Online Fraud Detection Using Deep Learning Algorithm

Rubin Bose S*
Assistant professor
Department of Electronics and Communication Engineering
SRM Institute of Science and Technology, Ramapuram,
Chennai, India.
rubinbos@srmist.edu.in

CHIRANJEEVI S[1], SUKJAL K[2], SADWIK N[3],
[1,2,3] UG student
Department of Computer Science and Engineering
SRM Institute of Science andTechnology,
Ramapuram, Chennai, India.

***Abstract*—**Fraudsters find it easy to commit credit card fraud because it is an easy target. There has been an increase in online payment modes in due to e-commerce and other online platforms, there is now a higher danger of online fraud. Due to an increase in fraudulent online transactions, researchers have begun to evaluate and detect fraud using machine learning. In order to examine past transaction information and extract consumer behavioral patterns, our main goal in this study, a novel fraud detection algorithm for streaming transaction data is built and created. A system that clusters cardholders according to the amount of their transactions. In order to extract the behavioral pattern of the groups, we should aggregate the sliding window method transactions done by cards from various groupings. It is then decided which classifier with the best rating score can be chosen as one of the best methods to predict frauds after training different classifiers over the groups separately.

I. INTRODUCTION

Online fraud detection systems typically focus on new account origination, account takeover and payment fraud. With account takeover and new account origination fraud detection, organizations attempt to root out unauthorized or fraudulent users posing as legitimate users. Payment fraud detection involves determining whether purchases are being or have been made with stolen payment cards.

Numerous inventions in the field of artificial intelligence and vision-based technologies made the real-time active protecting system simpler. The tasks like object classification and detection have achieved impressive milestones because of improvements in deep learning and current machine technologies.

Some vendors also offer fraud intelligence services, authentication, malware detection(such as man-in-the-browser infections on computers and mobile devices) and secure clients, as well as managed services in which the vendor is primarily responsible for monitoring and taking action on instances of fraud.

In this paper shows how the model is related to convolutional neural networks and afterward adding classifiers algorithms, for example, Isolation Forest, Local Outlier, and SVM can be utilized to recognize misrepresentation. As a result, concept drift can be solved via a feedback mechanism. We used the Kaggle credit card fraud dataset for this article algorithm that is Online fraud detection is the use of the internet to defraud or take financial advantage of you. Fraudsters do this by accessing your online bank account or by presenting you with false offers in order to get you to transfer money or provide them with your card details. The internet is part of our daily lives for shopping, banking and connecting socially. While it brings many opportunities it also allows criminals attempt crimes from a distance reducing their chances of being caught. Online fraud comes in many forms.

II. LITERATURE REVIEW

Ahmed et al. [1] suggested Online fraud detection theory is the foundation for safeguarding digital transactions and interactions against fraudulent activities. It is a multifaceted field that draws upon a variety of techniques and algorithms to proactively identify and prevent fraudulent behavior in the digital realm. These methods range from simple rule-based systems that establish predefined criteria to sophisticated machine learning and deep learning models that adapt and evolve based on historical data.

Bhattacharyya et al. [2] presents this paper we developed a novel method for fraud detection, where customers are grouped based on their transactions and extract behavioural patterns to develop a profile for every cardholder. Then different classifiers are applied on three different groups later rating scores are generated for every type of classifier. This dynamic changes in parameters lead the system to adapt to new cardholder's transaction behaviours timely. Followed by a feedback mechanism to solve the problem of concept drift. We observed that the Matthews Correlation Coefficient was the better parameter to deal with imbalance dataset. MCC was not the only solution. By applying the SMOTE, we tried balancing the dataset, where we found that the classifiers were performing better than before. The other way of handling imbalance dataset is to use one-class classifiers like one-class SVM. We finally observed that Logistic regression, decision tree and random forest are the algorithms that gave better results

Vaishnavi et al [3], suggested As in today's era of technology, especially in the Internet commerce and banking, the transactions by the Mastercards have been increasing rapidly. The Mastercard becomes the highly useable equipment for Internet shopping. This increase in use causes a considerable damage and enhances inflation rate of fraud cases also. It is very much necessary to stop the fraud transactions because it impacts on financial conditions over time the anomaly detection is having some important application to detect the fraud detection. This paper has reviewed several algorithms to identify fraud in card transaction. Autoencoder is used to classify the alert as fraudulent or even authorized in spark environment. Next, it will aggregate every probability to discover alerts. Further, proposed model utilizes ranking approach where alert is positioned based on priority. The model

is able to resolve the class imbalance. In today's era, we just detect the fraudulent transaction, but we are not able to prevent it. Preventing fraud transaction dynamically is not easy, but it is possible. The system which proposed is design to detect fraud transaction, but in future by some advancement, it can became fraud prevention system

Zhang et al. [4] suggested This paper addressed credit card fraud detection using AIS (Artificial Immune System), and a new model called AIS-based Fraud Detection Model (AFDM) was introduced for this purpose. The model added some improvements to AIRS (Artificial Immune Recognition System) algorithm which helped to increase the precision, decrease the cost and system training time. Affinity between antigens was calculated using a novel method in AFDM. Negative Selection was used along with Clonal Selection in order to.

Phua et al. [5] Ultimately, online fraud detection is vital for protecting digital ecosystems, including financial institutions, e-commerce platforms, and user data. It serves as a crucial defense against financial losses, reputational damage, and security breaches in an increasingly interconnected and digital world, where the threats of online fraud are ever-evolving.

Cardenas et al. [6] presents In this paper we showed that better result is achieved with ANN when trained with simulated annealing algorithm. As the result shows that the training time is high but the fraud detection in real time is considerably low and the probability of predicting the fraud case correctly in online transaction is high, which is a main measure to evaluate any ANN. In the table 3 we can see that 65% of total fraud case is correctly classified which is a very high percentage in comparison with genetic, resilient backpropogation and any other training algorithm. The main problem in credit card fraud detection is the availability of real world data for the experiment. This approach can also be used in other applications which require classification task [20] e.g. software failure prediction, etc.

Phua et al. [7], The process begins with the collection of data from diverse sources, such as transaction records, user profiles, and network logs. This data is then subjected to preprocessing, where it is cleaned, structured, and transformed into a suitable format for analysis. Feature engineering plays a crucial role in creating relevant attributes from the data, enabling algorithms to distinguish between normal and fraudulent patterns effectively.

Neda et al [8] The appropriate algorithm is a pivotal step in online fraud detection. Various approaches, including supervised and unsupervised machine learning, anomaly detection, and ensemble methods, can be employed depending on the specific fraud detection requirements and the nature of the data.

Azeem Ush et al [9] The appropriate algorithm is a pivotal step in online fraud detection. Various approaches, including supervised and unsupervised machine learning, anomaly detection, and ensemble methods, can be employed depending on the specific fraud detection requirements and the nature of the data.

Bhatia et al [10] Model training is the next step, where machine learning models are trained on historical data labeled as fraudulent or non-fraudulent transactions. Real-time monitoring systems continuously analyze incoming data, scoring each transaction or interaction for signs of suspicious behavior. When a potential fraud case is detected, alerts are generated, initiating further investigation or actiotion..

Joy et al [11] Continuous improvement is integral to the effectiveness of online fraud detection systems. Feedback loops ensure that the models are regularly updated with new data and insights gained from investigations. Post-processing techniques are applied to reduce false positives, fine-tuning the system's performance

Ragavendra et al [12] In this paper we saw different technique that is being used to execute credit card fraud how credit card fraud impact on the financial institution as well as merchant and customer,fraud detection technique used by VISA and MasterCard.Neural network is a latest technique that is being used in different areas due to its powerful capabilities of learning and predicting.

Venkata et al [13] In this thesis we try to use this capability of neural network in the area of credit card fraud detection as we know that Back propagation Network is the most popular learning algorithm to train the BPN is used for training purpose and then in order to choose those parameter (weight, network type, number of layer, number of node e.t.c) that play an important role to perform neural network as accurately as possible, we use genetic algorithm, and using this combined Genetic Algorithm and Neural Network (GANN) we try to detect the credit card fraud successfully. The idea of combining Neural Network and genetic Algorithm come from the fact that if a person is inherently very talented and he is trained properly then chances of individual of success is very high.

Sarita et al [14] An observational analysis has been conducted on respective machine learning strategies except for random forest, tree classifiers, artificial neural networks, vector supporting machine, Naïve Baiyes, logistic regression as well as gradient boosting classifier techniques, but also multiple such as precision, recall, F1-score, accuracy, and FPR percentage, for any method which has better results for evaluation parameters can be treated as best performing method. Here Random forest is showing better results as compared to In future work proposed method can be implemented and tested on large size realtime data with different more machine learning methods

Elena et al [15] The model used accounts for categorical values and data unbalance. Feature engineering and selection allowed us to improve the detection performance step by step.The literature confirms that the chosen algorithm can significantly outperform XGBoost (eXtreme Gradient Boosting) and SGB (Stochastic Gradient Boosting) in terms of computational speed and memory consumption (Ke et al., 2017; Chen and Guestrin, 2016; Mitchell and Frank, 2017). Also, in the study made by Ke et al (2017), we find the idea that LightGBM algorithm is the fastest while maintaining almost the same accuracy as baselines.The barrier in our experiment was the fact that the data and 19 features and performance was limited by insufficient resources for training with all the dataset.

III . REFERENCES

[1] Samir Chopra, Suman Bharti, Tarun Singh Negi, P. D Kulkarni, “Missile Detection by Ultrasonic and Auto Destroy System,” (IJESRT)May 2014.

[2] S Nagakishore Bhavanam, Acharya Nagarjuna, Microcontroller Based Missile Detection and Destroying System. (ICIECE), July 2014.

[3] Ms. Palwe Pooja Balasaheb, Ms. Shinde Tejashree Anil, Ms. Sonawane Chaitali Shivajirao, and S. M. Bhilegaonkar, “Missile Detection and Auto Destroy System on a Robot Platform. (IJSRD), 2015.

[4] K. Anbalagan, V. Divakar, Y. Sathik Basha, and M. Senthil Kumar, “Automatic Mystery Detection and Destroy Using Embedded Systems,” (IJRE), 2016.

[5] Yang, Y & Song, H & Wang, P & Zhang, Y. (2020). A simulation method of active protection system defeat probability. Journal of Physics: Conference Series. 1507. 082020. 10.1088/1742- 6596/1507/8/082020.

[6] Likun Yang and Jiagang Xu 2021 J. Phys.: Conf. Ser. 1855 012034.

[7] Bose. S. R., Kumar. V. S. “Efficient Inception-V2 based Deep Convolutional Neural Network for Real-Time Hand Action Recognition”. *IET Image Processing*, Vol. 14, no. 4, pp. 688 – 696. 2022

[8] Bose. S. R., Kumar. V. S., “Precise Recognition of Vision-Based Multi-hand Signs Using Deep Single Stage Convolutional Neural Network”. In: Singh S.K., Roy P., Raman B., Nagabhushan P. (eds), *Computer Vision, and Image Processing. CVIP 2020*. *Communications in Computer and Information Science*, vol 1377. *Springer*, Singapore. https://doi.org/10.1007/978-981-16-1092-9_27.

[9] Bose. S. R., Kumar. V. S., ‘In-situ Identification and Recognition of Multi-hand Gestures Using Optimized Deep Residual Network’. Journal of Intelligent & Fuzzy Systems, vol. 41, no. 6, pp. 6983-6997, 2021.

[10] Bose. S. R., Kumar. V. S., ‘In-situ recognition of hand gesture via Enhanced Xception based single-stage deep convolutional neural network’. *Expert Systems with Applications*, Volume 193, 116427. 2022

[11] Sreekar. C., Sindhu. V. S., Bhuvaneshwaran. S., Bose. S. R., and Kumar., V.S., "Positioning the 5-DOF Robotic Arm using Single Stage Deep CNN Model," *Seventh International conference on Bio Signals, Images, and Instrumentation (ICBSII)*, pp. 1-6, 2021 doi: 10.1109/ICBSII51839.2021.9445124.

[12] Nepal, U.; Eslamiat, H. Comparing YOLOv3, YOLOv4 and YOLOv5for Autonomous Landing Spot Detection in Faulty UAVs. Sensors 2022, 22, 464. https:// doi.org/10.3390/s22020464

[13] Rahman, E.U.; Zhang, Y.; Ahmad, S.; Ahmad, H.I.; Jobaer, S. Autonomous vision-based primary distribution systems porcelain insulators inspection using UAVs. Sensors 2021, 21, 974

[14] Ge, Z.; Liu, S.; Wang, F.; Li, Z.; Sun, J. Yolox: Exceeding yolo series in 2021. arXiv 2021, arXiv:2107.08430

[15] Yan B, Fan P, Lei X, Liu Z, Yang F. A Real-Time Apple Targets Detection Method for Picking Robot Based on Improved YOLOv5. Remote Sensing. 2021; 13(9):1619. https://doi.org/10.3390/rs13091619.