 \end{cases} \tag{5}$$

-478	494
460	-477

0	494
460	0

The above equation 5 is the final FCNN output which gives the rank of prediction, this rank is used to predict the frauds in the cloud system. For classification we are moving to GBML technique, which is explained in below section. The 1st layer in FCNN is connected with 81 neurons, it is getting information from all layers in cloud. The 2nd layer is convolutional layer it is designed with 20 CNN neurons with 4x4 kernel size. The output of individual layers are connected between kernel matrix and fitting matrix. The over fitting layers and internal functions are managed by 3rd module in FCNN. The max pooling layers are interact with 4x4 size kernel and connected with last layer.

3.2. GBML-classifier

Gradient boosting is a powerful and popular machine learning technique, it is used in massive big data analysis, cloud computing and data mining. GBML is a method which converts the week classification model into strong classifier.

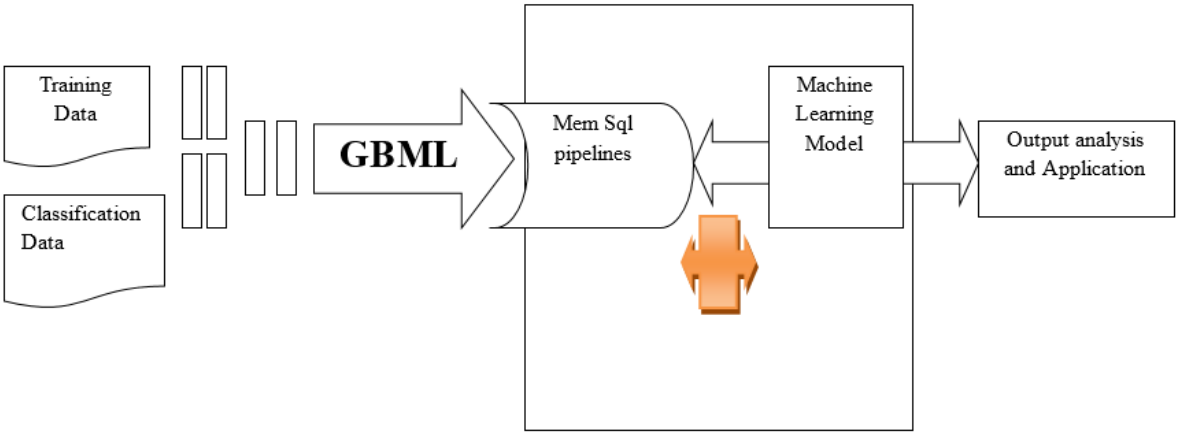


Figure 8 GBML for cloud frauds classification.

In boosting every tree is modified with validation of original dataset and can easily assigned the weights to each tree. After evaluation of 1st tree can increases the weights of another observations of trees. In this lower weights are very simple to classify the prediction, therefore this GBML is tree1+ tree2...+tree N of residuals are classified. GBML trains the every datasets which are taken from input and classify the frauds in the clouds at real time. Our main agenda is to classify the credit faults compared to good transactions. This entire discussion is explained by using the below mathematical computations.

3.2.1. Mathematical computations of GBML [15]

$$r_{2m} = \frac{-\partial L}{\partial f(xi)} (yi, f(xi)) \quad (6)$$

Here r_{2m} is the differential rank function which can differentiate the fitness function as per Trees in gradient boosting mechanism.

$$\alpha = \text{argmin}_{\alpha} \text{L (yi,} f_{m-1} \text{(x)} + \alpha h_m \text{(x))} \quad (7)$$

Here alpha is the argument function, in this L is linear cross validation function. It is differentiate the over fitting activity of weights.

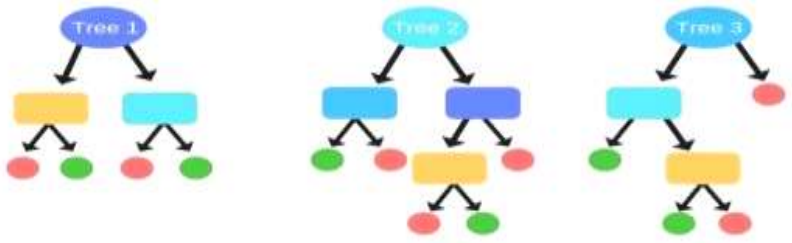


Figure 9 Tree structure in GBML [15].

$$Loss = \sum_{i=1}^{n} L(yi, f_{m-1}(xi) + h_m(xi)) + \sum_{j=1}^{T} \Omega(h_m(xj)) \quad (8)$$

After cross validation we want to estimate the loss function, here x, y are input parameters, Ω is fraud margin function. The selected dataset is estimating through following equation 8.

$$Loss=\sum_{i=1}^{n}\left[L(yi,f_{m-1}(xi))+\frac{\partial L}{\partial f_{m-1}^{xi}}(yi,f_{m-1}(xi))h_m(xi)+\frac{1}{2}\frac{\partial^2 L}{\partial^2_{f_{m-1}(xi)}}(yi,f_{m-1}(xi))h_m^2(xi)\right]+$$

$$\sum_{j=1}^{T}\Omega(h_m\,(xj))\Omega(h_{mT}) \quad (9)$$

Fig 9 & equation 9 is the GBML model training computations, these are explains about cloud interaction depth and arguments. The cloud is a time varying platform, when it moves to busy stage there may be a chance of frauds. This can handle the GBML method to prevent the busy stage of clouds using loss function, gain function equations.

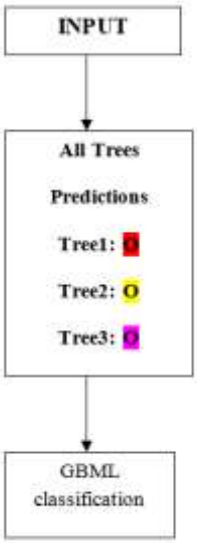


Figure 10 Tree classifier

$$\text{Loss} = -\frac{1}{2}\sum_{j=1}^{T}\left[\frac{G_j^2}{x_j+\lambda}\right]+\text{ET} \quad (10)$$

Gain = Loss before – Loss a filter split

$$= \text{- E} + \frac{1}{2}\left[\frac{G_L^2}{(H_R+\lambda)}+\frac{G_R^2}{(H_R+\lambda)}-\frac{(G_L+G_R)^2}{H_R+H_L+\lambda}\right] \quad (11)$$

Fig 10 explains about internal calculations with ET (exact time) and variable interactions validation, in this GBM assigns the number of trees and respective weights using this point predictor classify the influence of cloud parameters.

4. EXPERIMENTAL RESULTS

4.1. Dataset

DN- CON2 dataset is used in this work, this is input of both FCNN predictor and GBML classifier. The ULB group on big data and fraud detection datasets are available freely named as Kaggle, which is shown in table 1 clearly.

Table 2 Dataset features

1.	Data set	Multivariate
2.	Attributes	Categorical, Integer
3.	Associated function	Classification
4.	N.of instances	284997
5.	N.of Attributes	40
6.	Missing	N/A

Table: 1 explains about features of DN-CON2 consists of various instances like 285000 around, type of attributes are either by an integers or by categorical model, and in this datasets no missed data is placed.

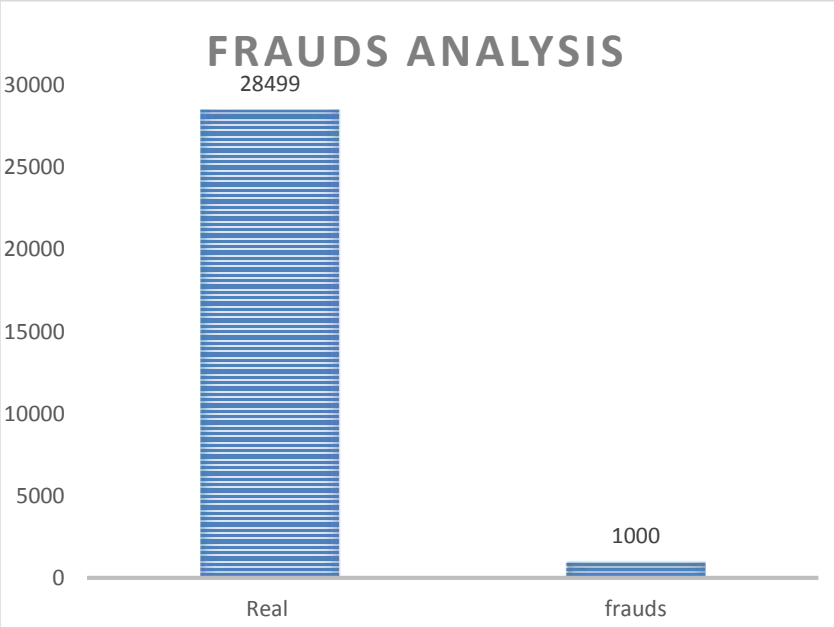


Figure 11 Data set distribution.

Time and over sampled fraud classes count is shown in fig 11, which consist of 3.12% all transactions represented by A_0, A_2, A_3, ……. A_n, above analysis is clearly explains about no of frauds and regular transactions.

Example:

```
(284807, 31)>  Time        V1        V2        V3        V4
V5        V6        V7  \
0   0.0 -1.359807 -0.072781  2.536347  1.378155 -0.338321  0.462388
0.239599

         V8        V9  ...         V21       V22       V23
V24  \
0  0.098698  0.363787  ...   -0.018307  0.277838 -0.110474
0.066928

        V25       V26       V27       V28  Amount  Class
0  0.128539 -0.189115  0.133558 -0.021053  149.62      0

>  False
```

The above dataset consists of 284807 rows and 31 columns. The column number 1 to 28 are the principal FCNN + GBML component. The main reason to attain these frauds, only one feature be taken as reference i.e. FCNN+GBML. The time and amount are the main class parameters there is no null value present in the dataset. As per proposed algorithm results 284315 class zero i.e normal transactions are identified and 492 class 1 i.e fraud transactions are identified.

4.2. Performance Analysis

DANCON2 and local datasets are being used to identify the transaction is fraud or not. The entire technique identify the 493 frauds out of 284997, which is a highly balanced that is 0.173 to solve this class FCNN and GBML distribution classes are applied into training and testing

sets. The entire dataset is split into training sets-2 and independent test-1. The comparison table, which is shown in below.

Table 3 Attributes

Variable name	Description	Type
A_0, A_2, A_3, .A_n,	Transaction features after FCNN	"Integer
Time	GBML	Integer
Amount	GBML trees	Integer
Class	Non fraudulent or fraudulent	0 or 1"

Table 3. Explains about GBML analysis and FCNN truncations fraud predictions, based on binary digital data computations. In this 0 and 1 represents FRAUD or NO FRAUD respectively.

Table 4 Comparison of algorithms

SVM	Linear regression	It is proven that SVM is good choice for solving variant data structures for fraud detection [22].
Regression	LR	Various credit card frauds are identified and compete with traditional methods.
ANN	Non-linear	Nonlinear regression with ANN provides the better results compared to linear models.
FCNN-GBML	Deep learning and machine learning	Using FCNN auto encoder predictor and GBML machine learning classifier can achieves the fraudulent transactions, these are best fitted for current technology.

Table 4 Explains about comparison algorithms, with respect to cloud disorders identifications, in this various models and its functionality is described based performance analysis. FCNN-GBML model can handle real-time problems like dynamic nature of clouds and variable environment of software Mis-functionalities. By using deep learning "FCNN" and machine learning "GBML" is utilized to solves the any type of problems which are explained clearly in above table

Table 5 confusion matrix.

Sl.No.		TP	FP	TN	FN
1.	SVM	342	2112	115174	235
2.	LR	303	1291	116001	271
3.	NN	385	2228	115048	199
4.	Non linear	431	3870	113409	152
5.	FCNN-GBML	359	1458	115794	256

Table: 4. Explains about True positive rate, false positive rate, True negative rate, false negative rate of all described methods "SVM, LR, NN, Nonlinear and FCNN-GBML". In this proposed method got more improvement compete with current models.

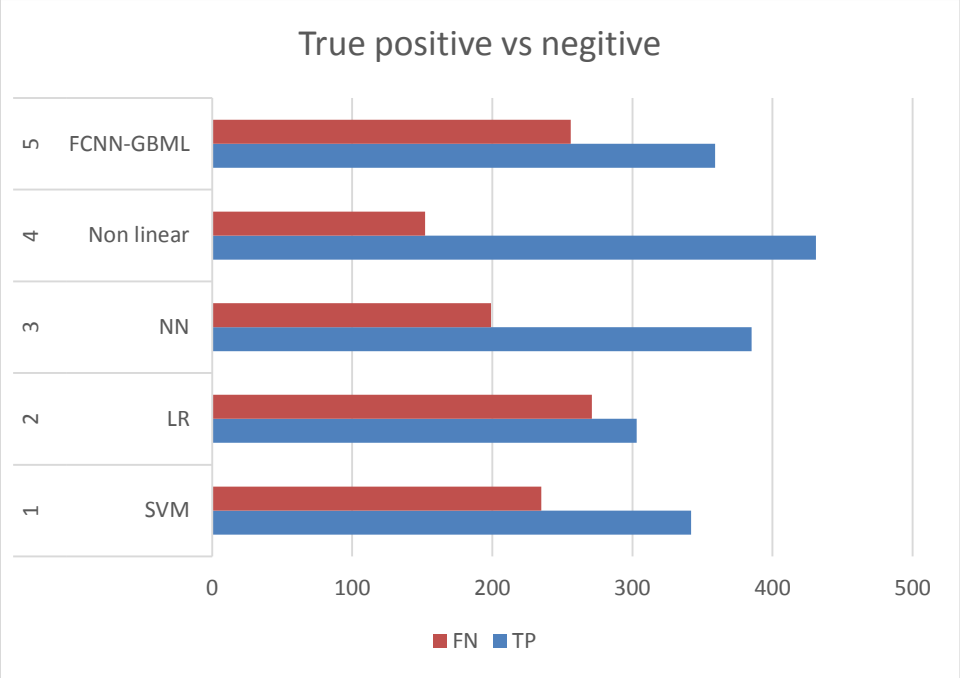


Figure 12 T_p analysis

Figure .12 explains about graphical representations of True positive rate vs negative rate, in this proposed method" FCNN-GBML" archives more improvement compared to survey methods.

Table 6 F1 scores

Model	F1 score
SVM	0.226
LR	0.270
NN	0.241
Non linear	0.177
FCNN-GBML	0.299

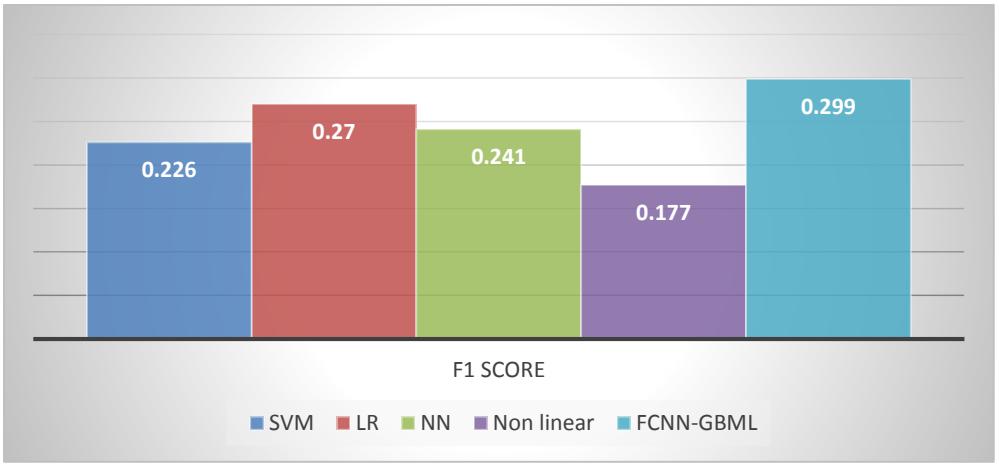


Figure 13 F1-score

Table: 5 and Figure 13 explains about computational achievement of F_1- score results, in this proposed method got 0.299 F_1- score. This is best improvement compared to reaming methods which are discussed.

Table 7 Accuracy

Model	Accuracy
SVM	0.9812
LR	0.982
NN	0.978
Non linear	0.965
FCNN-GBML	0.998

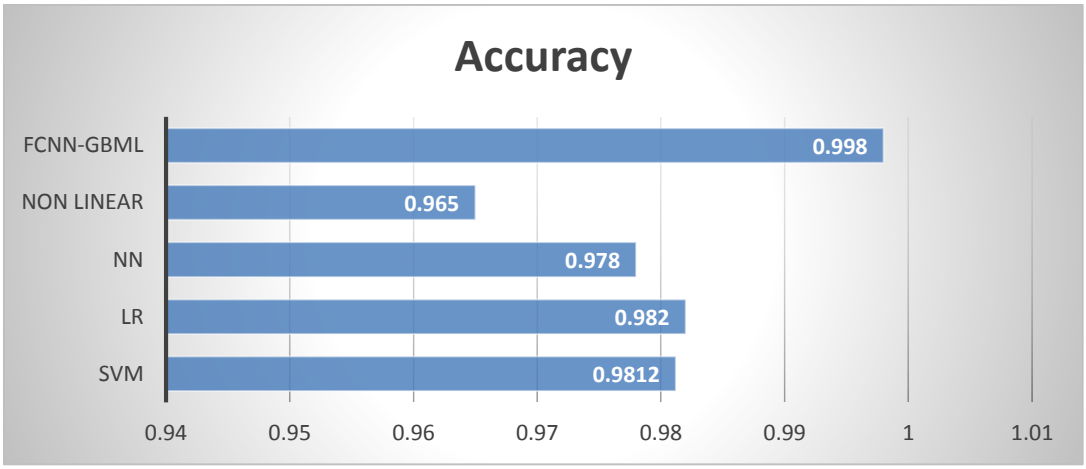


Figure 14 accuracy analysis

Table 6 and Figure .14 explains about Accuracy discriminations of FCNN-GBML method, in this 0.998 accuracy is achieved. Nonlinear methods, LR, NN, and SVM attains more accuracy but improvement is needed, proposed method has achieves more Nemours accuracy.

5. CONCLUSION

In this investigation a real time credit card fraud detection system on cloud computing has been implemented. It is useful for real time transactions, in this a real life database of credit card transaction utilized at deep learning (FCNN) auto encoder. The GBML is used to classify the frauds on clouds with effective manner. In this work the accuracy is 0.98 F1 score, 0.299 and TP is 359 is achieved. Which is a good improvement. This experiment further useful for real time cloud based fraud identification system. To monitor any time invariant behavior of clouds this application is helpful for future technologies.

REFERENCES

[1] J.P.Morgan. "Payments Fraud and Control Survey", PNC Financial Services Group, 2018.

[2] Boston Consulting Group. (2017). Global Payments 2017 – Deepening The Customer Relationship.

[3] Bose, Indranil, and Radha K. Mahapatra. "Business data mining—a machine learning perspective." Information and management 39.3 (2001): 211-225.

[4] TUNG, Hui-Hsuan, CHENG, Chiao-Chun, CHEN, Yu-Ying, et al. Binary Classification and Data Analysis for Modeling Calendar Anomalies in Financial Markets. In : Cloud Computing and Big Data (CCBD), 2016 7th International Conference on. IEEE, (2016). p. 116-121.

[5] Jacomo Corbo, Carlo Giovine, and Chris Wigley(2017, April). Applying analytics in financial institutions fight against fraud. McKinsey Analytics. Retrieved from https://www.mckinsey.com.

[6] Vapnik, V.: Statistical learning theory. Wiley, New York.(1998)

[7] I. Goodfellow, Y. Bengio, A. Courville.: Deep learning, Cambridge, Massachusetts, The MIT Press, (2016)

[8] Phyu, Thair Nu. "Survey of classification techniques in data mining." Proceedings of the International MultiConference of Engineers and Computer Scientists. Vol. 1. (2009).

[9] Bolton, Richard J., and David J. Hand. "Statistical fraud detection: A review." Statistical science (2002): 235-249.

[10] Zhou, Xun, et al. "A state of the art survey of data mining-based fraud detection and credit scoring." MATEC Web of Conferences. Vol. 189. EDP Sciences, 2018.

[11] John A. Stankovic. :Misconceptions about real-time computing. IEEE Computer, 21(10), 10-19 (1988).

[12] S. Benson Edwin Raj, A. Annie Portia.: Analysis on Credit Card Fraud Detection Methods. In: International Conference on Computer, Communication and Electrical Technology – ICCCET2011, 18th & 19th March, (2011)

[13] Martin, James.: Programming Real-time Computer Systems. Englewood Cliffs, NJ: Prentice-Hall Inc. p. 4. ISBN 0-13-730507-9.)(1965)

[14] Masoumeh Zareapoor, Seeja.K.R, and M.Afshar.Alam.: Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria. In: International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August (2012)

[15] Bhattacharyya, Siddhartha, et al. "Data mining for credit card fraud: A comparative study." Decision Support Systems 50.3 (2011).

[16] Ghosh, Sushmito, and Douglas L. Reilly. "Credit card fraud detection with a neural-network." System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on. Vol. 3. IEEE, (1994).

[17] Bakar, Nor Mazlina Abu, and Izah Mohd Tahir. "Applying multiple linear regression and neural network to predict bank performance." International Business Research 2.4 (2009): 176.

[18] Landi, Alberto, et al. "Artificial neural networks for nonlinear regression and classification." Intelligent Systems Design and Applications (ISDA), 2010 10th International Conference on. IEEE, (2010).

[19] Aleskerov, Emin, Bernd Freisleben, and Bharat Rao : Cardwatch: A neural network based database mining system for credit card fraud detection. Computational Intelligence for Financial Engineering (CIFEr), 1997., Proceedings of the IEEE/IAFE 1997. IEEE, 1997.

[20] Dorronsoro, Jose R., et al. : Neural fraud detection in credit card operations. IEEE transactions on neural networks 8.4 (1997).

[21] Seeja, K. R., and Masoumeh Zareapoor. "FraudMiner: A novel credit card fraud detection model based on frequent itemset mining." The Scientific World Journal 2014 (2014).

[22] Hassibi, Khosrow. "Detecting payment card fraud with neural networks." World Scientific Book Chapters (2000): 141-157.

[23] ALTMAN, Edward I., MARCO, Giancarlo, et VARETTO, Franco.: Corporate distress diagnosis: Comparisons using linear discriminant analysis and neural networks (the Italian experience). Journal of banking & finance, vol. 18, no 3, p. 505-529.(1994)

[24] D.W. Hosmer, S. Lemeshow : Applied Logistic Regression, 2nd Ed, Wiley-Interscience, (2000).

[25] GOH, King-Shy, CHANG, Edward, et CHENG, Kwang-Ting.: SVM binary classifier ensembles for image classification. In : Proceedings of the tenth international conference on Information and knowledge management. ACM. p. 395-402.(2001).

[26] Raju, K., Pilli, S.K., Kumar, G.S.S., Saikumar, K., Jagan, B.O.L.(2019). Implementation of natural random forest machine learning methods on multi spectral image compression, Journal of Critical Reviews6(5), pp. 265-273

[27] Wang, Z., Wang, N., Su, X., & Ge, S. (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. International Journal of Information Management, 50, 387-394.

[28] Giri, S., & Shakya, S. (2019). Cloud Computing and Data Security Challenges: A Nepal Case. International Journal of Engineering Trends and Technology, 67 (3), 146, 150.

[29] Garg, S., Singh, A., Kaur, K., Aujla, G. S., Batra, S., Kumar, N., & Obaidat, M. S. (2019). Edge computing-based security framework for big data analytics in VANETs. IEEE Network, 33(2), 72-81.

[30] Nayyar, A. (2019). Handbook of Cloud Computing: Basic to Advance research on the concepts and design of Cloud Computing. BPB Publications.