

AN EXPERIMENTAL STUDY ON FINANCIAL FRAUD DETECTION BASED ON DEEP LEARNING

Mr Pramod Salunkhe*1, Dr. Ashish Chaurasia*2

*1 Research Scholar, Department of Computer Science, University of Technology, Jaipur

*2 Professor, Department of Computer Science, University of Technology, Jaipur

DECLARATION: I AS AN AUTHOR OF THIS PAPER / ARTICLE, HEREBY DECLARE THAT THE PAPER SUBMITTED BY ME FOR PUBLICATION IN THE JOURNAL IS COMPLETELY MY OWN GENUINE PAPER. IF ANY ISSUE REGARDING COPYRIGHT/PATENT/OTHER REAL AUTHOR ARISES, THE PUBLISHER WILL NOT BE LEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MY CONTENT FROM THE JOURNAL WEBSITE. FOR THE REASON OF CONTENT AMENDMENT/OR ANY TECHNICAL ISSUE WITH NO VISIBILITY ON WEBSITE/UPDATES, I HAVE RESUBMITTED THIS PAPER FOR THE PUBLICATION. FOR ANY PUBLICATION MATTERS OR ANY INFORMATION INTENTIONALLY HIDDEN BY ME OR OTHERWISE, I SHALL BE LEGALLY RESPONSIBLE. (COMPLETE DECLARATION OF THE AUTHOR AT THE LAST PAGE OF THIS PAPER/ARTICLE)

Abstract

Financial fraud is a problem that has wide-ranging effects on the financial industry, the government, corporate sectors, and regular consumers. The problem has gotten worse recently as a result of our growing reliance on new innovations like cloud computing and portable processing. Financial fraud is a problem that has wide-ranging effects on the financial industry, the government, corporate sectors, and everyday consumers. Recent increases in reliance on new innovations like cloud computing and portable processing have made the problem worse. The consistency and sequential correctness of the information, as well as the timing of the feedback deliveries, affect how exact and accurate those systems are. One of these technologies, a fraud detection system, is the subject of this essay. Banks and financial institutions are investing more and more today in completing the calculations and information examination advancements used to differentiate and combat fraud in order to have a more precise and exact fraud detection system. In order to address this issue, various arrangements and calculations utilising AI have been suggested in writing. However, the focus of examination is on research. Few deep learning standards exist, and nobody seems to believe that the offered works consider the importance of a continuous methodology for problems of this nature. As a result, in order to address this problem, we suggest a live charge card fraud detection system based on deep learning technology.

Keywords: *Deep Learning, Intelligent Financial, Fraud Detection, System*

1. Introduction

Financial fraud is a problem that affects both the financial world and daily life in a significant way. Fraud can erode consumer confidence in businesses, undermine economies, and alter the prices that people often pay for numerous commonplace things. Traditional procedures relied on manual techniques, such as appraising, which are wasteful and unreliable due to the difficulty of the problem. The ability of information mining-based approaches to spot minute abnormalities in huge informational indexes has been shown to be helpful. The optimal approach for each situation is continually being explored because there are numerous types of fraud and numerous information mining approaches.

Financial fraud is a broad phrase with many potential meanings, but for our purposes, it is very likely to be defined as the intentional use of illegal tactics or activities to obtain financial gain. Financial fraud also has more serious repercussions for the company, such as supporting criminal activities like drug trafficking and organised crime. The cost of Visa fraud is typically borne by the dealers, who end up shelling out for delivery, chargeback, and regulatory costs as well as losing the buyer's confidence after falling victim to a fraudulent transaction. This helps us understand the impact that fraud can have and the importance of preventing it.

Modern technological advancements like the internet and flexible processing have recently led to an increase in financial fraud. Social variables like the increased use of Mastercards for purchases have increased spending while also leading to an increase in fraud. Since fraudsters are always changing their tactics, it is essential that detection approaches have the flexibility to adapt as necessary. Information mining has already been shown to be useful in contexts like Visa endorsement, liquidation expectation, and offer business sector evaluation. Although fraud detection is seen as a comparative characterisation problem, there is a significant disparity between exchanges that are fraudulent and those that are legitimate. Due to their ability to handle big datasets and their ability to function without requiring knowledge of the underlying information elements, information mining technologies are also important for fraud detection.

Financial fraud is a problem that affects both daily life and the financial world in a significant way. Fraud can harm economies, undermine public trust in business, and affect consumers' average cost of living. Traditional methods of detecting fraud relied on manual techniques, such as appraising, which are inefficient and unreliable because of the complexity of the problem.

The number of bank transactions made using Mastercards increased significantly, as did the number of scams and card thefts. Because of Mastercard fraud, financial foundations have lost billions with the rise of computerised instalment. This problem puts banks and other financial institutions to the test in terms of building effective and pro-active fraud detection systems. By using the accumulated verified client information and their continuous exchange details, AI offers a viable solution to handle this problem.

AI is currently used successfully in the banking and financial sectors for a variety of applications, most notably in portfolio management, trading, risk analysis, fraud detection, and counteraction. For instance, AI is used in the financial industry to create Talk bots, artificial intelligence programming that can communicate with customers and respond to their inquiries. Algorithmic exchanging or Choice exchanging Emotionally supporting networks are used in exchanging to go with extremely quick decisions. The security against fraud is another crucial function of AI in the financial industry. Recognizing doubtful workouts became a simpler task with the aid of ML computations. Given the history of the exchanges, AI demonstrated interesting new methods to analyze client behavior and determine whether or not there is fraud.

2. Literature Review

According to Tuyls et al., there are a few challenges with fraud detection. First off, creating effective models is extremely challenging due to the severely unbalanced datasets in this application, where only a small percentage of the available information is false. From noisy information and covering designs, further concerns surface. Above all, fraud components are always evolving, and arrangement models must keep up with and adapt to these changes. Following, we review the studies that have used AI and deep learning models in the field of fraud detection that are the most relevant.

2.1. A Comparative study on KNN and SVM

A report on fraud detection using multiple techniques—specifically, gullible Bayes, KNN, SVM, and packing gathering classifier—was distributed by Zareapoor and Shamsolmoali. In their paper, they look at the various concerns that arise when dealing with this issue. For instance, the inaccessibility of verifiable information makes it harder to investigate how to deal with false information because banks and other financial institutions are reluctant to share their information due to security concerns because it is sensitive information. Additionally, while there are only 2% of exchanges that are fraudulent and 98% of swaps are real, information is sometimes very unequal. They make references to the concerns of massive amounts of data and the lengthier computation times for larger datasets in these situations. One of the key issues that frequently surfaces in many exam papers is the distinct notion of fraud. There isn't a single event or manner that perfectly sums up the concept of fraud. As a result, it is necessary for AI calculations to be updated often so that harmful activities can be caught earlier.

2.2. Random Forest in Fraud Detection

Randhawa et al. on "Charge card fraud detection using AdaBoost and greater part voting" examines a variety of AI algorithms, including "Guileless Bayes," "Irregular Woods," "Inclination Helped Tree," and others. In this study, they combine at least two calculations using "Greater part casting a ballot." The focus also investigates the AdaBoost gathering mechanism and indicates that AdaBoost is very susceptible to anomalies and oddities.

They use the Fast Excavator as an execution programming tool, and the trials are managed using MasterCard location data for South-East Asia. To lessen the tendency, the classifiers were all evaluated using a 10-overlay cross approval. The Matthews Relationship Coefficient is used to evaluate the classifier's performance (MCC).

2.3. Detecting Fraud using Auto Encoders based on Reconstruction Error

In his novel, "Single Man," Tom Sewers describes auto encoders as a potent brain network that can both encode and translate information. In this method, the Auto encoders are ready for non-

irregularity focuses and are familiar with the oddity focuses to classify it as "fraud" or "no fraud" depending on the remake error that would be thought to be high due to peculiarities that the system has not been prepared on. Any value above the upper bound value or limit in this situation would be considered unusual.

3. Financial Fraud Detection Practices Classifications

We shall categories current financial fraud detection practices in the subsequent sub-segments based on success rate, used detection approach, and fraud type. This setup will enable us to identify trends in ebb and flow works on, including which have been successful, plausible factors influencing the results, and also any gaps in the analysis.

3.1. Performance-Based Categorization

Although there have been other criteria used to determine execution, the three that are most frequently used are precision, responsiveness, and explicitness. Exactness calculates the ratio of all examples that are effectively grouped to those that are not. Awareness measures the ratio of truthful advantages over deceptive advantages, or the amount of items that are accurately identified as fraud versus the amount falsely recorded as fraud. Particularity refers to similarities between ideas with genuine exchanges or the relationship between real negatives and false negatives.

Other execution measures have been used in the work in addition to the three execution estimates that are being reviewed here. As an illustration, Duman et al. chose to display their results for responsiveness in diagram structure rather than deterministic attributes, which were gathered by each arrangement of information boundaries. In addition to other charting methods, several analyses used case-based approaches or achievement levels determined by programming to determine the results of their fraud detection processes.

The findings show that CI techniques are typically recommended to progress rate than measured strategies. With comparable explicitness and exactness, responsiveness was somewhat better for arbitrary woods and backing vector machines than calculated relapse. Support vector machines, probabilistic brain organisations, genetic programming, and information-gathering techniques are

used to address beat relapse in each of the three regions. Furthermore, a brain network with thorough pruning was thought to be more exact and unambiguous than CDA. Despite this, one factual strategy appears to contradict this claim: Brain organisations and choice trees were accounted for to be less precise than Bayesian conviction networks.

The great majority of the research revealed a stark discrepancy between the results of each strategy's responsiveness and explicitness. Bhattacharyya et al. demonstrated, for instance, that strategic relapse, support vector machines, and irregular timberlands all performed usually better at reliably differentiating real exchanges from fraudulent ones. Support vector machines, genetic programming, brain organisations, group information handling techniques, and particularly calculated relapse were also a little less sensitive. Similar to this, a brain network with thorough pruning demonstrated more explicitness than responsiveness.

3.2. Based on Detection Algorithm Classification

Organizing fraud detection exercises according to the detection formula used is a useful technique for identifying the practical solutions for this problem space. It can also help us determine why particular tactics were chosen or successful. By looking at calculations that have not been sufficiently studied, we can also spot any gaps in the research. According to the detection calculation (conventional information mining and CI-based methodologies) used, Table 4 displays the hierarchy of financial fraud detection practices.

Early research on fraud detection centered on measurable models and brain organisations, as was already said; yet, it was apparent that these tactics continue to be widely used. Many used at least one sort of brain network, while some used Bayesian conviction organisations and others researched strategic relapse. The use of CDA has been unusual to some extent. A lot of the time, brain organisations and planned relapse are chosen for their well-established reputation, which enables them to be used as a control technique by which other methods are attempted. Support vector machines and hereditary programming, for example, stand out as more advanced solutions. Without any research on bunching or time-series techniques, Yue et al. also stated that every

strategy included in their analysis was a type of grouping and that the majority of the research was focused on controlled learning rather than solo learning.

3.3. Fraud Classification Based on Type

Given the varying perceptions of each type of fraud, the problem area can change significantly depending on the structure that is being identified. By classifying current practises according to the type of fraud under investigation, we may identify the tactics that are more logical and frequently employed for a given type of fraud. Depending on the strength and scope of an effect, we can also infer the categories that are thought to be the most important for examination. Table 5 shows the classification in relation to the categories of fraud taken into account as well as the detection methods applied.

With each selected calculation, the highlight determination will differ based on the problem area. Inside specific companies, there is explicit financial declaration fraud, hence characteristic proportions rather than pure traits are used. The crucial ratios, such as total profit to add up to resources, premium instalments to profit before revenue and expense, and market value of value to add up to resources, are accurately illustrated by Koh and Low. Correspondingly, investigations into Mastercard fraud frequently select independent variables or overall features that can be either quantitative or subjective. Bhattacharyya et al., for instance, used exchange sum and straight-out data such account number, exchange date, and cash. They also gathered information on attributes like the daily total of exchanges and the average amount spent at a single vendor.

We can see that the current investigation has been incredibly unfair when considering the type of fraud. The majority of research has focused on two specific types of financial fraud: financial articulation fraud and charge card fraud.

4. 4 EXPERIMENTAL RESULTS

4.1.Dataset

The transactions made by European cards over the course of two days in September 2012 were gathered and dissected during a study collaboration between World Line and the AI Gathering of

ULB on large-scale information mining and fraud prevention. This informational collection is used in this work. Only mathematical properties are included in the information. Due to classification, PCA change affected the characteristics.

4.2. Performance metrics

This informational collection sets up trades based on whether they are fake or not. Arbitrary over-Testing is used to address this class imbalance. The dataset is split into test and preparation sets. We divided the data into two independent preparation sets and one unrestricted test set for a pre-prepared model exhibition check. Refer to Tab.1

Table: 1. Distribution of instances

Number of instance	173706
Split ratio for pre-training	0.3
Split ratio for training	0.5
Independent test set	0.5

4.3. Paradigms

Three learning order procedures were chosen for correlation, adding up to four standard calculations, in order to evaluate the effectiveness of deep learning in this review context. The methods used for correlation were chosen due to their obvious recurrence in several paired grouping research publications and their well-known positive results.

We combined the disarray structure and a segment outline with the accuracy and review for the measures. An unorganised network of a parallel classifier is a table that displays the number of events that were correctly/inaccurately categorized into each class. The chaotic grid of a double classifier is depicted in Fig. 1.

		<i>Predicted class</i>	
		<i>P</i>	<i>N</i>
<i>Actual Class</i>	<i>P</i>	True Positives (TP)	False Negatives (FN)
	<i>N</i>	False Positives (FP)	True Negatives (TN)

Figure: 1. Illustration of a confusion matrix

In our case, positive refers to fraudulent exchanges while negative refers to genuine swaps. Genuine positive (TP) addresses the delegated fraud in fraudulent trades. Genuine Negative (TN) addresses true delegations of exchanges that are genuine. Genuine exchanges that were mistakenly categorized as fraud are addressed by misleading positive (FP). Negative misrepresentation (FN) refers to exchanges that were mistakenly classified as authentic fraud.

The quantity of positive forecasts divided by the absolute number of positive class anticipated by the model, as follows, characterizes the accuracy, which is defined as the proportion of the model's precision.

$$\text{Precision} = TP / (TP + FP).$$

The review is a component of the model's consummation; it is the exactness on fraud exchanges defined as the sum of positive expectancies divided by the sum of positive class upsides of the test data, as follows:

$$\text{Recall} = TP / (TP + FN).$$

We utilise the F1 score to represent the equilibrium between recall and precision, which is defined as follows:

$$F1Score = 2((precision * recall) / (precision + recall)).$$

5. Results analysis

When an exchange raises a fraud banner, the exchange is refused by card fraud detection systems, and the client is required to complete a check cycle to determine whether the fraud banner is deceptive or real. From a call to a series of check structures, this confirmation procedure changes. The cost of a fake banner is then the same as the cost of these cycles, which is far less expensive than the cost of a fraud case. However, when there are a lot of fake banners, purchases are mistakenly blocked more often, making using a credit card difficult and time-consuming. It can also result in considerable losses for both parties to the transaction. In this way, our model should have a respectable amount of phony transactions obtained and false banners raised.

The trial-related effects of our calculated formulas are displayed in Tab. 2. For each computation, we created a new lattice, addressed the TP FN FP TN in the table, and repeated the calculation numerous times. The non-direct auto relapse has amassed the most fraudulent exchange measures, albeit at the expense of fake banners. Calculated relapse raised the least amount of deceptive banners, but it isn't very good at detecting fraudulent swaps. Deep Learning has changed findings in light of the auto encoder, resulting in a significant amount of frauds and deceptive banners. Initial results for the Deep Brain Network model seem promising. Let's check the accuracy of our models.

Table: 2. as a result, Confusion Matrix

	TP	FP	TN	FN
Linear SVM Regression	252	1222	224262	325
Logistic Regression	203	2380	225003	360
NN Based Classification	273	3338	224038	289
Non Linear Auto Regression	340	2762	224307	242
Deep NN Auto encoders	247	2568	224682	346

The right expectations divided by the total number of forecasts produced is how accuracy is defined. The data reveals that the conventional brain network order strategy has horrible exactness whereas Strategic relapse followed by the Auto-encoder has the best exactness. We shouldn't draw conclusions from exactness, as it were, because our information isn't consistent. Due to calculation, exactness might be misleading. to its circumstances (precision paradox). Review and correctness are thus shown in Fig. 2.

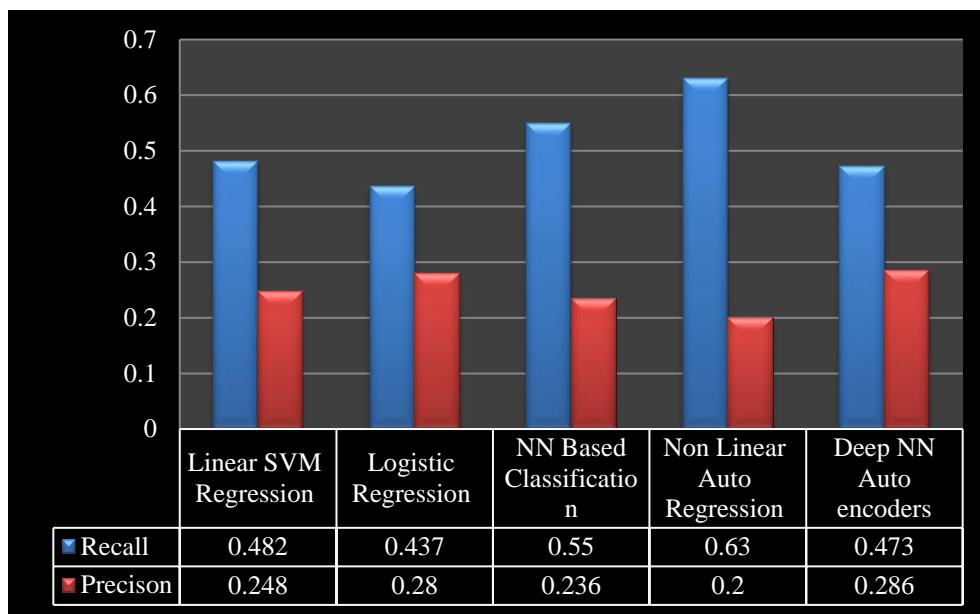


Figure: 2. metrics comparison for results

Fig. 2's results demonstrate that Non direct auto relapse has the best Review in our model, but at the sacrifice of accuracy. On the other hand, Deep NN auto encoder has the best accuracy, with outcomes that are close to strategic relapse. We cannot draw conclusions from a review of accuracy alone; rather, our model must have equal quality for the two measurements. The F1 scores Tab 3 should appear. Deep NN Auto encoder has the overall best F1 score for this review situation, followed by computed Relapse, proving that it is the best-fitting calculation out of those that have been tried. Additionally, the deep learning computation used in this study is rather simple; hence, our results might be enhanced by further boundary tuning (Hyper-boundary Tuning with

Framework Search). This provides excellent insight into the calculations that should be used to construct our expectation model, and we choose Deep Brain network with auto-encoder.

Table: 3. F1 scores outcomes

Classifier	F1 score
Linear SVM Regression	0.114
Logistic Regression	0.168
NN Based Classification	0.130
Non Linear Auto Regression	0.267
Deep NN Auto encoders	0.183

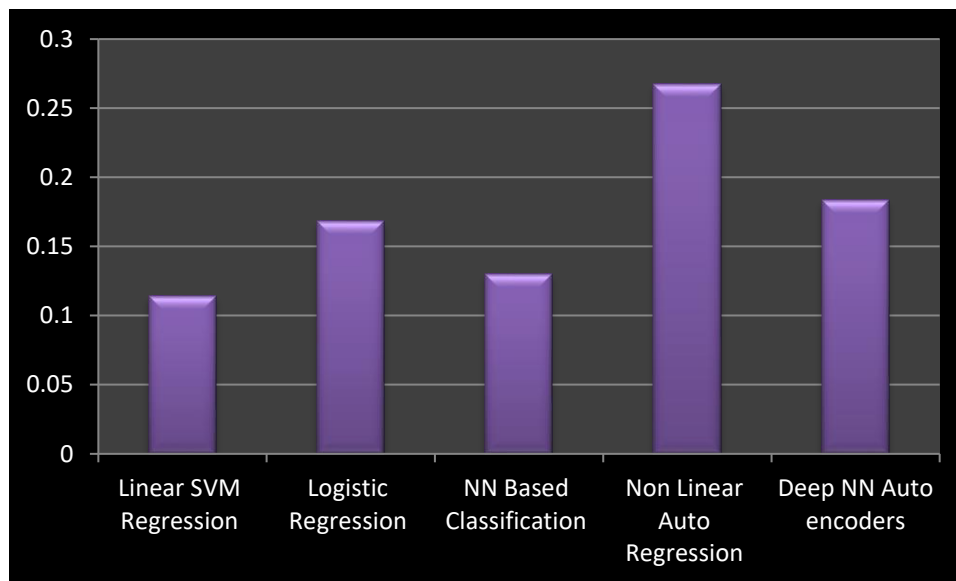


Figure: 3. F1 scores outcomes

6. Conclusion

For a true comprehensive collection of Charge card exchanges, we suggested a Constant model for Visa fraud detection using deep learning. The benchmark tests reveal that Deep NN Auto encoder has incredibly encouraging results, with the best F1 score, when compared to various

typical continuous parallel classifiers presented against Deep Brain Organization with Auto-encoder. That is what the analysis confirms, notwithstanding the noteworthy display of deliberate relapse where Deep learning outperforms it. Future tests will therefore focus mostly on cutting-edge deep learning requirements for these kinds of Constant Information Arrangement problems. The suggested System can be used with charge card providers to filter any unusual behavior and spot potential fraud attempts. Charge card fraud is a serious corporate concern. These frauds have the potential to cause enormous losses for both individuals and businesses. As a result, businesses invest an increasing amount of money in developing ground-breaking ideas and strategies that will aid in identifying and preventing frauds. A important segment of the advanced money sector is fraud detection. This writing audit focused on research on intelligent, quantifiable, and computational approaches to fraud detection. Despite the differences in their presentations, it was shown that each method was effective at identifying various forms of financial fraud.

7. References

1. A. Mishra, C. Ghorpade, "Credit Card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques" 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) pp. 1-5. IEEE.
2. Alae Chouiekha, EL Hassane Ibn EL Haj. "ConvNets for Fraud Detection analysis". *Procedia Computer Science* 127, pp.133–138. 2018.
3. Apapan Pumsirirat, Liu Yan. "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine". *International Journal of Advanced Computer Science and Applications*, Vol. 9, No. 1, 2, pp 18-25. 2018.
4. C. Wang, Y. Wang, Z. Ye, L. Yan, W. Cai, S. Pan, "Credit card fraud detection based on whale algorithm optimized BP neural network", 2018 13th International Conference on Computer Science & Education (ICCSE) pp. 1-4. IEEE.
5. I. Goodfellow, Y. Bengio, A. Courville.: *Deep learning*, Cambridge, Massachusetts, The MIT Press, (2016)

6. J. O. Awoyemi, A. O. Adentumbi, S. A. Oluwadare, "Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis", *Computing Networking and Informatics (ICCNI), 2017 International Conference on pp. 1-9. IEEE.*
7. Giacomo Corbo, Carlo Giovine, and Chris Wigley(2017, April). *Applying analytics in financial institutions fight against fraud. McKinsey Analytics. Retrieved from <https://www.mckinsey.com>.*
8. Kuldeep Randhawa, Chu Kiong Loo, Manjeevan Seera, Chee Peng Lim, Asoke K. Nandi. "Credit card fraud detection using AdaBoost and majority voting". *IEEE Access (Volume: 6), pp 14277 – 14284. 2018.*
9. Masoumeh Zareapoor, Pourya Shamsolmoalia. "Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier" *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015). Procedia Computer Science 48 pp 679 – 686. 2015.*
10. N. Malini, Dr. M. Pushpa, "Analysis on Credit Card Fraud Identification Techniques based on KNN and Outlier Detection", *Advances in Electrical, Electronics, Information, Communication and BioInformatics (AEEICB), 2017 Third International Conference on pp. 255- 258. IEEE.*
11. S. Dhankhad, B. Far, E. A. Mohammed, "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study", *2018 IEEE International Conference on Information Reuse and Integration (IRI) pp. 122-125. IEEE.*
12. Tom Sweers. "Autoencoding Credit Card Fraud". *Bachelor Thesis, Radboud University. June 2018.*
13. 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.*
14. Z. Chen, C. K. Yeo, B. S. Lee, and C. T. Lau. "Autoencoder based network anomaly detection." *Wireless Telecommunications Symposium, pp 1-5. 2018.*

15. Z. Kazemi, H. Zarrabi, "Using deep networks for fraud detection in the credit card transactions", *Knowledge-Based Engineering and Innovation (KBEI), 2017 IEEE 4th International Conference on pp. 630-633. IEEE.*

Author's Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism / Guide Name / Educational Qualification/ Designation/Address of my university/college/institution/ Structure or Formatting/ Resubmission / Submission /Copyright / Patent/ Submission for any higher degree or Job/ Primary Data/Secondary Data Issues, I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who find trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof and Address Proof and Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be considered for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Mr Pramod Salunkhe
Dr. Ashish Chaurasia
