iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VII **Month of publication:** July 2023

DOI: https://doi.org/10.22214/ijraset.2023.54891

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

A Succinct Analysis of Deep LSTM Model-Based Credit Card Fraud Detection

Swati Jadav[1], Manoj Patil[2]
Department Computer Engineering, Mumbai University

Abstract: ***More people today use credit cards to buy their essentials thanks to technological advancements, which has sparked a gradual rise in credit card theft. Today, credit cards are used almost universally by businesses, whether they are small or large. All types of businesses, including banks, the auto and appliance industries, are susceptible to credit card theft. Fraud is defined as a deceit committed with the aim of generating unauthorised financial benefit. Some of the ways that scams happen include hacking billing systems at stores or restaurants, hacking an online retailer, losing or stealing cards, and installing fraud devices in card readers at petrol stations or ATMs to acquire credit card PIN data. The 2 basic types of card fraud are behavioural fraud and application fraud. Application fraud describes scenarios in which a credit card application is false. It happens when a fraudster submits an application for a new credit card using false identification information, and the card issuer accepts it. Behaviour fraud occurs after a credit card has been approved and issued. Credit or debit card transactions that exhibit fraudulent conduct are referred to. Fraud identifying and prevention have long been big issues for card providers and key research areas for researchers due to the fact that identifying and preventing even a little amount portion of fraudulent behaviour would prevent millions of dollars in losses. Our study focuses on the challenge of recognising fraud behaviour.***
Keywords: LSTM Model, Credit Card fraud detection System, ML, Deep Learning.

I. INTRODUCTION

The majority of people now purchase their requirements using credit cards due to technological advancements, which has led to a progressive increase in credit card fraud. Nowadays, almost all businesses accept credit card payments, whether they are little or large. Credit card theft affects every firm, including banks, the automotive sector, the appliances industry, and others. The detection of fraud in debit or credit or debit card transactions uses a various technique, such as data mining and computer algorithms, however the outcomes are frequently unsatisfactory. It is crucial to develop algorithms that are very effective and efficient as a result. By employing an ANN technique and comparing it to a few other ML algorithms before the transaction is approved, we strive to stop a fraudster from using our credit card. Fraud is an offensive act committed by a third party by defrauding the innocent. The necessary login information from the cardholder is obtained when a credit card is used fraudulently, and the fraudsters use it in an unlawful manner—typically, through phone calls or SMS messages. Credit card fraud may occur if certain software packages used by thieves are used. Credit card fraud occurs when somebody uses another person's card without that person's consent. This can happen with or without the physical card when the appropriate PIN, password, and other credentials are stolen. Using ML and DL, a fraud identification module may determine whether the subsequent transaction is fraudulent or not. The most common and frequently used technique is machine learning, which has a numerous application, rapid turnaround times, and consistent results. The field of "machine learning" technology is concerned with the methods that enable computers to learn from experience and develop without explicit programming. Machine learning is frequently employed. Examples include medical, diagnosis, regression, etc. Combining static models with algorithms is known as machine learning, which enables computers to do tasks without the use of hard coding. Using training data, a model is created, and it is then tested using the trained model. A part of machine learning methods like deep learning are neural networks. Examples of deep learning approaches include ANN, CNN, autoencoders, RNN, restricted Boltzmann machines, etc. Neural networks used in DL process data and make judgements in a manner akin to the human brain.

II. LITERATURE REVIEW

A. R. B. Asha, S. K. Suresh, et al Describe a DL-based methodology for identifying fraud in card transactions. First, we evaluate it against machine learning methods like the SVM and k-Nearest Neighbour. Finally, we used a neural network even though it was difficult to create a model that would work well for identifying fraud in debit or credit or debit card transactions. Because it gives accuracy that is almost 100%, an artificial neural network (ANN) is best utilised in our method to identify credit card fraud. It offers higher accuracy in compared to unsupervised learning systems. In this study attempt, normalisation, data pre-processing, and under-sampling were employed to solve the challenges caused by using an unbalanced dataset [1].

©IJRASET: All Rights are Reserved

Fatima Zohra, Jamal Riffi, Mohamed Adnane Mahraz et. al This study uses the artificial neural network algorithms MLP and ELM to look for credit card fraud. According to the findings, MLP outperforms ELM in terms of a number of criteria, including recall, accuracy, Tp: true positive, Fp: false positive, and classification time [2]. The authors recommended using an ensemble model based on consecutive data modelling with deep RNN and a cutting-edge voting system based on an ANN to detect fraudulent behaviour. For the previously mentioned voting strategy, we additionally provide a cutting-edge training technique. Our experimental results on two real-world datasets show that the suggested model outperforms the state-of-the-art models in every evaluation criterion. Additionally, a temporal study shows that the suggested model performs better in real-time when compared to more recent models in the field [3]. In order to fit the cost-sensitive meta-classifier, the proposed framework adopts the strategy of enabling classifiers to fit conventionally while introducing cost-sensitive learning into the ensemble learning process. Basic classifiers and a trained cost-sensitive meta-classifier's predictive accuracy was evaluated using the area under the receiver operating characteristic curve. According to categorization results, the cost-sensitive ensemble classifier consistently outperforms the competition across the dataset's spectrum of fraud rates and has a very high AUC value. These results demonstrate that the cost-sensitive ensemble methodology is successful in producing cost-sensitive ensemble classifiers capable of correctly recognising fraudulent transactions in various payment system datasets, independent of the percentage of fraud episodes. This is in contrast to the results of conventional ensemble classifiers [5].

Altab Althar Taha and Sareef Jameel et al Malbery claim that transaction fraud is on the rise along with the popularity of using debit or credit cards as a form of payment. They employed an improved Light GBM, which blends Bayesian-based hyper-parameter optimisation with Light GBM parameter adjustment. Two sets of real, publicly accessible datasets from actual transactions—including both fraudulent and non-fraudulent transactions—were subjected to this methodology. Their suggested strategy performed more accurately when compared to other approaches. The suggested system has an accuracy of 98.40%, an area under the receiver operating characteristics curve (AUC) of 92.88%, a precision of 97.34%, and an F1-score of 56.95% [31].

To enhance the accuracy of the predictions made throughout the CCFD process, many machine learning techniques' strengths will be used. Our hybrid approach-based model incorporates three techniques: the Synthetic Minority Over Sampling Technique (SMOTE), the Hyper-Parameters Optimisation (HPO) method, the Recursive Features Elimination (RFE) method, and the Hyper-Parameters Optimisation (HPO) approach to estimate the optimum hyper-parameters to our RFC based model [6].

The objective or goal of this research is to develop a system for identifying card fraud using transaction patterns using LSTM networks as a sequence learner. The proposed methodology aims to keep track of credit card holders' prior purchasing behaviours in order to enhance the precision of fraud identification on recently received transactions. Experiments show that our suggested model has a high degree of accuracy and generates effective results [7].

Emin Aleskerov, Bharat Rao et. al [13] As a database mining method for identifying credit or debit card fraud, we provide CARDWATCH. The system provides access to several commercial datasets, a neural network learning module, and a friendly graphical user interface. Results from tests using credit card data that was generated artificially and an auto associative neural network model demonstrate very high rates of fraud detection.

Yelong Shen, Xiaodong He et. al [20] With the aid of a sizable, real-world data set, after being trained on clickthrough data, the proposed convolutional latent semantic model (CLSM) is evaluated on a Web page ranking task. The proposed research design captures essential semantic information in queries and texts for the job substantially better than current top-of-the-line semantic models, according to results.

Siddhartha, Sanjeev Jha, and others [15] In an effort to more efficiently detect (and consequently manage and prosecute) credit or debit card fraud, SVM , random forests, and the well-known logistic regression are discussed and examined. Real transaction data from a sizable, global credit card business served as the study's foundation.

Wensi Yang, Kejiang Ye, Yuhang Zhang, et al. [24] Using a sizable dataset of actual credit card transactions, we assess the performance of our credit or debit card FDS with FFD architecture. The average test AUC for the federated learning-based FDS is 95.5%, which is roughly 10% higher than for the conventional FDS, according to experimental results.

III. SYSTEM ARCHITECTURE

Among the input and output are several LSTM layers in a deep LSTM. It is useful that the input values supplied to the network travel via many LSTM layers and one LSTM cell in addition to time. As a result, the parameters are distributed uniformly throughout numerous levels. Long Short-Term Memory (LSTM) type RNN may Recognise order dependence in sequence prediction issues. This kind of behaviour is required in complicated problem domains. I'm using an LSTM to represent a set of inputs as a single input.

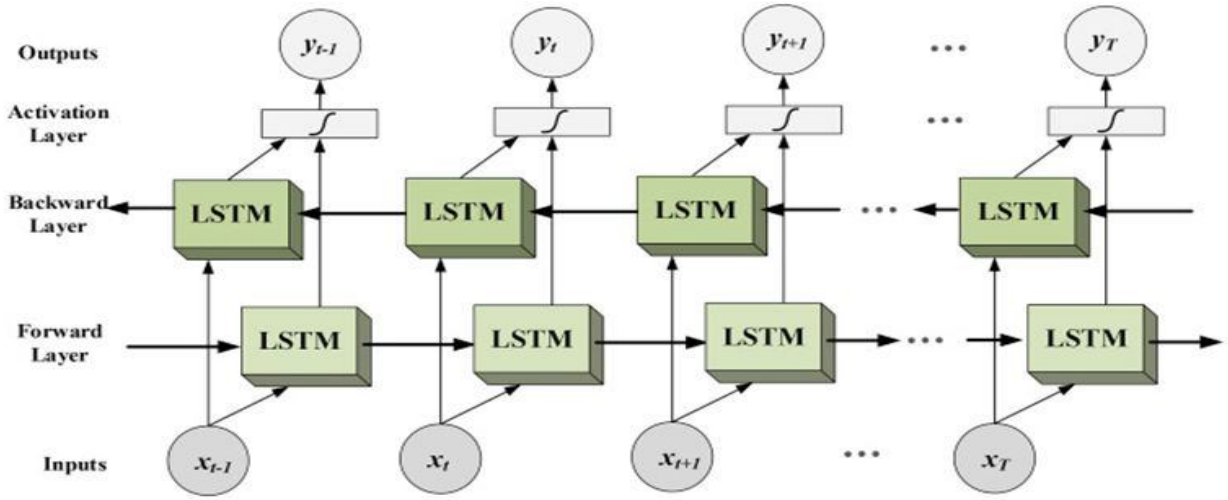


Figure 1: Deep LSTM architecture

IV. CONCLUSIONS

The method is believed to achieve accuracy above 95 %, which will be more efficient. The proposed method will be compared with some bench mark methods, which would be believed to be more efficient. The proposed method will be beneficial due to the fact that the enabling of optimization algorithm and their enhanced characteristics will helps in boosting the convergence of the classifier. The enhanced metrics values make the system more suitable for real time applications. The use of a distributed clustered LSTM classifier model aids in the accurate identification of credit cards. Finally, the model successfully predicts whether the data is genuine or fraudulent [31].

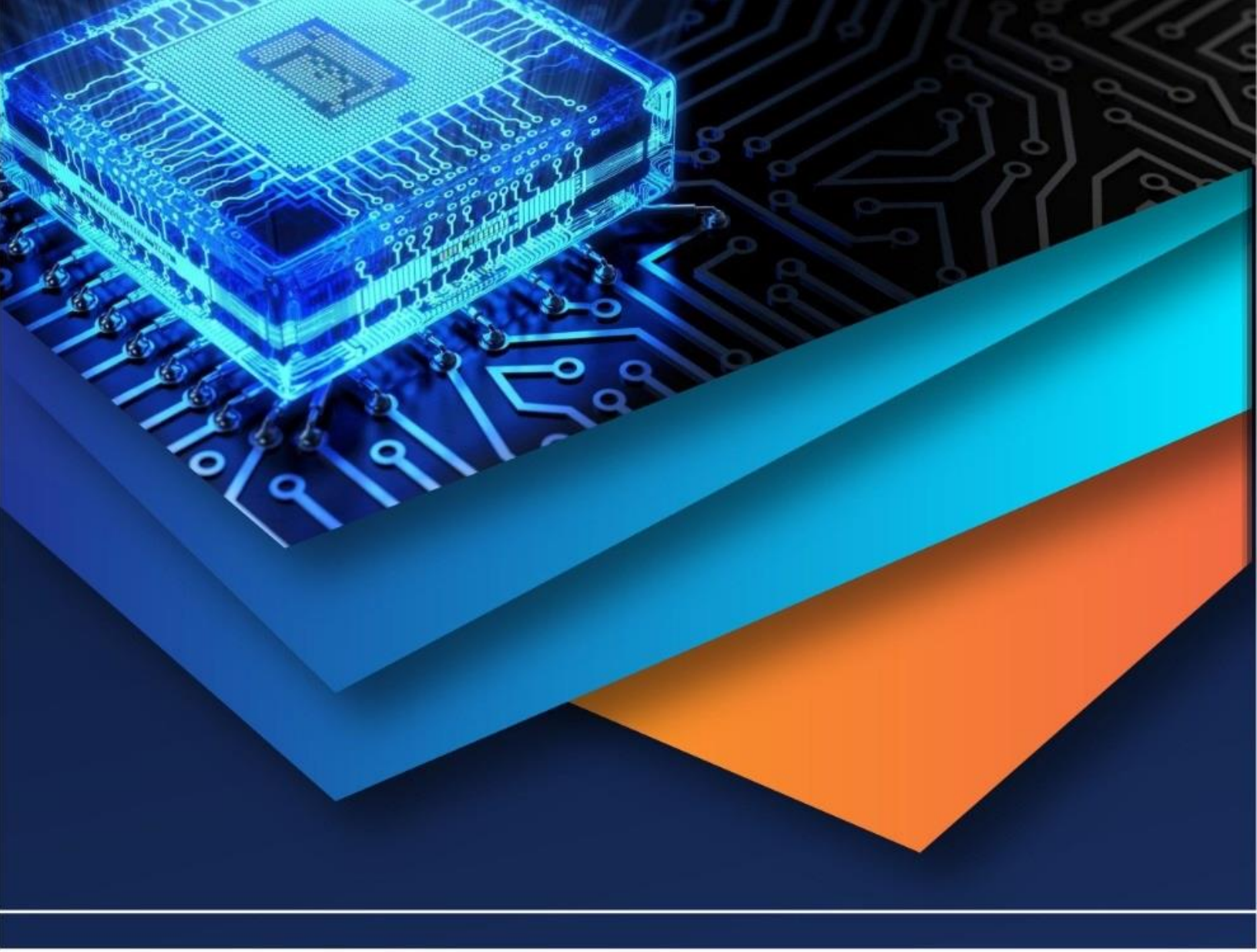
V. ACKNOWLEDGMENT

I want to first and foremost convey my sincere thanks to my mentor for his unwavering support of my academic endeavours as well as for his tenacity, inspiration, enthusiasm, and depth of knowledge. His advice was really helpful to me during the whole research and writing process for this study. I appreciate the assistance and direction I have received from my department head, the dean, and the institute principal.

REFERENCES

[1] Asha, R. B., and Suresh Kumar KR. "Credit card fraud detection using artificial neural network." Global Transitions Proceedings 2, no. 1 (2021): 35-41.
[2] Riffi, Jamal, Mohamed AdnaneMahraz, Ali El Yahyaouy, and Hamid Tairi. "Credit card fraud detection based on multilayer perceptron and extreme learning machine architectures." In 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), pp. 1-5. IEEE, 2020.
[3] Forough, Javad, and SaeedehMomtazi. "Ensemble of deep sequential models for credit card fraud detection." Applied Soft Computing 99 (2021): 106883.
[4] Taha, AltyebAltaher, and Sharaf Jameel Malebary. "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine." IEEE Access 8 (2020): 25579-25587.
[5] Olowookere, ToluwaseAyobami, and Olumide Sunday Adewale. "A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach." Scientific African 8 (2020): e00464.
[6] Rtayli, Naoufal, and NourddineEnneya. "Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization." Journal of Information Security and Applications 55 (2020): 102596.
[7] Benchaji, Ibtissam, Samira Douzi, and Bouabid El Ouahidi. "Credit card fraud detection model based on LSTM recurrent neural networks." Journal of Advances in Information Technology 12, no. 2 (2021).
[8] Zhang, Xinwei, Yaoci Han, Wei Xu, and Qili Wang. "HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture." Information Sciences 557 (2021): 302-316.
[9] Phua, Clifton, Ross Gayler, Vincent Lee, and Kate Smith-Miles. "On the communal analysis suspicion scoring for identity crime in streaming credit applications." European Journal of Operational Research 195, no. 2 (2009): 595-612.
[10] Bolton, Richard J., and David J. Hand. "Statistical fraud detection: A review." Statistical science 17, no. 3 (2002): 235-255.
[11] A. Abdallah, M.A. Maarof, A. Zainal, Fraud detection system: A survey, J. Netw. Comput. Appl. 68 (2016) 90-113.
[12] O. Abdel-Hamid, A.R. Mohamed, H. Jiang, L. Deng, G. Penn, D. Yu, Convolutional neural networks for speech recognition, IEEE-ACM Trans. Audio. Spe. 22 (10) (2014) 1533-1545.
[13] E. Aleskerov, B. Freisleben, B. Rao, Cardwatch: A neural network based database mining system for credit card

[14] Fraud detection, in: Proceedings of the IEEE/IAFE Computational Intelligence for Financial Engineering (CIFEr), IEEE, 1997, pp. 220-226.
[15] S. Bhattacharyya, S. Jha, K. Tharakunnel, J.C. Westland, Data mining for credit card fraud: a comparative study, Decis. Support Syst. 50 (3) (2011) 602-613.
[16] M. Hayat, M. Bennamoun, S. An, Learning non-linear reconstruction models for image set classification, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, IEEE Computer Society, 2014, pp. 156-163
[17] A. Karpathy, G. Toderici, S. Shetty, T. Leung, R. Sukthankar, F.F. Li, Large-scale video classification with convolutional neural networks, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, IEEE Computer Society, 2014, pp. 1725-1732.
[18] H. Lee, R. Grosse, R. Ranganath, A.Y. Ng, Convolutional deep belief networks for scalable unsupervised learning of hierarchical representations, in: International Conference on Machine Learning, ACM, 2009, pp. 609- 616.
[19] H. Lee, P.T. Pham, L. Yan, A.Y. Ng, Unsupervised feature learning for audio classification using Convolutional deep belief networks, in: Advances in Neural Information Processing Systems, 2009, 1096-1104
[20] Y. Shen, X. He, J. Gao, L. Deng, G. Mesnil, A latent semantic model with convolutional-pooling structure for information retrieval, in: Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management, ACM, 2014, pp. 101-110.
[21] Credit card dataset https://datahub.io/machine-learning/creditcard#readme accessed on December 2015
[22] Mirjalili, Seyedali, Seyed Mohammad Mirjalili, and Andrew Lewis. "Grey wolf optimizer." Advances in engineering software 69 (2014): 46-61.
[23] Pierezan, Juliano, and Leandro Dos Santos Coelho. "Coyote optimization algorithm: a new metaheuristic for global optimization problems." In 2018 IEEE congress on evolutionary computation (CEC), pp. 1-8. IEEE, 2018.
[24] Yang, Wensi, Yuhang Zhang, Kejiang Ye, Li Li, and Cheng-Zhong Xu. "Ffd: A federated learning based method for credit card fraud detection." In Big Data–BigData 2019: 8th International Congress, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 8, pp. 18-32. Springer International Publishing, 2019.
[25] Li, Zhenchuan, Guanjun Liu, and Changjun Jiang. "Deep representation learning with full center loss for credit card fraud detection." IEEE Transactions on Computational Social Systems 7, no. 2 (2020): 569-579.
[26] Li, Zhenchuan, Mian Huang, Guanjun Liu, and Changjun Jiang. "A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection." Expert Systems with Applications 175 (2021): 114750.
[27] Najadat, Hassan, Ola Altiti, Ayah Abu Aqouleh, and Mutaz Younes. "Credit card fraud detection based on machine and deep learning." In 2020 11th International Conference on Information and Communication Systems (ICICS), pp. 204-208. IEEE, 2020.
[28] Somasundaram, Akila, and Srinivasulu Reddy. "Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance." Neural Computing and Applications 31 (2019): 3-14.
[29] Kim, Eunji, Jehyuk Lee, Hunsik Shin, Hoseong Yang, Sungzoon Cho, Seung-kwan Nam, Youngmi Song, Jeong-A. Yoon, and Jong-il Kim. "Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning." Expert Systems with Applications 128 (2019): 214-224.
[30] Darwish, Saad M. "An intelligent credit card fraud detection approach based on semantic fusion of two classifiers." Soft Computing 24, no. 2 (2020): 1243-1253.
[31] A.A. Taha, S.J. Malebary, An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine, IEEE Access 8 (2020) 25579–25587, doi:10.1109/ACCESS.2020.2971354.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)