Online Credit Card Fraud Detection and Anomaly User Blocking

Sudha R.V.[1], Pradeepa G[2], Abinaya K[3], Sudarvizhi V[4] & Tharani V[5]

[1,2]Assistant Professor, Department of Information Technology, Vivekanandha College of Technology for Women.
[3-5]Student, Department of Information Technology, Vivekanandha College of Technology for Women.

ABSTRACT

The use of credit cards has expanded considerably as a result of rapid advancements in electronic commerce technologies. As credit cards become the most popular method of payment for both online and offline purchases, incidences of credit card fraud are on the rise. Transactions with Credit Cards continue to expand in number, capturing a larger share of the US payment system and resulting in a higher rate of stolen account numbers and bank losses. Improved fraud detection has thus become critical to the payment system's long-term stability in the United States. For several years, banks have deployed early fraud warning systems. Large-scale data mining tools have the potential to improve commercial practice. Scalable strategies for analysing enormous volumes of transaction data and efficiently computing fraud detectors in a timely way, especially for e-commerce, is a critical issue. Aside from scalability and efficiency, the fraud-detection task has technical issues such as skewed training data distributions and non-uniform cost per error, both of which have received little attention in the now-established ledge-discovery and data mining communities.

1. Introduction

This paper is titled "credit card fraud detection," and it uses PHP for the front end and MySQL for the back end. E-commerce aids countries in improving trade efficiency and facilitating developing country entry into the global economy. It gives firms and entrepreneurs a competitive advantage.

Many of the restrictions of traditional commerce are eliminated with this trading method. The existence of virtual markets, routes, and storefronts that do not take up physical space, allowing access and circulation in these markets for a brief period of time and from anywhere in the globe without leaving home. Select and order things from virtual shop windows in unspecified regions of the world, as well as advertise on virtual networks, with payment made via electronic services.

Communication technologies, data management systems, and security are the three essential components of E-commerce. PHP and CSS are the programming languages utilised to create the system. a. PHP is one of the most widely used programming languages for developing online applications nowadays. The web server interprets and executes the code before sending the result to be displayed in the client browser. It is known as server-side scripting language since the web server interprets and executes its own code.

CSS (Cascading Style Sheets) is a simple design language used to make web pages more aesthetically pleasing. CSS controls the appearance of a webpage, including text colour, font style, paragraph spacing, and how columns are sized and laid out. It gives you a lot of control over how an HTML (XHTML) document looks. E-commerce is a business process that involves purchasing and selling between parties (buyer and seller) for the purpose of transferring the right to use products or services through the internet using electronic mechanisms.

The important factor in defining the concept of E-commerce is the electronic approval between the vendor and the buyer to hold the transaction or purchase.

2. System Study

2.1. Existing System

The needs of the present system "credit card fraud detection" are studied in the system study phase. There are more precious and uncommon objects, which are collected from various sources and will be sold on auction so that people can see more profit over the product than ordinary sales.

Although rewarding, there are additional risks, such as organising the auction. Currently, auctions are handled manually. The consumer who needs to purchase an item must visit the store and consult the sorts of things offered, which he can do by consulting the index or contacting a store staff. He must then select the things for purchasing after referring them. The customer needs to stand in some queue for the billing.

2.2. Proposed System

The proposed system's key goals are to eliminate human labour, reduce maintenance time, and make the system more user-friendly, efficient, accurate, and quick to process. This application was built using the web service idea.

3. System Design and Implementation

3.1. Input Design

One of the most crucial phases of system design is input design. Input design is the process of planning and designing the input received by the system in order to obtain the necessary information from the user while avoiding unnecessary data. The goal of the input design is to guarantee that the input is as accurate as possible while simultaneously being accessible and understandable to the user. The input design is a component of the overall system design that demands close consideration. The processing and output will compound the faults if the input entering the system is wrong. The objectives considered during input design are :

Nature of input processing.

Flexibility and thoroughness of validation rules.

Handling of properties within the input documents.

Screen design to ensure accuracy and efficiency of the input relationship with files.

Careful design of the input also involves attention to error handling, controls, batching and validation procedures. Input design features can ensure the reliability of the system and produce result from accurate data or they can result in the production of erroneous information.

3.2. Output Design

The most essential and immediate source of information for the user is computer output. Efficient, understandable output design should strengthen the system's user relationships and aid decision-making. The physical copy from the printer is a common form of output. The output devices to consider are determined by considerations such as system compatibility, response time requirements, estimated print quality, and the quantity of copies required. Unpredictably, all nodes in the network may leave or fail. The continuous

measurement data is partitioned into time slots, with a source block referring to the quantity of data generated in one time slot on a node. Clearly, how many time slots of data can be cached depends on the size of the node cache storage.

A synchronization packet (also known as the timing reference signal) comes before the first active sample on each line and after the last active sample on each line (and before the start of the horizontal blanking region). The master files, transaction files, and computer applications are all listed in a systems flowchart. Data is collected and arranged into groupings that are similar. After that, the proper input media for processing is chosen. The output devices to consider are determined by considerations such as system compatibility, response time requirements, estimated print quality, and the quantity of copies required. Unpredictably, all nodes in the network may leave or fail.

3.3. Database Design

To manage enormous amounts of data, database design is essential. The definition of the structure of information storage and the supply of mechanisms for information modification are both part of data management. Furthermore, the database system must ensure the security of the information handled, even if the system crashes due to unwanted access attempts. The database design process entails creating a database and its consistent tables, which are utilised by applications for data storage.
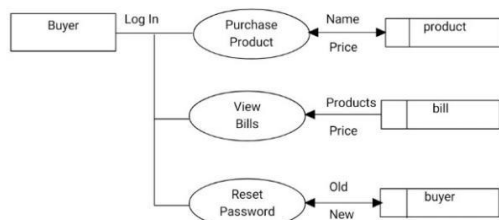
4. Data Flow Diagram

Level 0:
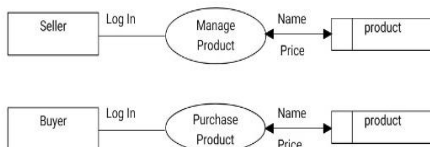
Level 1:
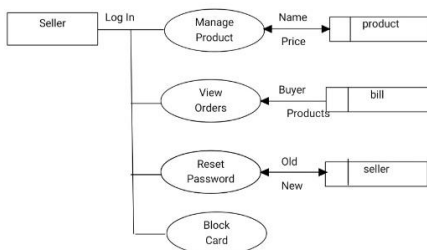
Level 2:

5. Related Works

In this section, we go over some previous fraud detection research. Authors in [1] presented a credit card fraud detection tool based on a bagging ensemble. The experimental step used an ensemble technique based on a decision tree algorithm. Furthermore, this research examines the methodologies employed, including Nave Bayes (NB), kNearest Neighbor (KNN), and Support Vector Machines (SVMs). The UCSD-FICO competition provided a real-world credit card dataset that was utilised to evaluate their trials using 10-fold cross-validation techniques.

Authors in [2] combined the genetic algorithm with an artificial neural network (ANN) to detect fraudulent transactions. When a credit card holder uses the card in an unlawful manner, the suggested system checks the pattern used by the fraudster and compares it to the pattern used by the original cardholder to see if the two patterns are same. When there is a significant variation between the original pattern and the retrieved one, it indicates the possibility of an illegal transaction. For each transaction that fed the network, NN utilised several attributes such as the current transaction descriptor, transaction history descriptor, payment history descriptor, and other descriptors. Furthermore, Feed Forward Back Propagation was utilised as a Learning Algorithm; it is a common learning approach that uses gradient descent in the error space to improve efficiency. It also aids in the selection of network parameters such as weight, network type, number of layers, and node count. The suggested system, Genetic Algorithm and Neural Network (GANN), attempts to successfully detect credit card fraud.

In [3], authors used six classifiers with a dataset before and after pre-processing; the results show that using the Undersampling technique with the dataset improves the results significantly. The dataset used in this study included 284,807 transactions, with only 492 of those being fraudulent. They altered the ratio to 1:1 after applying the Random Undersampling technique, which means the number of fraud transactions is the same as the number of lawful transactions. They evaluated the classifiers using precision and recall with both datasets, and discovered that utilising the Undersampled dataset greatly increased the precision for all classifiers.

To detect fraudulent transactions, the evolutionary algorithm was combined with an artificial neural network (ANN) [4]. When a credit card holder uses the card in an unlawful manner, the suggested system checks the pattern used by the fraudster and compares it to the pattern used by the original cardholder to see if the two patterns are same. When there is a significant variation between the original pattern and the retrieved one, it indicates the possibility of an illegal transaction. For each transaction that fed the network, NN utilised several attributes such as the current transaction descriptor, transaction history descriptor, payment history descriptor, and other descriptors.

Furthermore, Feed Forward Back Propagation (FFBP) was applied. Learning Algorithm: This is a standard learning technique that employs gradient descent in the error space and plays an important role in increasing efficiency. It also aids in the selection of network parameters such as weight, network type, number of layers, and node count. The suggested system, Genetic Algorithm and Neural Network (GANN), attempts to successfully detect credit card fraud.
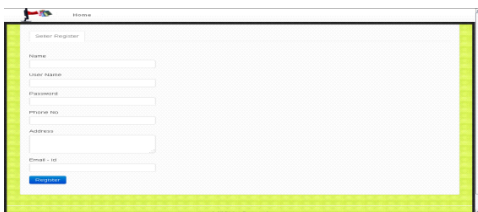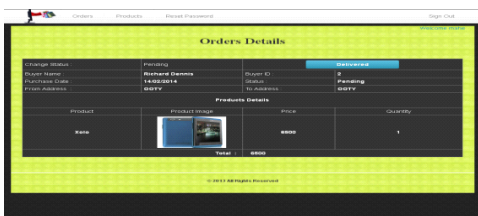
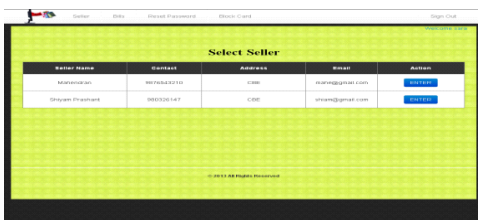## 6. Experimental Results

Home Page
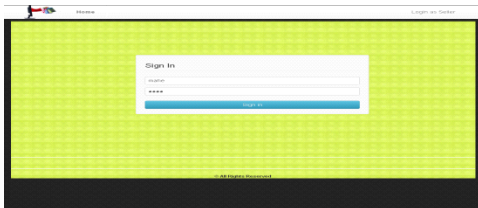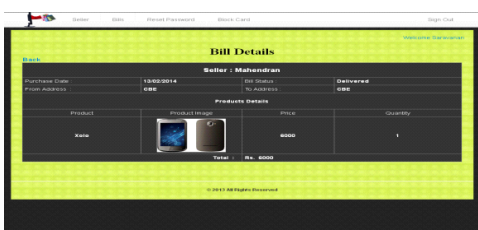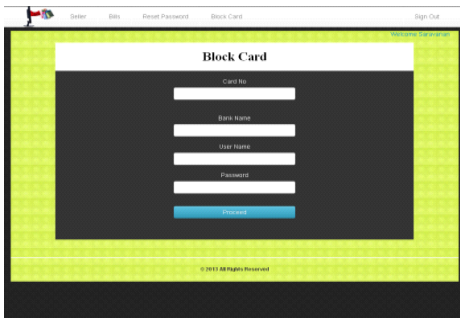

Seller Login Page

Seller Register Page

View Order Page

Seller Page

Bill Details Page

Block Card Page

7. Conclusion

The "Credit Card Fraud Detection" was created to meet all of the requirements. The system is user-friendly and scalable. Almost all of the system's goals have been achieved. The system has been put to the test in every way. The solution eliminates human errors and decreases the problems that arise in the existing manual system. The database is designed to be adaptable, allowing the system to be implemented. It has been implemented and tested thoroughly. Methodologies were used throughout all phases of development. The desired report can be obtained by a user with minimum training. By achieving the paper's goals, the programme succeeds. With modest tweaks, more extensions to this system can be made necessary best.

References

[1] HSN Consultants, Inc. (Oct. 17, 2019). The Nilson Report 2018. Available: https://nilsonreport.com.

[2] A. D. Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," Expert Syst. Appl., vol. 41, no. 10, pp. 4915-4928, Aug. 2014.

[3] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection and concept-drift adaptation with delayed supervised information," in Proc. Int. Joint Conf. Neural Netw. Jul. 2015, pp. 1-8.

[4] A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: A realistic modeling and a novel learning strategy," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 8, pp. 3784–3797, Aug. 2018.