INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 4)
Available online at: https://www.ijariit.com

Review on credit card fraud detection and classification by Machine Learning and Data Mining approaches

Aaushi Sharma
Yamuna Group of Institutions Engineering and Technology, Yamuna Nagar, Haryana

Neha Bathla
Yamuna Group of Institutions Engineering and Technology, Yamuna Nagar, Haryana

ABSTRACT

The strategies for this are divided into 2 broad types: fraud detection as well as consumer activity analysis. The initial category of strategies works with controlled recognition processes at transaction stage. Transactions are classified as illegitimate or regular depending on preceding historical evidence in such systems. This dataset can then be used to construct classified models that can forecast the status of new documents (normal or fraudulent). A standard two-classification function, including rule inference, decision trees, as well as neural networks, has various model development approaches. This method has been shown to accurately identify most previously found fraud techniques, often known as identification of misuse essential to illustrate the main discrepancies in an overview of consumer behaviour and methods to fraud investigation. The system of fraud detection can identify established tricks from fraud, with a small false positive rate. Such schemes derive the sign as well as pattern of fraudulent strategies provided in the revelation data set as well as can therefore quickly decide precisely that frauds; the machine is witnessing at the moment.

Keywords: *Credit, Card, Fraud, Machine Learning, Analysis*

1. INTRODUCTION

The solutions to the fraud can be categorized into prevention, which involves preventing the fraud in the source itself and detection, which the action is taken after the occurrence of the event. The technologies like the Address Verification System (AVS) as well as Card Verification System (CVM) are generally activated for stopping fraudulent. Basically, rule-based filter and data mining methods are however, when fraud cannot be prevented from occurring, then it is must to identify at the earliest, and essential steps should be taken not in favor of it. False revealing is the procedure of detecting either a transaction is legitimate or not [47]. Automatic deception discovery systems are necessary especially considering the huge traffic of transaction data, and this doesn't potential for individuals to check by hand every transaction one by one if it is fraudulent or not. This thesis is based on the usual fraudulent recognition scheme using machine-learning techniques.

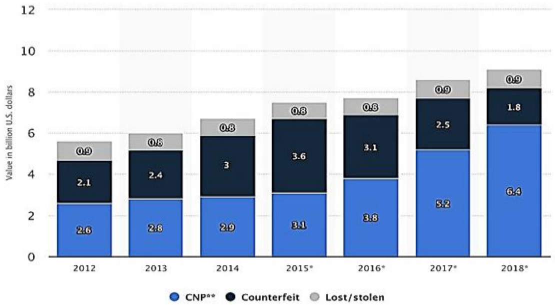

Fig. 1: failure because of card fraudulent in the U.S. in 2012-2018 as reported by [55]

1.1 Fraud Detection Process

The transactions are first checked at the terminal point to be valid or not, which is shown in figure1.2. At the terminal point, certain essential conditions such as sufficient balance, valid PIN (Personal Identification Number), etc. are validated and the transactions are cleaned so. Every suitable transaction are then scored by the prognostic form, that then classifies the transactions as genuine or fraudulent. The investigators investigate each fraudulent alert and provide feedback to the predictive model to improve the model's performance [30]. This thesis only deals with the predictive model.

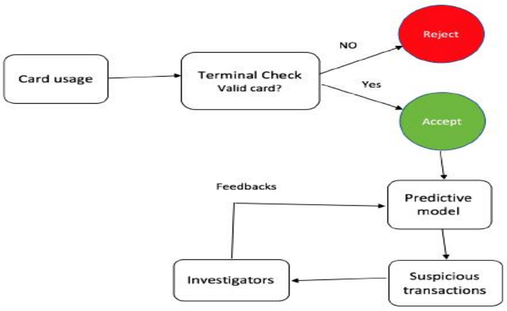

Fig. 2: Fraud detection process

1.2 Challenges in fraud detection

Building a fraudulent discovery scheme is not as simple as it looks. The practitioner needs to decide which learning approach to use, which algorithms to use, which features to use, as well as mainly significant, how to deal with the class imbalance trouble (fraudulent cases are extremely sparse as compared to the legitimate cases) [30]. Class imbalance is not only the major concern in fraud detection system. Overlapping of the genuine and fraudulent classes due to limited information about the transaction records is another problem in the classification task [52], and most machine learning algorithms underperform under these scenarios [48]. In a real-life scenario, a fraud detection model predicts the nature of class (genuine or fraudulent) and gives the alert for the most suspicious transaction to the investigators. Investigators then perform a further investigation and give response to the fraud detection scheme to get better its presentation. However, this process can be an overhead for the investigators due to which only a few transactions are validated on time by the investigators. In such a case, just a few feedbacks are provided to the predictive model, which generally results in a lesser accurate model [30]. Lastly, as financial institutes very rarely disclose the customer data to the public due to confidentiality issues, this is really challenging to locate the true financial databases. It is one of the big obstacles in the study work on fraudulent identification.

1.3 Credit card fraudulent

Illegitimate usage of card or the records is pointed to as credit card theft, not including the permission of the owner. Related credit card theft techniques primarily relate to two customer categories as well as behavioral fraud[43]. Payment fraud happens as fraudsters use fraudulent or other details to implement new cards from banks or issuing agencies. A single consumer with single collection of user info or separate consumer with same details can request various applications. In the other side, behavioural fraud has 4 major types: stolen money, postal theft, bogus money as well as non-fraud cardholder. Theft / missing card theft arises as frauds rob a credit card or activate a misplaced wallet. Mail identity abuse happens when the fraudster accepts a credit card from either the bank via post or personal details before meeting the real card holder[43]. Credit card data are collected through both fraudulent and "cardholder not current" frauds w/o consent of the card holders. Online transfers can be carried out in the former utilizing card information via fax, email, or the Internet. Falsified cards are rendered in the above, dependent on card details

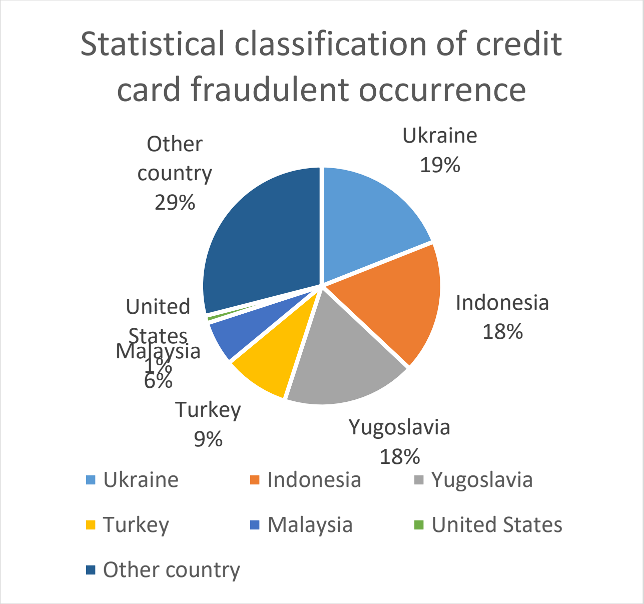

Fig. 3: High risk countries suffering credit card fraud threat [26]

Fig.1 shows the more risk nation suffering the danger of credit card fraudulent, focused on observational evidence published in [34] in 2012. Ukraine has the most shocking 19 percent fraud rate, that Indonesia strongly matches at a fraud rate of 18.3 percent. After such two, Yugoslavia is the most dangerous nation with a pace of 17.8 per cent. Malaysia (5.9 per cent), Turkey (9 per cent) as well as eventually the United States lead to the second largest fraud rate. Many nations pruning payment card theft at a pace below 1 percent are not demonstrated in figure 3.

1.4 Problems of Credit Card Fraudulent finding

Fraudulent prevention scheme are prune to many problems as well as challenges mentioned bellow. A successful strategy for detecting fraud would have the potential to overcome such challenges and produce the highest results.

- **Unbalanced results:** Results on credit card fraud identification is unbalanced in design. This indicates that low numbers of all purchases by credit card are fraudulent. Which causes quite complex as well as inaccurate identification of fraudulent transactions?
- **Lack of adaptability**: Classification algorithms continue to face the difficulty of identifying different forms of natural or deceptive patterns. The managed as well as unmonitored fraud identification methods, however, are ineffective in identifying emerging forms in regular as well as fraud behaviour.
- **Specific value of misclassification:** Various misclassification failures have different meaning in fraudulent identification activities. Misclassification of a legitimate activity as theft is not as dangerous as legitimate fraud identification. Since the recognition problem during the first case can be found in more investigations [26].
- **Overlapping data**: Many transactions might be deemed fake, although they are completely legal (false positive) as well as vice versa, fraud transactions may often seem genuine (false negative). A main obstacle for fraud identification programs is also maintaining a small incidence of false positives and false negatives [26, 47, 49].
- **Fraud identification costs:** The program will take into consideration both the identified criminal behavior costs and the avoidance costs. For eg, by preventing a dishonest transaction of a few dollars no revenue is received [26, 47].

1.5 Kinds of Credit Card Fraudulent

With time goes on; credit card fraudulent forms are starting to be categorized, as well as sophisticated fraud monitoring technologies are being built to counter card fraudulent in the game of cat and mouse. To recognize what algorithms identify fraudulent depends on the form of crime, knowledge of the forms of card fraud is important.

1.5.1 Lost as well as Stolen Card Fraudulent: Cards obtained through deception or deception-by-finding fraudsters may be utilized for making online transactions. Without the Card's Personal Identification Number (PIN), cash withdrawals are not feasible [45].

Methods of Detection

Crooks who procure cards by fraud-by-finding don't recognize the rightful cardholder's code. The identification of missing and stolen cards is possible through an Address Verification System (AVS). As electronic payment cards are utilized, the bill address is inserted as well as verified toward the address held in the history of the bank, an address discrepancy increases doubt and prevents the transaction. Visa follows a common approach; called Verified by Visa (VBV), where code word should be submitted to carry out purchases electronically as a second verification mechanism (M.Sriganesh and Jon T.S.Quah, 2008).

1.5.2 Card not Received Fraudulent: That is where the receiver stoles a credit card in movement until it is collected. An indication of a card that has not been issued is where a delivery or other person of mutual occupation removes the card from the mail [30].

Methods of Detection

Mail couriers use knowledgeable shipping and signature-based authentication systems to guarantee credit cards are sent to the rightful person. When card was not sent to the right individual, the account holder may contact the courier and has the details about who agreed to sign the shipment.

2. RELATED WORK

Saad M. Darwish [1] Suggested a smart two-level card fraudulent identification system through extremely unnecessary databases, focused on the semiconductor fusion of k-means as well as artificial bee colony algorithm (ABC) to get better recognition accuracy as well as speeding up convergence. ABC as a second category stage carries out a kind of neighborhood quest in conjunction with the worldwide search to manage the failure of the k-means classifier to find the real cluster if the similar data is entered in a different format it may yield specific clusters. In fact, the classifier k-means will be encircled by the maximum central, because it is prone to the original state. The recommended framework filters the attributes of the dataset that used a built-in rule engine to determine if the purchase is legitimate or illegitimate depending on several criteria of consumer activity (profile) such as regional areas, frequency of usage as well as book balance. Investigation demonstrates that perhaps the new model will advance the precision of detection in opposition to the probability of irregular transactions as well as have increasing consistency relation to conventional approaches.

Altyeb Altaher Taha et al. [2] proposed Smart method for identifying credit card theft utilizing an Automated Light Gradient Boost System. A Bayesian-based hyperparameter optimization algorithm is smartly implemented into the planned approach to tuning the parameters of a light gradient enhancing system (LightGBM). In order to show the efficacy of our experimental OLightGBM in identifying credit card fraud, tests were conducted utilizing two real-world government card transaction data sets composed of fraud as well as legal purchases. Focused on a compare with other methods utilizing the two data sets, the suggested solution exceeded the other solutions and obtained the best accuracy value (98.40 percent), accuracy (92.88 percent), accuracy (97.34 percent), as well as F1 (56.95 percent).

E. Saraswathiet al. [3] elucidate Artificial Neural Network (ANN) has the capacity to act like a human mind if appropriately equipped. We have also introduced SOM for reason of exactness. In this article the author addressed the network efficiency as well as its accuracy.

K. Karthikeyanet al. [4] detects credit card abuse utilizing machine learning algorithms. Firstly regular versions are included. Then hybrid techniques are implemented that utilize AdaBoost as well as methods of bulk vote. To test the feasibility of the model, a sample of credit card data is used and is publicly accessible. Then a Financial institution's real-world payment card data collection is assessed. Additionally, noise is applied to the data samples to help test algorithm robustness. Favorably, the investigational findings show that the plurality voting system reaches strong accuracy levels in the identification of credit card fraudulent events.

Diwakar Tripathi et al. [6] proposed usage of the local outlier element (LOF) for credit card fraud identification. We used the buying number as fraud verification. The planned program is introduced in MATLAB code, and device output is measured in terms of the system's factual unhelpful, fake optimistic rate as well as consistency over the various closest neighbours. Accurateness of the suggested solution varies among 60-69 per cent for dataset 1 and 96 per cent for dataset 2 with community variance.

Kuldeep Randhawa et al. [7] Suggested a strategy for the analysis of card fraudulent utilizing machine learning. Normal versions were first used following alternative versions were imagined using AdaBoost as well as plurality voting systems. The publicly accessible data collection was used for assessing the performance of the model. The experiments were conducted on the basis of the theoretical results which show that the majority of voting methods achieve good accuracy rates so that notice the fraudulent in the credit cards. The experimental data was applied to the noise of between 10 per cent to 30 per cent for further assessment of the hybrid versions. A strong result of 0.942 for 30 per cent applied noise was obtained through multiple voting processes. And it was assumed that in the midst of noise, the voting system displayed more reliable efficiency.

Abhimanyu Roy et al. [8] Deep learning topologies suggested for the analysis of online transaction abuse. This method is adapted through hierarchical artificial network of built-in time as well as remembrance elements for instance short long-term memory and many other parameters. I used centralized cloud storage system for strong efficiency. The researchers' proposed study offers an appropriate guide to the sensitivity analysis of the proposal criteria, based on the fraudulent detecting results. The researchers have suggested a method for the parameter tuning of topologies for detecting falsification in deep learning. This helps the financial company to popular the damages by eliminating illegal practices.

Shiyang Xuan et al. [9] used 2 forms of random woods, that educate regular and irregular transaction behavioral distinctiveness. The investigator contrasts these 2 random woods, that are distinguished by success in identify card fraudulent based on their classificators. The data used is from a China e-commerce business that is used to evaluate the output of the random forest model of these two forms. In this article the researcher utilized the B2C dataset to define as well as diagnose credit card fraud. Thus, the researcher concludes through the outcome that perhaps the proposal random forests have fine consequences on a limited dataset however are still troubles for instance unfair data that render it less successful than other dataset.

Johannes Jurgovskyet al.[12] phrased the issue of fraud identification as a sequence recognition function, utilizing Large Short-Term Memory (LSTM) networks to integrate sequences of transactions. The article also incorporates hi-tech aggregation techniques for apps as well as utilizes conventional retrieval measures to monitor our performance.

Dastgir Pojee et al. [13] proposed a novel mechanism using which the payment of invoice or bill is initiated. This approach is named as "NoCash" mobile application which is mainly used by the merchants through which the payment facility of clients can be eased. There is no need for NFC-Enabled Point of Sales (PoS) Machines in this approach and only the mobile phones are required. Minimizing the burden of clients for bringing cards when outside, by providing easy payment transferring mechanisms is the only aim for which this system is designed. The client's experience of shopping is improved when NoCash application that includes many features is applied on the basis of the increase in a number of NFC-based mobiles. To provide benefits to merchants, the fraud activities are minimized using this proposed application. The application clients can be related to the expense history and minimize any unwanted costs using this proposed method.

Zahra Kazemi et al. [15] planned deep auto encoder that is utilize to retrieve the good credit card transaction detail. It would also incorporate softmax functionality to address issues with the class names. An above-complete automatic encoder is being used to map the data into a high-dimensional domain, as well as a sparse model could be used in a concise fashion that offers advantages in classifying a form of deception. This is among the majority driven or efficient methods used to identify credit card fraudulent. Such kinds of networks have a dynamic data delivery that is really hard to understand. In certain points, Deep autoencoder was used to select the best data functionality as well as for identification needs. Better precision as well as low variance within such networks are also obtained.

Baoping Cai et al. [16] Provides a bibliographic analysis of the usage of BNs in fault diagnosis across the past years, with a emphasis on engineering. This research also provides general method for the modeling of fault diagnosis for BNs; procedures involve modeling of BN configuration, modeling of BN parameters, BN inference, detection of fault, confirmation and testing. The article presents a set of categorization systems for BNs for error analysis, BNs paired with additional methods as well as the defect diagnosis area for BN. At last, this review examines existing differences & problems, as well as a variety of avenues for potential studies.

N. Balasupramanian et al. [17] Proposed a machine learning methodology as well as Big Data Analytics to spot along with avoid fraudulent electronic purchases. The model requires the vast amount of electronic transaction data to be processed, and is then clean as well as functionality removed as well as the using the primary method of review of components. The decreased functions may be utilized to instruct the model of machine learning that detects as well as recognizes consumer habits relevant to e-transactions.

Suman Arora et al. [18] Suggested an strategy based on the sum rule of the Coefficient. This method is used to rate models for fraud prevention to determine the best model from different models for fraud detection. Different model selection parameters are provided for rating the FDMs, for a collection of FDMs. Actual data sets are utilized to clarify the Coefficient total process. The consequence of this thesis provides a system of rating dependent on the Total value of every FDM parameters.

John O. Awoyemi et al. [19] Suggested an analysis that assessed the output of multiple algorithms while applying heavily biased data on credit card fraud. The European cardowners' 284,807 transactions have been utilized as a guide to produce the credit card transaction dataset. A mixed method of under as well as over-sampling is conducted on the corrupted data. There are 3 separate approaches implemented in Python on the basis of raw or pre-processed data.

2.2 Inferences drawn from literature survey

S no.	Author's Name	Tool/Method Used	Paper Title	Application Domain	Inferences
1.	***Saad M. Darwish***	Intelligent two-level credit card fraud detection model	*An intelligent credit card fake identification way depends on semantic fusion of 2 classifiers.*	Semantic fusion of k-means as well as artificial bee colony algorithm (ABC)	Improve detection performance against the chance of fraudulent transactions to have better precision than conventional approaches.
2.	***Altyeb Altaher Taha et al.***	An intelligent method for identify fake in credit card transactions utilizing an optimized light gradient boosting machine (OLightGBM)	*An Intelligent method to Credit Card Fake Detection Utilizing an Optimized Light Gradient Boosting Machine.*	Bayesian-based hyper parameter optimization algorithm	The suggested solution outperformed the other methods and obtained the best quality value (98.40%), Field under receiver operating characteristic curve (AUC) (92.88%), Reliability (97.34%) as well as F1-score (56.95%).
3.	***E. Saraswathiet al.***	Artificial Neural Network (ANN)	*Credit Card Fraud forecast as well as recognition using Artificial Neural Network along with Self-Organizing Maps.*	SOM-Self algorithm	Examine the Network efficiency as well as its quality.
4.	**K. Karthikeyan *et al.***	Machine learning algorithms	*Credit Card Fake identification Using Machine Learning*	Hybrid methods which use AdaBoost	Positively, the experimental findings show that the plurality vote system reaches strong

					precision levels in the identification of credit card fake events.
5.	*Tinubuet al.*	HMM model	*Towards detecting credit card frauds using Hidden Markov Model*	Combination of K-Means and Baum Welch algorithms	. This approach was implemented using PHP and was tested with a simulated dataset. Four performance metrics were used on the model which includes a Fraud Detection Rate (FDR), False Alarm Rate (FAR), Accuracy (A) and Sensitivity (S) to design a credit card fraudulent discovery system.
6.	***Diwakar Tripathi et al.***	Local Outlier Factor (LOF)	*Credit card fake finding utilizing local outlier factor.*	MATLAB technology	Accuracy of the planned way is lying from 60-69% for dataset 1 as well as 96 % for dataset 2 with variation in neighbors.
7.	***Johannes Jurgovskyet al.***	Long Short-Term Memory (LSTM) networks	*Sequence classification for credit-card fake detection.*	Fake finding difficulty as a sequence categorization activity	Integrates modern aggregation techniques for apps and publishes our tests using standard methods for retrieval.
8.	***Dastgir Pojee et al.***	NFC-based intelligent fraud detection.	*Safe as well as fast NFC payment with data mining in addition to intelligent fake finding.*	No Cash mobile application	To provide benefits to merchants, the fraud activities are minimized using this proposed application.
9.	***Oberoi et al.***	Genetic Algorithm	*Credit Card Fake identification scheme: Utilizing Genetic Algorithm.*	Designing of the neural network	Genetic Algorithm could be utilized to build the neural network to address our credit question-bank fraud detection.
10.	***Suman Arora et al.***	Coefficient sum method	*collection of optimal credit card fake identification models utilizing a coefficient sum method*	Fraud detection models	This paper provides a classification system focused on the Total value of increasing FDM criterion.
11.	***John O. Awoyemi et al.***	Naïve Bayes, logistic regression approaches, and k-NN	*Credit card fake identification utilizing machine learning methods: A relative inspection.*	Python	It is shown from the results obtained that the efficiency of k-NN is higher relative to naïve Bayes as well as logistic regression approaches.
12.	***Aderemi O. Adewumiet al.***	Credit card fraud detection	*A study of machine-learning as well as nature-inspired focused credit card fraudulent identification methods*	Gives a picture of recent trend in credit card fraudulent detection.	This analysis acts as a roadmap and turning point for financial companies and individuals exploring innovative as well as successful strategies for identifying credit card fraudulent.
13.	***Dilip Singh Sisodia et al.***	Principal Component Analysis (PCA)	*Output review of the class matching strategies for identifying credit card fraud*	Evaluation of the performance of several sampling techniques on the classifier	This approach applied five over-sampling and four under-sampling approaches. Further, on the data, few cost sensitive and ensemble classifiers are applied.

3. CONCLUSION

E-commerce has come a long way since its inception. It has become an essential means for nearly all organizations, as well as government agencies for enhancing its efficiency in international trade. One of the major causes for the achievement of e-commerce is the easy online credit card transaction . Whenever we talk about monetary transactions, we also have to take financial fraud into consideration.

Financial fraud is an intentional crime in which a fraudster benefits himself/herself by denying a right to a victim or by obtaining financial gain . As credit card transaction is the very common method of paying in the recent years, the fraud activities have increased rapidly. Enterprises and public institutions are facing a massive problem as huge amount of financial loss are caused by fraud activities. As per The Nilson Report , the failure due to the credit card, debit card, and prepaid card fraud reached $16.31B worldwide in 2015. And the recent report by The Nilson Report shows that the gross fraud loss has reached $22.8B in 2018 which is 4% more than that in 2015 and it is expected to exceed by an even more significant amount in the coming years. According to Statista, as shown in figure 1.1, the gross fraud reached $5.6B in 2012, whereas in 2018, the fraud loss has reached $9.1B, which is approximately two-fifths of the total loss. In specifically, 70% of such fraudulent are Card-Not-Present (CNP) frauds (i.e., frauds conducted online or over the telephones), 20% are counterfeits and remaining 10% cases are related to losses due to lost or stolen cards [55].

4. REFERENCES

[1] Mani, P. K., and Dr K. Siddappa Naidu. "Unified Power Quality Conditioner (UPQC) with Hysteresis Controller for Power Quality Improvement in Distribution System." International Journal of Applied Engineering Research10.9 (2015): 9124-9130.

[2] Sukumaran, Jithin, Amal Thomas, and Avik Bhattacharya. "A reduced voltage rated unified power quality conditioner for harmonic compensations." Power India International Conference (PIICON), 2016 IEEE 7th. IEEE, 2016.

[3] Vijayasamundiswary, S., and J. Baskaran. "A novel approach to nine switch unified power quality conditioner for power quality improvement." Innovative Research In Electrical Sciences (IICIRES), 2017 International Conference on. IEEE, 2017.

[4] Bouzelata, Yahia, Erol Kurt, Rachid Chenni, and Necmi Altın. , "Design and simulation of a unified power quality conditioner fed by solar energy." international journal of hydrogen energy 40.44 (2015): 15267-15277.

[5] Gautam, A. K., Singh, S. P., Pandey, J. P., Payasi, R. P., & Gupta, N ,"Performance investigation of Unified Power Quality Conditioner for Power Quality improvement in distribution system." Electrical, Computer and Electronics Engineering (UPCON), 2016 IEEE Uttar Pradesh Section International Conference on. IEEE, 2016.

[6] Samal, Sarita, and Prakash Kumar Hota, "Power Quality Improvement by Solar Photo-voltaic/Wind Energy Integrated System Using Unified Power Quality Conditioner." International Journal of Power Electronics and Drive Systems8.3 (2017): 1424.

[7] Cheung, Victor SP, Shun Cheung Ryan YEUNG, Henry SH Chung, Alan WL Lo, and Weimin Wu, "A Transformer-less Unified Power Quality Conditioner with Fast Dynamic Control." IEEE Transactions on Power Electronics (2017).

[8] Vadivu, U. Senthil, and B. K. Keshavan, "Power quality enhancement of UPQC connected WECS using FFA with RNN." Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), 2017 IEEE International Conference on. IEEE, 2017.

[9] Senthilkumar, A., and P. Ajay-D-Vimal Raj, "ANFIS and MRAS-PI controllers based adaptive-UPQC for power quality enhancement application." Electric Power Systems Research126 (2015): 1-11.

[10] Kumar, R., Singh, B., Shahani, D. T., & Jain, C. (2017),"Dual-Tree Complex Wavelet Transform-Based Control Algorithm for Power Quality Improvement in a Distribution System." IEEE Transactions on Industrial Electronics 64.1 (2017): 764-772.

[11] Tareen, W. U., Mekhilef, S., Seyedmahmoudian, M., & Horan, B. (2017),"Active power filter (APF) for mitigation of power quality issues in grid integration of wind and photovoltaic energy conversion system." Renewable and Sustainable Energy Reviews 70 (2017): 635-655.

[12] Patjoshi, Rajesh Kumar, and Kamalakanta Mahapatra. "Resistive optimization with enhanced PLL based nonlinear variable gain fuzzy hysteresis control strategy for unified power quality conditioner." International Journal of Electrical Power & Energy Systems 83 (2016): 352-363.

[13] Hasan, Mashhood, Abdul Quaiyum Ansari, and Bhim Singh. "Parameters estimation of a series VSC and shunt VSC to design a unified power quality conditioner (UPQC)." Systems Conference (NSC), 2015 39th National. IEEE, 2015.

[14] Kow, K. W., Wong, Y. W., Rajkumar, R. K., & Rajkumar, R. K. (2016),"A review on performance of artificial intelligence and conventional method in mitigating PV grid-tied related power quality events." Renewable and Sustainable Energy Reviews 56 (2016): 334-346.

[15] Sharma, Ankit Kumar, Om Prakash Mahela, and Sheesh Ram Ola. "Detection of Power quality disturbances using discrete wavelet transform." Electrical Power and Energy Systems (ICEPES), International Conference on. IEEE, 2016.

[16] Das, Santanu, Arpan Kumar Pradhan, Ayush Kedia, Sovan Dalai, Biswendu Chatterjee, and Sivaji Chakravorti. "Diagnosis of Power Quality Events Based on Detrended Fluctuation Analysis." IEEE Transactions on Industrial Electronics 65, no. 9 (2018): 7322-7331.

[17] Monteiro, Luís Fernando Corrêa. "New Trends in Active Power Filter for Modern Power Grids." Power System Harmonics: Analysis, Effects and Mitigation Solutions for Power Quality Improvement (2018): 65.