

Fraud Detection and Prevention Using Machine Learning Algorithms: A Review

¹G. Jaculine Priya
Research Scholar, Department of
Computer Science
VELS Institute of Science
Technology & Advanced
Studies(VISTAS)
Chennai, Tamilnadu, India
privajaculine@gmail.com

²Dr.S. Saradha
Assistant Professor, Department of
Computer Science
VELS Institute of Science
Technology & Advanced
Studies(VISTAS)
Chennai, Tamilnadu, India
saradha.research@gmail.com

Abstract— Digital Fraud has become a threat across all the sectors. Its pivotal for any organization now to have a dedicated focus to detect and prevent fraud and increase their focus on Security. Digitization has revolutionized the way we perform our day to day transactions with a click of a button. On the flip side, it has also opened up threats through bad actors who can misuse the missing controls in digital apps and thereby impersonate themselves as real customers and perform costly transactions on their behalf resulting in financial losses. Organizations will have to pay attention as it also impacts its brand value. Organizations have learnt their lessons from the past to detect the fraudulent activities in real time by using multitude of factors like using complex algorithms trying to detect fraud patterns. However, fraudsters are also getting intelligent day by day and it requires continuous focus to prevent frauds and to stay ahead of the fraudsters. It is important to monitor key patterns that might help differentiate a real vs fraud transaction. Capturing Customer information like Geo location, authentication, session, device IP address can be maintained. Machine Learning and application of Artificial Intelligence will play an important part in learning and detecting fraud patterns automatically.

Keywords— *Fraudulent transactions, monitoring , authentication and real -time decision making, machine learning algorithms, cyber security, artificial intelligence*

I INTRODUCTION

Fraud attacks is a major issue when a message is transmitted through the communication channel. In this technical world the applications/tools what we are using its going on changing day by day. The transformation towards digitally helping all the sectors to improve drastically. At the same

time we are leaving our digital foot prints where ever and whenever we are using. It causes the users to be very caution about their credentials. The users are expecting secured environment to proactively to prevent from fraud. In this paper we will be discussing about how to boost the fraud prevention and detection features. Unfortunately, fraudsters don't seem to be lagging behind when finding loop holes with innovations. To safe guard the organization , should ensure their security measures keep step with the innovation efforts.

For example in the Banking Sector, in their daily transactions lot of fraudulent transactions are happening. If we are taking credit card fraudulent transactions alone, after the fraud happened it will be reported to the corresponding bank management. For the immediate solution bank is blocking the particular card for future transactions and advising his customer to change his password and related secured information.

After that only, the particular bank/corporate started working with, how this fraud activity happened, what pattern the fraudsters used to hack the customer account. Once they find the pattern, the banking/corporate sector will work towards the loop hole and take necessary security actions to stop permanently with the same pattern related fraudulent transactions. Meanwhile by using the same pattern fraudsters would have done multiple fraudulent transactions which leads to huge amount loss.

When face to face transaction demand is decreasing , Real time transaction are increasing due to fraction of second the works are getting complete. But the same time fraudsters are also become very intelligent to steal money from customers and organizations using different patterns[4]. So, the organizations have to address this problem and also responds

with the new approaches by bringing intelligent approaches and technologies to predict and prevent fraud. [6]

The report to the nation's 2020 global study on fraud cases is shown in the below figure 1.1



Fig 1.1 The Typical Fraud Loss by region



Fig 1.2 – Fraud Loss globally each year

From the above Fig1.2 can able to understand due to fraud huge amount money all the organizations are losing. Computer fraud is the threat/challenge faced by all the industries across all the sectors. All the industry should think about a paradigm shift in their approach to reduce the fraud risks moving forward[7]. Currently, Digital transformation happening rapidly in every field and the fraud risks arising. To mitigate this fraud risk the industry is desperately looking for fraud risk management framework in an efficient manner.[8] Existing framework available within the all institutions, are more over reactive soiled approach, costly to maintain, are not capable of finding complex fraud patterns and more over its not giving real time solution.

The rest of the paper is structured as follows. Literature Survey is described in section II. Need for Machine Learning In Fraud Detection in section III. Structure of Fraud Detection Algorithms using Machine Learning in Section IV.. The proposed model is illustrated in section V. Finally, section VI ends with conclusion.

II LITERATURE SURVEY

This section presents the various works which have been done in Computer Fraud and Security.

In this paper, Cashless payments becomes very convenient to the user to make payment without carrying cash in hand. High possibilities are there to stole individual information moving towards digital payments. Using imbalanced data set checked with different supervised machine learning algorithms, decision tree is the best suitable algorithm for detecting the fraud . [2]

In this Study, Fraudsters are bypassing the security checks in different illegal attempts which leads to loss of millions amount of money. For large dataset SVM combined with CNN and For smaller dataset SVM , Random Forest and KNN can provide enhanced results. [3]

Fraud Detection techniques becomes essential one to sustain the goodwill of the organization from customers. Proposing a predictive classification model by hybridizing KNN, Random Forest, Multi-layer, Bagging classifier and Extreme learning machine.[9]

Payment using credit card become a frequent mode of payment. Fraud associated with this payment also increased which leads to huge loss. Proposing an aggregate model using random forest to classify legitimate and fraudulent pattern. But, finally can observe random forest to over fit for some datasets with noisy classification/regression tasks.[10]

The growth in the credit card transactions has led to rise in the fraudulent activities. Customer or Customer card details are mandatory to do the transactions. The merchant also cant able find whether authentic cardholder or not. Random Forest is the proposed model to improve the sensitivity, accuracy, precision and specificity in fraud detection.[11]

Credit Card usage is one of the main functions of banking. Banks can identify the risk profile according to their activities. Random forest is the proposed algorithm due to its optimization and accuracy. SVM algorithm can be used, but due to its imbalanced data set problem its requires more pre-processing.[12]

This Paper is focused on real time credit card fraudulent transactions due to increasing in number to early days.

Technology also rapidly growing the pattern used by the fraudsters also changing smartly. By Collecting used data set of credit card and classify as test data set and train data set using random forest algorithm to analyse the performance based on the accuracy. [13]

In this paper credit card fraud happening due to its highly imbalanced data sets which carries both legitimate and fraudulent transactions. Different Supervised Machine Learning algorithms applied to compare their accuracy, recall, precision by using real world data set. [14]

III . NEED FOR MACHINE LEARNING IN FRAUD DETECTION

For years, fraud has been a serious issue in sectors like banking, medical, insurance and almost all the areas especially because of the rise in online transactions through different online mode like net banking, credit/debit cards payment, PhonePe. These transformations digitally helping all the sectors to do the work faster. But same time digital footprints left by the customers where ever they used. Moreover, fraudsters became terribly masterful to find escapes so they will loot additional. Nowadays, Machine Learning Algorithms in Artificial Intelligence provides intelligent solutions to most of the problems that manual and traditional approach beings find tough to deal with particularly within the field of fraud detection. Previously, industries were believing in their employee and their historical approach to find out fraud preventions and detection. Government and across the all sector organizations is spending more money to prevent fraud. Traditional method is no longer enough to solve this problem. In the historical approach, the algorithms are written by fraud domain experts. The methods and algorithms currently used are strictly based on rules. Also, the need of the hour is to prevent fraud proactively rather than current reactive approaches. Due to the popularity, efficiency, speed and accuracy of Artificial Intelligence, every industry now moving from the historical approach to fraud detection method using ML-based solutions.

Fraud detection and prevention algorithm can be able to learn by itself find complex hidden patterns. It's not a static process. It's an ongoing process. Organizations ought to

attempt to continually learn from fraud patterns. This need complete life cycle approach which consists of monitoring, learning, detecting, preventing and improving in real time decision making. Fraud Detection using Machine Learning, a machine tries to be learn by itself and becomes higher by expertise. With the right Supervised and Unsupervised learning algorithms, we will be able to prevent and detect the fraudulent transactions. The advantage here is, we can leverage either of the models or use both in tandem to detect anomalies.

IV STRUCTURE OF FRAUD DETECTION ALGORITHMS USING MACHINE LEARNING

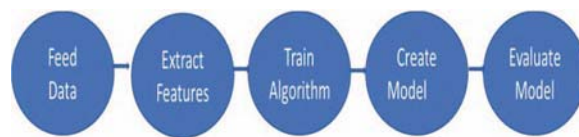


Fig 3.1 Structure of Fraud Detection ML Algorithm

The accuracy of the model depends upon amount of the training data sets and test data sets . Extract fraud pattern from the data sets like channels/patterns used by the fraudsters. Accordingly can train the detection algorithm to differentiate between genuine and fraud transactions. Trained model can start detecting and preventing fraud transactions real time allowing the transaction to be rejected or kept on hold for further analysis. Using proposed Centralized Global Model this newly find fraud pattern can be shared across the organizations.[1]Companies need to join hands sharing their fraud experiences, it will prevent fraud globally and win-win situation for all the organizations.

V PROPOSED MODEL

Machine Learning Algorithms can be used in fraud detection, since the algorithms can be trained by using the test data set to give quick , accurate and efficient result. This need complete life cycle approach which consists of monitoring, learning, detecting, preventing and improving in real time decision making. With sophisticated Machine Learning Algorithms in place now, if used in the right way, will play an extremely crucial role in prevent fraudulent transactions. In order to stay ahead of the fraudsters, organizations should come forward to share fraudulent historical activities instead of restricting themselves within a boundary as per the proposed model.

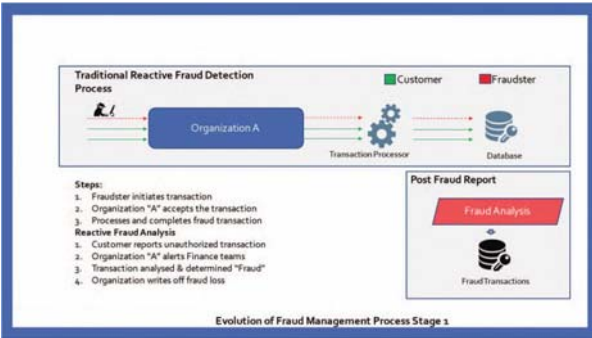


Fig 5.1. Evolution of Fraud Management Process–Stage 1

The proposed method is divided in to two stages, the first stage is to identify the pattern of the Fraud and the second stage is to enhance the security methods.

Stage 1 : Pattern Identification

In the proposed method, fraudulent transactions are identified after the loss of the fraudulent activity .Based on the fraudulent activity the pattern/path can be identify used by the organization. These patterns can be stored in database. [Fig 5.1]

Stage 2 : Security Enhancement

Based on the these patterns only security can be improved by resolving the security threat faced already by the customer. Each organization having their own security model to provide a secure environment to the customers[Fig 5.2]. In the proposed method , patterns from organizations are maintained in a centralized global database and any real time transaction is verified and validated for fraud. Geo location , IP Address, Date, Time are some of the critical fraud related attributes that can be shared and stored centrally.

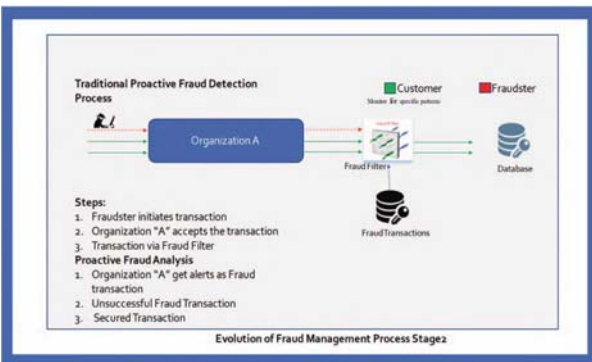


Fig 5.2. Stage 2 Evolution of Fraud Management Process

Though, frame works are available to detect frauds and alert about the fraudulent transactions with in the organization, it’s siloed and does not allow other organizations to learn from each other and minimize fraud impact. That’s the reason why industry is looking for some real time platform that alerts organizations globally and learns from history automatically. Here Proposing a global model leveraging artificial intelligence and machine learning techniques. A centralized fraud management platform is the need of the hour to facilitate a shared fraud prevention approach. Proposal is to develop an operating platform to bring organizations across the globe to leverage this framework through adhering to its standards and hence share and leverage fraud patterns to proactively alert and be alerted on fraudulent transactions there by building a strong layer of protection for their applications. For these need to go for digital handshake between organizations. These organizations can share the Database in a uniformly accepted structure by the organizations those who got into the agreement. Now the fraud transactions will be accessed by all accordingly remaining organization can take the preventive security measurement to avoid huge loss. This centralized structure can be implemented in across all the sectors like financial sector, telecom industry, stock market, online sector and social engineering area. Today’s industry needs to create a dynamic, intelligence driven approach to cyber risk management not only to prevent, but also detect, respond to, and recover from the potential damage that results from these attacks.

VI CONCLUSION

Siloed approach to prevent fraud is not an effective model, rather organizations will have to come together and share their historical fraud impacts. A centralized fraud management platform is the need of the hour to facilitate a shared fraud prevention approach. Proposal is to develop an operating framework and model to bring organizations across the globe to leverage this framework through adhering to its standards and hence share and leverage fraud patterns to proactively alert and be alerted on fraudulent transactions there by building a strong layer of protection for their applications. Companies join hands sharing their fraud experiences with the

right technology in place and applying modern techniques on top of the data provided it will prevent fraud globally and win - win situation for all the organizations.

[18] Seeja, K.R. and Masoumeh Zareapoor, "Fraud Miner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining", The Scientific World Journal, Hindawai Publishing Corporation, Volume 2014, Article ID 252797, pp. 1-10

REFERENCES

- [1] G. Jacqueline Priya and Dr.S.Saradha., "Real Time Global Fraud Detection and Prevention", International E-Conference On Advances In Information Technology.,June-2020 BIHER.,ISBN NO.978-93-5407-796-8
- [2] Samidha Khatri.,Aishwarya Arora., and Arun Prakash Agarwal., "Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison",.IEEE.,2020
- [3] Pradheephan Raghavan., and Neamat EI Gayer., "Fraud Detection using Machine Learning and Deep Learning",.International Conference on Computational Intelligence and Knowledge Economy.,IEEE,December 2019
- [4] Mehak Mahajan and Sandeep Sharma., "Detect Fraud in Credit Card using Data Mining Techniques",. International Journal of Innovative Technology and Exploring Engineering.,ISSN:2278-3075,Volume 9,Issue 2,December 2019
- [5] Mandeeep Singh and Sunny Kumar and Tushant Garg., "Credit Card Fraud Detection Using Hidden Markov Model",. International Journal Of Engineering And Computer Science, Volume 8, Issue 11, NOVEMBER 2019. pp.24878-24882
- [6] Olawale Adepoju., Julius Wosowei., Shiwani lawte and Hemaint Jaiman.,"Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques",. Global Conference for Advancement in Technology,IEEE, 2019,978-1-7281-3694-3
- [7] Shiv Shankar Singh ., "Electronic Credit Card Fraud Detection System by Collaboration of Machine Learning Models",. International Journal of Innovative and Exploring Engineering, ISSN:2278-3075,Volume 8,Issue 12S, October 2019, pp.92-95.
- [8] Maniraj, S.P., Aditya Saini., Swarna Deep Sarkar and Shadap Ahmed., "Credit Card Fraud Detection Using Machine Learning and Data Science",. International Journal of Engineering Research & Technology,ISSN:2278-0181,Volume 8,Issue 9, SEPTEMBER-2019.
- [9] Debachudamani Prusti., and Santanu Kumar Rath., "Fraudulent Transaction Detection in Credit Card by Applying Ensemble Machine Learning techniques",.10th ICCCNT July 2019., IEEE
- [10] Swatee Kadu.,Shailesh Kumar.,Ajay Wankhade., and Sharmila Kharat., "Credit Card Fraud Detection Using Random Forest and SMOTE tool ",.Journal of Applied Science and computations.,ISSN:1076-5131.,Voulme 6,Issue 6,June 2019
- [11] Devi Meenakshi B.,Janani B.,Gayathri S., and Indira N., "Credit Card Fraud Detection Using Random Forest",. International Research Journal of Engineering and Technology (IRJET).ISSN:2395-0056,Volume 06,Issue 03,March 2019
- [12] S Monika., K Venkataramanamma., P Pritto Paul.,and M Usha., "Credit Card Fraud Detection Using Random Forest",. International Journal of Research in Engineering and Technology".ISSN:2581-5792,Volume 2,Issue 3,March 2019
- [13] Yashvi Jain., Namrata Tiwari., Shripriya Dupey., and Sarika Jain., "A Comparative Analysis of Various Credit Card Fraud Detection Techniques",. International Journal of Recent Technology and Engineering,ISSN:2277-3878,Volume 7,Issue 5S2, January 2019
- [14] Anish Halimaa A and Dr. K.Sundarakantham "Machine Learning Based Intrusion Detection System",.ISBN:978-1-5386-9439-8.,IEEE 2019
- [15] Vaishnave Jonnalagada.,Priya Gupta., and Eesita Sam "Credit Card Fraud Detection Using Random Forest Algorithm",. International Journal of Advance Research, Ideas and Innovations in Technology",.ISSN:2454-132X,Voulme 5,Issue 2.,2019
- [16] Sahil Dhankhad., Emad A. Mohammed.,and Behrouz Far., "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study",.International Conference on Information Reuse and Integration for Data Science.,IEEE.,2018
- [17] Masoumeh Zareapoor, Pourya Shamsolmoali, "Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier", Elsevier, 2015, pp.679-685.