Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

ONLINE MARKETING SYSTEMS ADAPT TO HIGH-LEVEL SECURITY AND DATA HANDLING TECHNOLOGY SOLUTIONS USING MACHINE LEARNING

BATTU VASANTHI , MCA, DCA, DVR & Dr.Hima Shekar MIC College of Technology, A.P., India.

SK.UDDANDU SAHEB, Assistant Professor, Dept.of AI & IT, DVR & Dr.Hima Shekar MIC college of Technology, A.P., India.

Abstract— This paper reviews the different advance technologies commonly used to deal with this type of data forms a comparison among them and suggests the most efficient and informative method to use in this sector. Through the end of the review, feature engineering and its selection of parameters for achieving better performance are discussed. This makes online marketing systems adapt to high-level security and data handling technology solutions like machine learning, deep learning and predictive analytics which are efficient enough to deal with highly sensitive data, predict frauds and unwanted behavioral patterns in this data.

INTRODUCTION

Fraud detection in online shopping systems is the hottest topic nowadays. Fraud investigators, banking systems, and electronic payment systems such as PayPal must have an efficient and complex fraud detection system to prevent fraud activities that change rapidly. According to a CyberSource report from 2017, the present fraud loss by order channel, that is, the percentage of fraud loss in their Web store was 74 percent and 49 percent in their mobile channels. Based on this information, the lesson is to determine anomalies across patterns of fraud behavior that have undergone change relative to the past The rising of E-commerce business has resulted in a gentle growth within the usage of credit cards for online transactions and purchases. With the rise in the usage of credit cards, the number of fraud cases has also been doubled. Credit card frauds are those which are done with an intention to gain money in a deceptive manner without the knowledge of the cardholder.

LITERATURE REVIEW

[1] Saputra, Adi & Suharjito, Suharjito. (2019). Fraud Detection using Machine Learning in e-Commerce. 10.14569/IJACSA.2019.0100943.

The volume of internet users is increasingly causing transactions on e-commerce to increase as well. We observe the quantity of fraud on online transactions

is increasing too. Fraud prevention in e-commerce shall be developed using machine learning, this work to analyze the suitable machine learning algorithm, the algorithm to be used is the Decision Tree, Naive Bayes, Random Forest, and Neural Network. Result of evaluation using confusion matrix achieve the highest accuracy of the neural network by 96 percent, random forest is 95 percent, Naïve Bayes is 95 percent, and Decision tree is 91 percent. Synthetic Minority Over-sampling Technique (SMOTE) is able to increase the average of F1-Score from 67.9 percent to 94.5 percent and the average of G-Mean from 73.5 percent to 84.6 percent.

[2] Renjith, Shini. (2018). Detection of Fraudulent Sellers in Online Marketplaces using Support Vector Machine Approach. International Journal of Engineering Trends and Technology. 57. 48-53. 10.14445/22315381/IJETT-V57P210.

The e-commerce share in the global retail spend is showing a steady increase over the years indicating an evident shift of consumer attention from bricks and mortar to clicks in retail sector. In recent years, online marketplaces have become one of the key contributors to this growth. Fraudulent e-commerce buyers and their transactions are being studied in detail and multiple strategies to control and prevent them are discussed. Another area of fraud happening in marketplaces are on the seller side and is called merchant fraud. Goods/services offered and sold at cheap rates, but never shipped is a simple example of this type of fraud. This paper attempts to suggest a framework to detect such fraudulent sellers with the help of machine learning techniques.

[3] A. K. Rai and R. K. Dwivedi, "Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 421-426, doi: 10.1109/ICESC48915.2020.9155615.
Development of communication technologies and e-commerce has made the credit card as the most common technique of payment for both online and regular purchases. So, security in this system is highly expected to prevent fraud transactions. Fraud transactions in credit card data transaction are increasing each year. In this direction, researchers are also trying the novel techniques to detect and prevent such frauds. However, there is always a need of some techniques that should precisely and efficiently detect these frauds. This paper proposes a scheme for detecting frauds in credit card data which uses a Neural Network (NN) based unsupervised learning technique. Proposed method outperforms the existing approaches of Auto

Encoder (AE), Local Outlier Factor (LOF), Isolation Forest (IF) and K-Means clustering. Proposed NN based fraud detection method performs with 99.87% accuracy whereas existing methods AE, IF, LOF and K Means gives 97%, 98%, 98% and 99.75% accuracy respectively.

IMPLEMENTATION

1. System:

1.1Store Dataset:

The System stores the dataset given by the user.

1.2Model Training:

The system takes the data from the user and fed that data to the selected model.

1.3 Model Predictions:

The system takes the data given by the user and predict the output based on the given data.

1.4Graphs Generation:

The system takes the dataset given by the user, selects the model and generates the graph corresponding to the selected model

2. User:

2.1 Load Dataset:

The user can load the dataset he/she want to work on.

2.2 View Dataset:

The User can view the dataset.

2.3 Select model:

User can apply the model to the dataset for accuracy.

2.4 Predictions:

User can enter random values for prediction.

2.5 Graphs:

User can evaluate the model performance using the graphs.

PROPOSED WORK

In existing system, models are build based on Logistic Regression and K-Means clustering to estimate fraudulent and non-fraudulent transactions. This techniques gives low precision scores and recall scores and also lacks the robustness because of higher computational time.

DISADVANTAGES:

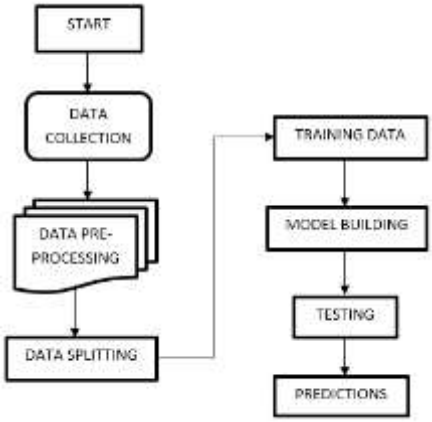
- Low accuracy.
- Time consuming.
- High complexities.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

PROPOSED METHOD

We propose this system to investigate a problem of whether it is valuable or not to use machine learning techniques to detect whether the credit card is fraud or not fraud using Decision Trees, KNN Classifier, Random Forest Algorithm.

Flow of the project:



ADVANTAGES:

- High accuracy.
- Time Saving.
- Low complexities.
- High reliability.

CONCLUSION

In this paper, we propose created unsupervised models to detect whether the transaction is fraud or not fraud. We noticed that out of Extreme Gradient Boosting, Random Forest, KNN, Random Forest performs well with good accuracy along with good precision and recall scores.

REFERENCES

[1] Taha, Altyeb&Malebary, Sharaf. (2020). An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine. IEEE Access. 8. 25579-25587.

[2] Assaghir, Zainab&Taher, Yehia&Haque, Rafiqul&Hacid, Mohand-Said &Zeineddine, Hassan. (2019). An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection. IEEE Access.

[3] L. Meneghetti, M. Terzi, S. Del Favero, G. A Susto, C. Cobelli, “DataDriven Anomaly Recognition for Unsupervised Model-Free Fault Detection in Artificial Pancreas”, Ieee Transactions On Control Systems Technology, (2018) pp. 1-15

[4]F. Carcillo, Y.-A. Le Borgne and O. Caelen et al., “Combining unsupervised and supervised learning in credit card fraud detection”, Information Sciences, Elsevier (2019), pp. 1-15.

[5] Ashphak, Mr. & Singh, Tejpal& Sinhal, Dr. Amit. (2012). A Survey of Fraud Detection System using Hidden Markov Model for Credit Card Application Prof. Amit Sinhal. 1.

[6] Renjith, Shini. (2018). Detection of Fraudulent Sellers in Online Marketplaces using Support Vector Machine Approach. International Journal of Engineering Trends and Technology. 57. 48-53. 10.14445/22315381/IJETT-V57P210.

[7] Saputra, Adi & Suharjito, Suharjito. (2019). Fraud Detection using Machine Learning in e-Commerce. 10.14569/IJACSA.2019.0100943.

[8] A. K. Rai and R. K. Dwivedi, "Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 421-426, doi: 10.1109/ICESC48915.2020.9155615.

[9] John O. Awoyemi, Adebayo O. Adetunmbi, Samuel A. Oluwadare et al., “Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis”, IEEE, 2017.

[10] Rajendra Kumar Dwivedi, Sonali Pandey, Rakesh Kumar “A study on Machine Learning Approaches for Outlier Detection in Wireless Sensor Network” IEEE International Conference Confluence, (2018).

About authors:

MR.SK.UDDANDU SAHEB He Completed Master of Computer Application in Kavitha PG Memorial College, jaggayyapeta, NTR(DT). Currently working as an Assistant professor in the department of AI and IT at DVR & DR. HS MIC College of Technology (Autonomous), Kanchikacherla, NTR(DT). His areas of interest include C language, Data science, Java and Python.

Ms. BATTU VASANTHI is MCA Student in the department of DCA at DVR & DR. HS MIC College of Techonology (Automonous), Kanchikacherla, NTR(DT). Her Completed B.Sc. (electronics) in Autonomous Government college , Rajahmundry. Her areas of interests are Machine Learning, Java and Data Analytics.