www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 449-451

e-ISSN : 2583-1062

Impact Factor : 5.725

FRAUD DETECTION USING DATA MINING

Subbaiah. S[1], Akash. M[2], Kishore Kumar. J[3]

[1]Assistant Professor, Departement Of Computer Science, Sri Krishna Arts And Science College Coimbatore, India

[2,3]Student, Departement Of Computer Science, Sri Krishna Arts And Science College Coimbatore, India

ABSTRACT

Credit card fraud has become one of the most prevalent problems in the credit card industry. A basic thought process is to distinguish between different types of credit card counterfeiting and review the optional techniques that have been used to detect fraud. Depending on the different types of credit card fraud faced by financial institutions such as banks and credit card companies, different measures can be takento reduce fraud. The purpose of using these strategies and techniques is to minimize credit card fraud. There are certain unsolved problems with existing techniques that result in some legitimate credit card customers being identified as fraudulent. This white paper focuses on including the best classification algorithms from a set of four different algorithms that are likely to indicate the level of fraud in the financial sector. Data mining (DM) includes core algorithms that enable data beyond basic insight and knowledge. In fact, data mining is part of the knowledge discovery process. A credit card provider (CC) allows customers to use multiple cards. All credit card users must be genuine and honest. Dealing with every mistake can lead to a financial crisis. With cashless transactions growing rapidly, counterfeit transactions are also unlikely to increase. Fraudulent transactions can be identified by looking at credit cards that behave differently than previous transaction history records. Any deviation from the available cost pattern is a bogus trade. DM and machine learning (MLT) techniques are commonly used to detect credit card fraud (CCFD).

1. INTRODUCTION

A credit card is a large, convenient plastic card that contains personal information such as your signature, photo, card number, magnetic stripe/chip data, etc., and allows the person named on the card to charge purchases and manage your account. I can. They are billed from time to time. Card data is now accessed via automated ATM(TM), bar code readers in stores and banks, and is also used in his web banking framework online. Most importantly have a unique her CCV number. Security, much like the protection of credit card numbers, relies on the physical security of plastic cards [1]. The number of credit card exchanges is increasing rapidly, resulting in a significant increase in fraud. Credit card fraud is a general term that refers to theft or misrepresentation of credit cards as a source of fraudulent and fraudulent assets on certain exchanges. Often, measurable strategies and numerous information mining computations are used to solve this fraud detection problem. Also known as artificial intelligence, most credit card extortion frameworks are based on artificial thinking, learning,and pattern matching

2. LITERATURE REVIEW

Research into data mining techniques for detecting credit card fraud began in the last two decades. Chan et al. (1999) addressed the growth of credit card transactions in the US payment system under consideration. It leads to an increase in stolen credit card accounts. In the early days of credit cards, banks faced a major problem of analyzing large amounts of transaction data very efficiently.Calculate fraud detector in time. There are also some issues related to skewed distribution of training data and uneven cost per error. Chan et al. (1999) conducted a study to address the top three issues related to credit card transactions specifically in ecommerce, including scalability, efficiency, and technical issues. Chang et al. (1999) proposed a fraud detection model characterized by a combination of multiple fraud detectors, called distributed data mining of the model. This represents a significant reduction in credit card fraud. Rather than using a single algorithmic technique, the second research group focused on applying multiple algorithmic techniques in credit card fraud detection. The most cited work is the meta-learning method proposed by Chan and Stolfo (1998). In their work, they used Naive Bayesian,C4.5, CART, and RIPPER as base classifiers and combined them by implementing a stacking method. Their multi-classifier meta-learning approach can significantly reduce the magnitude of losses from fraudulent transactions by splitting fraudulent and legitimate data in the raining dataset 50:50. understood.

3. TYPES OF FRAUDS AND PAYMENT GATEWAY

A payment gateway is an e-commerce software service provider that authenticates credit card purchases from e-businesses, online retailers, and more. payment gateway. It is nothing but a digital alternative to the "credit card payment" function found in supermarkets. Also, every online retailer wants to process every purchase correctly.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

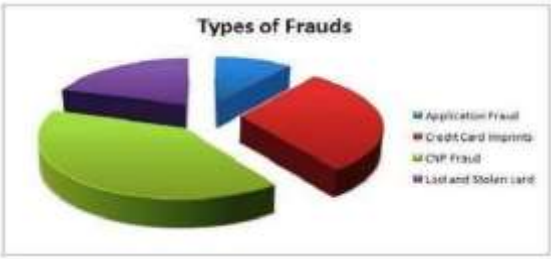
www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 03, March 2023, pp : 449-451

e-ISSN : 2583-1062

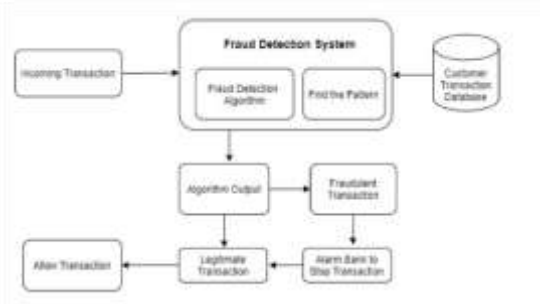
Impact Factor : 5.725

Bridge to Payments acts as a gateway between the website where the transaction takes place and the bank. It can be transparent to the customer or communicated to the end user.However, ensuring that the transaction goes through successfully without the intervention of fraudsters is very important for transaction protection.When you purchase at Over the Internet, encrypted credit card data is transferred to payment gateways. Details will be outsourced soon. This greatly reduces the chances of the information being thereAccess by hackers. Secondly, on the website, the bank collects payment gateway details to enable communication with card companies (Visa, MasterCard, etc.). Finally, the payment provider performs all backend validations from their servers and sends payment authorizations to the portal.



4. PROPOSED METHODOLOGY

A payment gateway is an e-commerce software service provider that authenticates credit card purchases from e-businesses, online retailers, and more. payment gateway.This is just a digital version of the "credit card payment" function in supermarkets. Additionally, every online retailer wants to process every purchase correctly. Bridge to Payments acts as a gateway between the website where the transaction takes place and the bank. This may be transparent to the customer or communicated to the end user. However, in order to protect your transaction, it is very important to ensure that the transaction succeeds without the intervention of fraudsters. When purchasing at Encrypted credit card data is sent over the internet to a payment gateway. Details will be outsourced soon. This greatly reduces the chances of the information being there Access by hackers. The bank then collects payment gateway details on his website to enable communication with card companies (Visa, MasterCard, etc.). Finally, the payment provider performs all backend validation from their server and sends payment authorization to the portal.



5. THE FRAUD DETECTION MODULE WORKS LIKE THIS:

- Payment gateways must provide credit card information such as card number and expiration date
- Retailers provide information such as mailing address, sales number, delivery date and time.
- Payment Gateway must forward
- relevant specifications to the Fraud Detection Program.
- The proposed program trains itself using effective data mining techniques and produces results using the best classification algorithms.
- The final outcome of the transaction (fraudulent or not) is delivered to the payment gateway accordingly.
- Results, including verdicts and other relevant details, are sent to merchants by payment gateway administrators in final UI reports.

6. EXPERIMENTAL RESULTS

The dataset used for the experiments was obtained from kaggle.com. The selected dataset has 3075 rows and 11 key features. The metrics used to evaluate performance are accuracy, recall, and precision. Experimental results prove that the performance of the random forest algorithm shows the correct level of cheating.

Figures 4 and 5 show that using Random Forest improved the scoring results for detecting fraudulent transactions compared to other algorithms. A highly accurate algorithm for identifying fraudulent transactions is integrated into the proposed system to improve.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

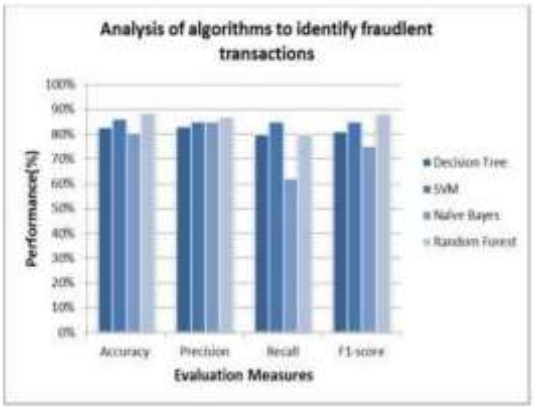
www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 03, March 2023, pp : 449-451

e-ISSN : 2583-1062

Impact Factor : 5.725

	Evaluation Measures			
Algorithms	Accuracy	Precision	Recall	F1-score
Decision Tree	83%	83%	80%	81%
SVM	86%	85%	85%	85%
Naive Bayes	80%	85%	62%	75%
Random Forest	88%	87%	80%	88%



7. CONCLUSION

The dataset used for the experiment was obtained from kaggle.com. The selected dataset has 3075 rows and 11 key features. The metrics used to evaluate performance are precision, recall,and precision. Experimental resul tsprovethat the performance of the Random Forest Algorithm exhibits an adequate level of cheating. Figures 4 and 5 show that using Random Forest improves the fraudulent trans actiond etection scoring results compared to other algorithms. The proposed system incorporateshigh-precision algorithms for identifying fraudulent transactions, resulting in improved performance.

8. REFERENCES

[1] Ayushi Agrawal, Shiv Kumar, Amit Kumar Mishra, "A Novel approach forCreditCard Fraud Detection", 2nd International Conference on Computing for Sustainable Global Development(INDIACom), 2015.

[2] N. Sivakumar, R. Balasubramanian, "Cheating identification in Visa Transactions: Classification dangers Also counteractive action Techniques", universal diary for PC science and majority of the data Technologies, vol. 6, no. 2, 2015.

[3] Ray-I Chang, Liang-Bin Lai, Wen-De Su, Jen-Chieh Wang, Jen-Shiang Kouh, "Intrusion identification by Back propagation neural Networks for SampleQuery and Attribute- Query", Research India Publications, pp. 6-10, 2006.

[4] V. G. T. Costa, A. C. P. L. Carvalho, S. Barbon, "Strict Very Fast Decision Tree: a memory conservative algorithm for data stream mining", May 2018.

[5] A. Aye Khine, H. Wint Khine, "A Survey of Decision Tree for Data Streams to Detect Credit Card Fraud", PROMAC-2019. [6] Y. Sahin, E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines", IMECS, vol. 1, 2011.

[6] B Meenakshi, J. B.. S Gayathri, "Credit Card Fraud Detection Using Random Forest", vol. 06, no. 03, March 2019, ISSN 2395-0072.

[7] M. Zareapoora, P. Shamsolmoalia,"Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier", International Conference on Intelligent Computing Communication & Convergence (ICCC-2014).

[8] G. T. Costa, A. C. P. L. Carvalho, S. Barbon, "Strict Very Fast Decision Tree: a memory conservative algorithm for data stream mining", May 2018.