ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OPTIMIZED DEEP AUTO-ENCODER INTEGRATED WITH QUADRATIC SUPPORT VECTOR MACHINE FOR ENHANCED CREDIT CARD FRAUD DETECTION

DEEPIKA SIRMORIA [1], S. SENTHIL [2]
[1]Research Scholar, Computer Science and Engineering, REVA University
[2] Former Professor and Director, School of Computer Application, REVA University
Email: [1]deepikajaiswal9963@gmail.com,[2]dir.csa@reva.edu.in

ABSTRACT

Credit card fraud detection is a challenging research area in which many factors influence the performance of methods. The majority of credit card fraud detection systems relied on an examination of previous transactions. As long as changes in customer behaviour, we need different fraud detecting strategies. Every year, millions of rupees are lost due to a lack of awareness of changes and the fraud detection. For minimizing such loss, we need to develop and implement efficient framework which can adapt non-linear behaviours of transactions. In this paper, we used efficient and optimal deep auto encoders (DA) for optimal feature selection and then these features are given to nonlinear learning approach i.e. quadratic support vector machine (QSVM) for classifying the transaction as fraudulent or not. In this approach, iterative fine-tuning process is considered in testing phase which can update parameters of training model. The proposed method is tested using various training dataset ratios and the calculated sensitivity, specificity, and accuracy measurement parameters. We use real world dataset for classifying fraudulent and non-fraudulent transaction by focusing on the low-dimensionality, optimal feature selection and fine tuning. The proposed DA-QSVM solution achieves comparable performance values with existing state-of-the-art and costly solutions.

Keywords: *Credit Card Fraud, Non-Linearity, Fine- Tuning, Auto Encoder, Quadratic SVM.*

1. INTRODUCTION

Usage of credit card in online shopping through internet has amplified in entire global. And also large number of credit card Transactions (CCT) headed with fraud cases [1-3]. This scenario screwed to find different new techniques and methods need to be developing. The fraud is an unjust or criminal activity intended in personal gain [4-6]. Without having of cash in hand, we can do get services using credit card. Credit card Fraud detection (CCFD) is a strategy to decide whether a transaction is fraudulent or not fraudulent. The meaning of Credit Card Crime (CCC) [4,6] is of steal the identity of others and do fraudulent transaction. Actually, there are two kind of fraudulent transactions namely offline fraud and online fraud. Physical stolen the credit card at shopping centers is comes under offline fraud and stealing persons identities' such as credit card numbers, name of card holder, dates of expiry and passwords [6-8]. The detection and classification of credit card fraud detection is highly challenging with imbalanced data. In general normal transactions are more than fraudulent transactions [9,10]. Fraud identification model (FIM) [11,12] is most crucial for classification of minority- class (fraudulent transactions) apart from majority- class (Normal transaction) [6,13, 14). The Fig.1 gives the clear description of credit card usage scenario and sequence of steps are allows given in following Fig.1.

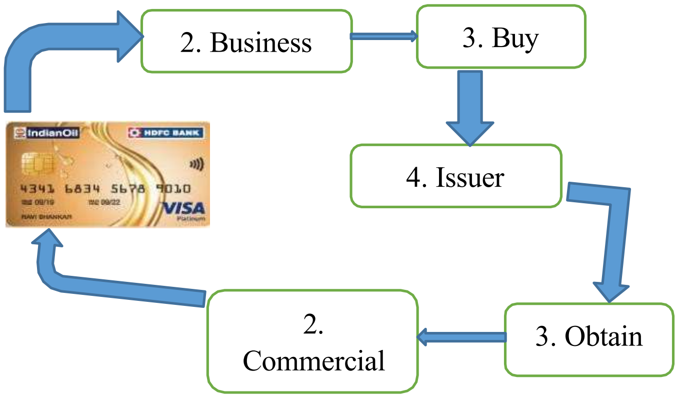


Fig. 1: Basic process flow of credit card usage.

Transactions are accepted or denied based on authorization. Card purchases continue to occur even though the authorising process is complete. And after permission expires, it can take some time. We must solve this problem, which includes classifying illegitimate and legitimate transactions. The dataset records both of these transactions. Last few years, the credit card fraud detection using machine learning becomes interesting research area to handle the problems [15-19]. Indeed, from literature, we understand that there are two approaches to identify and detect the fraud transactions: first one is supervised and un-supervised [2, 20-22]. The first one is performed to classify new transaction (normal or abnormal) based on transaction data record [15,20]. Some of the supervised credit card fraud detection methods as follows: Artificial Neural Networks [17,22], Support Vector Machines [16, 17,26], Random Forests [23,24], Bayesian Belief Networks [20], K-Nearest Neighbors [17,25] and Hidden Markov Models [26]. Similarly un-supervised approach is used to detect the hidden patterns in non-labeled transaction [27]. Some of un- supervised approaches are : As examples of the used unsupervised methods, SOMs (Self-Organized Maps) method and the K-Means method for problems associated with clustering.

The new research trends in CCF, is a kind of fight against cyber-crime [28] and it still in initial stage because of many barriers. Indeed, many research works used updated or existed datasets to investigate frauds, because of security reasons banks and financial organizations prohibit disclosure of their sensitive data for CCT, which

Credit card transactions, in general, consist of the following phases.

1. By using a credit card to buy goods, the cardholder must apply the card's details.
2. The dealer accepts the card and submits the information to the bank for approval.
3. The bank contacts the card issuer with the order.
4. The cardholder signs off on the transaction's specifics.
5. The bank communicates the merchant's answer.
6. The merchant verifies and completes the transfer. In this sequence of steps, stage (Authorization) carries the highest transaction risk, requiring the application of all fraud scoring algorithms.

is restrictions the CCFD research [29]. In addition, some metrics will be used to test efficiency of model namely: accuracy, specificity and sensitivity. Here accuracy and specificity will be used for measuring prediction correctness which is not enough to conclude the efficiency of model. Hence sensitivity is another metric used for testing the efficiency of model [6,26]. In addition F-Score is another metric which can combine sensitivity and precision metrics and gives more accurate prediction in classification [30,31]. Many researchers designed models without considering the complete behaviour of cardholder hence it is inadequate start of fraudulent detection [19, 31, 32]. Briefly, selection of most dominate features for fraud classification and detection models [33,34] are necessary for real time applications. One of the interesting fact that fraud cases(minority- class) are rare events which is most difficult to identify. Therefore, fraud case classification in imbalanced dataset is a big challenge. So final conclusion from literature is efficient fraud detection model design is depends on hypermeters and most dominant features set.

In this paper, we suggest an efficient hybrid model for credit card fraud detection using deep encoders, quadratic support vector machine and iterative fine tuning process. This model combines advantages of the robustness of many machine learning methods and techniques. Moreover, to overcome issues imbalanced dataset are resolved using fine tuning process.

The rest of this paper is structured as follows: Section 2 presents our proposed model based on a hybrid approach. Experiments and discussion of the obtained results are detailed in Section 3. The last section concludes the paper with some

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

perspectives.

2. PROPOSED FRAMEWORK

The proposed framework ensembles deep auto-encoder and quadratic support vector machine (QSVM)

2.1 Deep auto encoder

The deep auto encoder is an unsupervised tool for representing features with several hidden layers. When compared to other neural network-based approaches, this one is successful. Weights for hidden layers are not calculated manually in neural concepts; rather, they are automatically modified based on input data. Credit card fraud identification datasets include a variety of characteristics, including year, timeline, transaction date, volume, number of purchases, and number of declines.

Taking both of these characteristics into account when developing the model results in the over fitting problem. To fix this problem, deep features are compressed to small dimensions with marginal error while weights are simultaneously updated. Deep features are derived from the considered dataset in order to identify strong motivational features. Fig. 2 illustrates the efficient design of a five-layer stacked auto-encoder.

Table 1: The auto encoder framework - Numeric details.

Type	No. of features	Neurons
IL	15000	8000
HL_1	15000	8000
HL_2	15000	8000
HL_3	15000	8000
HL_4	15000	8000
HL_5	15000	8000
OL	15000	2

IL- Input layer, HL- hidden layer, OL-Output layer The auto encoder is composed of two steps, the first of which is data compounded by weights and biases, and the second of which represents a nonlinear function such as sigmoid or relu as seen in eqn. The mean square error is minimised during the operation by using a more reliable approach known as back propagation.

$$(xx) = sig(Wxx + b) \quad (3)$$

$$xx = s(W(h(xx)) + b) \quad (4)$$

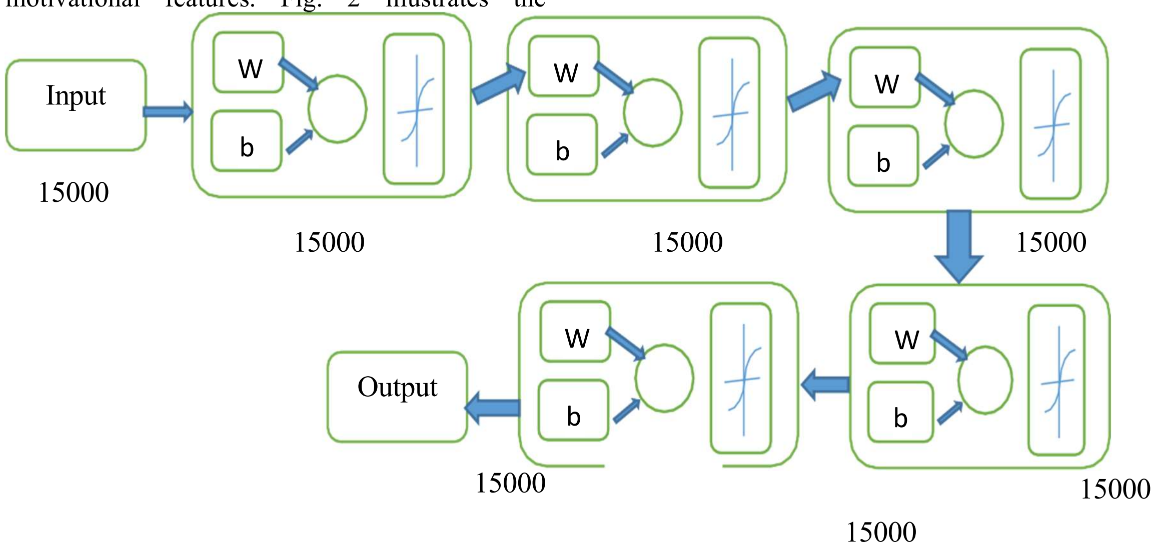


Fig.2: Five Hidden Layer Architecture Of Deep Auto Encoder.

The linear SVM is ineffective for high-dimensional features in which certain training samples converge

In the auto-encoder, the first hidden layer receives the input x, while the subsequent hidden layers receive the input from the previous hidden layer, as shown in the following Eqn.5 and 6.

Here, n denotes the number of encoding layers, and x^l,W^l, and b^l denote the corresponding layer's data, weights, and biases.

$$h(x)^{(l+1)} = sigm(W^l x^l + b^l) \quad (5)$$

$$^{(n+l+1)} = si(W^{(n-l)} x^{(n+l)} + b^{(n-l)} \quad (6)$$

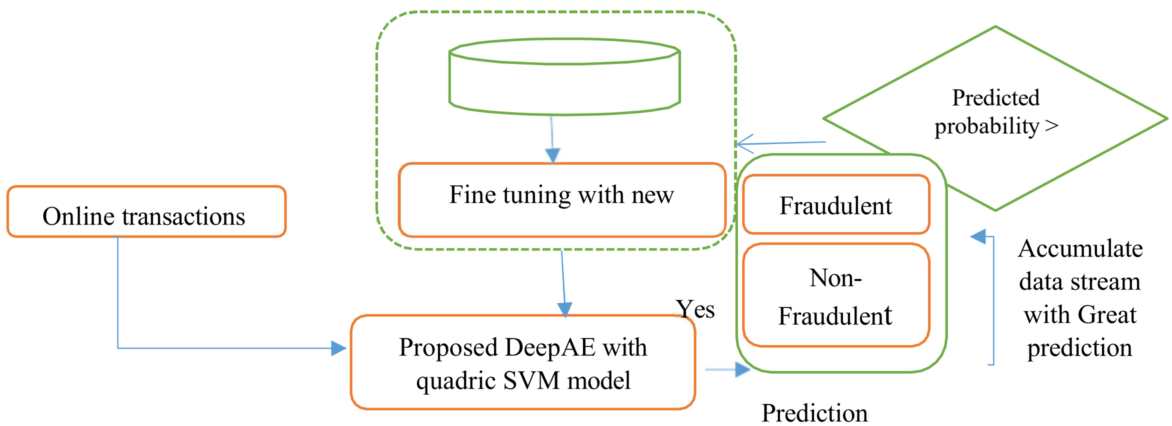
The DAE is conditioned for 500 epochs and L2 regularisation and sparsity control was implemented with a sigma value of 0.06; this ensures that each neuron outputs 0.6 on average over the training samples. The MSE is decreased from 15 to 2 after 400 epochs, and the error is reported as 0.0084 of the training period at the final epoch.

2.2 Use quadratic SVM for action learning

in order to separate two groups that are often straight lines. In non-linear SVM with two groups, the problems posed by linear SVM are overcome. SVM was originally designed for binary classification. When different groups are represented by SVMs, the issue of data imbalance arises. And if the optimal hyper line is used, the cost exponentially increases. As a result, we used quadratic SVMs in this paper to improve accuracy and speed.

$$\frac{(M-1)}{MN} = (M-1) \tag{7}$$

Two methods are available in multi-class SVMs: one-versus-one (OvO) and one-versus-all (OvA). OvO requires the training of "N" classifiers for "M" classes, which is prohibitively costly computationally and unsuitable for real-time applications such as credit card fraud detection. Credit card fraud identification uses two types of data: positive sample training data and negative sample training data. In this case, OvA is preferable for achieving greater precision.



Online data and iterative training

Fig. 3: The proposed Auto encoder-quadratic SVM frame work.

2.3 Metrics

There are many metrics in the literature that are used to quantify the efficacy of fraud detection, including precision [35, 36, 37, 38]. ii. the recall[35, 37, 39]
iii. Specificity [35, 39] iv. [35, 37, 40, 41] F-measure
v. the layer under the precision–recall curve (AUC- PR) vi. The receiver working characteristic curve's field under the curve (AUC-ROC) [35, 36, 39, 40].

3.2 A comparative review

This segment compares the proposed DA-QSVM for detecting credit card fraud. The comparative analysis is performed by varying the knowledge gain parameter's threshold of training features. The feature size is set to 20, 22, and 25 in this case.

3.2.1 A comparative study of the 18-point function

Vii. Particularity viii. Accuracy. In this work, we will focus on analysing the metrics that are considered the most relevant in matters of fraud detection i.e. Sensitivity 2. Specificity 3. Accuracy

3. 4. RESULTS AND DISCUSSIONS

The proposed method is considered real dataset of credit card fraud detection which contains 25 features. Any method or framework performance is purely depends on number features that are used for training. The proposed solutions is considered different combination and different ratio of training to test efficacy of proposed method.

3.1 Techniques for Comparative Fraud Detection

3.1.1 The Pro version of the K-nearest Neighbor Algorithm is used to identify deviations with respect to the target instance and is simple to implement.

Cons: detecting fraud is contingent upon memory deficits

3.1.2 DNN: Advantage: it can identify illegal transactions automatically, i.e. during the transaction.

Cons: It cannot have accuracy on such purchases.

3.1.3 Neural Network: Advantage: Using prior transactions to identify fraud in real-time credit card transactions.

Cons: There are several sub-techniques to remember, making it impossible to determine which technique is appropriate.

3.1.4 DBN classifier dependent on MF-EWA:

Pro: It uses relatively little memory during the credit card fraud detection process and performs well on massive datasets.

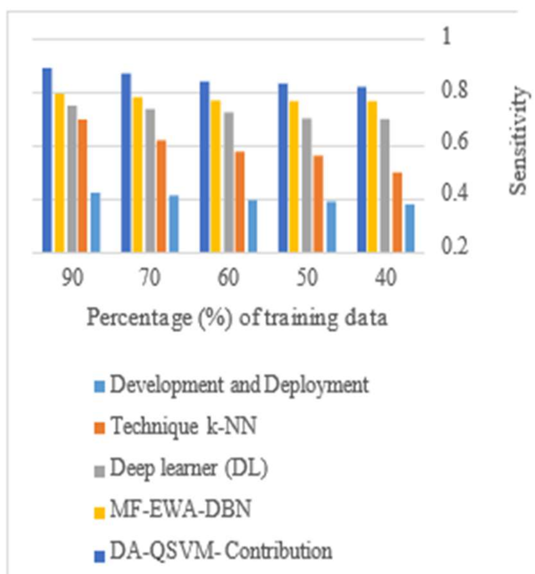
Cons: It is not as precise as other techniques of detecting deviations.

3.1.5 Deep Learning is advantageous for analysing and learning from massive unsupervised datasets of complex trends.

Cons: The deep learning library does not have all algorithms.

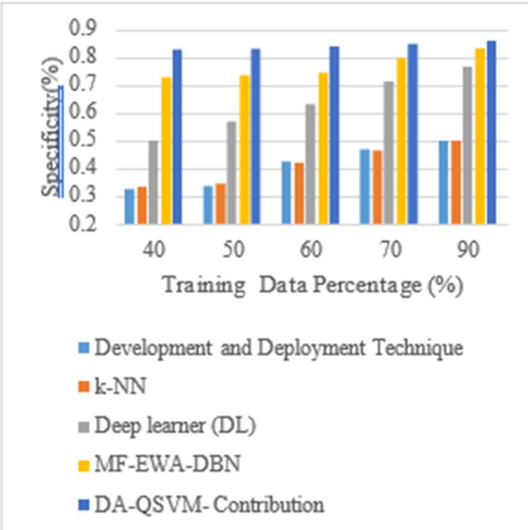
size

The proposed methodology is applied by considering 18 features of dataset. The proposed DA-QSVM is experimented with different ration of training set like 50, 60, 70, 80 and 90. The sensitivity, specificity and accuracy values are proportional to high training ratio. As we increase training ration, the performance of proposed method is increased. The proposed DA- QSVM method performance is compared with existing state-of-art methods like DDT [44], K-NN [45], Deep learner [46] and MF-EWA based DBN classifier. The sensitivity analysis is depicted in Fig.
4. With different rations of training phase ratios, the average sensitivity values existed methods like DDT, K-NN , Deep learner and MF-EWA based DBN classifier are 0.3964, 0.59226, 0.72254, 0.77946 respectively. The proposed DA-QSVM average sensitivity is 0.85164 which show good efficacy when compared to existing methods. Similarly corresponding specificity values of existing methods like DDT, K-NN , Deep learner and MF- EWA based DBN classifier are 0.41098, 0.41312, 0.63624, 0.768738 and proposed method specificity value is 0.84442 which is higher than existing. The accuracy is another important measurement factor considered to check the performance of proposed method. This accuracy of proposed method is also higher than existing methods. The average accuracy values of existing methods like Development and Deployment Technique (DDT), k-NN , Deep learner and MF-EWA based DBN classifier are 0.490.42, 0.6137, 0.745, 0.77834 and proposed method average accuracy value is 0.85248 which shows superiority when compared with other existing methods. The one of main reason for this is the dataset is grouped into some segments and trained the network. Another one is self-retrain the dataset. The benefit of auto encoders and QSVM is utilized effectively.

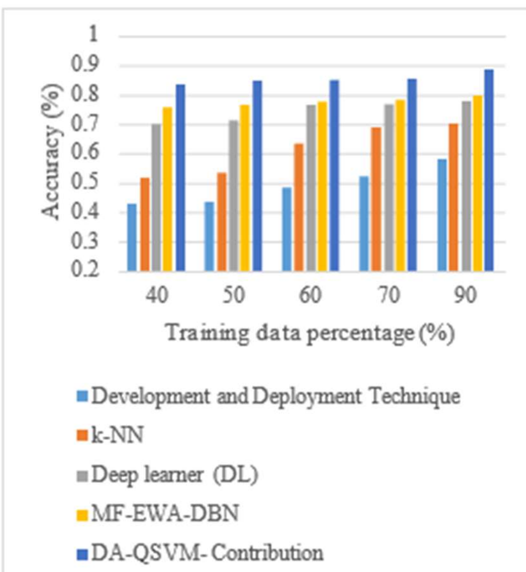


(a)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



(b)



(c)

Fig. 4: Comparative analysis of the proposed DA-QSVM for the feature size as 20, (a) sensitivity, (b) specificity, and (c) accuracy.

The Table 2 gives the details of average sensitivity, specificity and accuracy values of existing and proposed method. This table details clearly shows the high performance of proposed method when compare with existing methods.

Table 2: Proposed method comparison with state-art- of existing methods in terms of sensitivity, specificity and accuracy when features are 18.

Methods	Sensitivit	Specificit	Accurac
Development and Deployment	0.3964	0.41098	0.49042
k-NN	0.59226	0.41312	0.6137
Deep learner (DL)	0.72254	0.63624	0.745
MF-EWA-DBN	0.77946	0.768738	0.77834
DA-QSVM-Contribution	0.85164	0.84442	0.85248

when compared with other existing methods. The one of main reason for this is the dataset is grouped into some segments and trained the network. Another one is self-retrain the dataset. The benefits of auto encoders and QSVM are utilized effectively.

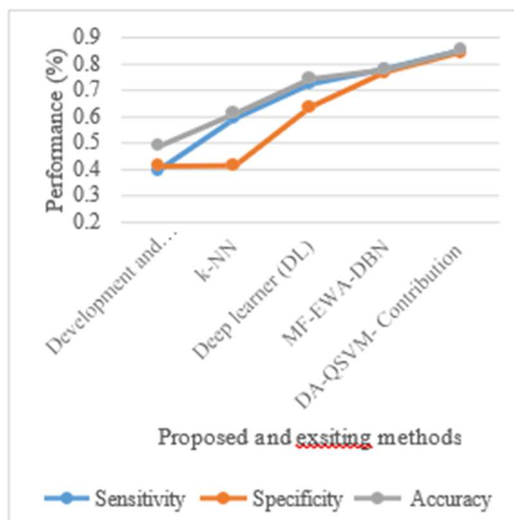


Fig.5: Comparison Graph Of Proposed And Existing Methods In Terms Of Average Sensitivity, Specificity And Accuracy For The Feature Size As 20.

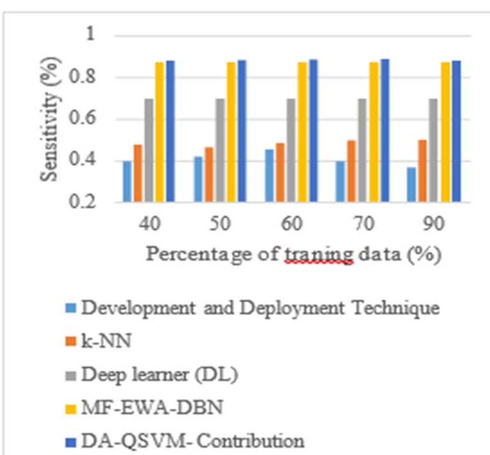
The Table 2 and Fig.5 exhibits the performance of proposed method over existing methods in terms of average sensitivity, specificity and accuracy when features are 22.

3.2.2 Comparative analysis for the feature size as 22

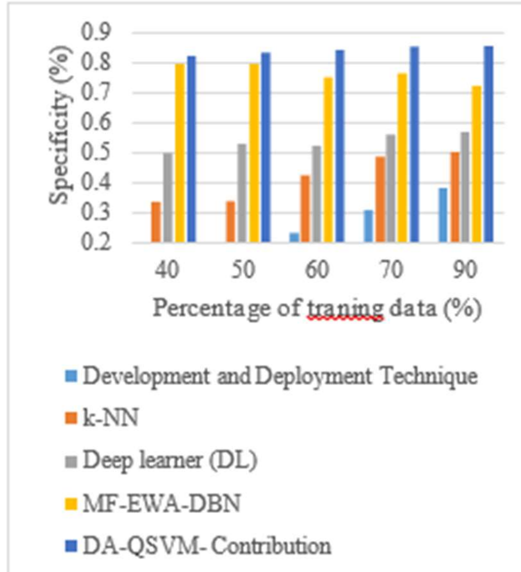
The proposed methodology is applied by

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

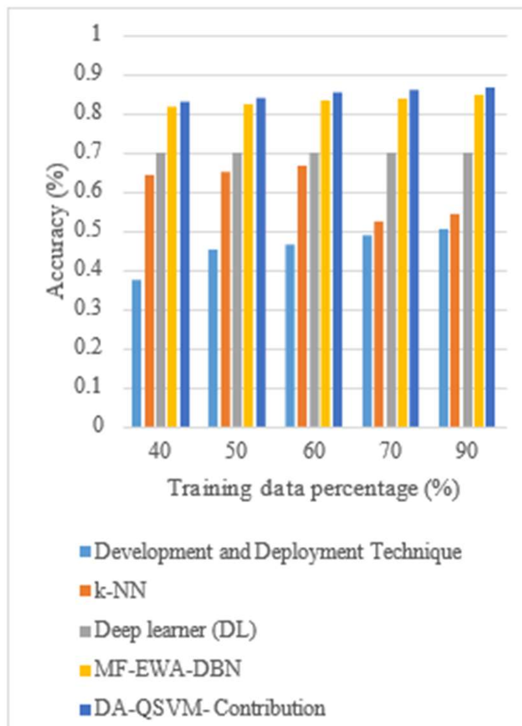
considering
22 features of dataset. Similar to 18 features experiment, we are proceed and calculated respective parameters. In this case also the proposed DA- QSVM method performance is compared with existing state-of-art methods like DDT, K-NN , Deep learner and MF-EWA based DBN classifier. The sensitivity analysis is depicted in Fig.6. With different rations of training phase ratios, the average sensitivity values existed methods like DDT, K-NN , Deep learner and MF-EWA based DBN classifier are 0.4089, 0.4853, 0.70028, 0.87534 respectively. The proposed DA-QSVM average sensitivity is 0.0.88402 which show good efficacy when compared to existing methods. Similarly corresponding specificity values of existing methods like DDT, K-NN , Deep learner and MF-EWA based DBN classifier are 0.23272, 0.41556, 0.53808, 0.76604 and proposed method specificity value is 0.8415 which is higher than existing. The accuracy is another important measurement factor considered to check the performance of proposed method. This accuracy of proposed method is also higher than existing methods. The average accuracy values of existing methods like DDT, K-NN , Deep learner and MF-EWA based DBN classifier are 0.45744, 0.60752, 0.70026, 0.83076 and proposed method average accuracy value is 0.85228 which shows superiority



(a)



(b)



(c)

Fig. 6: Comparative analysis of the proposed DA-QSVM for the feature size as 22, (a) sensitivity, (b) specificity, and (c) accuracy.

Table 3: Proposed method comparison with state-art- of existing methods in terms of sensitivity, specificity and accuracy when features are 22.

Methods	Sensitivity	Specificity	Accuracy
Development and Deployment Technique	0.4089	0.23272	0.45744
k-NN	0.4853	0.41556	0.60752
Deep learner (DL)	0.70028	0.53808	0.70026
MF-EWA-DBN	0.87534	0.76604	0.83076
DA-QSVM-Contribution	0.88402	0.8415	0.85228

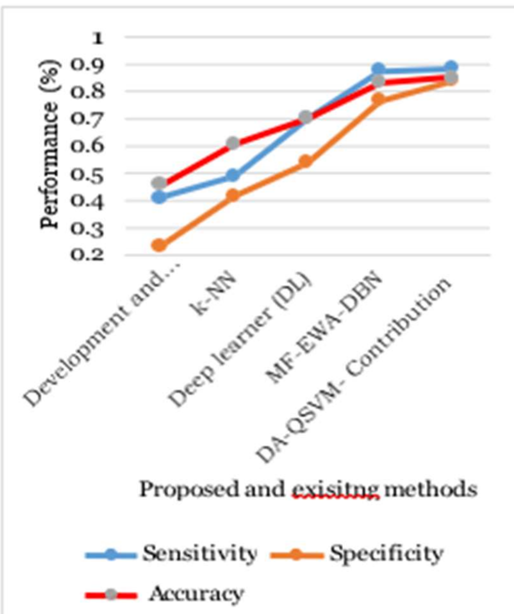


Fig.7: Comparison Graph Of Proposed And Existing Methods In Terms Of Average Sensitivity, Specificity And Accuracy For Feature Size 22.

The Table 3 and Fig.7 exhibits the performance of proposed method over existing methods in terms of average sensitivity, specificity and accuracy when features are 22.

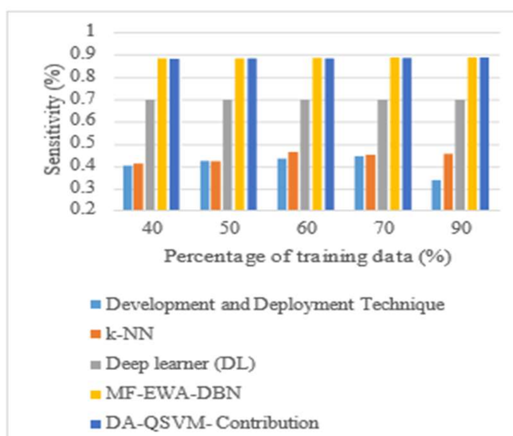
3.2.3 Comparative analysis for the feature size as 25

The proposed methodology is applied by considering
25 features of dataset. Similar to 18 features experiment, we are proceed and calculated respective parameters. In this case also the proposed DA- QSVM method performance is compared with existing state-of-art methods like DDT, K-NN , Deep learner and MF-EWA based DBN classifier. The sensitivity analysis is depicted in Fig.8 . With different rations of training phase ratios, the average sensitivity values existed methods like DDT, K-NN , Deep learner and MF-EWA based DBN classifier are 0.40568, 0.44172, 0.70026, 0.88572 respectively.

The proposed DA-QSVM average sensitivity is 0.88666 which show good efficacy when compared to existing methods. Similarly corresponding specificity values of existing methods like DDT, K- NN , Deep learner and MF-EWA based DBN classifier are 0.46662, 0.57578, 0.66536, 0.76244,

and proposed method specificity value is 0.79901 which is higher than existing. The accuracy is another important measurement factor considered to check the performance of proposed method. This accuracy of proposed method is also higher than existing methods. The average accuracy values of existing methods like DDT, K-NN , Deep learner and MF-EWA based DBN classifier are 0.46026, 0.58796, 0.70032, 0.83418 and proposed method

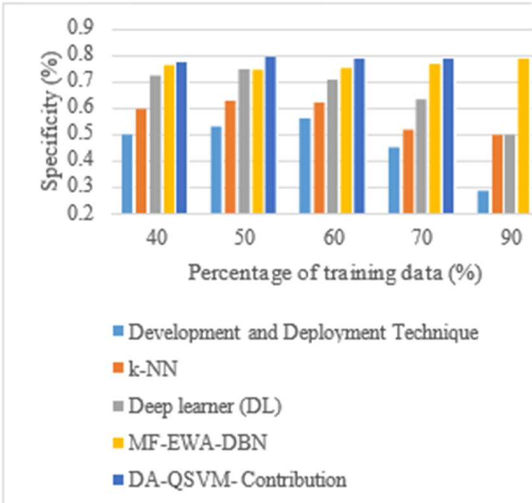
average accuracy value is 0.0.85406 which shows superiority when compared with other existing methods. The one of main reason for this is the dataset is grouped into some segments and trained the network. Another one is self-retrain the dataset. The benefits of auto encoders and QSVM is utilized effectively.



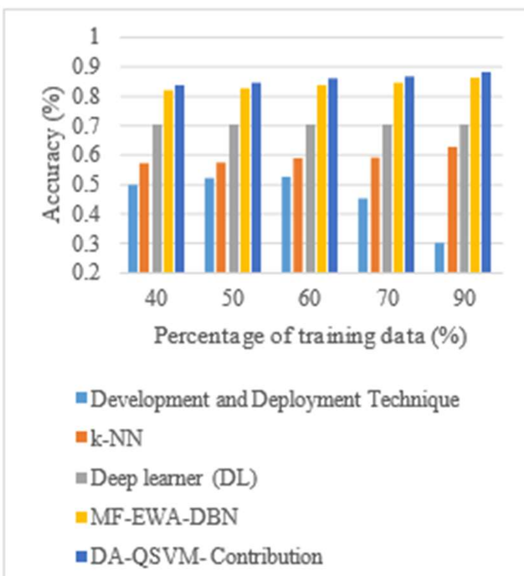
(a)

Journal of Theoretical and Applied Information Technology
15th January 2025. Vol.103. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



(b)



(c)

Fig.8: Comparative Analysis Of The Proposed DA-QSVM For The Feature Size As 25, (A) Sensitivity, (B) Specificity, And (C) Accuracy.

Table 4: Proposed Method Comparison With State-Art-Of Existing Methods In Terms Of Sensitivity, Specificity And Accuracy When Features Are 25.

Methods	Sensitivity	Specificity	Accuracy
Development and Deployment Technique	0.40568	0.46662	0.46026
k-NN	0.44172	0.57578	0.58796
Deep learner (DL)	0.70026	0.66536	0.70032
MF-EWA-DBN	0.88572	0.76244	0.83418
DA-QSVM-Contribution	0.88666	0.7901	0.85406

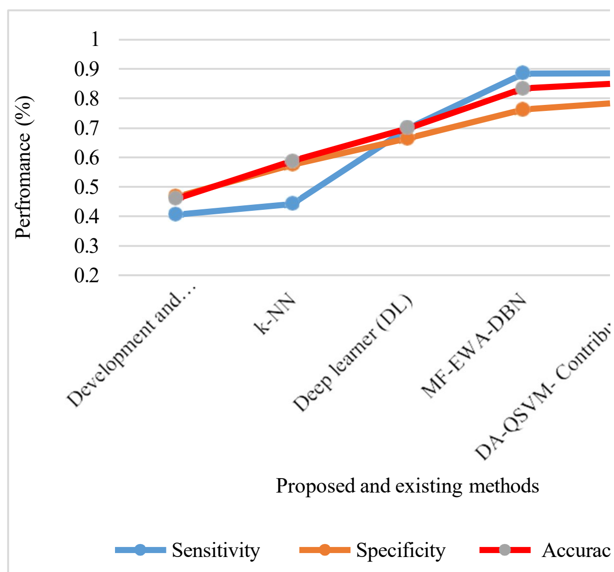


Fig.9: Comparison Graph Of Proposed And Existing Methods In Terms Of Average Sensitivity For Feature Size Is 25.

The Table 4 and Fig.9 exhibits the performance of proposed method over existing methods in terms of average sensitivity, specificity and accuracy when features are 25.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. CONCLUSIONS

The main motivation of this paper is to construct optimal and low dimensional feature set and considering non-linear approach for classifying fraudulent transaction. The detection based on following perspectives: fraud type, optimal features, total number of features considered for training, non- linearity and performance. Our framework in context of credit card fraud detection, it quite simple, general and can readily be extruded to other applications characterized by non-linear transaction. The proposed solution is intrinsically depends on availability of features with respect to fraudulent transaction. The proposed framework tested with different training rations and different feature set. The considered dataset consist of 25 features and there is a chance of 25! Combination of feature set is possible for training. In that all cases the proposed solution is shown its superiority when compared with existing state-of-art methods. The fine tuning of proposed framework based on Accumulate data with High prediction calculation is given better results.

REFERENCES

[1]. [1] "2018 INTERNET CRIME REPORT, " pp.1–28.
[2]. [2] Carcillo F, Le Borgne Y-A, Caelen O, Bontempi G. Streaming active learning strategies for real-life credit card frauddetection: assessment and visualization. Int.Data Sci. Anal. 2018. https://doi.org/10.1007/s41060-018-0116-z.
[3]. Zheng L, Liu G, Yan C, Jiang C. Transaction fraud detection based on total order relation and behavior diversity. IEEE Trans. Comput. Soc. Syst. 2018;5(3): 796–806. https://doi.org/10.1109/TCSS.2018.2856910
[4]. ACFE, "Report to the Nations 2018 Global Study on Occupational Fraud and Abuse,"2019. DOI: 10.1002/9781118929773.oth1.
[5]. Xuan S, Liu G, Li Z, Zheng L, Wang S, JiangC. Random forest for credit card fraud detection. ICNSC 2018 - 15th IEEE Int. ConfNetworking, Sens. Control 2018: 1–6. https://doi.org/10.1109/ICNSC.2018.8361343
[6]. Makki S, Assaghir Z, Taher Y, Haque R, Hacid MS, Zeineddine H. An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection. IEEE Access 2019;7:93010–22. https://doi.org/10.1109/ ACCESS.2019.2927266.
[7]. West J, Bhattacharya M. Intelligent financial fraud detection: A comprehensive review. Comput. Secur. 2016;57:47–66. https://doi.org/10.1016/j. cose.2015.09.005
[8]. Baader G, Krcmar H. International Journal of Accounting Information Systems Reducing false positives in fraud detection : Combining the red flag approach with process mining. Int. J. Account. Inf. Syst. 2018;31(June):1–16. https://doi. org/10.1016/j.accinf.2018.03.004
[9]. Krawczyk B. Learning from imbalanced data open challenges and future directions. Prog. Artif.Intell. 2016;5(4):221–32. https://doi.org/10.1007/ s13748-016-0094-0
[10]. de S´a AGC, Pereira ACM, Pappa GL. A customized classification algorithm for credit card fraud detection. Eng. Appl. Artif. Intell. 2018. https://doi.org/ 10.1016/j.engappai.2018.03.011.
[11]. Johnson JM, Khoshgoftaar TM. Survey on deep learning with class imbalance. J. Big Data 2019. https://doi.org/10.1186/s40537-019-0192-5.
[12]. Walke A. Comparison of Supervised and Unsupervised Fraud Detection, no. September 2013. Springer International Publishing; 2019.
[13]. Salazar A, Safont G, Vergara L. Semi-Supervised Learning for Imbalanced Classification of Credit Card Transaction. Proc. Int. Jt. Conf. Neural Networks 2018;2018-July:1–7. https://doi.org/10.1109/IJCNN.2018.8489755
[14]. Zareapoor M, Shamsolmoali P. Boosting prediction performance on imbalanced dataset. Int. J. Inf. Commun. Technol. 2018. https://doi.org/10.1504/ IJICT.2018.090556.
[15]. Mahmoudi N, Duman E. Detecting credit card fraud by Modified Fisher Discriminant Analysis. Expert Syst. Appl. 2015. https://doi.org/10.1016/j. eswa.2014.10.037.
[16] Ali Shah A, Khurram Ehsan M, Ishaq K, Ali Z, Shoaib Farooq M. An Efficient Hybrid Classifier Model for Anomaly Intrusion Detection System. IJCSNS Int. J. Comput. Sci. Netw. Secur. 2018

[17] Popat RR, Chaudhary J. A Survey on Credit Card Fraud Detection Using Machine Learning. In: Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018; 2018. https://doi.org/10.1109/ ICOEI.2018.8553963.

[18] Zafar A, Sirshar M. A Survey on Application of Data Mining Techniques; It's Proficiency In Fraud Detection of Credit Card. Res. Rev. J. Eng. Technol. 2018.

[19] Carta S, Fenu G, ReforgiatoRecupero D, Saia R. Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model. J. Inf. Secur. Appl. 2019;46:13–22. https://doi.org/10.1016/j.jisa.2019.02.007.

[20] Kültür Y, Ça˘glayan MU. Hybrid approaches for detecting credit card fraud. Expert Syst 2017. https://doi.org/10.1111/exsy.12191.

[21] Carcillo F, Le Borgne YA, Caelen O, Kessaci Y, Obl´e F, Bontempi G. Combining unsupervised and supervised learning in credit card fraud detection. Inf. Sci. (NY). 2019. https://doi.org/10.1016/j.ins.2019.05.042.

[22] Rushin G, Stancil C, Sun M, Adams S, Beling P. Horse race analysis in credit card fraud - Deep learning, logistic regression, and Gradient Boosted Tree. In: 2017 Systems and Information Engineering Design Symposium, SIEDS 2017; 2017. https://doi.org/10.1109/SIEDS.2017.7937700.

[23] Sohony I, Pratap R, Nambiar U. Ensemble learning for credit card fraud detection. In: ACM International Conference Proceeding Series; 2018. https://doi.org/10.1145/3152494.3156815.

[24] Jurgovsky J. Sequence classification for credit-card fraud detection. Expert Syst. Appl. 2018. https://doi.org/10.1016/j.eswa.2018.01.037.

[25] Bahl A. Recursive feature elimination in random forest classification supports nanomaterial grouping. NanoImpact 2019. https://doi.org/10.1016/j. impact.2019.100179.

[26] Robinson WN, Aria A. Sequential fraud detection for prepaid cards using hidden Markov model divergence. Expert Syst. Appl. 2018;91:235–51. https://doi.org/ 10.1016/j.eswa.2017.08.043.

[27] Caron M, Bojanowski P, Joulin A, Douze M. Deep clustering for unsupervised learning of visual features. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); 2018. https://doi.org/10.1007/978-3-030-01264-9_9.

[28] Abdullah FM. Using big data analytics to predict and reduce cyber crimes. Int. J. Mech. Eng. Technol. 2019.

[29] Zareapoor M, Shamsolmoali P. Application of credit card fraud detection: Based on bagging ensemble classifier. In: Procedia Computer Science; 2015. https://doi. org/10.1016/j.procs.2015.04.201.

[30] [34] Lever J, Krzywinski M, Altman N. Classification evaluation. Nat. Methods 2016. https://doi.org/10.1038/nmeth.3945.

[31] Correa Bahnsen A, Aouada D, Stojanovic A, Ottersten B. Feature engineering strategies for credit card fraud detection. Expert Syst. Appl. 2016. https://doi. org/10.1016/j.eswa.2015.12.030.

[32] Salazar A, Safont G, Rodriguez A, Vergara L. New Perspectives of Pattern Recognition for Automatic Credit Card Fraud Detection. In: Encyclopedia of Information Science and Technology, Fourth Edition; 2017.

[33] Nami S, Shajari M. Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors. Expert Syst. Appl. 2018. https://doi.org/10.1016/j.eswa.2018.06.011.

[34] Zareapoor M, Shamsolmoali P, Kumar Jain D, Wang H, Yang J. Kernelized support vector machine with deep learning: An efficient approach for extreme multiclass dataset. Pattern Recognit. Lett. 2018. https://doi.org/10.1016/j.patrec.2017.09.018

[35] F. Carcillo , Y.A. Le Borgne , O. Caelen , G. Bontempi , Streaming active learning strategies for real-life credit card fraud detection: assessment and visual- ization, Int. J. Data Sci. Anal. 5 (2018) 1–16 .

[36] N. Carneiro , G. Figueira , M. Costa , A data mining based system for credit-card fraud detection in e-tail, Decis. Support Syst. 95 (2017) 91–101 .

[37] V. Chandola , A. Banerjee , V. Kumar , Anomaly detection: a survey, ACM Comput. Surv. 41 (3) (2009) 15 .

[38] A. Dal Pozzolo , G. Boracchi , O. Caelen , C. Alippi , G. Bontempi , Credit card fraud detection: a realistic modeling and a novel learning strategy, IEEE Trans. Neural Netw. Learn. Syst. 29 (2017) 3784–3797 ..

[39] A. Dal Pozzolo , O. Caelen , G. Bontempi , When is undersampling effective in unbalanced classification tasks? in: Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Springer, 2015, pp. 200–215 .

[40] A. Dal Pozzolo , O. Caelen , Y.A. Le Borgne ,S. Waterschoot , G. Bontempi , Learned lessons in credit card fraud detection from a practitioner perspective, Expert Syst. Appl. 41(10) (2014) 4 915–4 928

[41] J. Davis , M. Goadrich , The relationship between precision-recall and ROC curves, in: Proceedings of the 23rd International Conference on Machine Learning, ACM, 2006, pp. 233–240

[42] Y. Freund , R. Schapire , N. Abe , A short introduction to boosting, Jpn Soc. Artif. Intell. 14 (771–780) (1999) 1612 .

[43] K. Fu , D.Cheng , Y. Tu , L. Zhang , Credit card fraud detection using convolutional neural networks, in: International Conference on Neural Information Processing, Springer, 2016, pp. 4 83–4 90

[44]K. Fu , D. Cheng , Y. Tu , L. Zhang , Credit card fraud detection using convolutional neural networks, in: International Conference on Neural Information Processing, Springer, 2016, pp. 4 83–4 90

[45]Nuno Carneiro, Gonc¸alo Figueira, and Miguel Costa, "A data mining based system for credit-card fraud detection in e-tail", Decision Support Systems, vol.95, pp.91-101, March 2017.

[46]Min-Ling Zhang and Zhi-Hua Zhou, "A k- nearest neighbor based algorithm for multi- label classification," 2005 IEEE International Conference on Granular Computing, Beijing, 2005, pp. 718-721 Vol. 2.
Hinton, G.E., “Deep belief networks,” Scholarpedia, vol. 4, no. 5, pp. 5947, 2009.

[47] Deepika, S., & Senthil, S. (2022). Credit card fraud detection using moth-flame earth worm optimisation algorithm-based deep belief neural network. International Journal of Electronic Security and Digital Forensics, 14(1), 53. https://doi.org/10.1504/ijesdf.2022.120021