|| Volume 5 || Issue 11 || November 2020 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

UTILIZING PRODUCT FEATURES FOR FRAUD DETECTION ON E-COMMERCE PLATFORMS IN BIG DATA TRANSACTIONS

Aashir Baig[1], Dr. K.Nagi Reddy[2]

Research Scholar, Dept. of Computer Science & Engineering, LIET, Hyderabad[1]

Professor, Dept. of Computer Science & Engineering, LIET, Hyderabad[2]

aashirbaig0@gmail.com[1]

k.nagireddy@lords.ac.in[2]

-- ***--

Abstract:- - Fraudulent transactions are a serious concern for e-commerce websites and other platforms that are operating their businesses on the web. With the advent and growth of Big Data technology, consumers who buy products online always assess the vendors or suppliers as per the ratings and reputation suggested by the e-commerce platform. The cause or motivation for the vendors to pursue high ratings and reputation scores for them on the e-commerce platform is that high ratings and positive comments about the products sold by them would fetch them high profits. The fraudulent vendors try to attain high reputation scores and thereby attract more customers to buy their products only. It is very much important for e-commerce websites to identify such imposters and identify fake reputation information as not identifying the fraudulent vendors would lead to the loss of business and reputation of the e-commerce platform itself. The e-commerce platforms nowadays are attempting to curb ongoing and growing issue by employing data mining mechanisms. With the advent of the Internet of Things (IoT) and Big Data has an important role to play in the economic growth in various domains. It supports the organizations and improves their decision-making capabilities by analyzing their operational data. It also helps the e-commerce platforms by providing online customers with an impartial and strong reputation system, thereby improving their online shopping experience. The objective of this technical paper is to present a conceptual framework to bring out the characteristics of fake transactions along with individual and transaction-related pointers. Product type and Product nature are two features to which are used to identify fraudulent transactions. These two features help in improving the accuracy of fake reputation detection. A dataset from the real-world is used to validate the effectiveness and accuracy of the fraud detection model which helps in identifying the fraudulent vendors from the genuine ones.

Keywords:- *E-business, Fraud Detection, Reputation System, SNA, K core*

-- ***--

I INTRODUCTION

With massive improvements in software technologies, data has grown rapidly due to social networks and E-Commerce applications [3]. Data mining techniques have improved, and they have provided an opportunity for online businesses to understand their data and get valuable insights from it. This helps to improve their business strategies and grow their market. Big data and the Internet of Things started playing an important role in the economic growth of various domains[1]. Many people now are interested in shopping for their needs online due to various reasons. However, they cannot touch or feel the products and judge their quality as they do in traditional shopping methods. Hence, they rely on vendor reputation and map it to their credibility[4]. The highly reputed the vendor the more he is likely to sell good quality products. As the consumers depend on vendor reputation for credibility many online platforms and E-Commerce businesses have developing and implementing recommendation systems and credibility systems which gives vendors a score[2] or rating based on the feedback given by consumers after purchasing and using their products. This makes potential buyers buy their products from vendors who have high credit scores. The more the vendor can sell things online the more he makes a profit [5]. As the credit score is directly linked or proportional to the profit margins of vendors, they are highly motivated to get better scores on the E-Commerce platforms [6].

Cybercriminals and fraudsters have started taking advantage of these credibility systems and started making collusive transactions in an organized way. They pay a fraudulent organization for the task of inflating their credibility scores[7]. The organization employs puppet buyers who buy products only from the fraudulent vendors and the system give positive feedback, high ratings, and proceed and detailed comments for the products that they have bought and thereby increase the credit score of the fraudulent vendor on the E-Commerce platform [8].

Over a period, the reputation of the fraudulent vendor increases immensely, and potential buyers tend to buy products from these vendors. But later they would have realized that the products they have bought are not worth the money they have spent[9]. This makes them lose their trust in the E-Commerce platform and they stop buying products from that online platform. As the number of consumers decreases, the e-commerce platform loses its reputation, credibility, and market[10]. Hence the e-commerce platform needs to be equipped with relevant mechanisms to battle the frauds.

In this paper, we try to understand the collusive behavior of fraudulent vendors, puppet buyers, collusive transactions, and misleading reviews and build a model based on it. The two new features identified for fraud detection are product nature and product type. These features are united with other characters in the system to identify the indicators that can recognize fraudulent transactions. In order, we also employ a real-time dataset and try to check the accuracy of the model. In the future, this model can be generalized to identify fraud in other domains.

II LITERATURE SURVEY

2.1 Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015

Financial fraud is a burning problem across multiple industries and domains and many organizations. a lot of money is being lost due to this fraud. With the latest developments in software technology like artificial intelligence and machine learning, data mining techniques are being used by organizations to detect financial fraud. This paper has reviewed the research conducted on the various data mining tools that are being used to identify fraudulent financial transactions over 10 years. This paper also came up with the trends of financial frauds and the ways of detecting it using the latest data mining techniques. It has been concluded that 41 data mining techniques are used to detect financial fraud in the insurance and credit card domains of which the logistic regression model is the most frequently used one. This review classified financial fraud into different categories and provided a handy solution to researchers and professionals working in this area.

2.2 Fraud Detection by Human Agents: A Pilot Study

With the rapid development of the Internet and associated technologies in recent years, electronic markets have grown significantly. Online auction websites hold a significant share in the market of e-commerce platforms. Fraudulent sellers pose a serious issue to online auction websites. Hence it is important to identify honest sellers and fraudulent sellers. It sometimes happens that when honest sellers are suspected they partner with competitors or slow down their sales and might even leave the market. This paper has presented a mechanism to identify fraudulent sellers from the perspective of human classifiers. This mechanism has proved to be helpful in identifying fraudulent sellers to a greater extent than the existing mechanisms and significantly reduced the false positives. This mechanism gave insights to detect fraudulent vendors in our scenario as well.

2.3 Spotting Fake Reviewer Groups in Consumer Reviews

With the rapid growth of the Internet, there has been a significant increase in people who purchase products from an online store. promoting products and reviewing them has also become a business e-commerce platform. Hence there is a huge chance that many platforms can try to promote or demote a set of target products by writing fake reviews and spamming their opinions over multiple social networks. This paper proposed a scheme to detect opinion spamming and fake reviewer groups using a combination of multiple data mining techniques and developed a model. This proposed model uses frequent item set data mining to identify the fake reviewer groups. The model is then trained to identify the patterns in the behavior of these fake reviewer groups. It is concluded that this model could detect fake reviewer groups in a more efficient way compared to other leading data mining techniques like supervised learning, regression, etc.

III SYSTEM ANALYSIS

Existing System:

With the rapid development of Internet-based applications, E-Commerce has become very popular. Many users tend to buy various products online. As the online consumers cannot touch and feel the product as compared to traditional shopping, they tend to rely on the reputation of the sellers based on user feedback. The existing oversimplified feedback mechanism and the process of giving ratings to vendors based on user feedback have given an opportunity to fraudulent vendors to perform fake transactions and illegitimately gain money. Such frauds are being performed in an organized way and pose a serious threat to the E-Commerce business as they lose their reputation over time due to collusive transactions. A fraudulent vendor gets in contact with the collusive organization to employ puppet buyers who will purchase his products and give him high ratings and detailed positive feedbacks which increase his reputation and rating and he will attract potential customers. The potential customers fall into the trap of buying products from a genuine vendor with a good rating, but they end up buying low-quality products that waste the money and degrades their shopping experience on the E-Commerce website. Such incidents with multiple customers reduce the trust on the Commerce website and their sales decrease and they lose their credibility in the market. It is important to identify such fraudulent transactions, vendors, and puppet buyers and block them from using the system to make illicit money.

Disadvantages:

1. Extremely simple and cannot identify collusive transactions.
2. Gives scope for fraudulent vendors and puppet buyers to make fraudulent transactions.
3. Unidentified fraudulent transactions result in loss of credibility and market share of the E-Commerce business.

Proposed System:

By analyzing fraudulent transactions that happened over the years using AI techniques, the following behavioral patterns have been identified:

1. Fraudulent vendors are involved in more transactions than genuine vendors.
2. Fraudulent vendors always try to sell cheap products online.

3. Newly registered accounts being involved in many transactions can be suspected as puppet buyers.
4. The nature of products that are being sold by fraudulent vendors is mostly virtual like music, subscriptions, etc.
5. Puppet buyers tend to give positive ratings and detailed reviews for cheap products.
6. Vendors with a high reputation and ratings can be suspected to take part in fake transactions.

Advantages:

1. By building a model using AI techniques for the above-mentioned behavior, it is easy to identify fraudulent vendors, puppet buyers, and collusive transactions.
2. Reduces cyber-crime and illicit ways of making money using the loopholes of the system.

IV IMPLEMENTATION

This project consists of three modules. They are:

1. User module
2. Vendor module
3. Admin module

User module:

This module has a detailed implementation of the functionalities of an online consumer. The user should first register on the application and then login with his user ID and password. If the user ID and password combination is correct, then he is redirected to go to the homepage. Otherwise, he gets a message saying that the user ID and password combination is incorrect. On the user home page, he can view all the products uploaded by various vendors and choose to buy them. In this process, he can also view the ratings of the product and give his feedback for a product. He can also add multiple products to his cart and perform a check out to buy them.

Vendor module:

In this module, the detailed implementation of the functionalities of an online vendor is listed out. To access the application, the vendor has to first register himself on the e-commerce website as a vendor using the vendor registration link present on the vendor login page. Once the vendor registers himself, he will be redirected to the login page and he can give his user ID and password to log in. If the user ID and password combination is correct the vendor will be redirected to the vendor homepage. Otherwise, he gets a message saying that the user ID and password combination is incorrect. On the vendor home page, the vendor can see all the products that he has uploaded. The home page also has links to upload a new product to the E-Commerce platform for sale and view the details of transactions associated with his products.

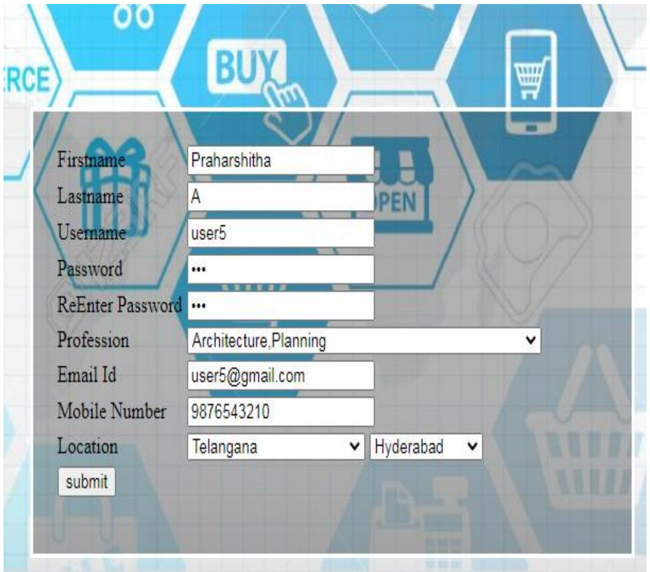
Admin module:

This module is for the E-Commerce admin to administrate the E-Commerce platform. As the project is related to fraud detection by getting high ratings and reputation by employing puppet buyers who give detailed and excellent feedback for the fraudulent vendors by buying virtual and cheap products, we have limited the admin functionality to identify the fraudulent vendors, puppet buyers, and false ratings. In this module, the admin gives his credentials to log in to the system. If this user ID and password combination is correct, then he is redirected to the admin homepage. Otherwise, he gets a message saying that the user ID and password combination is incorrect. On the admin homepage, the admin can view all the products that are uploaded by various vendors. The admin homepage also has links to give a summary of user analysis, vendor analysis, and review analysis based on the transactions that happened on the website. Based on our suggestions, the admin can continue monitoring the suspicious vendors, puppet buyers, or take appropriate action against them.

V PROJECT EXECUTION AND TESTING

User Registration:

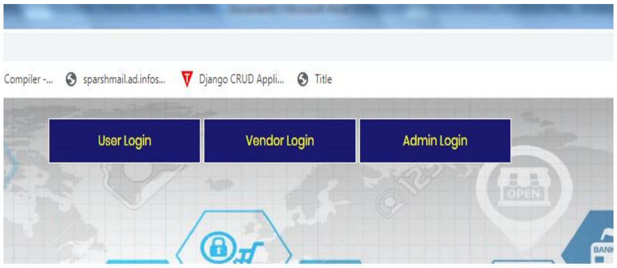
This page is a user registration page. The user enters his details like first name, last name, Password, email ID, mobile number, etc. These details are captured and inserted into the user table in the database.

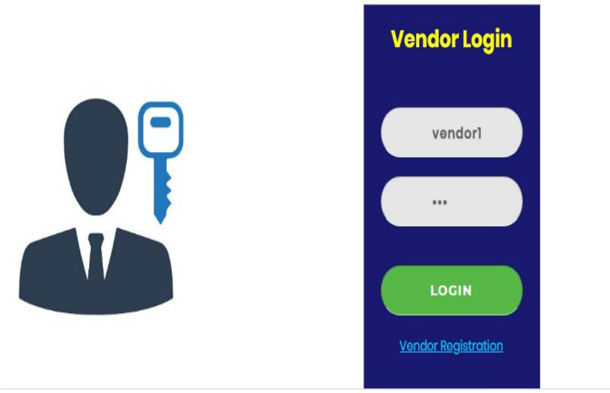


Firstname	Praharshitha
Lastname	A
Username	user5
Password	•••
ReEnter Password	•••
Profession	Architecture,Planning
Email Id	user5@gmail.com
Mobile Number	9876543210
Location	Telangana / Hyderabad

Vendor login page:

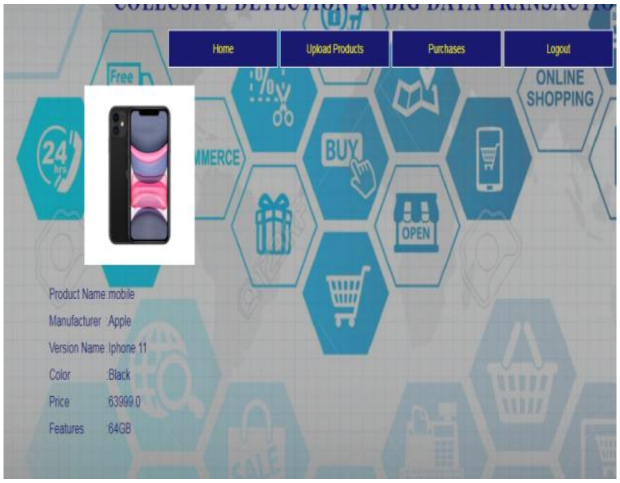
The below page is a page for vendors to log in to the website. They can give their username and password to log in and upload their products. There is also a link present for vendor registration on this page. The vendors can sign up on the E-Commerce website using this link.





Vendor home page:

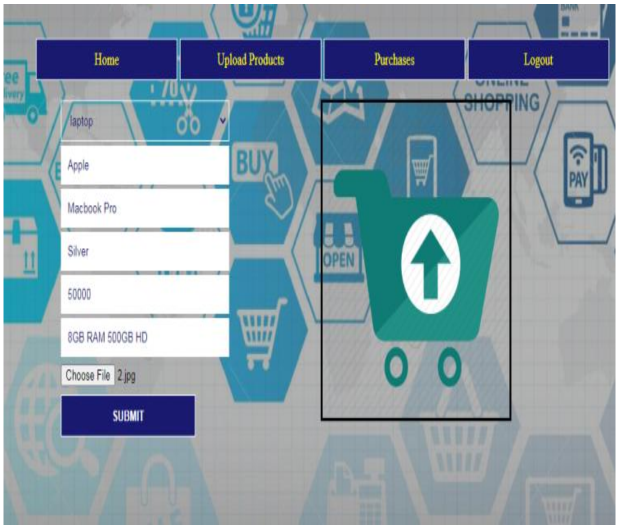
The below page is the vendor home page. Vendors can see the details of the products that they have uploaded on the website. It has links to other pages such as the upload products page, purchase page, and log out.



Product Name	mobile
Manufacturer	Apple
Version Name	Iphone 11
Color	Black
Price	63999.0
Features	64GB

Upload product page:

This page is used by the vendor to upload products. The vendor specifies the details of the product like the name, version, color, price, features, and uploads a picture of the product. On clicking the submit button the product details are saved into the database in the products table and the page is redirected to the home page displaying the details of the product that was added.



laptop

Apple

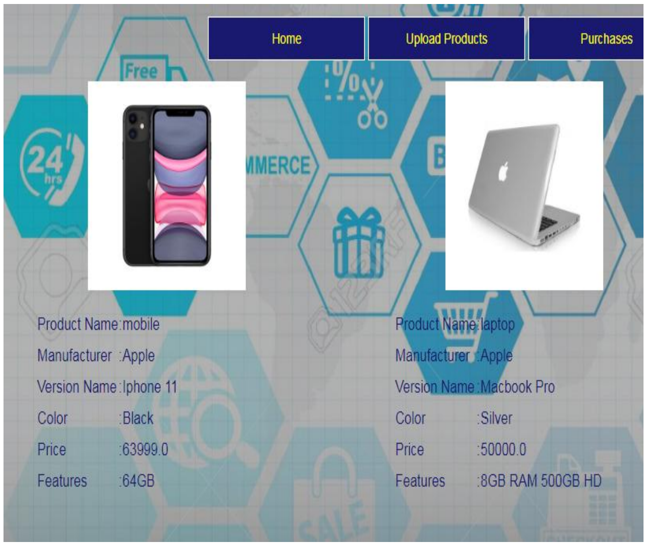
Macbook Pro

Silver

50000

8GB RAM 500GB HD

Choose File 2.jpg

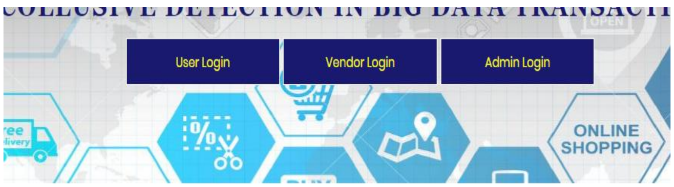


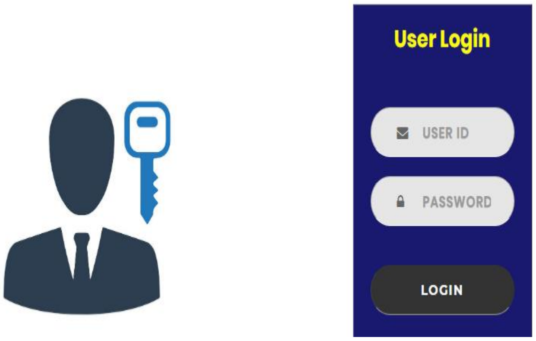
Product Name :mobile
Manufacturer :Apple
Version Name :Iphone 11
Color :Black
Price :63999.0
Features :64GB

Product Name :laptop
Manufacturer :Apple
Version Name :Macbook Pro
Color :Silver
Price :50000.0
Features :8GB RAM 500GB HD

User login page:

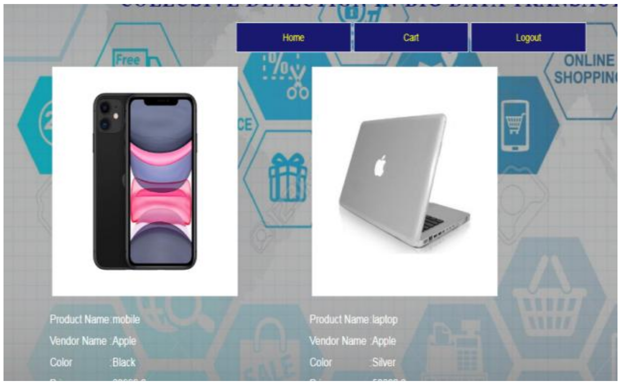
This page is the user login page. The users can log in to the website by giving their username and password and buy the products that they like. It also has a link to register the user on the website. the users can give their details and sign up on the website using this link.





User home page:

This page displays all the products uploaded by various vendors on the E-Commerce platform. The user can view the product's, their details such as name, version, color, price, and features by clicking the view button below the image of the product.

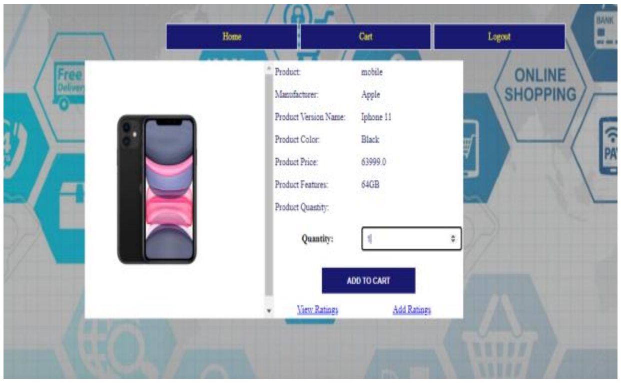


Product Name :mobile
Vendor Name :Apple
Color :Black

Product Name :laptop
Vendor Name :Apple
Color :Silver

Product details page:

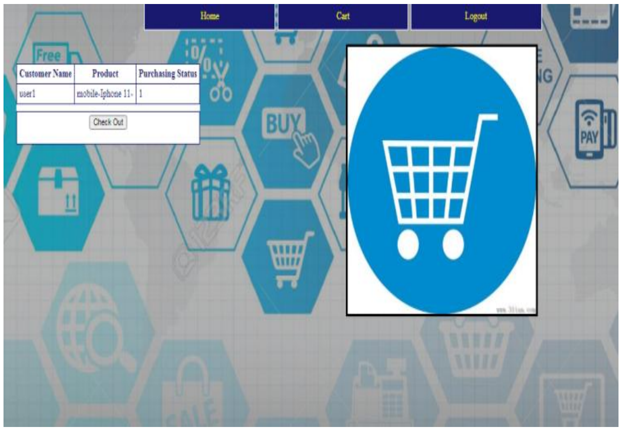
This page displays the details of the product and gives an option to enter the quantity of the product do user wishes to buy and add the product to the cart. It also has links to add the ratings and view the ratings of the product.



Product: mobile
Manufacturer: Apple
Product Version Name: Iphone 11
Product Color: Black
Product Price: 63999.0
Product Features: 64GB
Product Quantity:
Quantity: 1

User Cart Page:

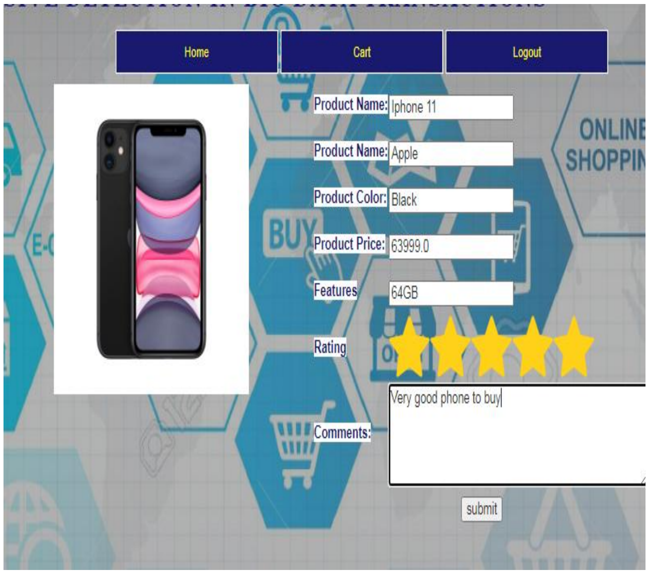
This page displays the products the user has added to his cart and gives an option to check out and buy the products



Customer Name	Product	Purchasing Status
user1	mobile-Iphone 11-	1

Add Rating page:

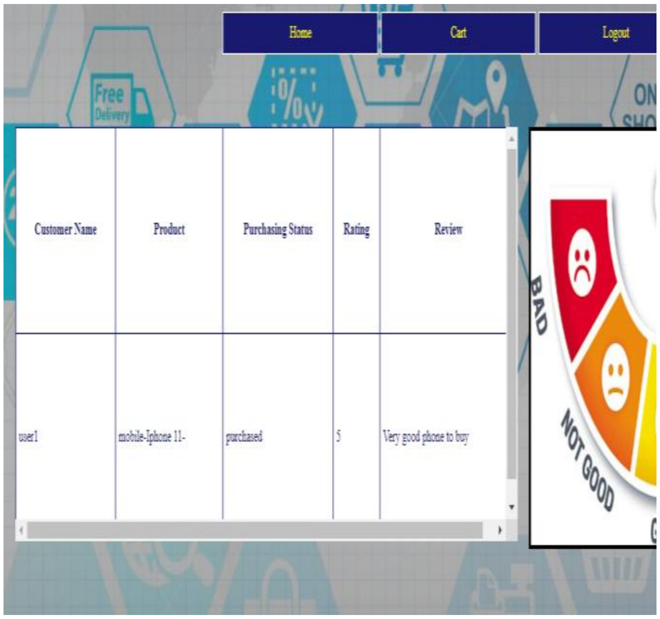
This page allows the user to give his rating and purchase experience in the form of comments. On the click of the submit button, the user feedback for the product is captured.



Product Name: Iphone 11
Product Name: Apple
Product Color: Black
Product Price: 63999.0
Features 64GB
Rating ★★★★★
Comments: Very good phone to buy

View rating page:

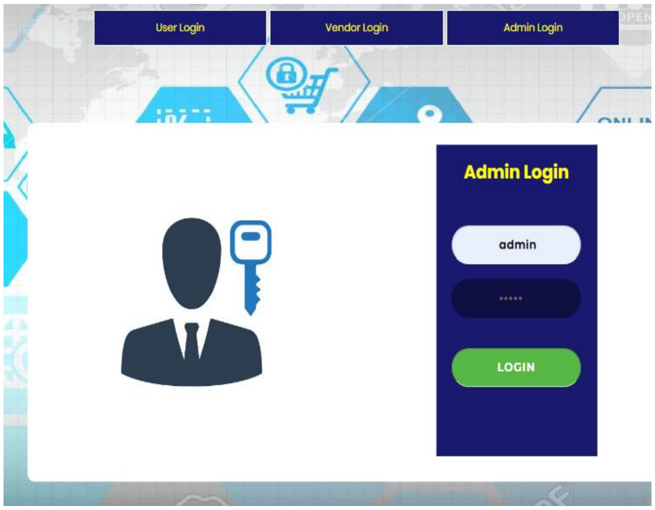
This page displays the ratings given by various users for the selected product so that the user can decide to purchase that product or not.



Customer Name	Product	Purchasing Status	Rating	Review
user1	mobile-Iphone 11-	purchased	5	Very good phone to buy

Admin Login Page:

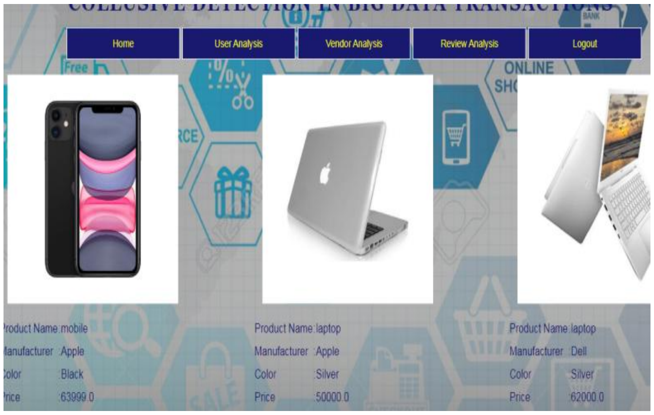
This page is the login page for the admin of the e-commerce website. He can give his credentials to login and view the activities that are happening on the website.



Admin Login
admin
*****

Admin Home Page:

This page is displayed after the admin successfully logs into the application. Here he can view the various products that are uploaded by the vendors. He also has an option to perform a fraud detection analysis of the users, the vendors, and the product reviews given by the users.



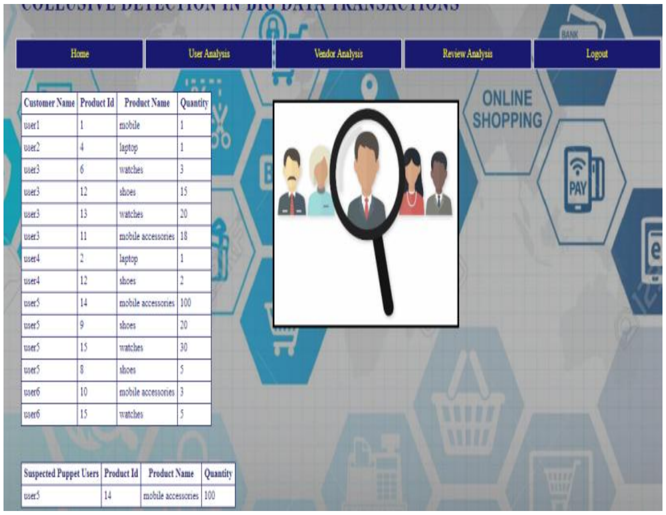
roduct Name :mobile
lanufacturer :Apple
olor :Black
rice :63999.0

Product Name :laptop
Manufacturer :Apple
Color :Silver
Price :50000.0

Product Name :laptop
Manufacturer :Dell
Color :Silver
Price :62000.0

User Analysis:

This page displays the list of users, the products they have purchased, and their quantities. It also displays suspicious fraudulent users in a table below.

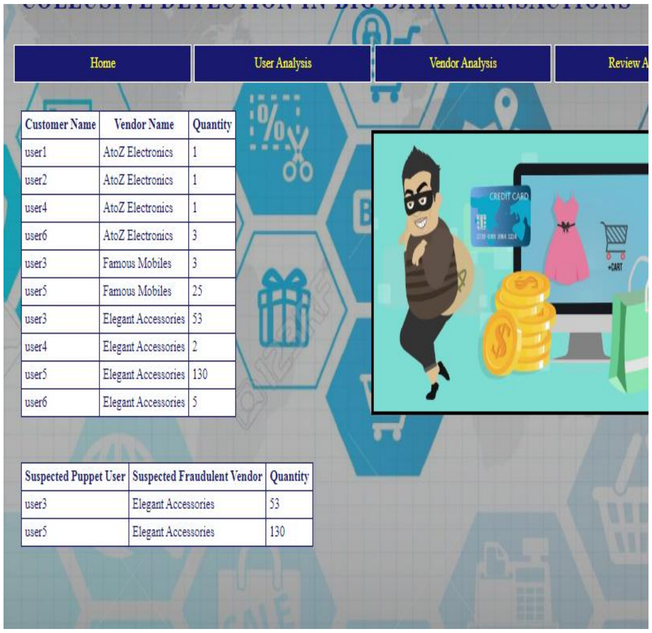


Customer Name	Product Id	Product Name	Quantity
user1	1	mobile	1
user2	4	laptop	1
user3	6	watches	3
user3	12	shoes	15
user3	13	watches	20
user3	11	mobile accessories	18
user4	2	laptop	1
user4	12	shoes	2
user5	14	mobile accessories	100
user5	9	shoes	20
user5	15	watches	30
user5	8	shoes	5
user6	10	mobile accessories	3
user6	15	watches	5

Suspected Puppet Users	Product Id	Product Name	Quantity
user5	14	mobile accessories	100

Vendor Analysis Page:

This page displays the details of users, the vendors from whom the products were purchased, and the number of products purchased. It also displays the details of suspected fraudulent vendors in a separate table below.

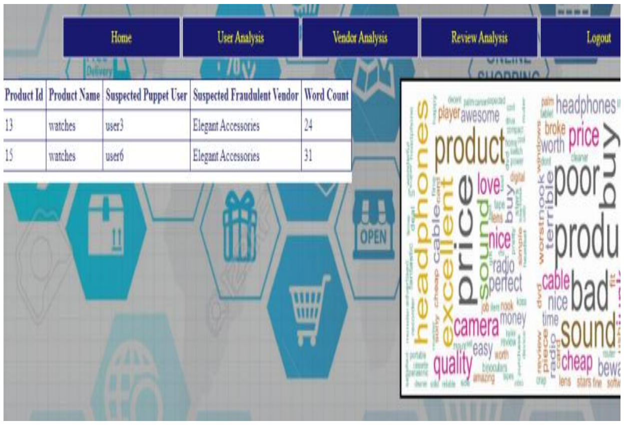


Customer Name	Vendor Name	Quantity
user1	AtoZ Electronics	1
user2	AtoZ Electronics	1
user4	AtoZ Electronics	1
user6	AtoZ Electronics	3
user3	Famous Mobiles	3
user5	Famous Mobiles	25
user3	Elegant Accessories	53
user4	Elegant Accessories	2
user5	Elegant Accessories	130
user6	Elegant Accessories	5

Suspected Puppet User	Suspected Fraudulent Vendor	Quantity
user3	Elegant Accessories	53
user5	Elegant Accessories	130

Review Analysis Page:

This page displays the details of suspected fraudulent vendors and suspected puppet users based on the analysis of the user feedback received for the products that are put up for purchase on the e-commerce platform.



Product Id	Product Name	Suspected Puppet User	Suspected Fraudulent Vendor	Word Count
13	watches	user3	Elegant Accessories	24
15	watches	user6	Elegant Accessories	31

VI CONCLUSION

Below are the contributions and conclusions from our study on fraudulent transactions in E-Commerce platforms:

1. Two new features of fraudulent transactions have been identified. They are product type and product nature. They are combined with other attributes and characters to identify fraudulent transactions. We propose a generalized way of identifying the indicators for fraud detection.
2. A Real-world dataset is used to validate the performance of the fraud detection model and identify suspicious fraudulent vendors and puppet users from genuine ones.
3. Some suggestions for safeguarding the online reputation system are given to the E-Commerce platforms so that they can be included in their policies.

The procedures used to obtain these indicators and text classification can be generalized and reused for the detection of fraudulent activities in other domains.

We have observed remarkable differences in the behaviors of genuine vendors and fraudsters. In fraudulent transactions, we observed that many newly registered customers actively take part in buying fake products end support fake transactions by buying virtual and cheap products from selected vendors and write very good comments and detailed feedback in their reviews and give a high rating level. This increases the reputation of the fraudulent vendor and he attracts more genuine buyers.

In the future, we aim to continue our research to make this model a more generalized and universal one so that it could be used in other domains for fraud detection.

REFERENCES

[1] Albashrawi, M. (2016). Detecting financial fraud using data mining techniques: a decade review from 2004 to 2015.

[2] Almendra, V. (2013). Finding the needle: A risk-based ranking of product listings at online auction sites for non-delivery fraud prediction. Expert Systems with Applications, 40(12), 4805–4811.

[3] Almendra, V., & Schwabe, D. (2009). Fraud Detection by Human Agents: A Pilot Study. E-Commerce and Web Technologies. Springer Berlin Heidelberg. 10th International Conference, Linz, Austria, September 1–4, Springer, New York, NY, 2009, 300–311.

[4] APAMukherjee, A., Liu, B., & Glance, N. (2012). Spotting fake reviewer groups in consumer reviews. International Conference on World Wide Web (pp.191-200). ACM.

[5] B. Bollob´as,(1984). in Graph Theory and Combinatorics: Proc. Cambridge Combinatorial Conf. in honour of Paul Erd˝os. B. Bollob´as, ed. Academic Press, NY,pp. 35-37.

[6] Ba, S., and Pavlou, P. (2002). Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior. Mis Quarterly, 26(3), 243-268.

[7] Becker, G. S. (1968). Crime and punishment: an economic approach. Journal of Political Economy, 76(Volume 76, Number 2), 169-217.

[8] Berlusconi, G. (2017). Social Network Analysis and Crime Prevention. Crime Prevention in the 21st Century. Springer International Publishing.

[9] Blume, M., Weinhardt, C., and Seese, D. Using network analysis for fraud detection in electronic markets. In T. Dreier, R. Studer, and C. Weinhardt (eds.). Information Management and Market Engineering, Volume 4 of Studies on eOrganisation and Market Engineering, vol. 4, University Atsverlag Karlsruhe, Germany, 2006, 101–112.

[10]Bolton, G. E., Katok, E., & Ockenfels, A. (2005). How effective are online reputation mechanisms? an experimental study. Management Science, 50(3).