IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12545

Credit Card Fraud Detection Framework for E-Commerce Sites

Mrs.Shakila[1], E. Praveen kumar[2], R. Pavithran[3], E. Priyadharshan[4]

Assistant Professor, Department of Computer Science and Engineering, DMI College of Engineering, Chennai, India[1]

B.E, Department of Computer Science and Engineering, DMI College of Engineering, Chennai, India[2]

B.E, Department of Computer Science and Engineering, DMI College of Engineering, Chennai, India[3]

B.E, Department of Computer Science and Engineering, DMI College of Engineering, Chennai, India[4]

Abstract - Fraud is a major problem in many industries, with pretenses being used to obtain money or property. Fraud detection is a crucial process that involves combining various datasets to create a comprehensive view of payment data to make informed decisions. Credit card fraud detection with deep learning is a method of data investigation by a data science team that uses all meaningful features of card users' transactions to identify fraudulent activities. The data is then processed by a trained model that finds patterns and rules to classify transactions as legitimate or fraudulent. Once integrated into an e-commerce platform, the deep learning-driven fraud protection module tracks transactions and determines the probability of fraud. Based on the predicted probability, transactions may be allowed, require additional authentication, or be frozen for manual processing. Fraud is a persistent problem in the financial industry, costing companies billions of dollars each year. Fraudulent transactions can take many forms, from stolen credit card information to account takeover attacks. As such, companies need to employ robust fraud detection methods to protect themselves and their customers. One popular method for detecting fraud is through the use of deep learning. Deep learning is a type of artificial intelligence that uses neural networks to analyze large amounts of data and identify patterns. By training a deep learning model on historical transaction data, a company can create a system that is capable of accurately detecting fraudulent transactions in real time. To develop a deep learning-based fraud detection system, a data science team will first gather and pre-process data from a variety of sources, including transaction logs, user behavior patterns, and other relevant data points. They will then use this data to train a deep learning model, which will learn to identify patterns and relationships between different data points that are indicative of fraudulent activity. Once the model is trained, it can be deployed within the company's payment processing system.

I.INTRODUCTION

A. Overview

Credit card fraud detection is a process used by organizations to prevent monetary theft resulting from unauthorized access to a customer's financial information. The majority of detection methods combine a variety of fraud detection datasets to form a connected overview of both valid and non-valid payment data to make a decision. This decision must consider IP address, geolocation, device identification, "BIN" data, global latitude/longitude, historic transaction patterns, and the actual transaction information. In practice, merchants and issuers deploy analytically based responses that use internal and external data to apply a set of business rules or analytical algorithms to detect fraud. Credit Card Fraud Detection with Machine Learning is a process of data investigation by a Data Science team and the development of a model that will provide the best results in revealing and preventing fraudulent transactions.

Mobile fraud: As more and more people use their smartphones for online shopping and payments, mobile fraud has become a growing concern. Fraudsters can use fake apps or malicious software to steal personal and financial information from users. Machine learning algorithms can help detect unusual activity or patterns in mobile transactions to identify potential fraud.

Chargeback fraud: This type of fraud occurs when a customer disputes a legitimate transaction, claiming that it was fraudulent or unauthorized, to get a refund or avoid paying for the goods or services. Chargeback fraud can be difficult to detect, but machine learning can help by analyzing patterns in chargebacks, such as frequent chargebacks from the same customer or unusual spikes in chargebacks from a particular merchant.

Data breaches: When a company's database is hacked and customer information is stolen, it can lead to a wave of credit card fraud as criminals use the stolen data to make unauthorized purchases. Machine learning algorithms can help identify suspicious patterns in transaction data following a data breach, such as a sudden increase in transactions from a particular geographic area.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12545

False declines: False declines occur when legitimate transactions are rejected by a fraud detection system, causing frustration for customers and lost revenue for merchants. Machine learning can help reduce false declines by improving the accuracy of fraud detection algorithms and reducing the number of false positives.

Figure 1: Number of Worldwide Non-Cash Transactions

Overall, credit card fraud detection is a complex and ever-evolving field, and machine learning is playing an increasingly important role in improving the accuracy and efficiency of fraud detection systems. By analyzing large volumes of transaction data and identifying patterns and anomalies, machine learning algorithms can help prevent fraudulent transactions and protect consumers, merchants, and financial institutions from financial losses. Credit card fraud is a major issue for banks and financial institutions.

Machine Learning (ML) has emerged as an effective solution for detecting and preventing credit card fraud. ML algorithms can be categorized into unsupervised and supervised learning methods. Unsupervised learning algorithms like PCA, LOF, One-class SVM, and Isolation Forest use unlabeled data to find patterns and dependencies in the credit card fraud detection dataset. These algorithms group data samples by similarities without manual labeling. PCA is one of the most popular unsupervised learning algorithms used for anomaly detection. It searches for correlations among features like time, location, and amount of money spent and determines which combination of values contributes to the variability in the outcomes. LOF is another popular unsupervised learning algorithm used for anomaly detection. It calculates a score factor that helps understand how high the chance is for a certain data sample to be an outlier (anomaly).

One-class SVM is a classification algorithm that helps identify outliers in data. Isolation Forest is an anomaly detection method from the Decision Trees family that precisely detects anomalies instead of profiling the positive data points. Supervised learning methods use labeled data samples, so the system will then predict these labels in the future unseen before data. Among supervised learning fraud identification methods, Decision Trees, Random Forest, KNN, and Naive Bayes are commonly used. K-Nearest Neighbours is a classification algorithm that counts similarities based on the distance in multi-dimensional space. The data point, therefore, will be assigned the class that the nearest neighbors have. XGBoost and Light GBM are a single type of gradient-boosted Decision Trees algorithm, which was created for speed as well as maximizing the efficiency of computing time and memory resources. Random Forest is a classification algorithm that is comprised of many Decision Trees.ML models for fraud detection have their pros and cons. Some models are very hard to interpret, explain, and debug, but they have good accuracy (e.g. Neural Networks, Boosting, Ensembles, etc.).

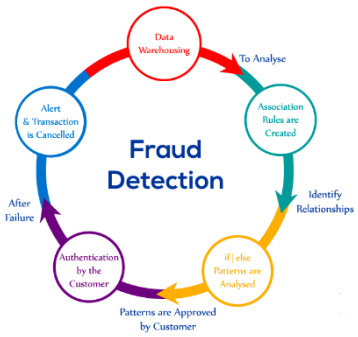

Figure 2: Fraud Detection

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12545

II.LITERATURE SURVEY

Kuldeep Randhawa1, Chu Kiong Loo1, Manjeevan Seera, Chee Peng Lim, and Asoke K. Nandi proposed an efficient methodology that is a machine learning algorithm used for the detection of credit card fraud. The typical type of model is initially used. Then, hybrid methods which utilize AdaBoost and majority voting methods are tested. The AdaBoost method can improve the individual results from different algorithms.

K. Kannan and G. Thamizhendhi (2019), This paper provides a survey of various credit card fraud detection techniques used in e-commerce sites. The study covers both supervised and unsupervised machine learning approaches, as well as the performance and limitations of different techniques. The paper also provides an overview of the future research directions in this field.

Mohammadreza Soleymani, Seyed Hamed Moosavi, and Mohammad Javad Kargar (2018) introduced an effective method by developing a credit card transaction payment system. Also, one has enhanced the system and analyzes credit card fraud, and 70% of U.S. customers are largely disturbed by identity fraud. This survey considered two methods of data mining one is SVM and another one is random forest. Also collectively worked on the well-known logistic regression to identify credit card fraud being part of an attack.

Ammar Almomani, Fadi Aloul, and Alaa Alawneh (2016) suggested that constructing a unified pattern per customer not only shows normal behavior but also a Fraud pattern that's represented previously and confirmed as fraud transactions that simplifies studying fraudsters' behavior. The most important algorithm proposed that an Apriori algorithm used in Fraud Miner for frequent Pattern creation and facilitate summarizing customer earlier behavior either within his Legal or Fraud transactions.

Ranjeeta Jha, Abhaya, and Vijay Kumar Jha have presented that the best method of credit card fraud is fraud dedicated through the use of another person's credit card. To maintain safe credit card control a capable fraud detection system is necessary. Currently, several modern techniques mainly depend on Artificial Intelligence, Sequence Alignment, Data Mining, Fuzzy Logic, Machine Learning, Genetic Programming, etc.

III.PROPOSED SYSTEM

Deep learning has revolutionized the field of fraud detection by enabling the creation of algorithms that can identify subtle and hidden patterns in user behavior that may indicate fraudulent activity. Unlike traditional rule-based systems, deep learning systems are capable of processing vast amounts of data quickly and with minimal manual intervention, making them a powerful tool for combating fraud. One key application of deep learning in fraud detection is the use of deep neural networks. These networks are modeled after the human brain and are capable of learning from patterns of legitimate behavior, adapting to changes in user behavior, and identifying patterns of fraudulent activity in real-time. To be effective, the model must be trained to identify common anomalies in the system, such as Multiple payment methods added from a single account within a short period, which could be an indicator of fraud. Purchases of premium goods in unusually large quantities, which may suggest fraudulent activity.
Inaccurate or fraudulent location or address information is provided in a user profile. Suspicious or fraudulent email addresses associated with a user account. Mismatches between the name on the account and the name on the associated payment card. Overall, deep learning represents a powerful and effective approach to fraud detection that is increasingly being adopted by businesses and organizations across a wide range of industries.

A. Implementation of User Interface

The user interface (UI) for the Credit Card Fraud Detection Framework for E-Commerce Sites is a crucial component of the system. It should be designed to provide a user-friendly experience for the users who will be interacting with the system, including fraud analysts, customer service representatives, and other relevant stakeholders. The UI should include role-based access control to ensure that only authorized users have access to sensitive data and features.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12545

Figure 3: User Interface

B. Admin Login

Admin login is a critical feature in the Credit Card Fraud Detection Framework for E-Commerce Sites. It provides access to the system's administrative functions, including managing user accounts, setting up rules for fraud detection, and viewing reports. The admin login feature should provide a dashboard to manage user accounts, including adding new users, modifying permissions, and deactivating accounts.

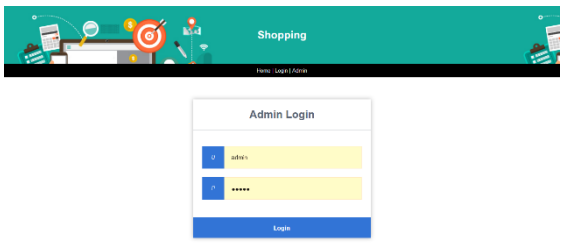

Figure 4: Admin Login

C. Shopping Page

The shopping page is a critical component of any e-commerce site, including the Credit Card Fraud Detection Framework for E-Commerce Sites. It is the page where customers can browse products, add them to their shopping cart, and make payments. The shopping page should include detailed product listings that provide customers with all the information they need to make an informed purchase. This can include product images, descriptions, and the price of the product.

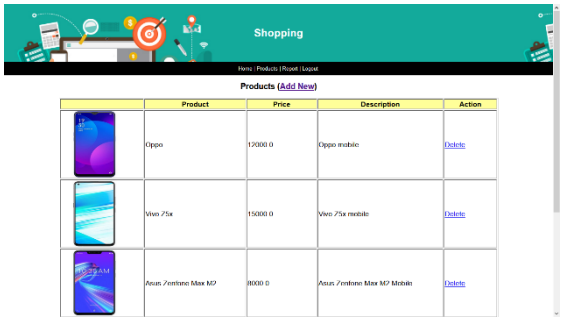

Figure 5: Shopping Page

D.Verification

Verification is an essential part of the Credit Card Fraud Detection Framework for E-Commerce Sites. Verification involves confirming the authenticity of user information and transactions to detect potentially fraudulent activities. All transactions should be verified to ensure that they are legitimate. Verification can involve checking the transaction details, such as the amount, date, time, and location, and comparing them to the user's history and behavior.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12545

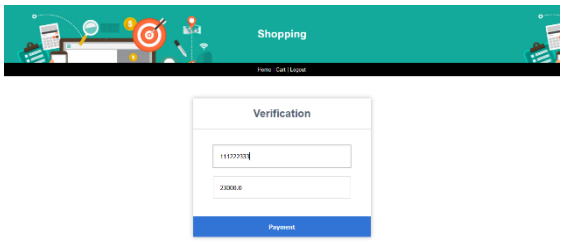

Figure 5: Verification

D. Giving Valid Input

The system should have robust data validation mechanisms in place to ensure that only valid input data is accepted. This can include checking for data type, format, length, and range. The system should validate user input data to ensure that the input conforms to predefined rules and patterns. This can include checking for valid email addresses, phone numbers, or credit card numbers.

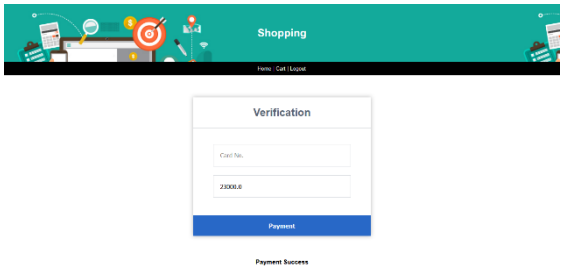

Figure 7: Payment Success

E. Giving Invalid Input

The system should implement robust data validation mechanisms to prevent invalid input from being accepted. Data validation can include checking for data type, format, length, and range, and rejecting any input that does not conform to these rules. The system should implement proper authentication and authorization mechanisms to prevent unauthorized access to sensitive data and functionality. User authentication can help to prevent malicious users from introducing invalid input into the system and shows the block message.

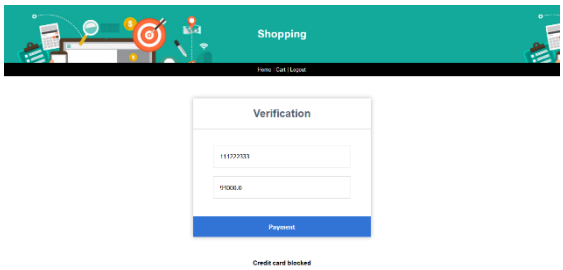

Figure 8: Credit Card Blocked

IV.RESULTS AND DISCUSSION

The results and discussion section of the Credit Card Fraud Detection Framework for E-Commerce Sites project is an important aspect that provides an evaluation of the system's effectiveness in detecting fraud. The system's performance metrics should be evaluated to determine its effectiveness in detecting fraud. Performance metrics can include accuracy, precision, recall, and F1 score. The metrics should be compared to industry benchmarks to assess the system's effectiveness. The evaluation dataset used to evaluate the system's performance should be representative of real-world transactions. The dataset should include a variety of transactions, including both legitimate and fraudulent ones, and

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12545

cover a range of transaction types, amounts, and locations. The system's performance should be compared to existing solutions in the market to assess its effectiveness. The comparison should consider factors such as accuracy, cost, ease of use, and scalability. By evaluating the system's performance metrics and comparing them to industry benchmarks, the results and discussion section can provide insights into the system's effectiveness in detecting fraud. Discussing the limitations of the system and potential areas for future work can help to guide future research and development efforts. Additionally, discussing the deployment and integration of the system into the e-commerce site can provide practical insights into implementing the system in a real-world setting. Overall, the results and discussion section is an important aspect of the Credit Card Fraud Detection Framework for E-Commerce Sites project that helps to evaluate and improve the system's effectiveness in detecting fraud. It can help to identify areas for improvement, guide future research and development efforts, and provide insights into how the system can benefit the e-commerce site's business.

V.CONCLUSION

Credit card fraud is a rapidly growing problem due to which financial institutions are losing huge amounts of money. Researchers are implementing various new techniques to enhance credit card fraud detection systems so that credit card fraud can be decreased. Many machine-learning methods have been implemented to prevent credit card fraud. Deep learning is a branch of machine learning that is used in many fields like image recognition, speech recognition, and many more. Deep learning provides a way to explore complex features within the data so that the model can learn better to predict fraud more efficiently with fewer false alarms.

REFERENCES

[1]. Y. Sahin, S. Bulkan, and E. Duman, “A cost-sensitive decision tree approach for fraud detection,” Expert Systems with Applications, vol. 40, no. 15, pp. 5916–5923, 2013.
[2]. A. O. Adewumi and A. A. Akinyelu, “A survey of machine-learning and nature-inspired based credit card fraud detection techniques,” International Journal of System Assurance Engineering and Management, vol. 8, pp. 937–953, 2017.
[3]. A. Srivastava, A. Kundu, S. Sural, A. Majumdar, “Credit card fraud detection using hidden Markov model,” IEEE Transactions on Dependable and Secure Computing, vol. 5, no. 1, pp. 37–48, 2008.
[4]. J. T. Quah, and M. Sriganesh, “Real-time credit card fraud detection using computational intelligence,” Expert Systems with Applications, vol. 35, no. 4, pp. 1721–1732, 2008.
[5]. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C., “Data mining for credit card fraud: A comparative study,” Decision Support Systems, vol. 50, no. 3, pp. 602–613, 2011.
[6]. N. S. Halvaiee and M. K. Akbari, “A novel model for credit card fraud detection using Artificial Immune Systems,” Applied Soft Computing, vol. 24, pp. 40–49, 2014.
[7]. S. Panigrahi, A. Kundu, S. Sural, and A. K.Majumdar, “Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning,” Information Fusion, vol. 10, no. 4, pp. 354–363, 2009.
[8]. N. Mahmoudi and E. Duman, “Detecting credit card fraud by modified Fisher discriminant analysis,” Expert Systems with Applications, vol. 42, no. 5, pp. 2510–2516, 2015.
[9]. D. Sánchez, M. A. Vila, L. Cerda, and J. M. Serrano, “Association rules applied to credit card fraud detection,” Expert Systems with Applications, vol. 36, no. 2, pp. 3630–3640, 2009.
[10]. Amol K. Kadam, “Analysis of Software Reliability using Testing Time and Testing Coverage, ” International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 5, 143-148, May 2015.