International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 9, Issue 01, January-2024, http://ijmec.com/, ISSN: 2456-4265

CREDIT CARD FRAUD DETECTION USING HMM AND NAÏVE BAYAS

Mattam Vaibhavi, Mrs. M. Anusha

[1]B.tech Student, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

[2]Assistant Professor, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

Abstract: The most accepted payment mode is credit card for both online and offline in today's world, it provides cashless shopping at every shop in all countries. It will be the most convenient way to do online shopping, paying bills etc. Hence, risks of fraud transaction using credit card has also been increasing. In the existing credit card fraud detection business processing system, fraudulent transaction will be detected after transaction is done. It is difficult to find out fraudulent and regarding loses will be barred by issuing authorities. Hidden Markov Model is the statistical tools for engineer and scientists to solve various problems. In this paper, it is shown that credit card fraud can be detected using Hidden Markov Model during transactions. Hidden Markov Model helps to obtain a high fraud coverage combined with a low false alarm rate.

I. INTRODUCTION

In today's digital age, online shopping has become a popular choice for many individuals due to its convenience and accessibility. However, with the increase in online transactions, there has been a rise in credit card fraud. Credit card fraud refers to the unauthorized use of a credit card to make purchases or withdraw cash. The objective of this project is to develop a system that can accurately detect credit card fraud using machine learning algorithms such as Hidden Markov Models (HMM) and Naive Bayes (NB).

The proposed system will be integrated into an e-commerce website, where users can log in and make purchases. When an admin logs in, The admin can also retrieve credit card details of users and apply Principal Component Analysis (PCA) to convert the data into numerical values that can be used for fraud detection. Hidden Markov Model and Naïve Bayas algorithms will be trained using patterns based on historical transaction data. These patterns will help the models to differentiate between legitimate transactions and fraudulent ones. When a new transaction is submitted, the system will apply these algorithms to determine whether it is fraudulent or not.

In addition to fraud detection, the system will also allow users to leave reviews about their shopping experience. This feedback will be used to improve the overall user experience and prevent potential fraud by identifying any suspicious activities or patterns in user behaviour. Overall, this project aims to provide a reliable and efficient solution for credit card fraud detection in online transactions, thereby enhancing the security and trustworthiness of e-commerce websites for both users and merchants.

II. LITERATURE SURVEY

Ghosh, S., and Reilly, D.L., published the paper "Credit Card Fraud Detection with a Neural-Network". In this paper Using data from a credit card issuer, a neural network based fraud detection system was trained on a large sample of labelled credit card account transactions and tested on a holdout data set that consisted of all account activity over a subsequent two-month period of time. The neural network was trained on examples of fraud due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud and NRI (non-received issue) fraud. The network detected significantly more fraud accounts (an order of magnitude more) with significantly fewer false positives (reduced by a factor of 20) over rulebased fraud detection procedures. We discuss the performance of the network on this data set in terms of detection accuracy and earliness of fraud detection. The system has been installed on an IBM 3090 at Mellon Bank and is currently in use for fraud detection on that bank's credit card portfolio.

Syeda, M., Zhang, Y. Q., and Pan, Y., published "Parallel Granular Networks for Fast Credit Card Fraud Detection". A parallel granular neural network (GNN) is developed to speed up data mining and knowledge discovery process for credit card fraud detection. The entire system is parallelized on the Silicon Graphics Origin 2000, which is a shared memory multiprocessor system consisting of 24-CPU, 4G main memory, and 200 GB hard-drive. In simulations, the parallel fuzzy neural network running on a 24-processor system is trained in parallel using training data sets, and then the trained parallel fuzzy neural network discovers fuzzy rules for future prediction. A parallel learning algorithm is implemented in C. The data are extracted into a flat file from an SQL server database containing sample Visa Card transactions and then preprocessed for applying in fraud detection. The data are classified into three categories: first for training, second for prediction, and third for fraud detection. After learning from training data, the GNN is used to predict on a second set of data and later the third set of data is applied for fraud detection. GNN gives fewer average training errors with larger amount of past training data. The higher the fraud detection error is, the greater the possibility of that transaction being actually fraudulent.

ANALYSIS

online transactions have become an integral part of our daily lives, offering convenience and accessibility. However, with the rise of online transactions, the risk of credit card fraud has also increased. Recognizing the critical need for robust security measures, our project focuses on developing an advanced Credit Card Fraud Detection System. This system integrates sophisticated techniques such as Hidden Markov Model (HMM) and Naive Bayes algorithms to provide a secure and seamless online shopping experience for users. As online shopping continues to grow, so does the sophistication of credit card fraud techniques. Traditional methods of fraud detection often fall short in identifying emerging patterns and anomalies. To address this challenge, our project leverages cutting-edge machine learning algorithms to enhance fraud detection accuracy and efficiency. Users can browse, shop, and make secure transactions on the website without interruption. The system's fraud detection processes operate transparently in the background, preserving a positive and user-friendly experience.

Users also have the option to contribute to the platform by leaving reviews for products.

The integration of HMM and Naive Bayes algorithms aims to improve the accuracy of fraud detection, ensuring that both known and emerging patterns are identified. By providing a secure and transparent online shopping environment, the project aims to build trust and confidence among users. The system's adaptability and the admin's ability to train the models with new patterns enable continuous improvement, making it resilient against evolving fraud tactics.

III. DESIGN

The credit card fraud detection system is intricately designed to ensure a secure and user-friendly environment for both administrators and regular users within the shopping website. The system incorporates advanced algorithms, specifically the Hidden Markov Model (HMM) and Naive Bayes, to effectively detect and prevent fraudulent activities. The design focuses on key components to guarantee the system's reliability and efficiency.

At the core of the system is a robust user authentication and authorization mechanism. This ensures secure access for both users and administrators, establishing a foundation for the protection of sensitive information. The user interface is thoughtfully crafted to offer a seamless and intuitive experience, allowing users to browse products, make purchases, and leave reviews effortlessly.

For administrators, a dedicated control panel is implemented to enable application of fraud detection mechanisms. Admins have the capability to access credit card details, a critical aspect for fraud analysis. To safeguard user privacy, the system employs Principal Components Analysis (PCA), converting credit card details into numerical components. This not only enhances security but also provides a layer of confidentiality for sensitive user information.

The heart of the fraud detection lies in the sophisticated algorithms, HMM and Naive Bayes. Admins play a pivotal role in training these models with historical transaction patterns, allowing the system to learn and adapt to evolving fraud scenarios. Real-time processing of incoming transactions utilizes the trained models to detect anomalies, thus ensuring timely and accurate fraud detection. The decision logic is carefully designed to combine outputs from both HMM and Naive Bayes, resulting in a comprehensive fraud detection decision. Admins can set parameters for sensitivity and specificity based on the specific needs of the system, providing a customizable approach to fraud prevention.

To facilitate user transactions, secure payment gateways are implemented, guaranteeing the confidentiality and integrity of financial information throughout the process. Additionally, users can engage with the platform by leaving reviews and feedback. The system incorporates moderation mechanisms to maintain the quality and authenticity of user-generated content.

UML Diagram:

Sequence diagram:

Sequence diagrams typically show the flow of functionality through a use case, and consist of the following components:

1. Actors, involved in the functionality.

2. Objects, that a system needs to provide the functionality.

.

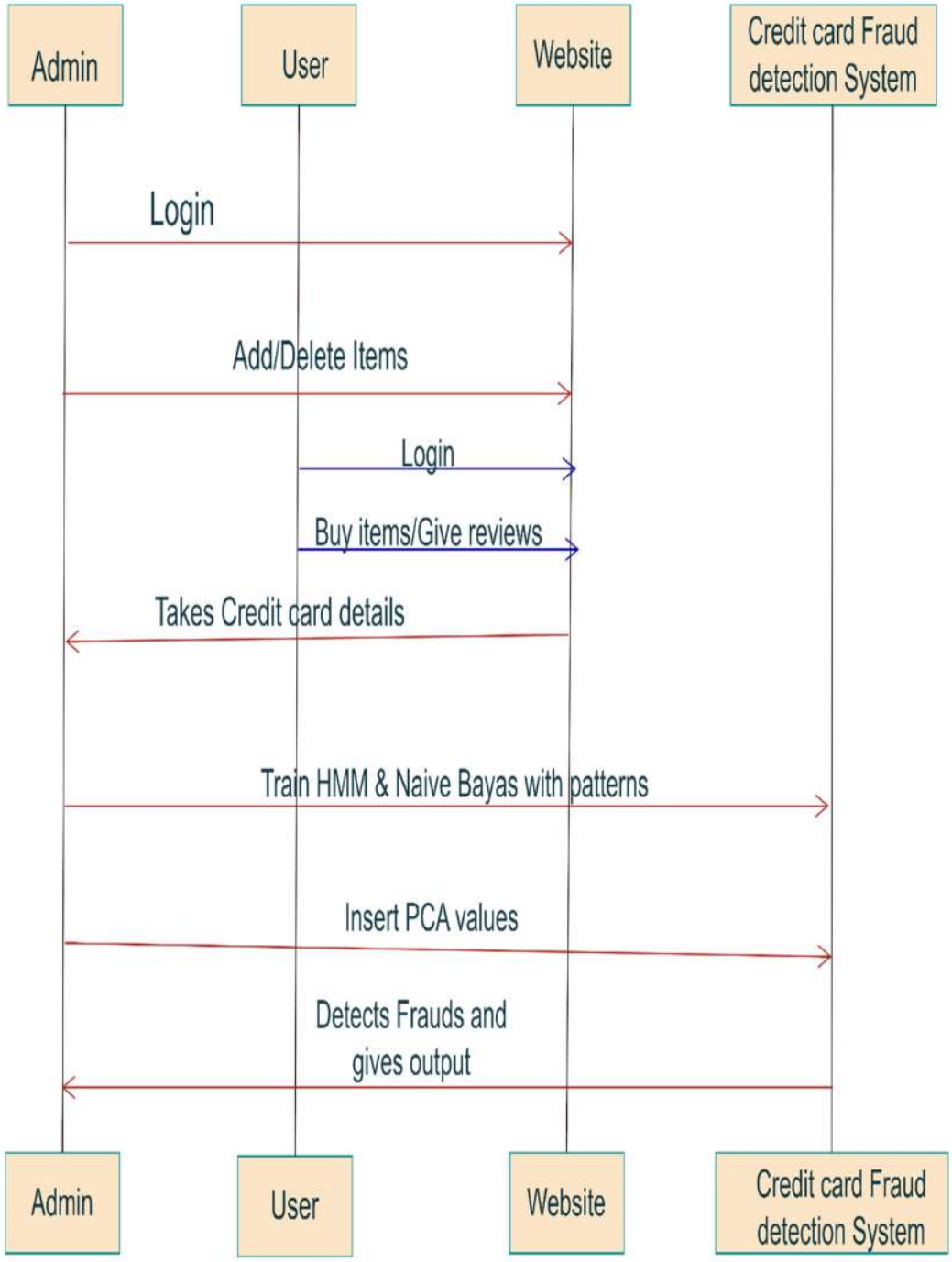


Fig 4.2.1 Sequence diagram

Sequence Diagrams Represent the objects participating the interaction horizontally and time vertically.

A Use Case is a kind of behavioral classifier that represents a declaration of an offered behavior. Each use case specifies some behavior, possibly including va2qriants that the subject can perform in collaboration with one or more actors. Use cases define the offered behavior of the subject without reference to its internal structure. These behaviors, involving interactions between the actor and the subject, may result in changes to the state of the subject and communications with its environment. A use case can include possible variations of its basic behavior, including exceptional behavior and error handling.

Activity diagram:

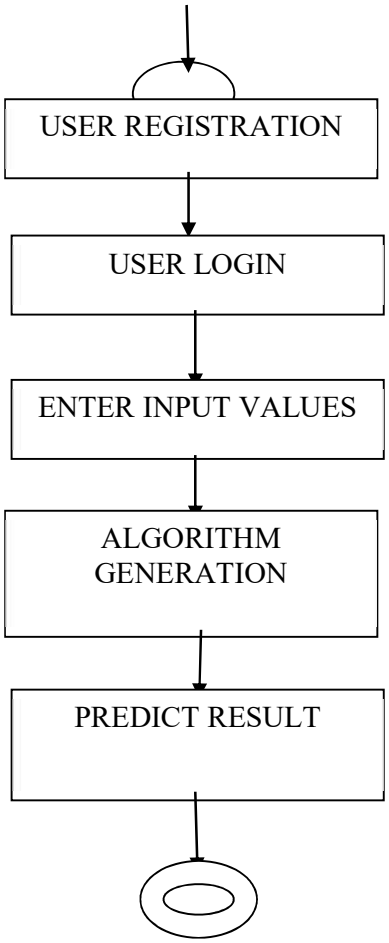


Fig 4.2.2 Activity Diagram

Deployment Diagram:

A deployment diagram in UML showcases the physical deployment of artifacts on nodes (hardware or software elements).

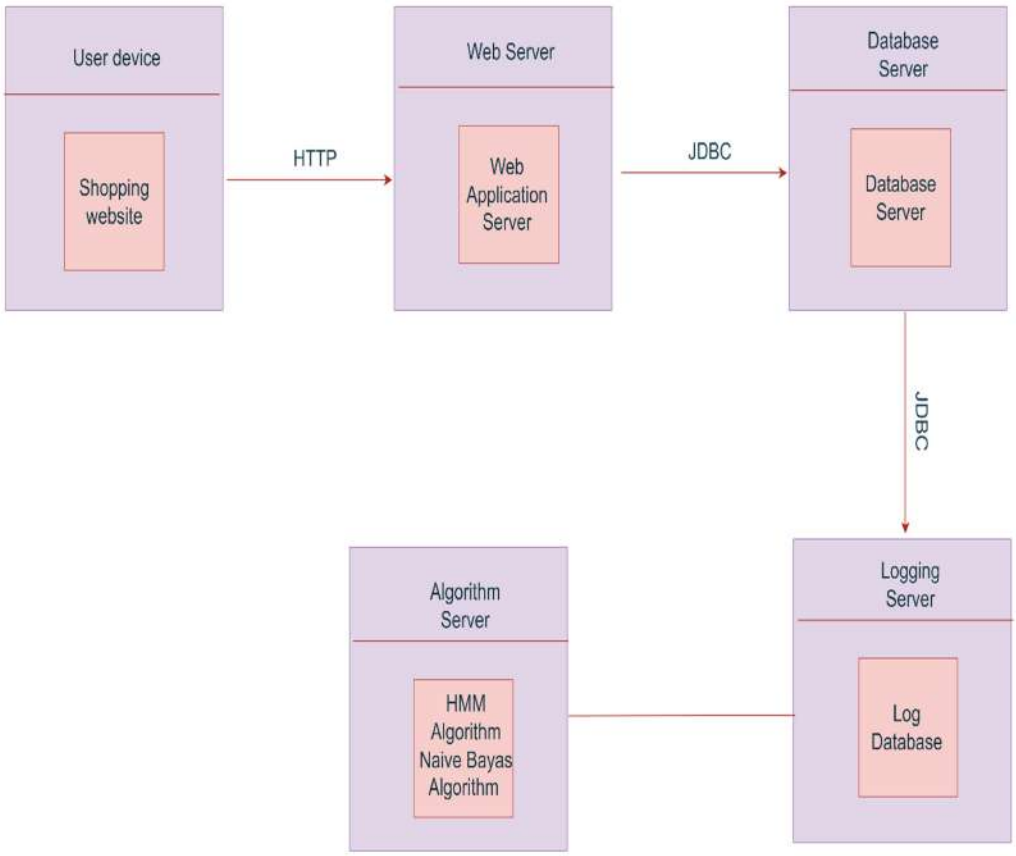


Fig 4.2.3 Deployment Diagram

Class Diagram:

The class diagram is the main building block of object-oriented modeling. It is used for general conceptual modeling of the systematic of the application, and for detailed modeling translating the models into programming code. Class diagrams can also be used for data modeling.[1] The classes in a class diagram represent both the main elements, interactions in the application, and the classes to be programmed. Class diagrams describe the static structure of a system, or how it is structured rather than how it behaves. These diagrams contain the following elements:

1. Classes, which represent entities with common characteristics or features. These features include attributes, operations, and associations.

2. Associations, which represent relationships that relate two or more other classes where the relationships have common characteristics or features. These features include attributes and operations.

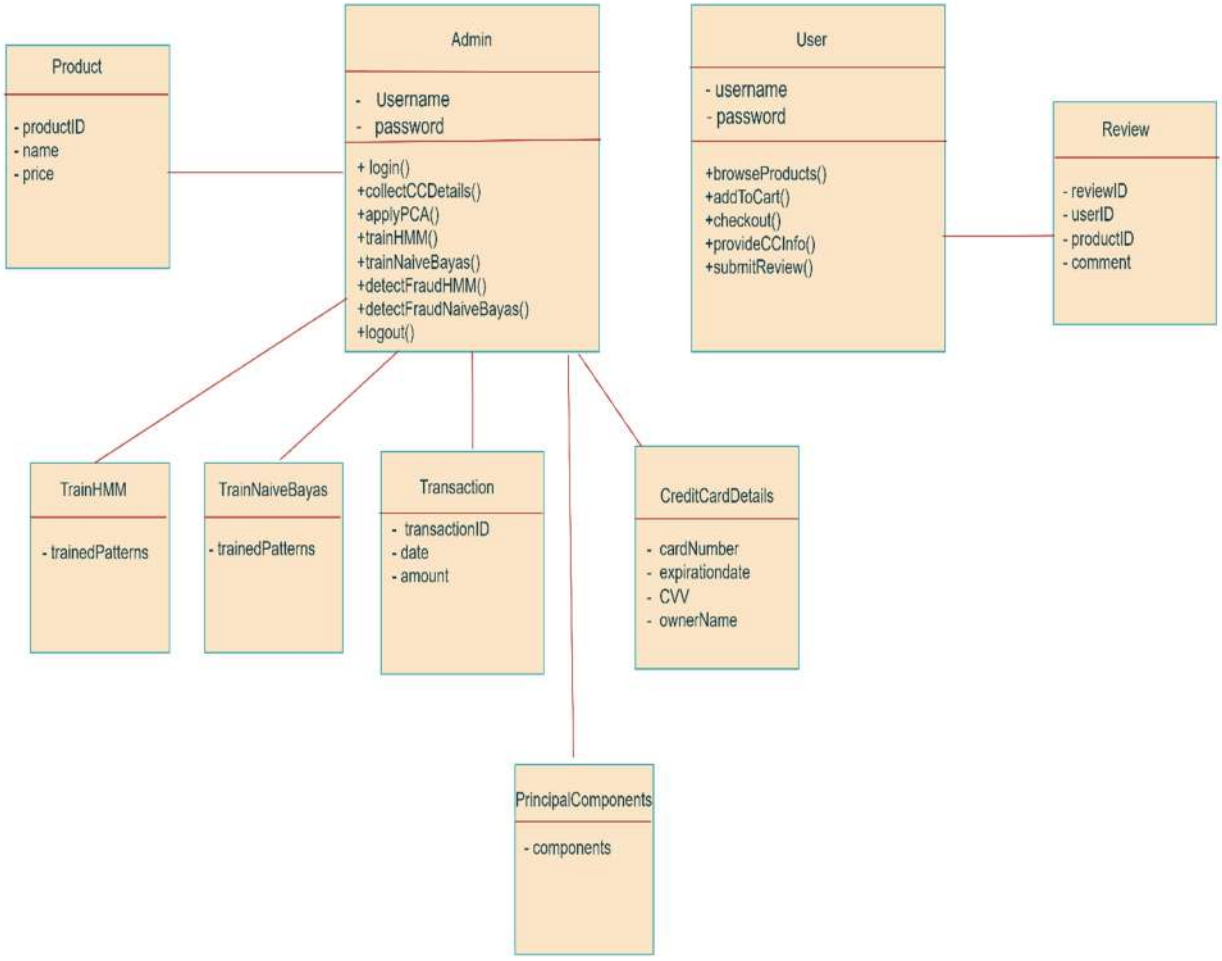


Fig 4.3.4 Class Diagram

IV. IMPLEMENTATION AND RESULTS

This chapter tells us about the implementation part of the website. This section deals with the brief introduction about the important functions used to create the Shopping Website. It consists of various source codes used in building this web page.

Output Screens

Main Page :

First create database in MYSQL by copying content from WEB-INF/db.txt file and paste in MYSQL. Then put 'CreditCardFraud folder inside tomcat webapp directory and start your tomcat server. Now Open browser and enter URL as 'http://localhost:9999/CreditCardFraud/' and then press enter key to get below page

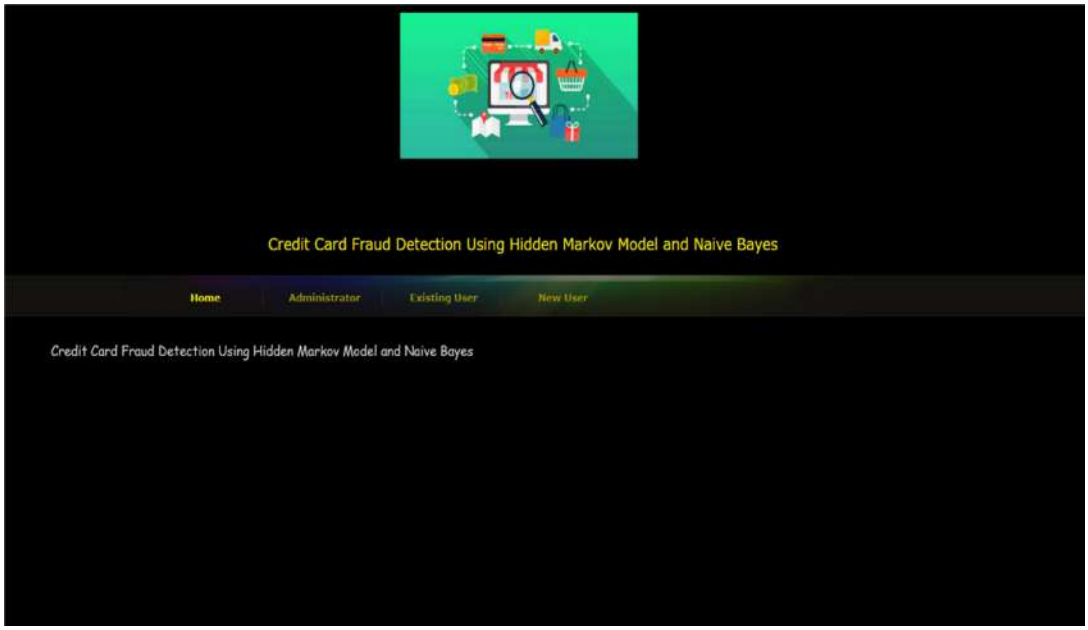
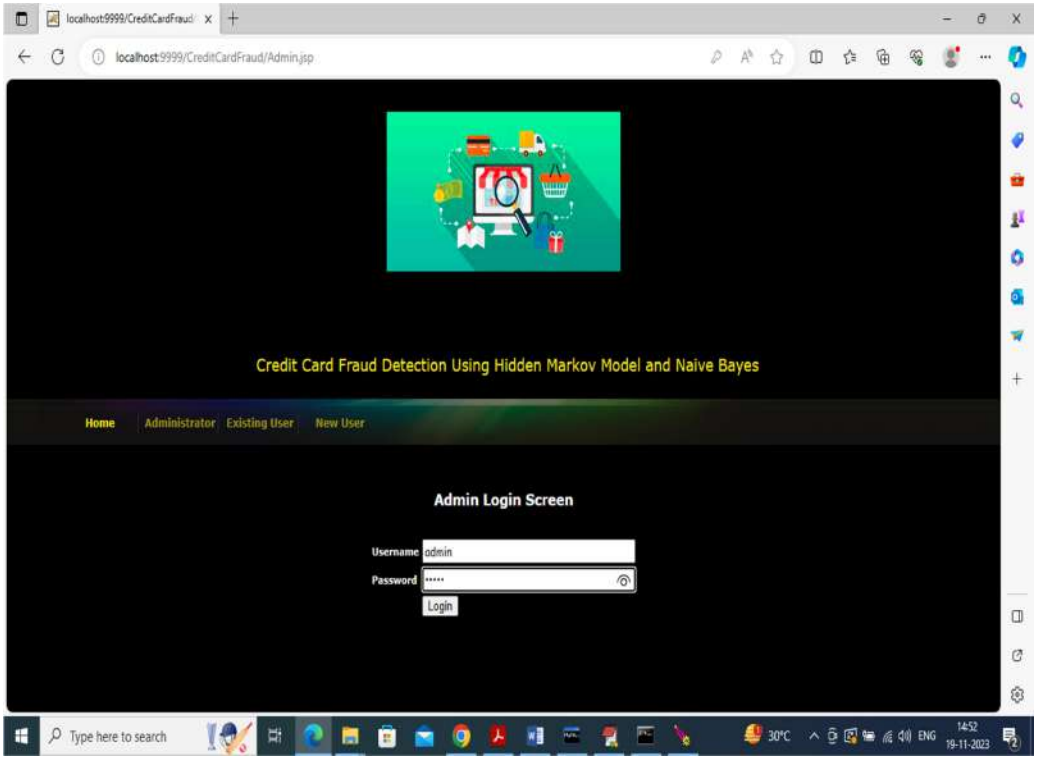
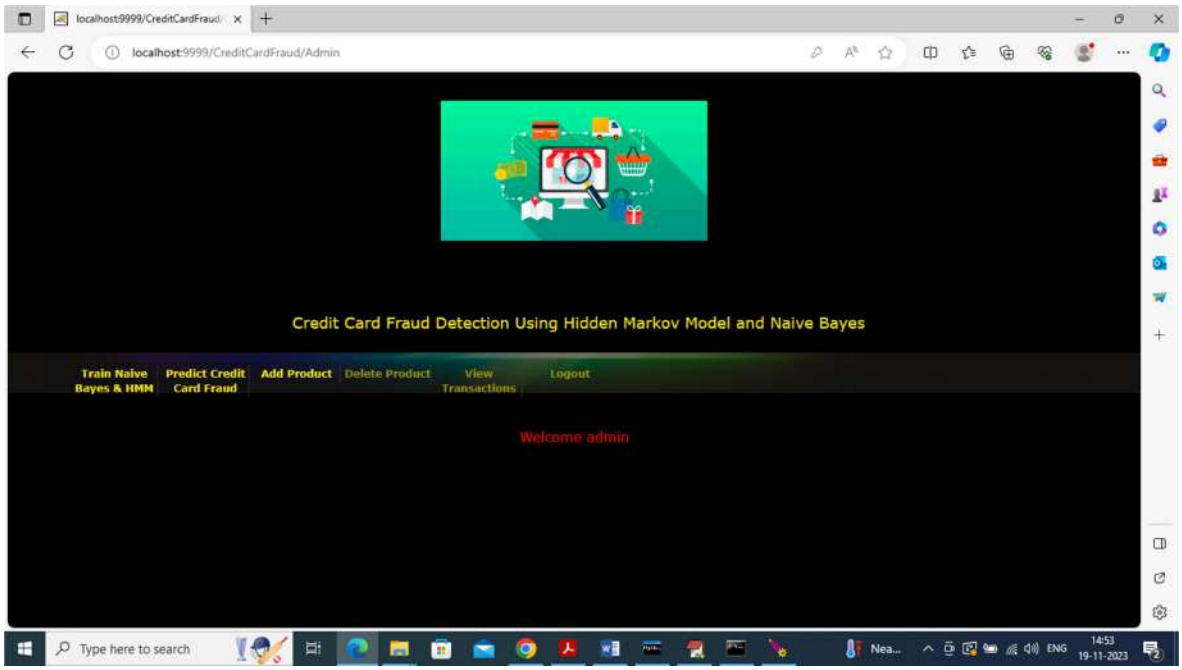


Fig 7.1 Main Page

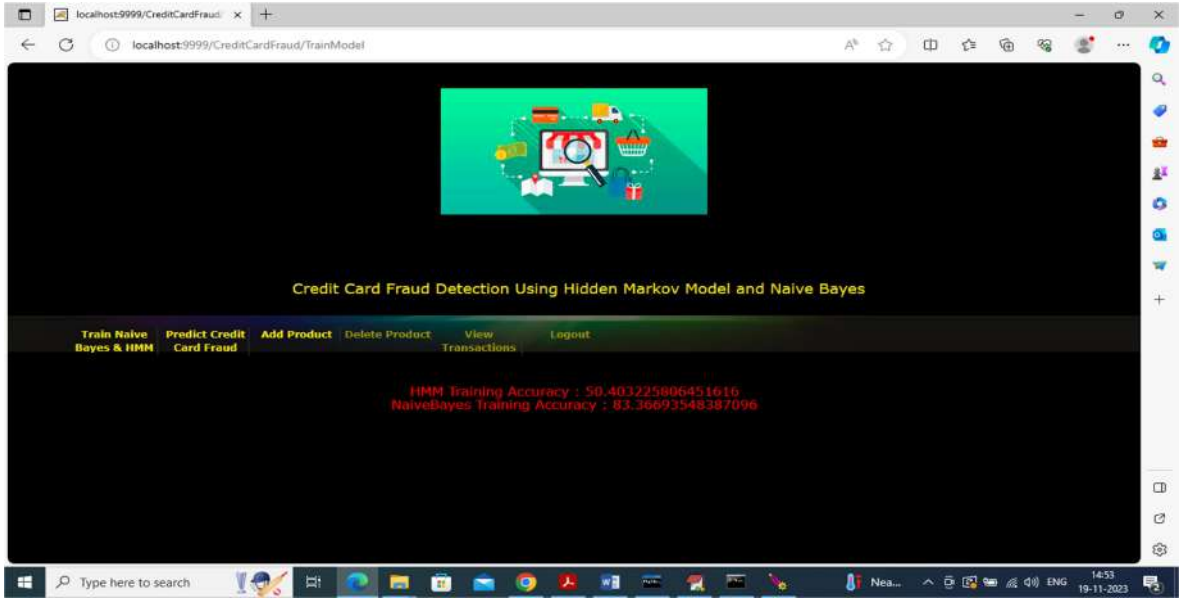
In above screen click on 'Administrator' link to get below admin login page



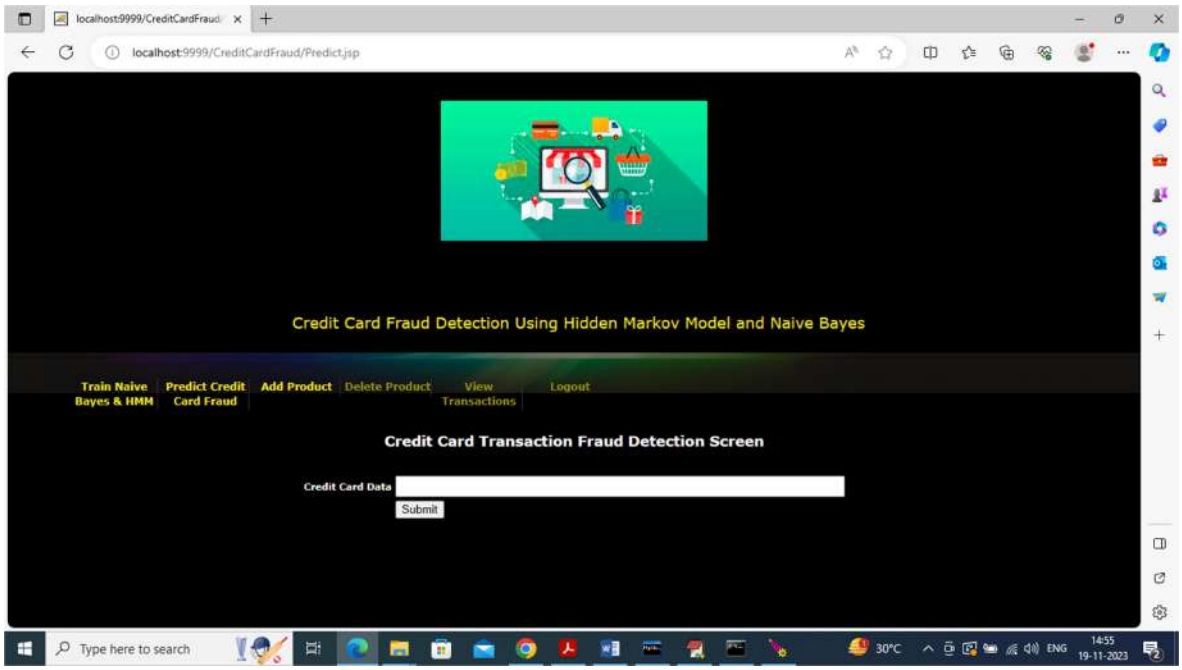
In above screen admin can login by using username and password as 'admin' and then press 'Login' button to get below page



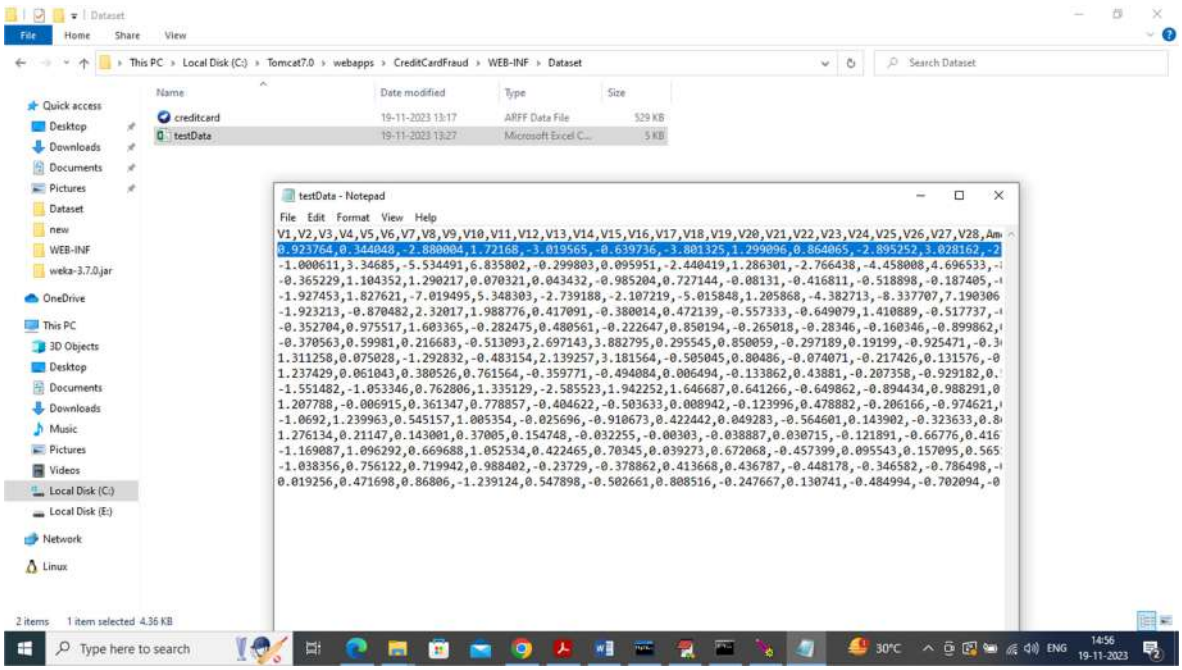
In above screen admin can click on 'Train Naïve Bayes & HMM' link to train model by using Credit Card Fraud dataset and then will get below output



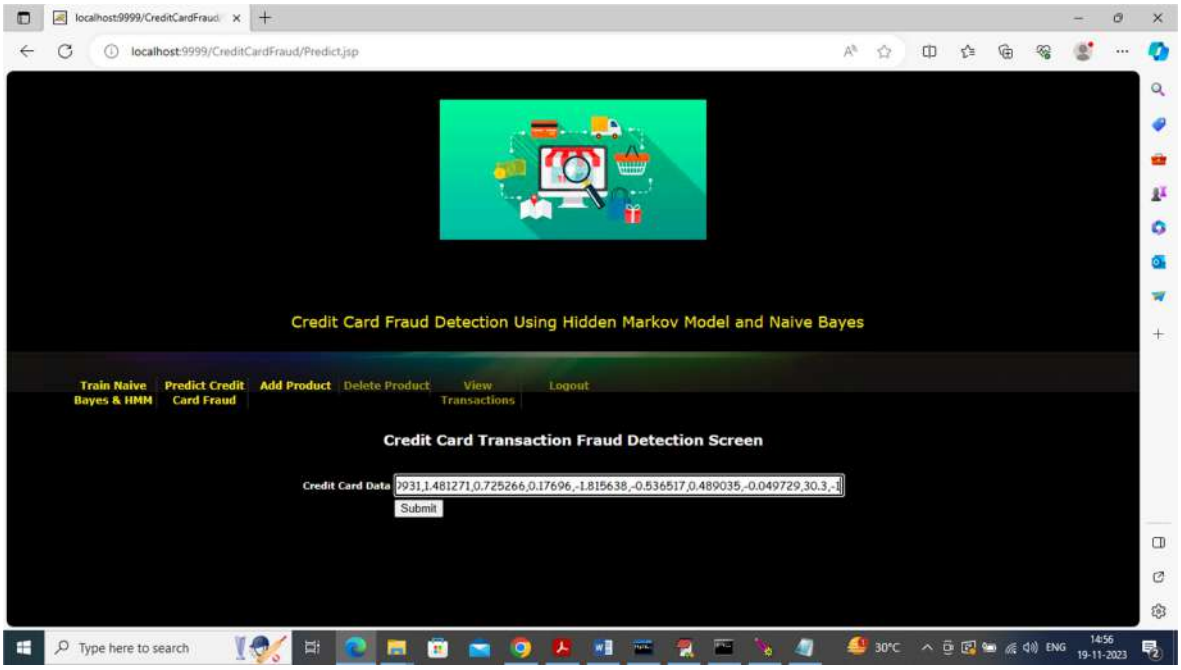
In above screen both algorithms training completed and HMM got 50% accuracy and Naïve Bayes got 83% accuracy and now click on 'Predict Credit Card Fraud' link to get below page



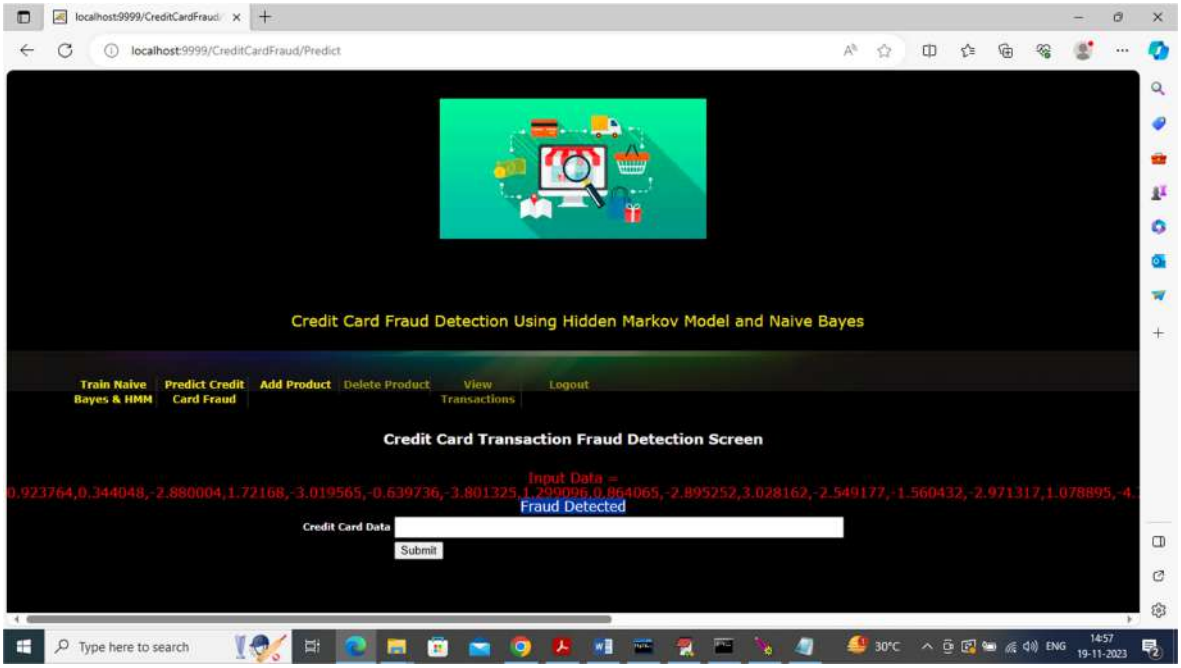
In above screen we need to enter credit card transaction details and this details you can copy from 'WEB-INF/Dataset/testData.csv' file like below screen.



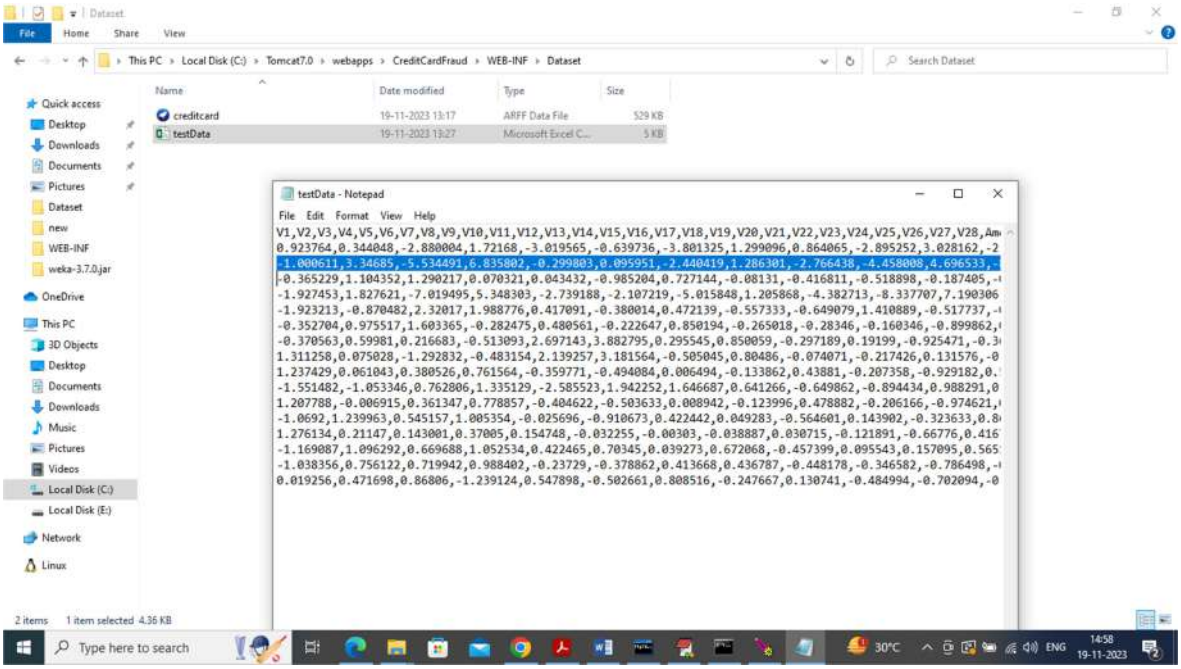
From above screen copying first line of credit card fraud and paste in application like below screen



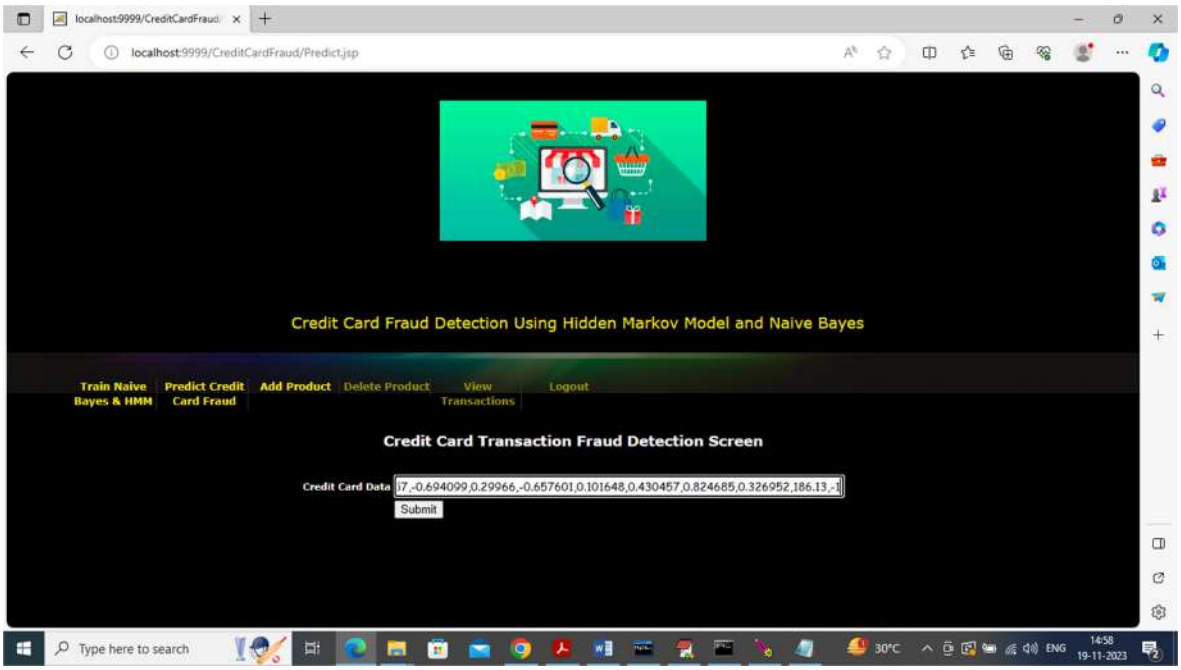
In above screen entered card transaction and then press button to get below output



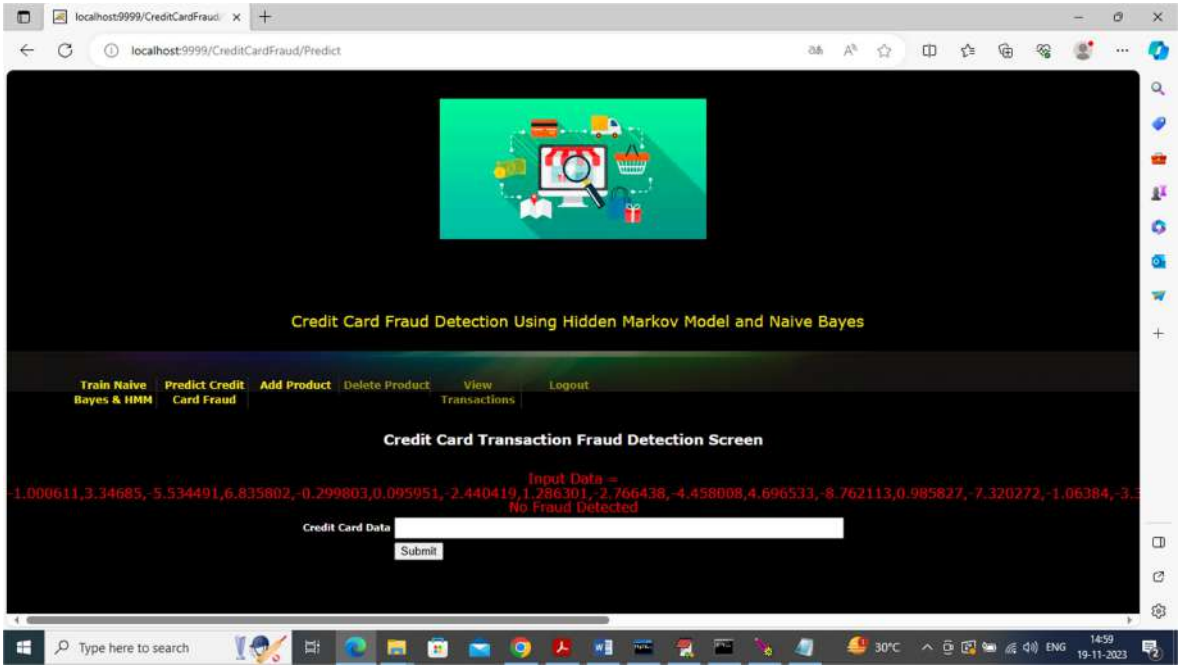
In above screen in blue colour text can see 'Fraud Detected' given transaction data and now try another transaction



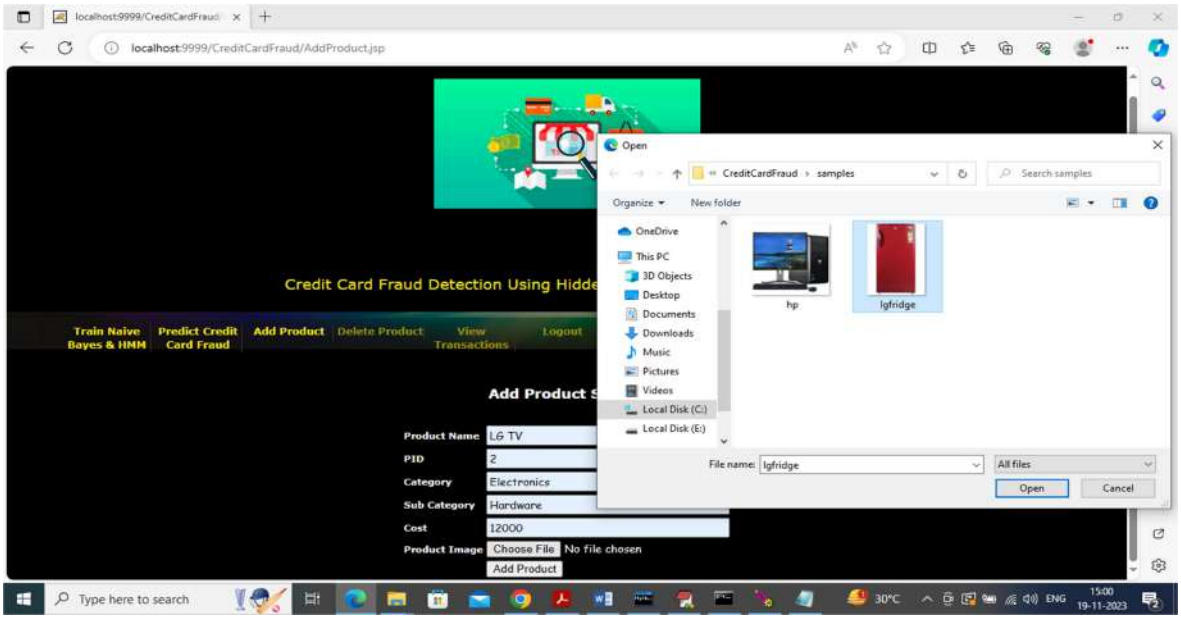
From above screen copying second record and now paste in application to get below output



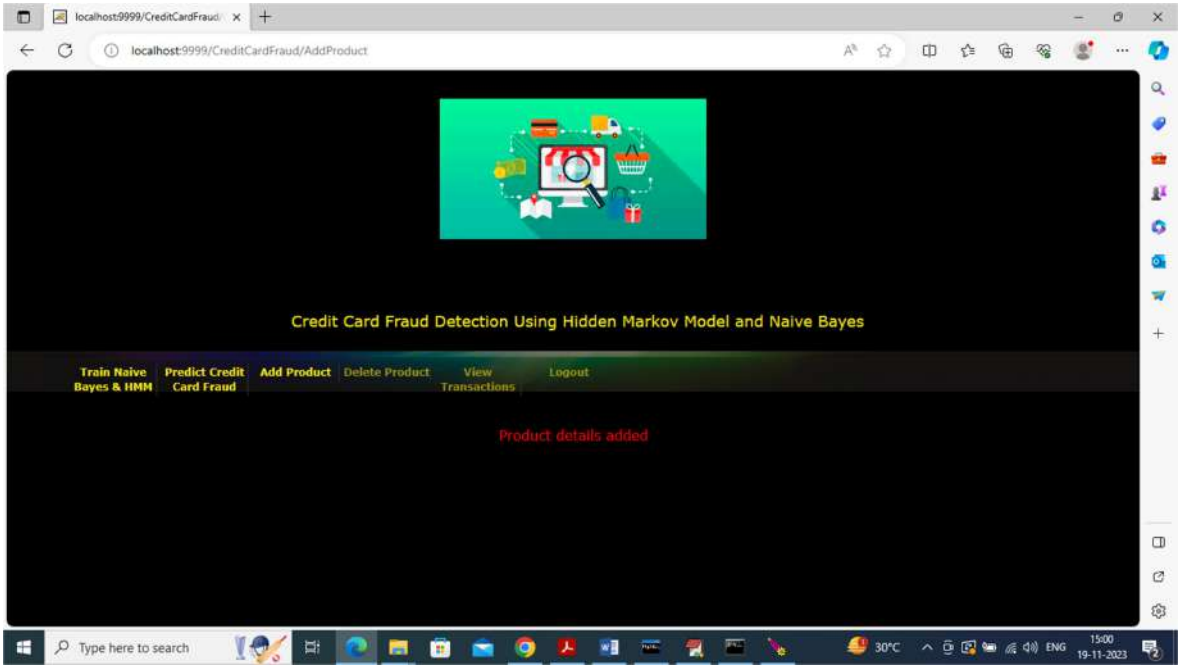
In above screen added new transaction and press button to get below page



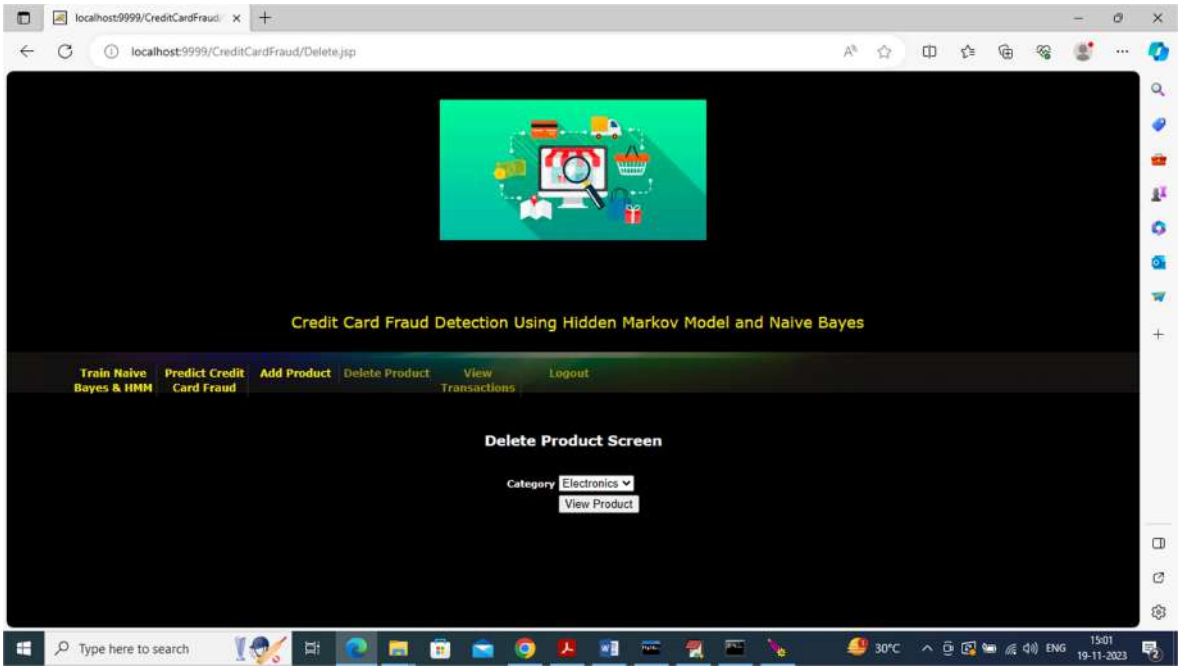
In above screen for second transaction we got predicted value 'No Fraud detected' and similarly you can test for remaining transactions and now click on 'Add Product' link to add new products



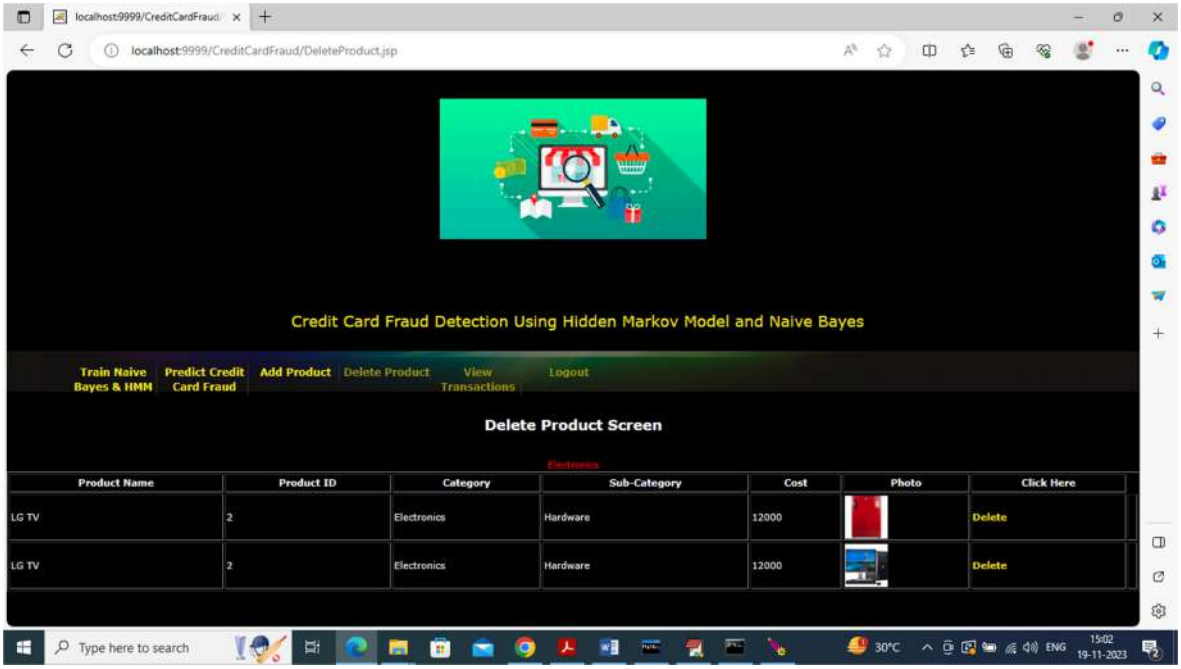
In above screen adding product details and uploading image and then press button to add details and get below page



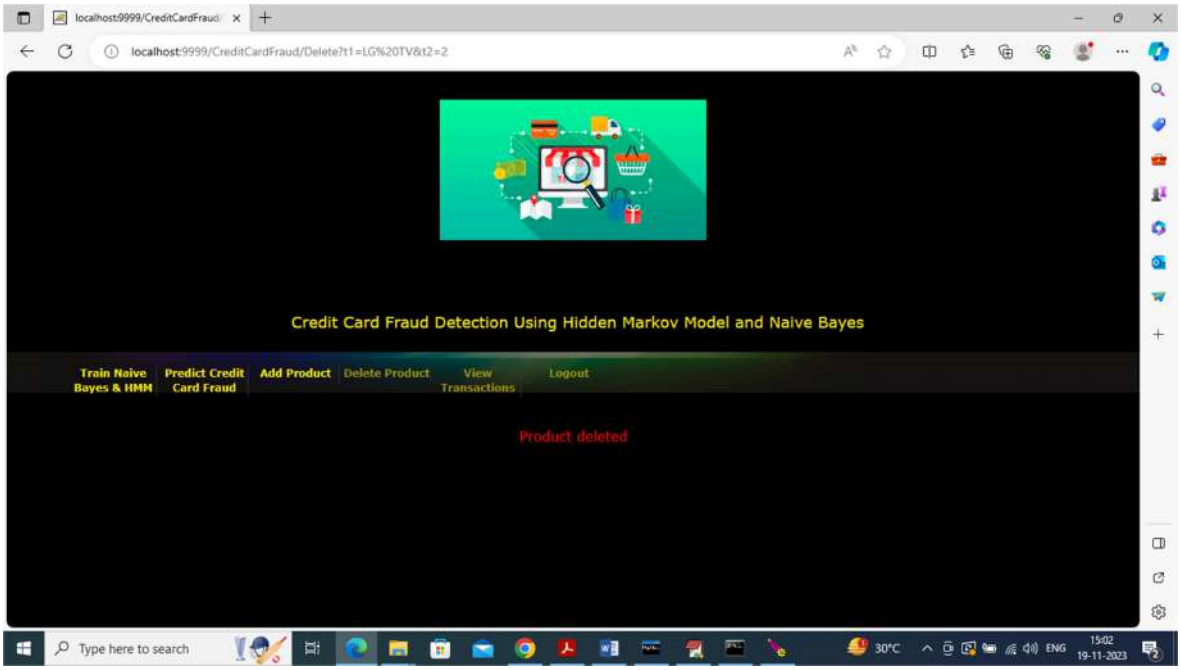
In above screen product details added and similarly you can add any number of products and now click on 'Delete Product' link to view and delete desired product



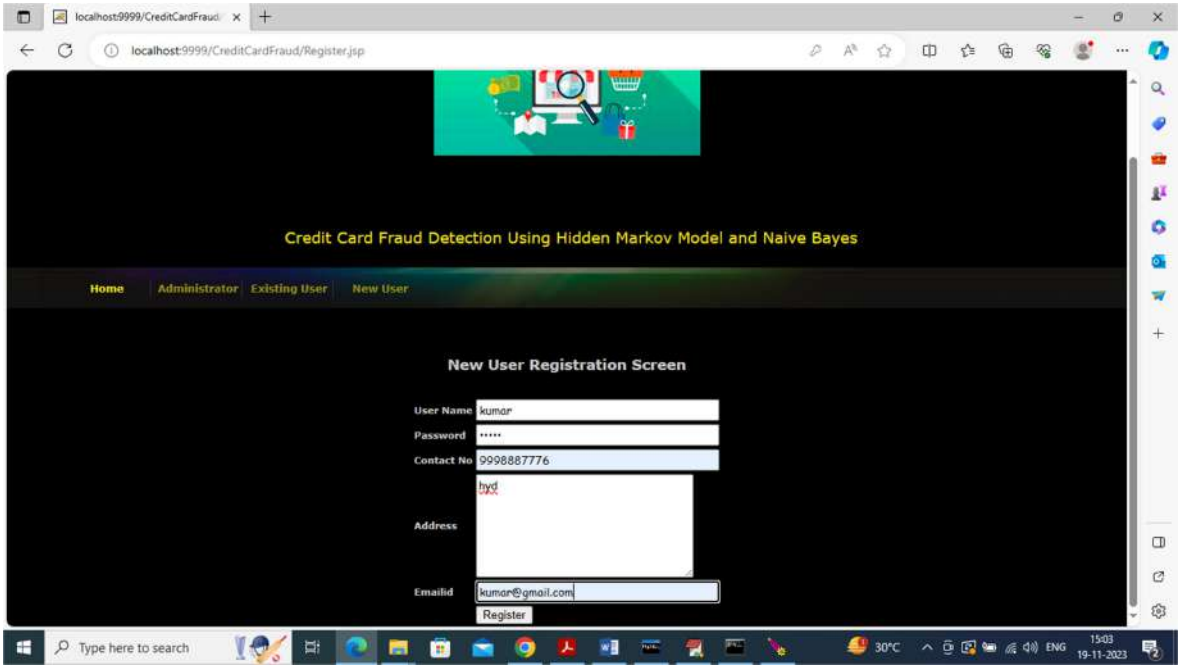
In above screen select product category to get list of products like below screen



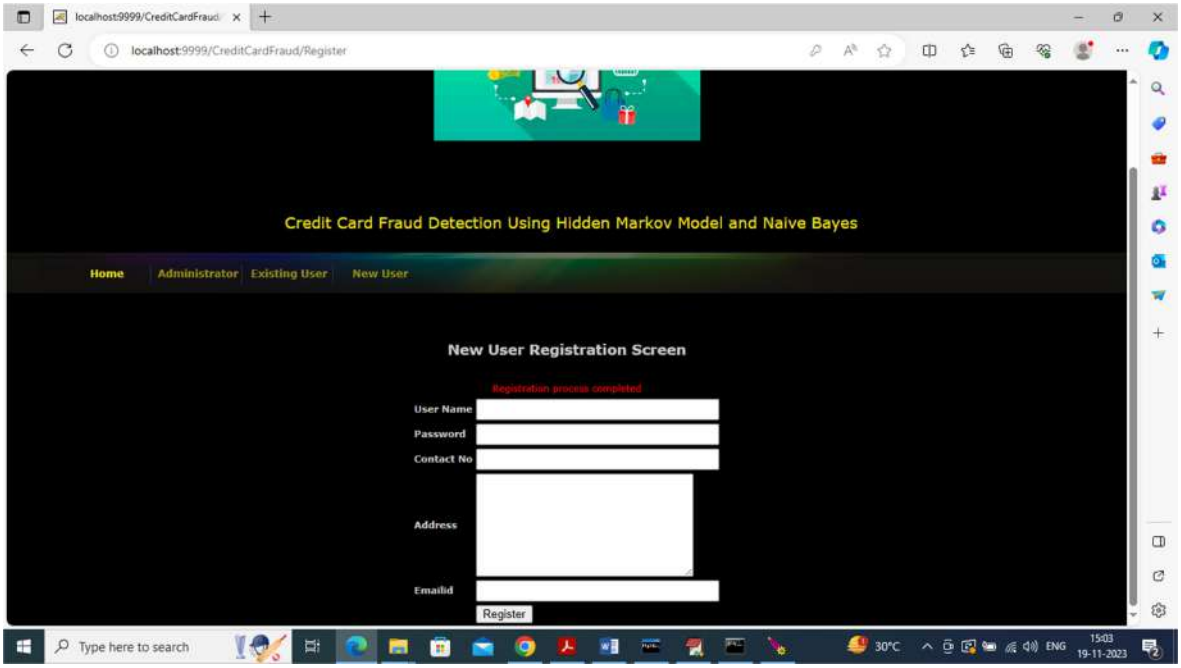
In above screen admin can view all product details and then press 'Delete' link to delete any product and get below page



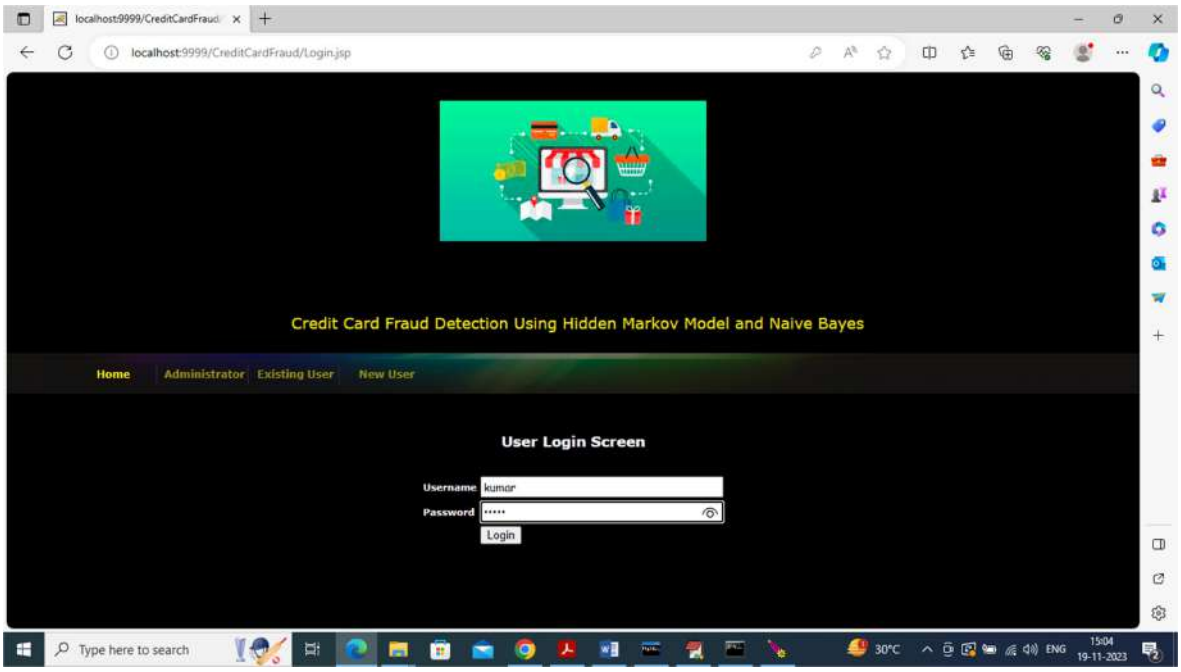
In above screen product deleted and now logout and sign up new user like below page



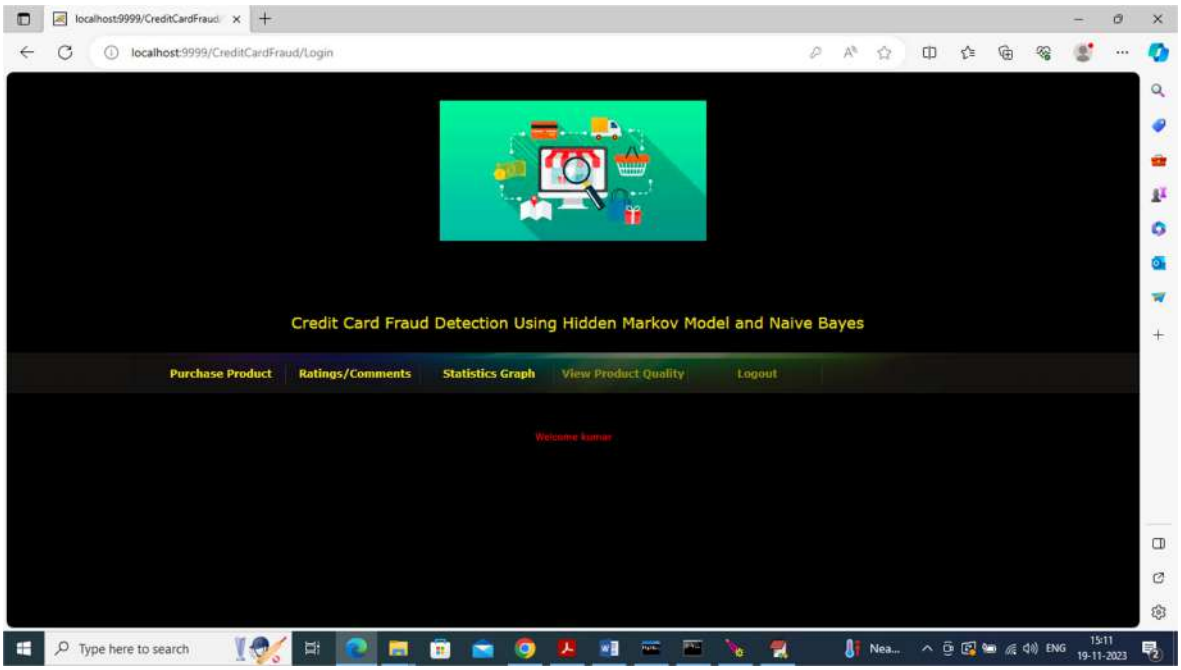
In above screen user is entering signup details and then press button to get below page



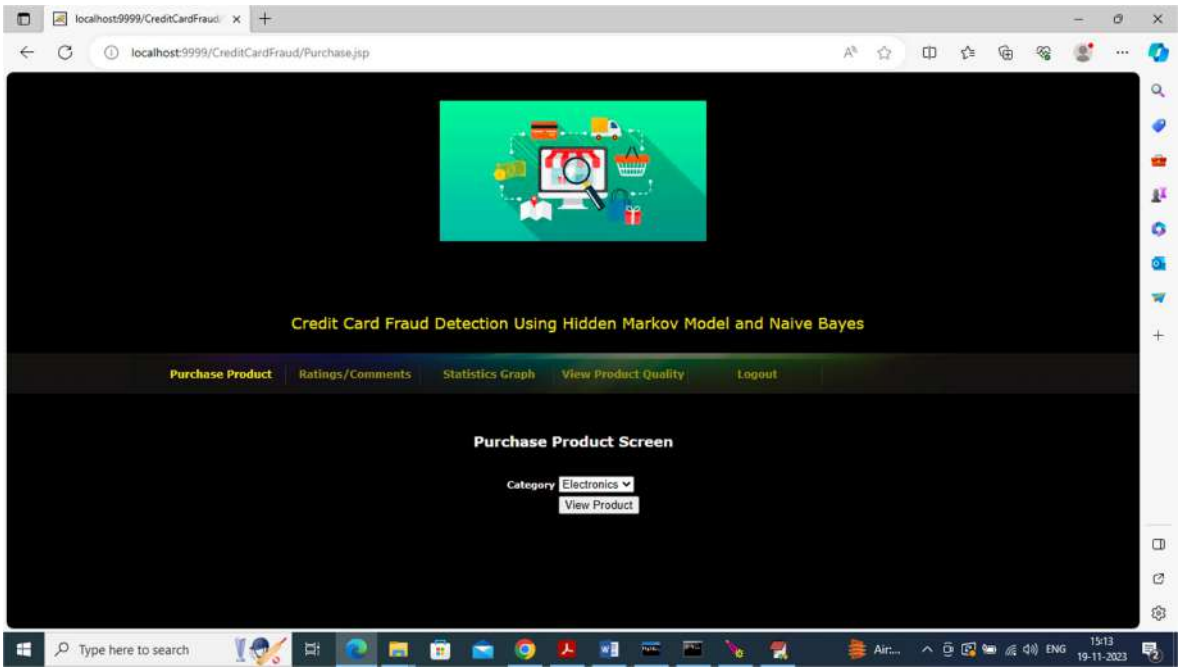
In above screen registration completed and now click on 'Existing User' link to login as user like below screen



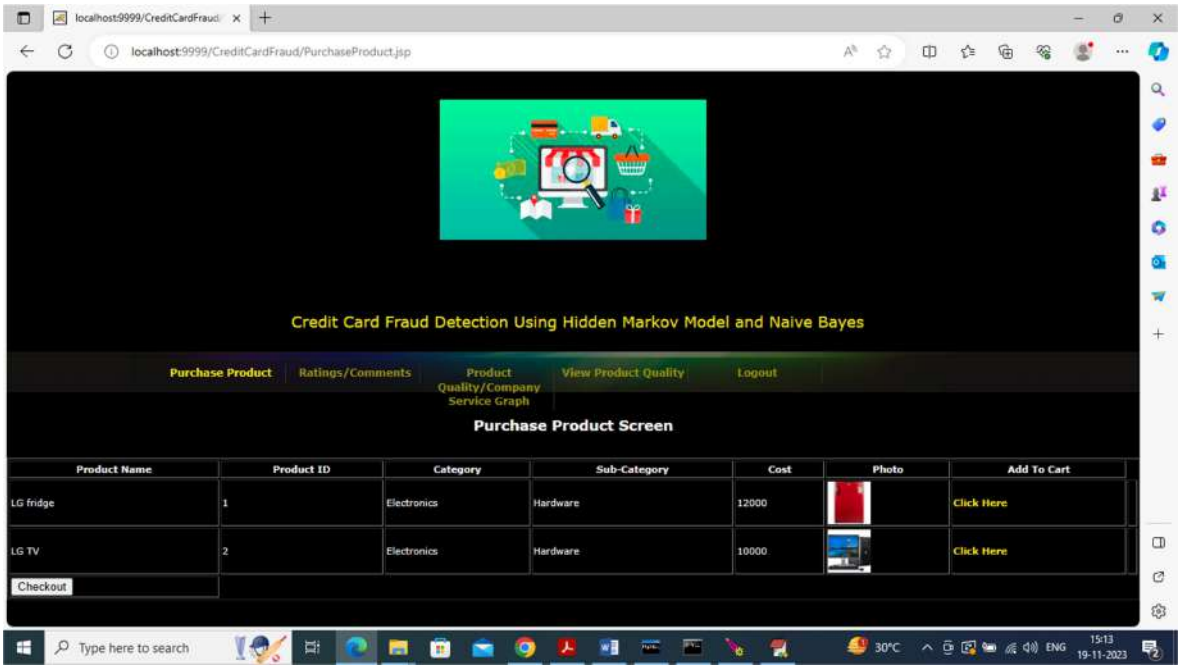
In above screen user is login and after login will get below page



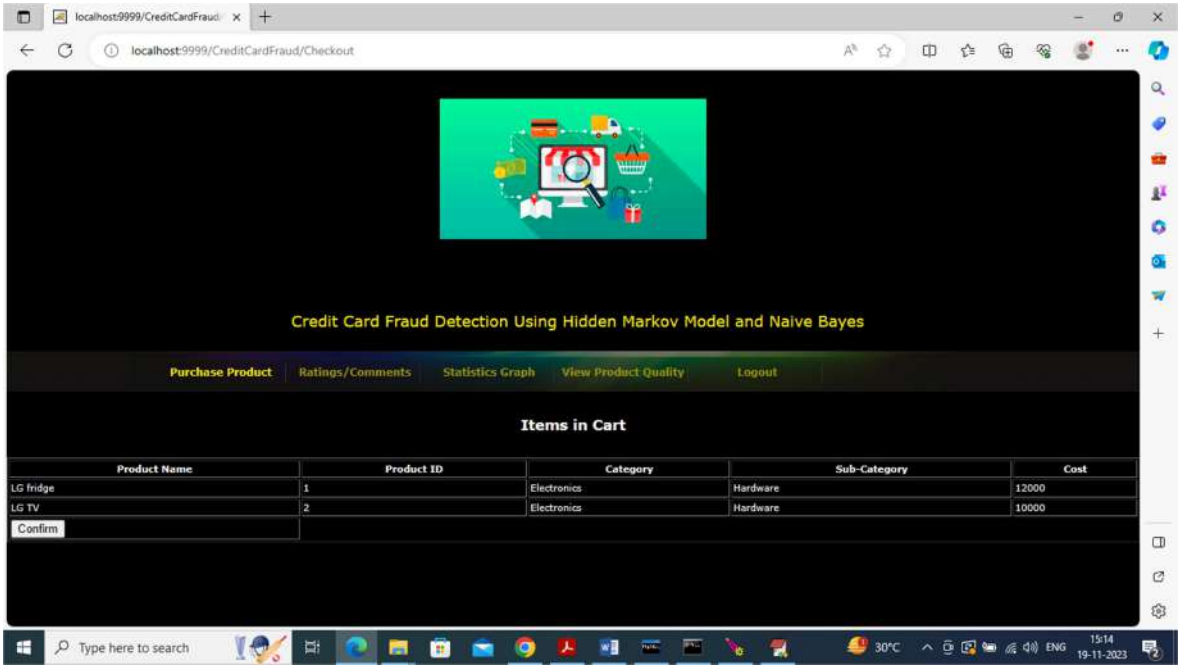
In above screen user can click on 'Purchase Product' link to get below page



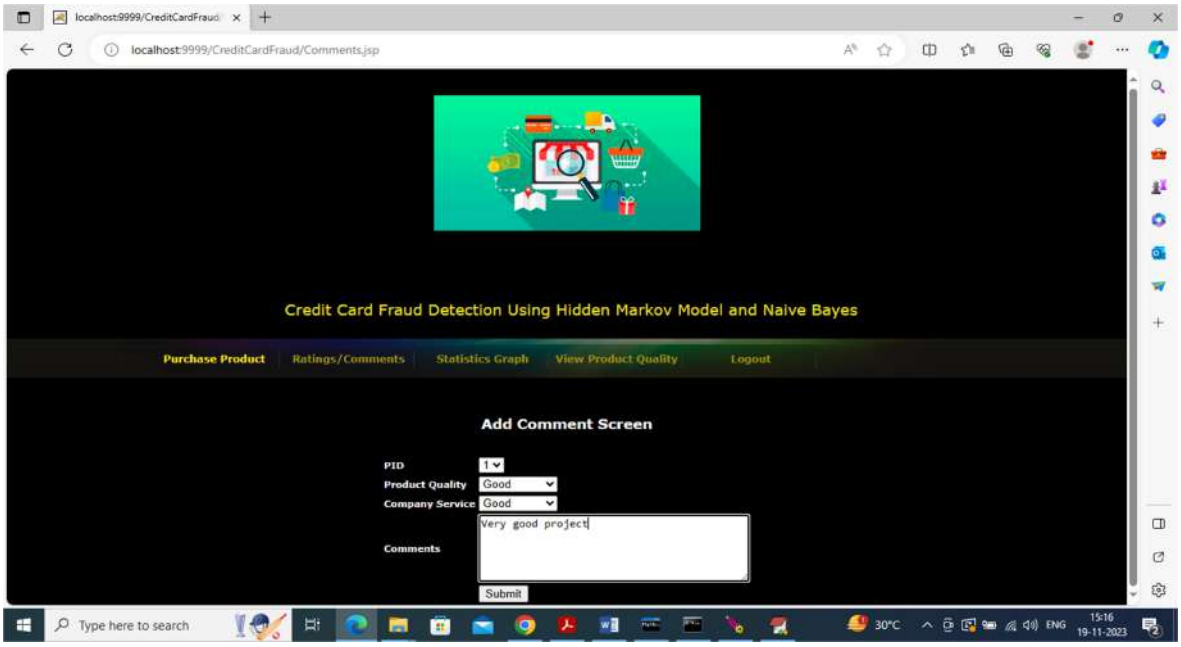
In above screen user can select category and press button to get below page



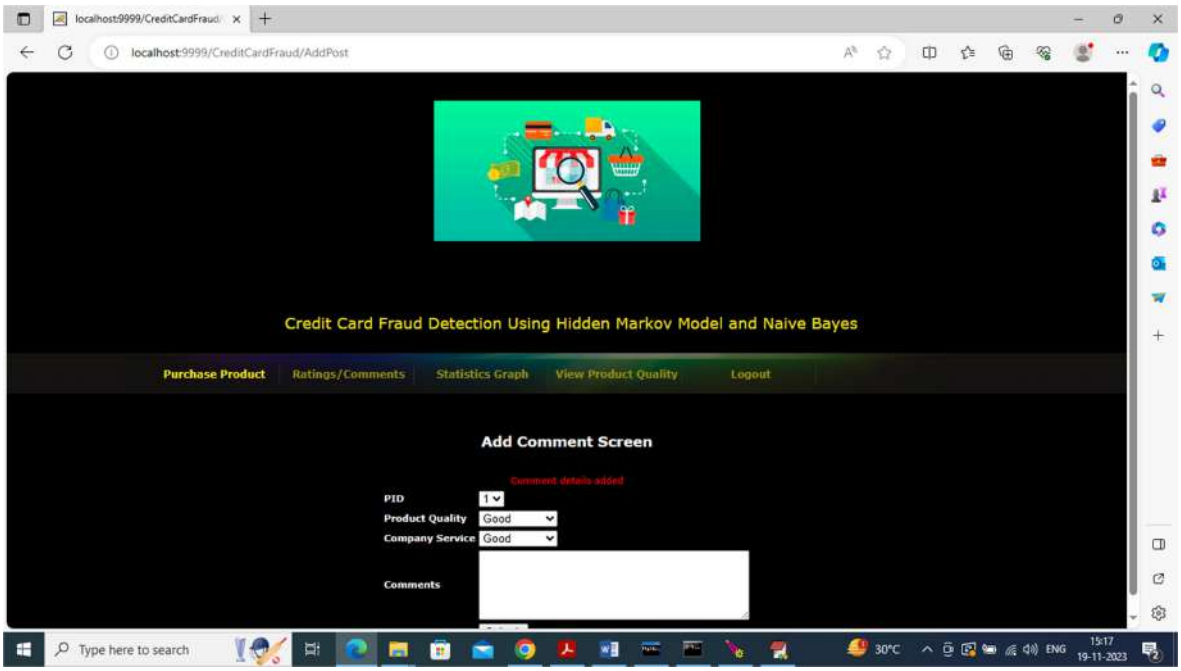
In above screen user can view all product details and then click on 'Click Here' link to add product to cart and once done can click on 'Check Out' to complete purchase and get below page



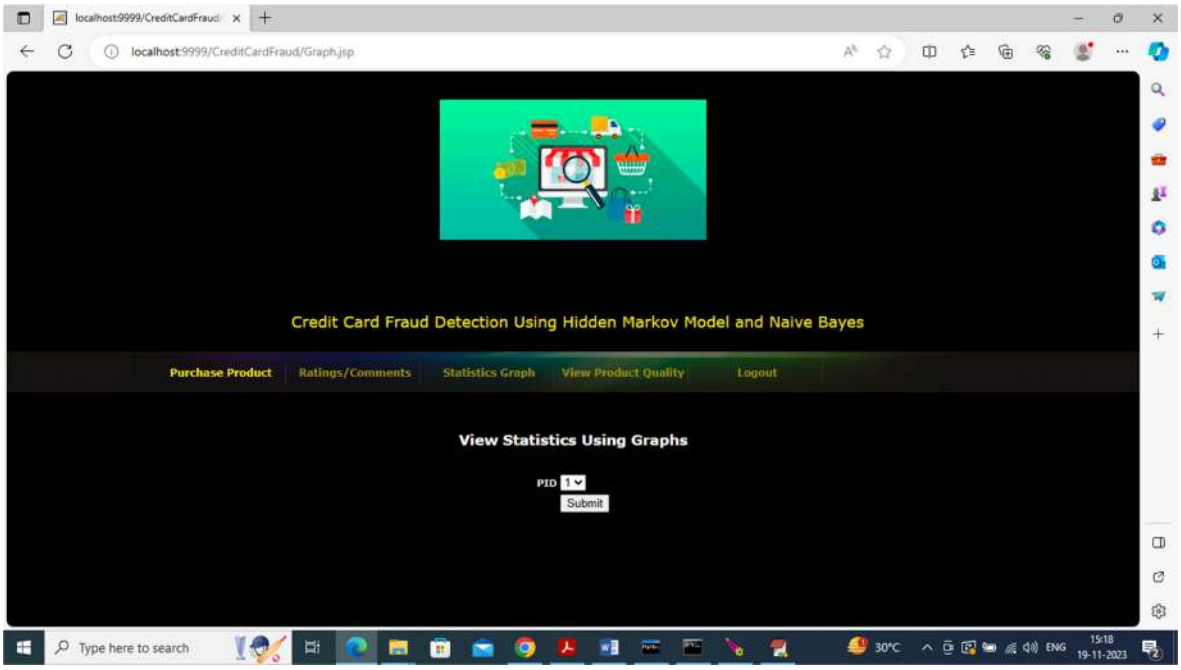
In above screen two items added to cart and now click on 'Confirm' to complete purchase and get below page and then click on 'Ratings/Comments' link to get below page



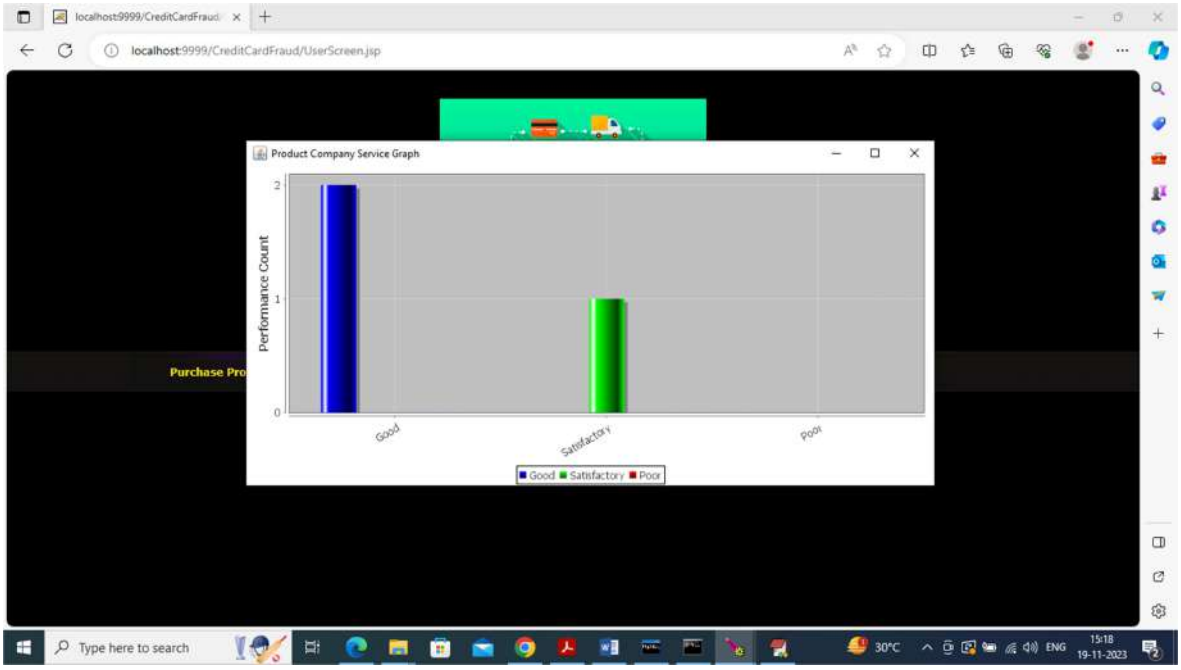
In above screen user can write product service quality and product quality and then write comments and press button to get below page



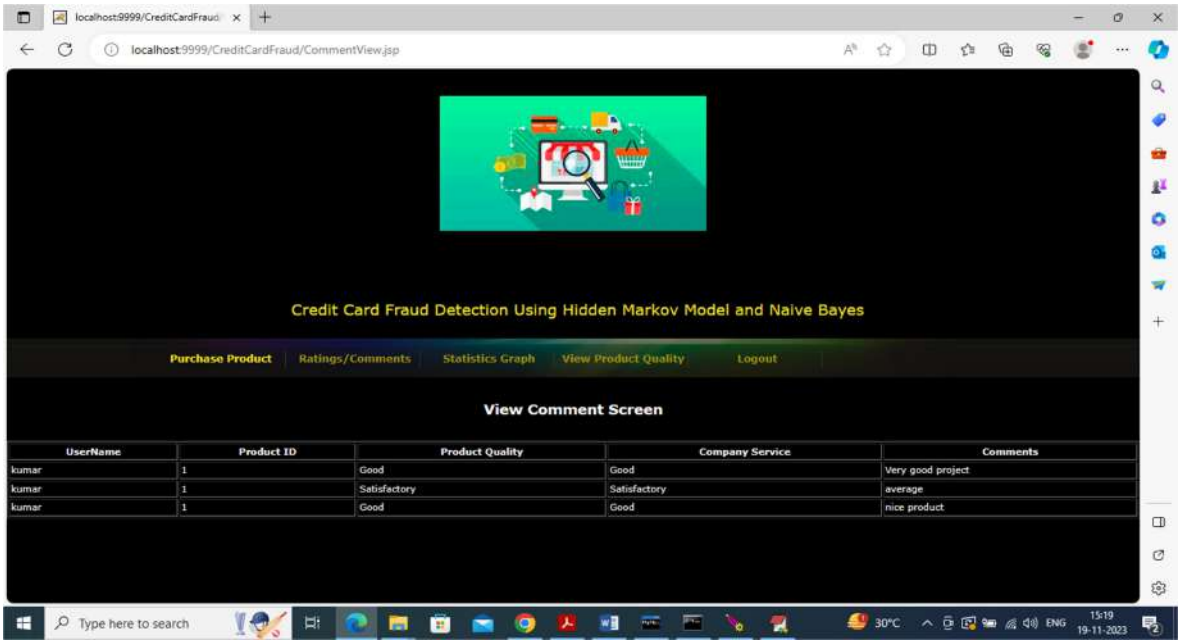
In above screen comments details added and now click on 'Statistics Graph' link to get below graph



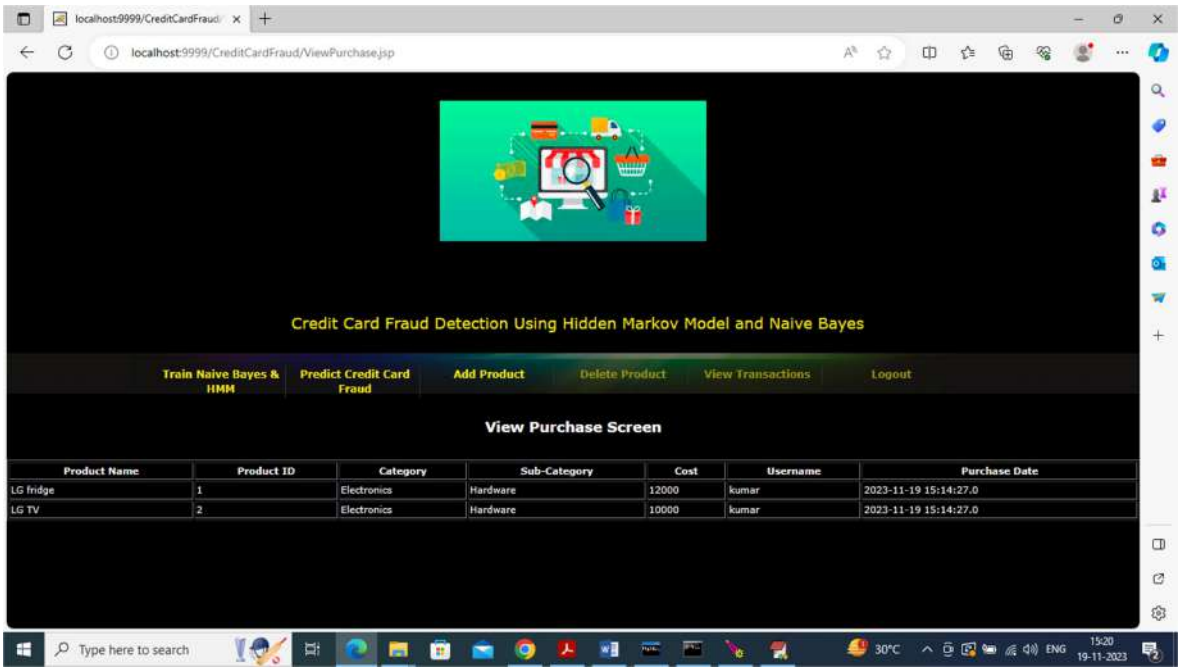
In above screen user can select product ID and then press button to get product statistics received from users



In above graph x-axis represents product quality Type and y-axis represents count for that quality and now close above graph and then click on 'View Product Quality' link to view all reviews and ratings



In above screen user can view ratings and reviews for selected product and now logout and login as admin to view transactions



In above screen admin can view all transactions or purchase made by users. So by following above screens you can detected fraud and can make online shopping.

V. Conclusion

We have proposed an application of HMM in credit card fraud detection. The different steps in credit card transaction processing are represented as the underlying stochastic process of an HMM. We have used the ranges of transaction amount as the observation symbols, whereas the types of item have been considered to be states of the HMM. We have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not. Comparative studies reveal that the Accuracy of the system is close to 80 percent over a wide variation in the input data. The system is also scalable for handling large volumes of transactions..

REFERENCES

[1] Ghosh, S., and Reilly, D.L., 1994. Credit Card Fraud Detection with a Neural-Network, 27th Hawaii International l Conference on Information Systems, vol. 3 (2003), pp. 621- 630.

[2] Syeda, M., Zhang, Y. Q., and Pan, Y., 2002 Parallel Granular Networks for Fast Credit Card Fraud Detection, Proceedings of IEEE International Conference on Fuzzy Systems, pp. 572-577 (2002).

[3] Stolfo, S. J., Fan, D. W., Lee, W., Prodromidis, A., and Chan, P. K., 2000. Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project, Proceedings of DARPA Information Survivability Conference and Exposition, vol. 2 (2000), pp. 130-144.

[4] Aleskerov, E., Freisleben, B., and Rao, B., 1997. CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection, Proceedings of IEEE/IAFE: Computational Intelligence for Financial Eng. (1997), pp. 220-226.

[5] M.J. Kim and T.S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc. Int'l Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.

[6] W. Fan, A.L. Prodromidis, and S.J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," IEEE Intelligent Systems, vol. 14, no. 6, pp. 67-74, 1999.

[7] R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. Tools with Artificial Intelligence, pp. 103-106, 1999.

[8] C. Chiu and C. Tsai, "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. e-Technology, e-Commerce and e Service, pp. 177-181, 2004.

[9] C. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," http:// www.bsys.monash.edu.au/people/cphua/, Mar. 2007.

[10] S. Stolfo and A.L. Prodromidis, "Agent-Based Distributed Learning Applied to Fraud Detection," Technical Report CUCS-014-99, Columbia Univ., 1999.