JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

Analytical Study On Prevention And Detection Of Financial Cybercrime And Frauds Using Transaction Pattern Generation Tool

Dr. Narendra Sharma[1], Krishna Annaboina[2]

[1]*Associate Professor, Dept. of Computer Science*, Sri Satya Sai University of Technology and Medical Sciences Bhopal, India.

[2]*Research Scholar, Dept. of Computer Science*, Sri Satya Sai University of Technology and Medical Sciences, Bhopal, *India. anneboina.krishna@gmail.com*

ABSTRACT

E-commerce is a vital sales avenue for multinational businesses in today's technology environment. Due to the fast growth of e-commerce, credit card sales have increased. Unfortunately, criminals have profited from credit card theft. The discovery of safety faintness in standard credit card dispensation schemes has increased credit card theft, costing billions of dollars yearly. Modern credit card thieves are agile and use cutting-edge tactics. Global fraud complicates credit card issues for banks and other financial businesses. Many **techniques, such as First Virtual, Cyber Cash, and SET, are employed to avoid financial cybercrime. Although customers and businesses rarely use these systems, they are very secure. These models protect our online transactions, but they cannot prevent fraud if a customer's credit card information is physically lost or falls into the wrong hands. The study is distinctive in that it uses data mining, statistics on one stage for modeling portion. Effort detailed in thesis necessity be beneficial to academics; in particular, a literature review of data mining techniques is an effort to offer a roadmap for the researchers to explore and choose the best data mining approach before putting it into practice. Additionally, building additional financial applications benefits from an considerate of the role data mining plays in detecting economic misconduct.**

Although the programme was developed with online transactions in mind, cardholders can also use it for offline transactions.

Keywords: Financial cybercrime, frauds, data mining.

I. INTRODUCTION

India's Internet usage is growing rapidly. It has opened doors in every field, including business. Every coin is two-sided. The internet has flaws. Cybercrime is a major negative. Internet connectivity has left us subject to security dangers connected with large networks, among other negatives.

Today, consumer-focused retail, financial, communication, and marketing enterprises employ data mining. It helps them assess sales, customer happiness, and business profitability. Finally, they may "dig down" into summary data to see transaction data. Data mining lets retailers offer tailored promotions based on a customer's point-of-sale record. Major components of data mining include a data warehouse, database, and other information repository. Servers retrieve data depending on client requests. Knowledge base evaluates pattern interestingness, while pattern evaluation module focuses search on interesting patterns.

E-commerce is a vital sales avenue for multinational businesses in today's technology environment. Due to the fast growth of e-commerce, credit card sales have increased. Unfortunately, criminals have profited from credit card theft. The discovery of safety faintness in standard credit card dispensation schemes has increased credit card theft, costing billions of dollars yearly. Modern credit card thieves are agile and use cutting-edge tactics. Global fraud complicates credit card issues for banks and other financial businesses.

The IC3 website received 275,284 complaints between January 1 and December 31, 2008, according to the 2008 Internet Crime Report [41]. From 206,884 complaints in 2007, there is a 33.1% increase. Online frauds and ethical issues dominated these publications' charges. 2008 recorded the biggest financial loss for referred complaints ($264.59 million)

According to a Gartner survey [40] of 160 firms, online transactions have 12 times more fraud and e-tailors spend 66 percent more for credit card discount rates than conventional merchants. In fraud incidents, Web retailers are liable, whereas credit card companies protect conventional businesses.

1.2 OBJECTIVE OF RESEARCH:

- To talk about many types of financial cybercrimes and scams that happen nowadays, such as phishing and credit card fraud.
- Two, learn about many data mining means,and
- Term "fraud prevention" refers to strategies aimed at preventing fraud from happening. The goal of fraud detection, on the other hand, is to promptly uncover fraudulent activity after it is safeguarded. After efforts to prevent fraud have been unsuccessful, the next step is fraud detection. Since it is common to be oblivious to the fact that fraud protection has failed, ongoing usage of fraud detection is essential in practice.

1.3 RELATED WORK IN FRAUD DECTECTION:

The difficulty of detecting credit card fraud is rising in tandem with the card's rising popularity. When it comes to improving accuracy—specifically in classification—traditional data mining techniques are woefully inefficient. Credit card fraud detection relies heavily on accurate categorization. There is a proposal to use a genetic algorithm for forced it card fraud detection in order to increase its accuracy. Because it is a smart algorithm that optimizes the issue to aid with prediction and increase accuracy. Credit card fraud detection systems that came before used rules as their foundation. Banks establish these standards to identify fraudulent transactions, however these procedures compromise accuracy for many transactions.

There has been a lot of talk in the academic community about data mining as a potential solution to the problem of credit card fraud detection. To combat this, Gosh and Reilly developed a method that uses neural networks to identify fraudulent activity [1]. They used a large dataset of tagged credit card transactions to train their algorithm. Among the many forms of fraud that fall under this category include applications, counterfeit items, mail-order purchases, lost or stolen cards, non-receipt issue (NRI) fraud.

Dorronsoro et al. [3] identifies a large frequency of credit card dealings and a short decision-making window as two distinguishing features. They distinguished between real and fake actions by using Fisher's discriminating analysis.

M.Syeda et al. [4] used similar granular neural networks to haste up data mining, information detection for detecting credit card scheme. There is a comprehensive mechanism in place for this.

By using distributed data mining to break down large amounts of transactions into smaller ones, P.K. Chan et al. [5] were able to construct models of user behavior. Combining the resultant basic models creates a meta-classifier, which in turn increases the detection's accuracy.

When discussing cross-bank data exchange, Chiu and Tsai [7] consider web services. We have developed a fraud pattern mining (FPM) method to prevent assaults by mining fraud suggestion instructions, which provide material about new fraud designs.

There are a few published survey studies that classify, compare, and synthesize literature about fraud detection. In a thorough study, Phua et al. [8] surveyed fraud detection systems that rely on data mining.Kouetal. [9] compiled a list of methods for detecting credit card fraud, phone fraud, and computer intrusions. According to

V.Hanagandi et al. [11] developed a deception notch by analyzing past transactions on credit card accounts. Using density-based clustering and radial basis function networks (RBFN), they provide a method for distinguishing fraudulent from legitimate transactions. After transforming input data into cardinal constituent interplanetary, clustering, RBFN modeling make use of a small number of components.

In their analysis of credit card fraud detection problems, Ashen et al. [12] determine how successful categorization methods are. They tested the efficacy of logistic regression, neural networks, and decision trees as fraud detectors.

H. Shao et al. [13] introduced a system for identifying fraudulent activity in customs declaration data by using data mining techniques, like extensible multi-dimension criteria statistics perfect, cross fraud-detection method.

For the purpose of securing online banking, K.B. Bignell [14] outlines the design of multi-layer artificial neural networks with feed-forward.

In their demonstration of its application to the detection of fraud, Srivastava et al. [15] use a Hidden Markov mimic (HMM) to mimic the stages involved in processing credit card transactions. When first trained, an HMM takes into account the usual actions of a card holder. For a trained HMM to reject an incoming credit card payment as fraudulent, the rejection probability must be sufficiently low. Simultaneously, they also strive to avoid the denial of legitimate transactions.

In order to identify cases of electrical energy theft, J.E. Carpal et al. [17] suggests a system that uses rough groups, KDD. Our technique detects patterns of fraudulent behavior by evaluating the area between fraudulent and genuine customers in great detail using previous data sets from electricity providers. Using these patterns, they create classification criteria that electricity providers may employ to identify fraudulent clients.

II. DATA MINING METHODS

A DEFINITION OF DATAMINING:

Data mining is practice of automatically analyzing and extracting information from database data using one or more machine learning algorithms. Data mining sessions aim to find patterns and trends in data. The act of " non trivial extraction of implicit, before unidentified, possibly beneficial material from data" is known as data mining. Additionally, "the science of collecting valuable information from huge datasets or databases." To begin, let's agree data mining is a clearly clear process that, given data, generates models or patterns. Data mining approaches include searching through large datasets for meaningful patterns and trends in order to extract actionable insights. Data mining initiatives have made use of a wide variety of methods, association, classification, clustering, decision trees, prediction, neural networks, among many others. The principles and procedures of each methodology define the kind of problems they tackle. Following this, we will income a quick look at those data removal methods.

2.1 SUGGESTION:

Well-known data mining approach known as suggestion finds patterns by analyzing the connection between variables in the same transaction. This method also goes by the name "relation approach" since it finds the most common occurrences of various objects in the data set by studying their relationships. One of the many common uses of association rules is the discovery of sales correlations in medical datasets or transactional data [3].Retailers often use association because it provides valuable insights on customer purchasing habits.

By analyzing past sales data, stores may discover patterns like people constantly purchasing crisps with beers. By strategically placing beers and crisps side by side, businesses can save customers time and boost sales [4]. Market basket analysis is a common name for association rule due to its roots in retail. [1].

2.2 CLASSIFICATION:

For precise analysis and prediction of massive data sets, classification techniques sort datasets into predefined categories. Customers, objects, and other data sets may be better understood by classification, which involves specifying several qualities to establish a certain class. If you want to classify buildings according to their occupancy or construction type, for instance, you may do so simply by looking for certain criteria like structure, height, or unit. You may apply a new construction to a certain class by comparing the database's declared properties. Using these guidelines, you may categorize your consumers according to their age, gender, and socioeconomic status. In addition to determining a classification, classification may contribute into the output of other approaches like clustering, which uses shared qualities across classes to find groups, or decision trees, which decide a classification.

2.3 CLUSTERING:

Data mining often makes use of clustering as one of its primary methods. The purpose of the clustering procedure is to comprehend the similarities and differences in the dataset by analyzing one or more qualities to find data that is similar to each other. Because it divides the data into several categories to find a cluster of related outcomes, clustering is also known as segmentation. If we want to make it easier for readers to find books on a certain subject without having to search the whole library, we can use the clustering strategy for book management in libraries. This involves grouping books that have certain commonalities onto one shelf and giving it a relevant name.

2.4 DECISION TREE:

Part selection criteria might be based on decision tree approaches. Moreover, to facilitate the selection and use of certain data within the broader framework.

The decision tree begins with an easy question with two (or more) possible solutions. With each response comes a new set of questions designed to bolster the data's categorization or identification, allowing for either prediction or classification. Classification systems often utilize decision trees to connect type information, and predictive systems use them to accelerate the structure of the tree and the output depending on different predictions based on past data. [5].

2.5 PREDICTION:

The process of making a forecast by studying previous occurrences or examples. For example, when using the credit card authorization, you may determine whether a purchase is fraudulent by combining decision tree analysis of previous transactions with categorization pattern matches. It is very likely that the transaction is legitimate based on the Match between the bought flights to the UK and transactions in the UK. [5].

2.6 NEURAL NETWORKS:

These days, many individuals rely on Neural Networks. Method often used when data mining technology was in its infancy. The AI community came together to build the artificial neural network. Users are not need to possess extensive expertise in the field or the database in order to operate neural networks, since they are highly automated (as stated in [4]). To get the most out of the neural network, you must be familiar with the following..

- Connections between the nodes.
- Get the most out of your computing power.
- Cutoff point for training completion. There are two primary components of a neural network: the node and the connection.
- Node—matching the node to a neuron in the human brain is completely free.
- The structure of the network is defined by this arrangement of neurons and the connections between them. One powerful method of predictive modeling is neural networks. Even for specialists, it's a challenging concept to grasp. It generates very complicated things that are difficult to grasp in their entirety. The neural network has many different types of uses. Using this, the company was able to uncover instances of fraud [4].

To improve the compression ratio, data compression techniques have made use of a variety of tools, including discrete cosine transforms, discrete wavelet transforms, neural networks, and deep learning algorithms [5, 6]. When it comes to data compression, unsupervised learning models, including self-organization feature maps, are the most popular neural networks. SOFM (6.3) the author laid up the foundation for SOFM, vector quantization, and entropy coding.

III. DATAWARE HOUSE IMPLEMENTATION

Once transaction data has served its operational purpose, it is removed from the database. If a company doesn't have a decision support facility, they collect data and then throw it away. A data warehouse, a kind of interactive media, receives the data, nevertheless, in the presence of a decision support environment. Think of the data warehouse as a repository for all relevant business records assembled to aid in decision-making. For a more comprehensive analysis, see W.H. Inmon's work from 1996.This definition states that a data warehouse is a collection of nonvolatile, subject-oriented, integrated, time-variant data that helps with management's decision-making.

3.1 DATA WAREHOUSE ARCHITECTURE

Providing business users with read-only access to summarized data from the past is a big challenge for data warehouse design.

The relational model lends itself well to the following data warehouse architectures:

- Star schema
- Snow flake schema
- Constellation schema

Star schema architecture:

Among data warehouse designs, star schema is the most basic. The two main parts of a star schema are fact table, dimension tables. These tables let you to browse through certain categories, summarize, dig down, and set criteria.

Today, data warehouse implementations still mostly employ the star schema, despite it being the most basic data warehouse design. This is because it accounts for 90–95 percent of all instances.

Snow flake schema architecture:

As a modification to the star schema concept, the snowflake schema normalizes some of the dimension tables and further separates the data into other tables. The schema graph that comes out of it looks like a snowflake.

Unlike star schema models, snowflake models provide for the possibility of maintaining dimension tables in normalized form to reduce repetition. With the dimensional structure incorporated as columns, a large dimension table may easily become massive. This reduction in area is negligible, however, when contrasted with the regular

JSRT JOURNAL

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

size of the fact table.

3.2 IMPLEMENTATION ENVIRONMENT

The FCDS implementation was carried out in Oracle 9i. As explained in Chapter 6, data warehouse is created, applied in Oracle 9i and comprises of a number of tables. Same chapter also contains images of each table. Lookup tables are made to keep track of a customer's recent spending patterns. Current online transactions are provided to the FCDS as input. For this transaction, a risk score is generated using a linear equation and the TRSGM's criteria.
To make the setup easier to use, stored procedures, functions, packages, and triggers were created. These were used to determine how each transaction differed from the typical profile of the consumer.

3.3 SAMPLE RESULTS

Genuine Transaction

Figure 1 Example output of Data Mining Submission for Genuine Transaction-I

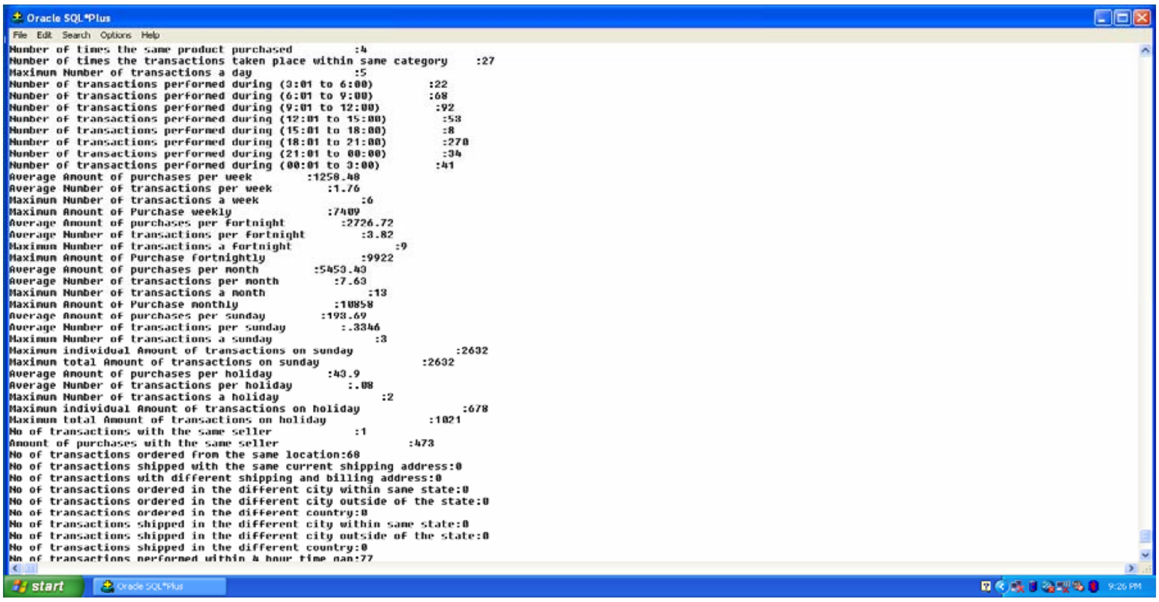

Figure 2 Illustration output of Data Mining Application for Genuine Transaction-II

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

Figure 3 Illustration output of Data Mining Submission for Genuine Transaction-III Fraudulent Transaction

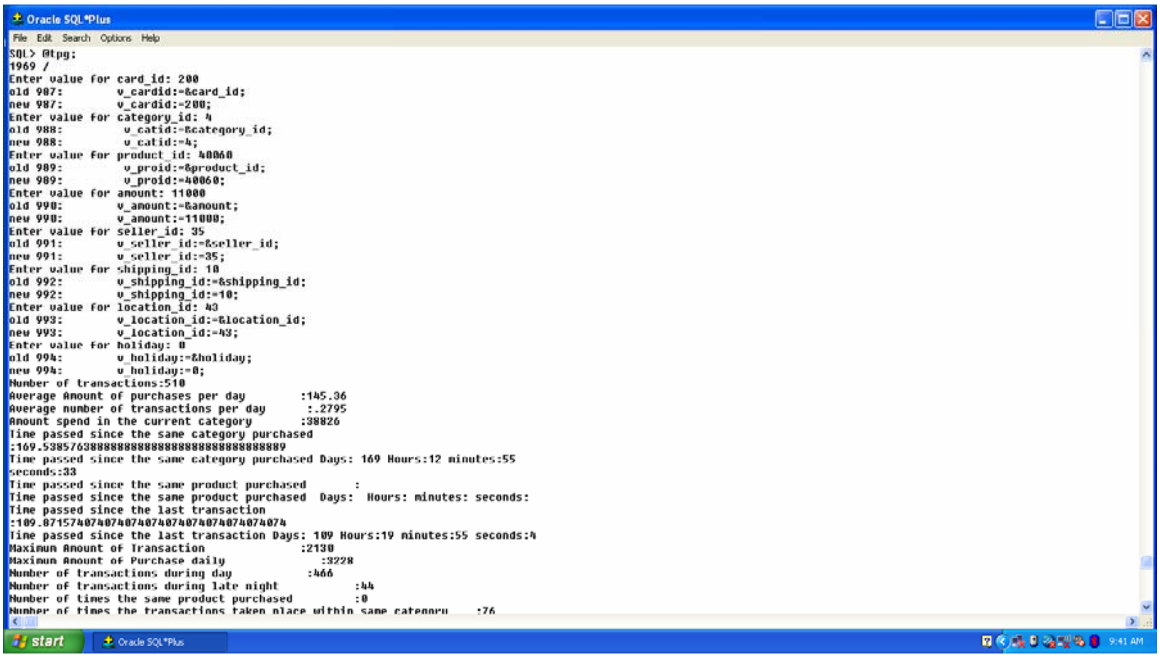

Figure 4 Illustration output of Data Mining Application for Fraudulent Transaction - 1.

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

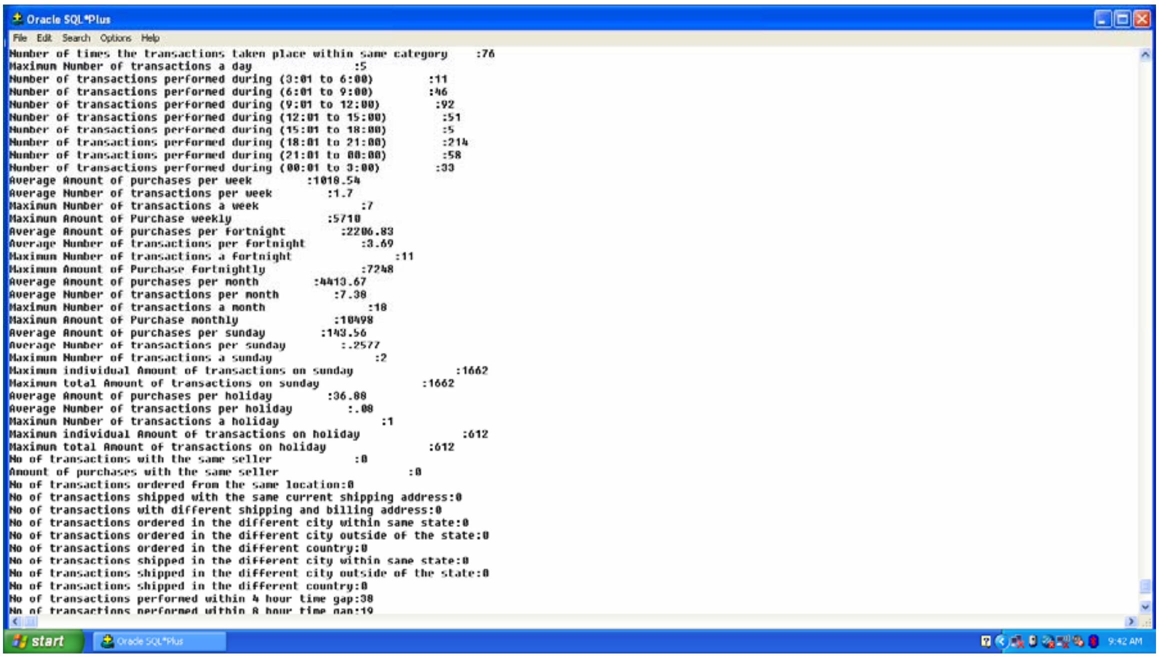

Figure 5 Mockup production of Data Mining Application for Fraudulent Transaction -II

Figure 6 Illustration output of Data Mining Application for Fraudulent Transaction -III

Doubtful business

Now a example of doubtful deal is shown along by chance of transaction being honest or fraudulent. Photo of table suspect is also revealed where filed suspect_count is incremented

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

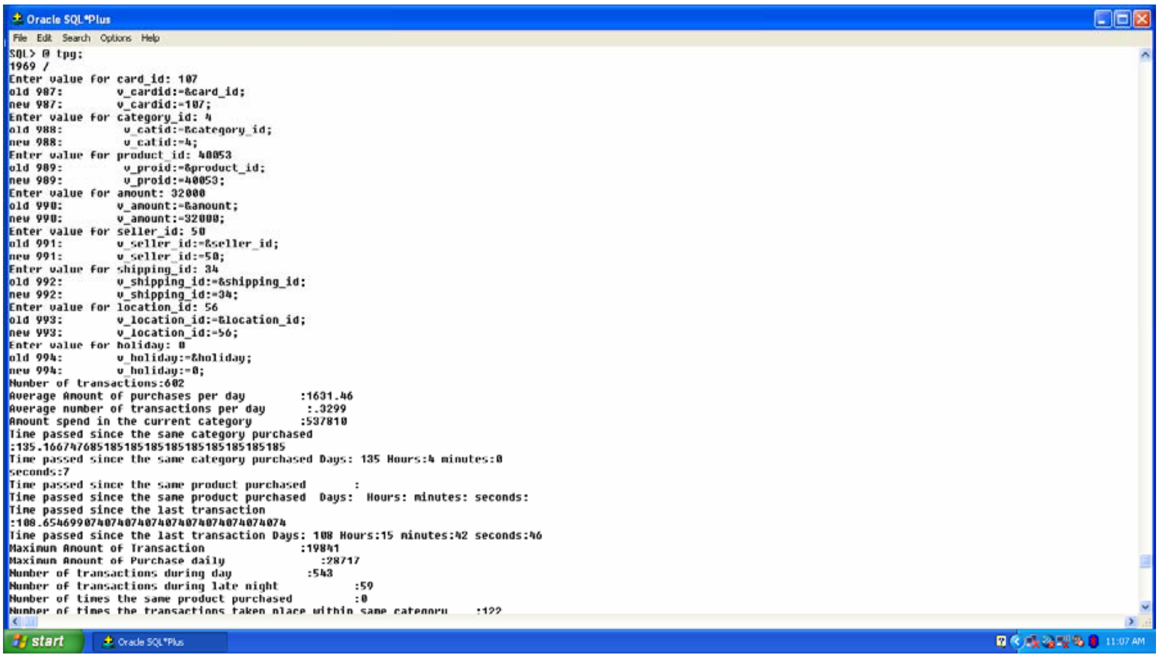

Figure 7 Example output of Data Mining Application for Doubtful Transaction-I

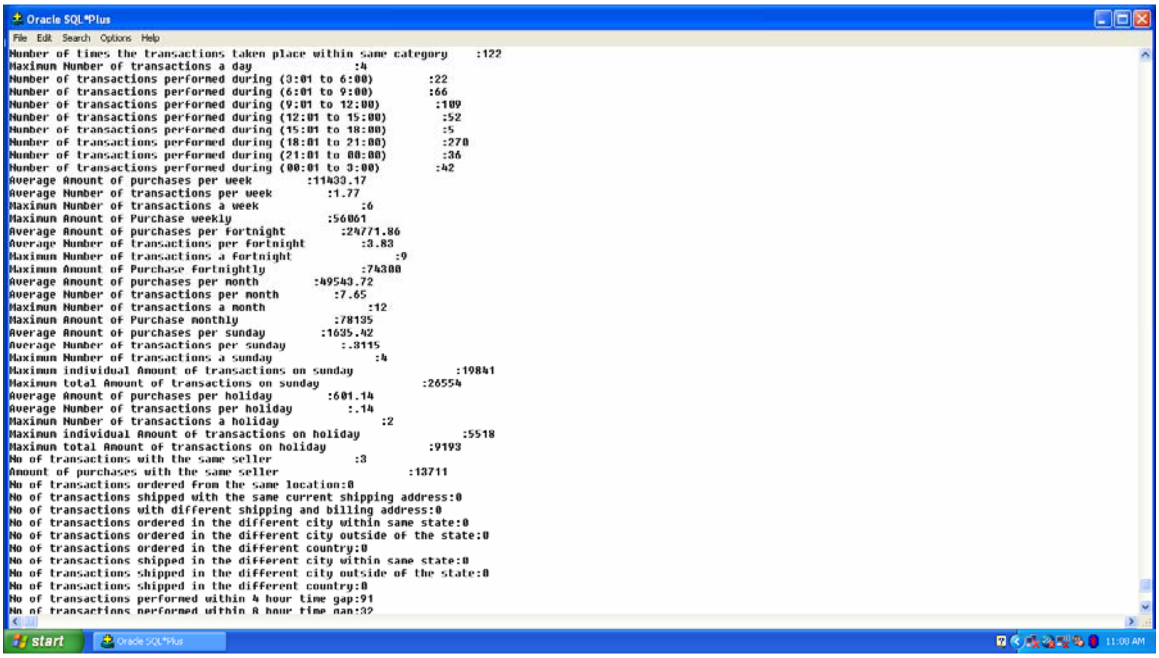

Figure 8 Illustration output of Data Mining Submission for Doubtful Transaction–II

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

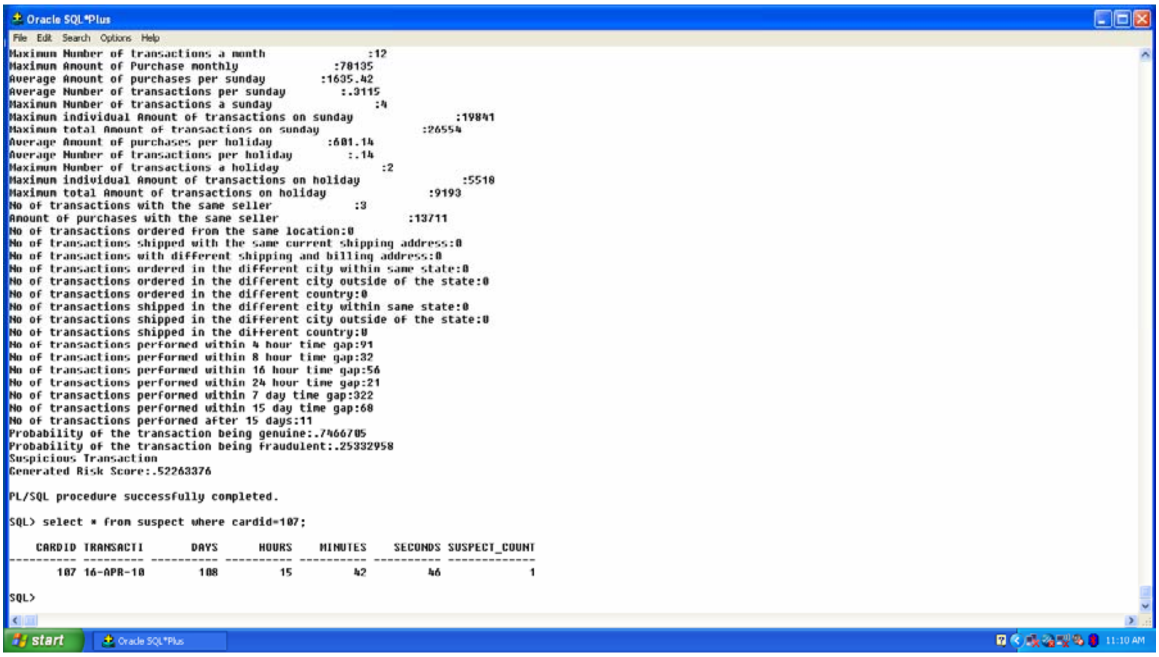

Figure 9 Illustration out put of Data Mining Application for Doubtful Transaction-III Multiple product instruction provision

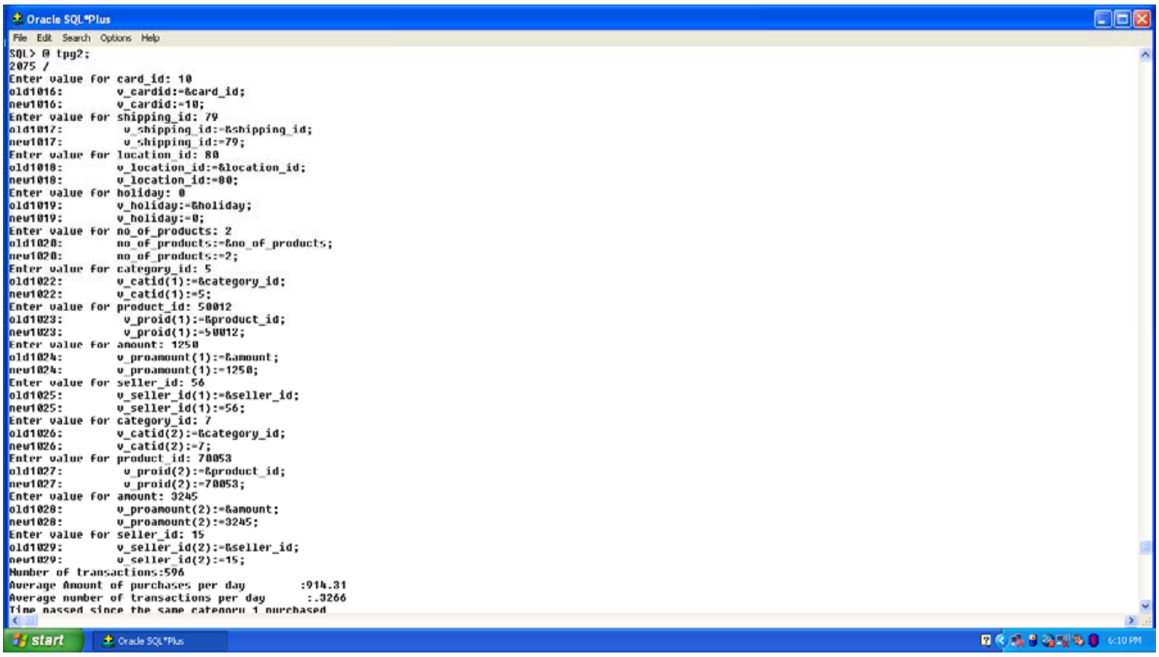

Figure 10 Example output of Data Mining Application for Multiple Order Creation Support - I

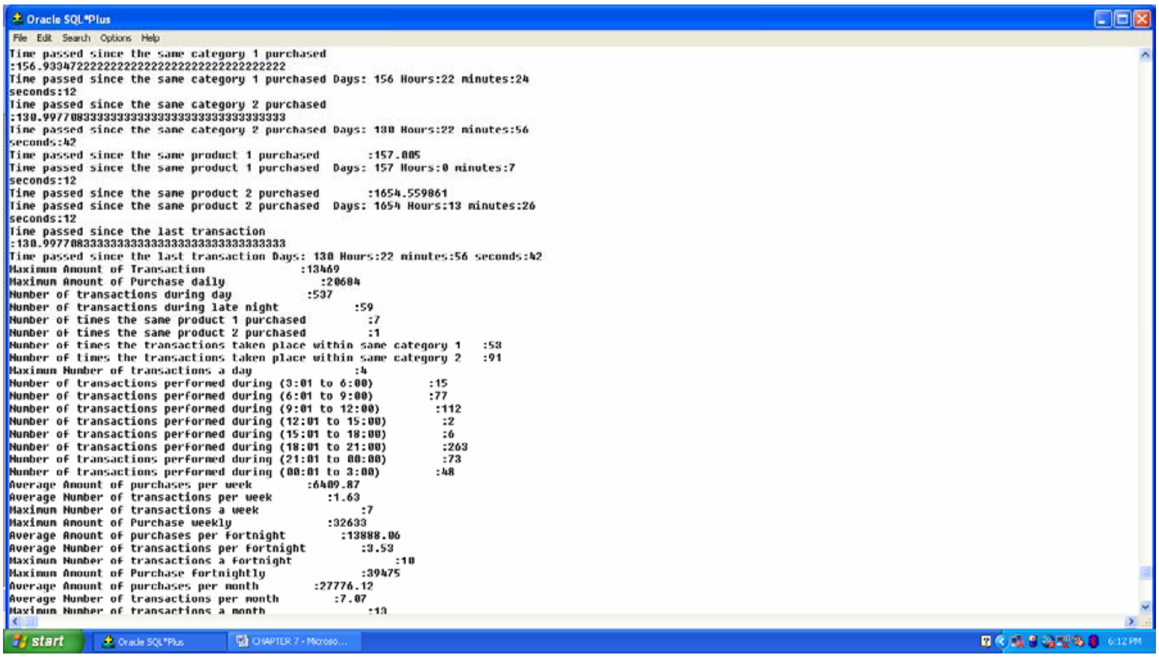

Figure 11 Example output of Data Mining Application for Multiple OrderProductSupport - II

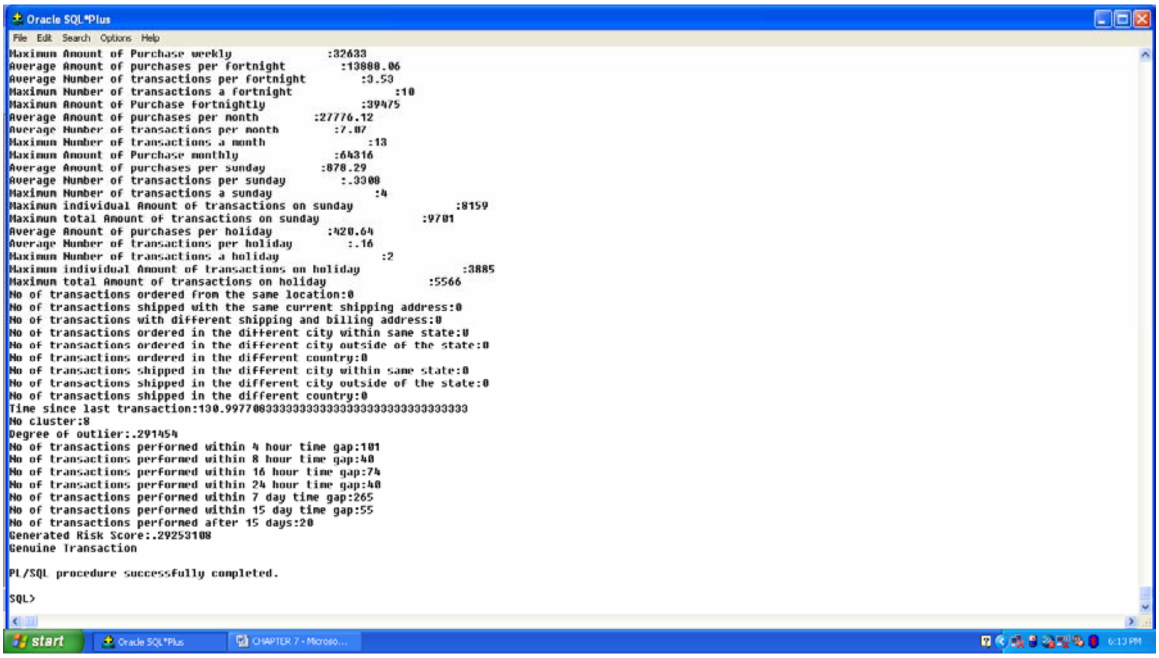

Figure 12 Example output of Data Mining Application for Several Order Product Support - III

3.4 RESULT ANALYSIS & DISCUSSIONS

The TRSGM's ability to produce a very dynamic risk score is by far its most intriguing finding. For example, if a consumer makes a purchase and the transaction value changes slightly while all other inputs remain constant, the risk score that is created will likewise be altered. The risk score would also take into account this small modification. We have repeatedly used the application for various transaction amounts with a small fluctuation while keeping all other inputs constant. Additionally, we reset all the lookup tables

JSRT JOURNAL

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

prior to taking the result a second time and moving forward. Here is an example.

For input Card Id 125
Category Id: 6ProductId 60050
Seller Id 750
Shipping Id: 410LocationId:980

Table 1 Example output of application for dissimilar transaction quantities

Amount	5000	50001	5002	5003
RiskScore	0.29277495	0.29277506	0.29277513	0.29287596

Figure 13 Sample output of Data Mining Application for dissimilar deal amounts–I

JSRT JOURNAL

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

Figure 14 Example output of Data Mining Request for dissimilar transaction amounts - II

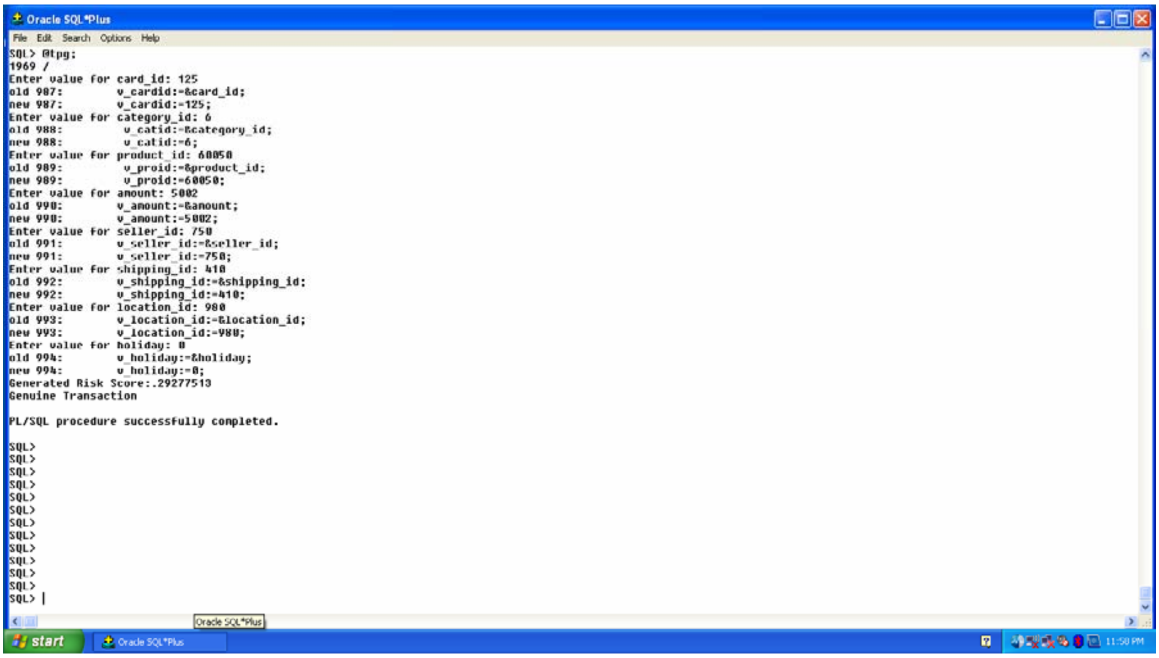

Figure 15 Example output of Data Mining Application for dissimilar transaction amounts - III

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

Figure 16 Example output of Data Mining Submission for different deal amounts - IV

For input Card Id :210
Category Id: 5ProductId:50010Amount : 4500Shipping Id : 590LocationId:110

Table 2 Example output of application for dissimilar sellers

SellerId	801	587	986	30
RiskScore	0.28811595	0.28780605	0.28811623	0.28802632

Figure 17 Example output of Data Mining Application for dissimilar sellers-I

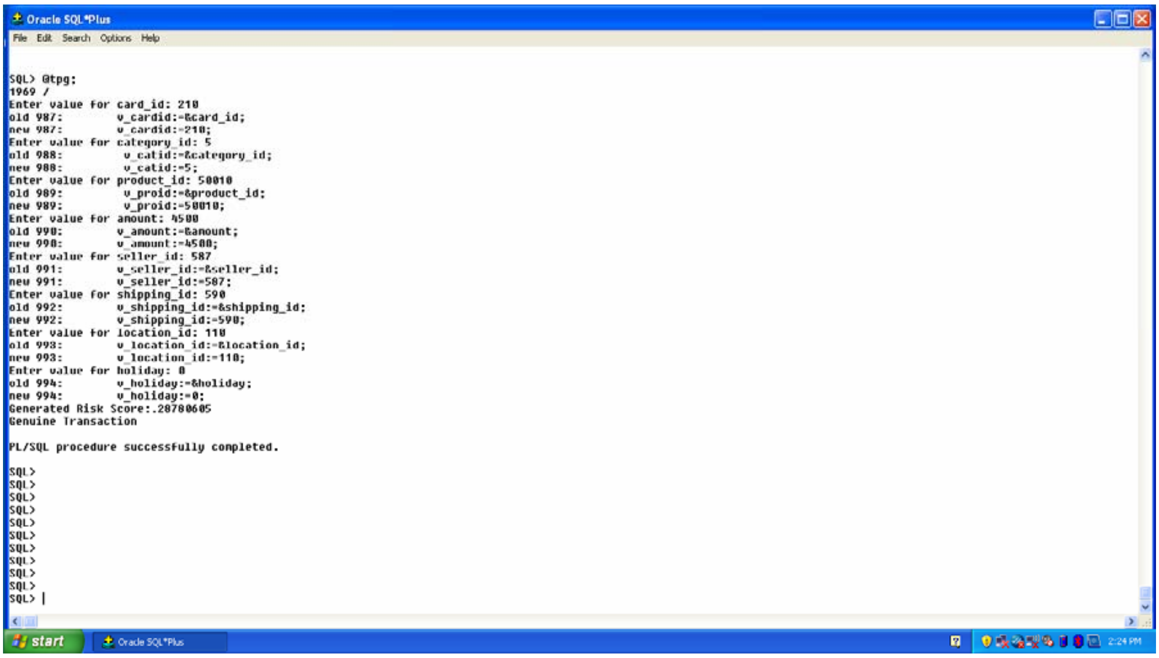

Figure 18 Illustration output of Data Mining Application for dissimilar sellers-II

JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

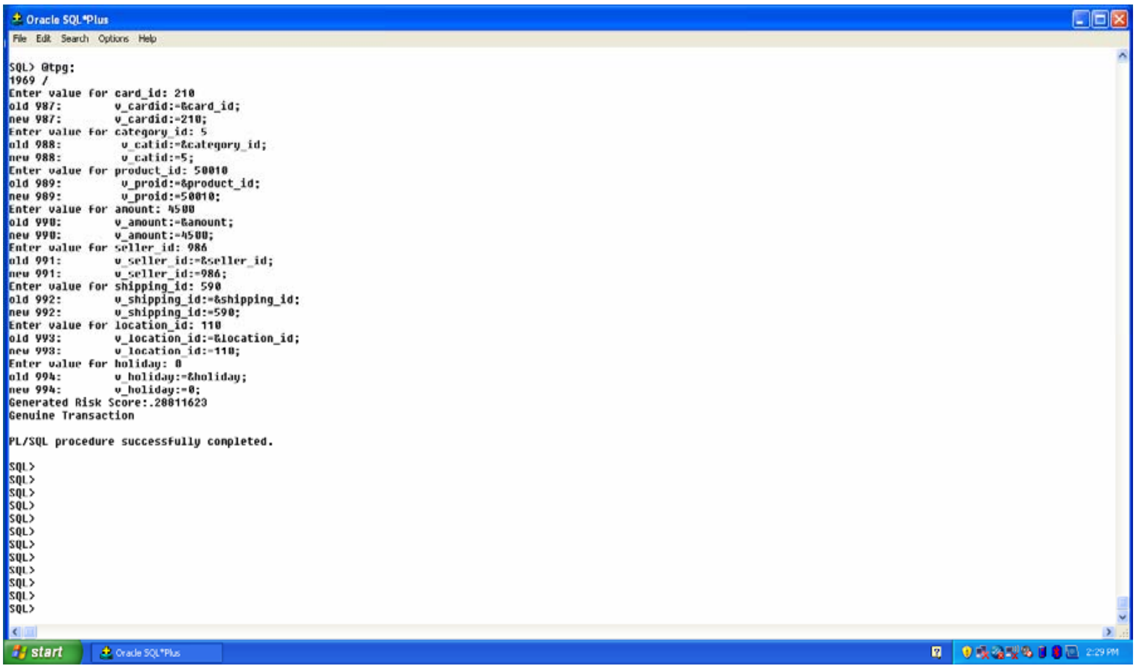

Figure 19 Example output of Data Mining Application for dissimilar sellers-III

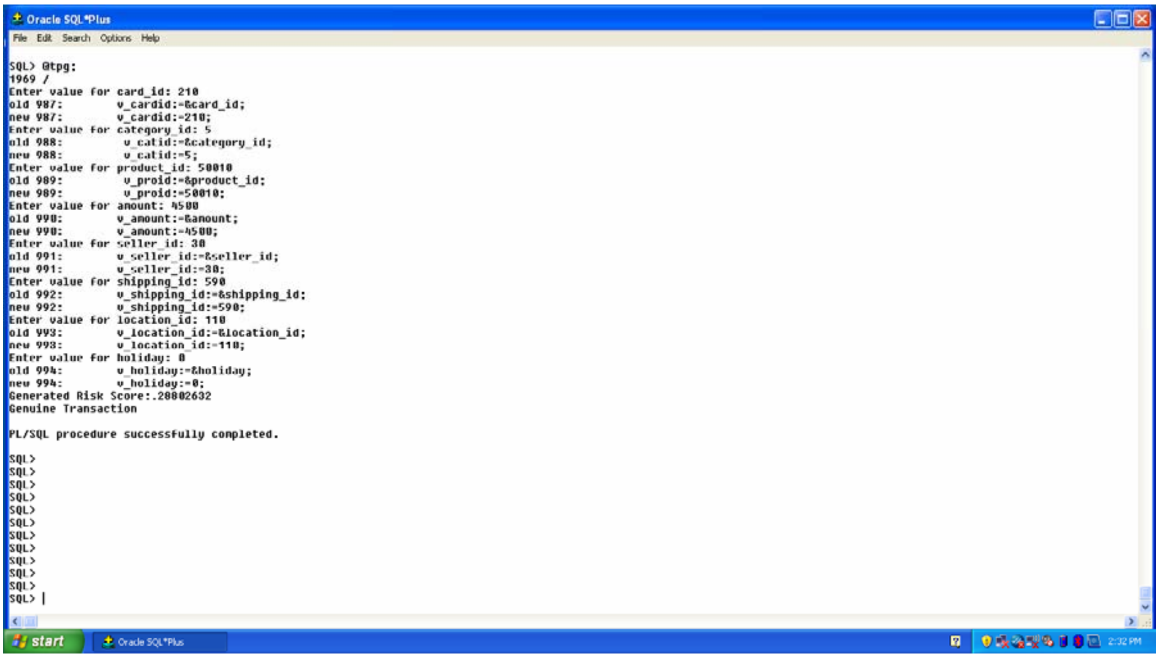

Figure 20 Example output of Data Mining Application for dissimilar sellers-IV

We have also checked if customer purchases the same product, category, amount, seller, shipping address on dissimilar location, then its alteration is reflected in risk score.

For input Card Id	1600
Category Id: 7ProductId	70150
Amount	5300
Shipping Id : 1596SellerId	110

JSRT JOURNAL

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

Table 3 Example output of application for dissimilar locations

LocationId	351	352	353	354
RiskScore	0.25453484	0.24608244	0.22881003	0.2497576

Figure 21 Example output of Data Mining Application for dissimilar locations-I

Figure 22 Example output of Data Mining Submission for dissimilar locations-II

JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

Figure 23 Example output of Data Mining Application for dissimilar locations-III

Figure 24 Example output of Data Mining Application for dissimilar locations–IV

- The program calculates cluster coverage of each new incoming transaction amount, if it is larger than 10%, the perfect shoulders, transaction is legitimate given the customer's history of regular payments. As a result, the application assigns the transaction a risk score of 0. Here's an illustration

JSRT JOURNAL
PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

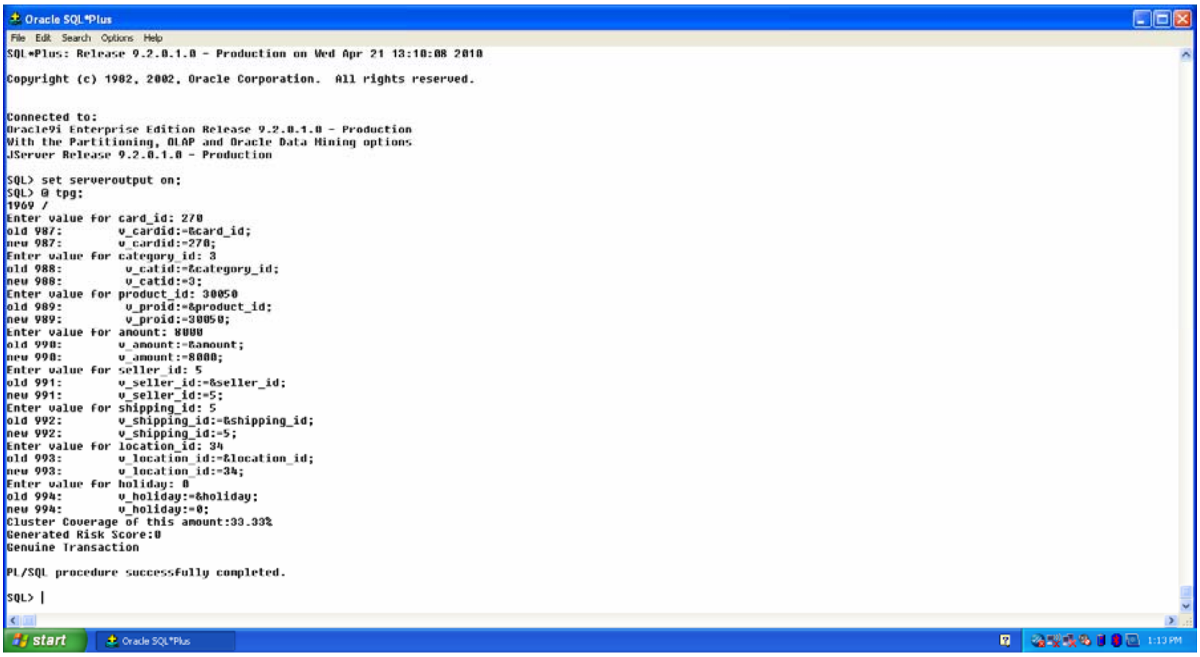

Figure 25 Example output of Data Mining Application for Cluster Attention

Author has thoroughly tested applications, verified that transactions that closely match customer buying patterns (such as the highest purchase in a given category, the most transactions in a given period of time, the most transactions ordered from the same location, etc.) generate the lowest scores. The transaction generates a higher risk score since it deviates more from the typical profile and the customer's purchasing patterns. Here's an illustration. As this particular group of transactions increased, the risk score declined.

Thecustomerhavingcardid1570hasthemaximumpurchasinghabitinthegivenfieldasbelow.

Category	2
Timeframe	:18:01to21:00
Location Id	205
Seller Id	257

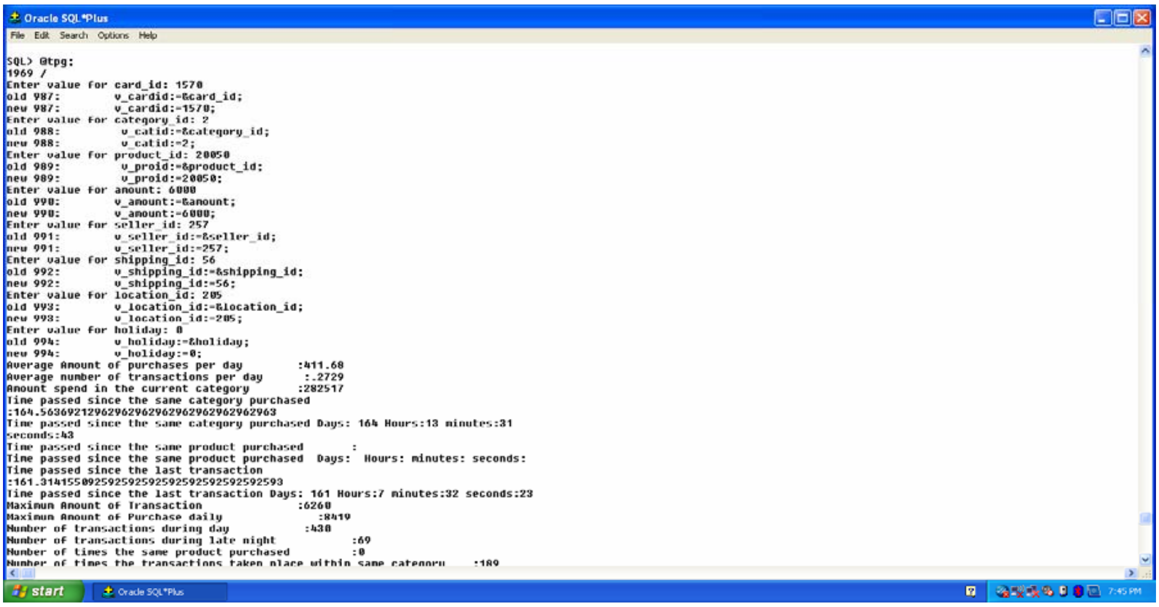

Figure 26 Example output of Data Mining Application for supreme buying practice input-I

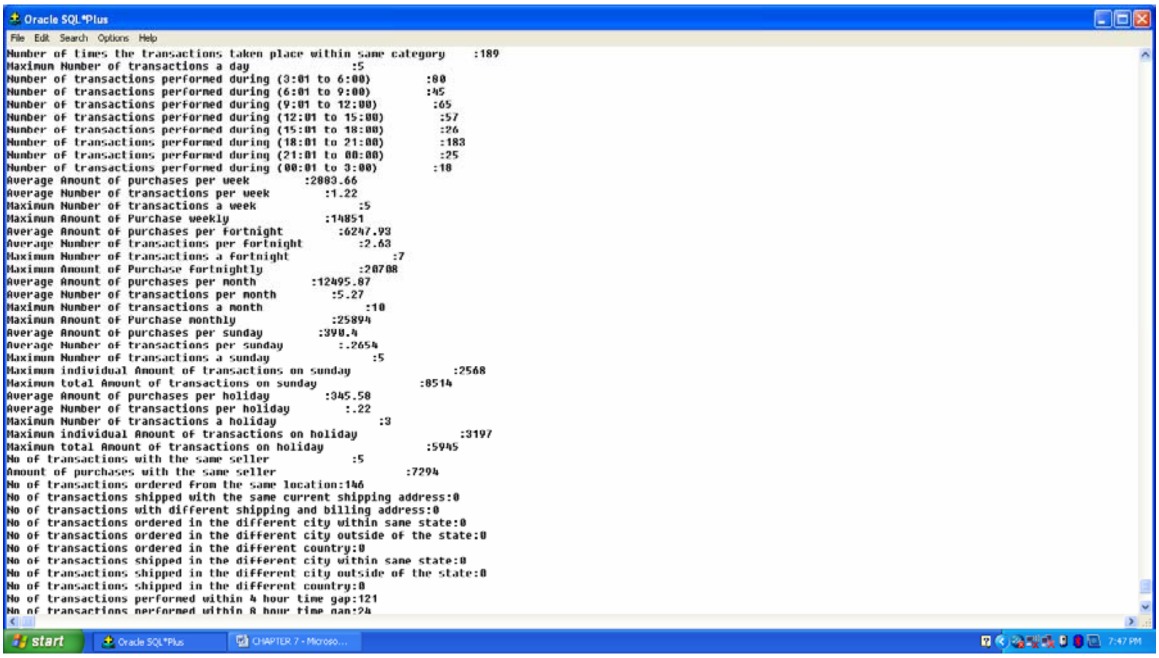

Figure 27 Model output of Data Mining Application for extreme buying practice input-II

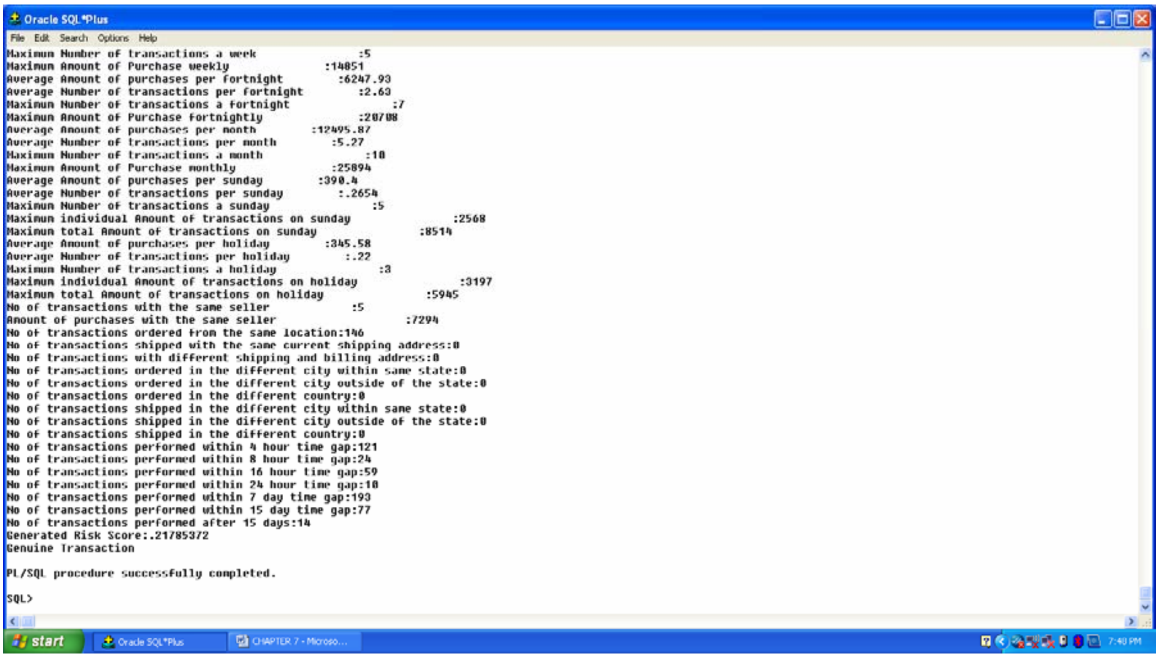

Figure 28 Model output of Data Mining Application for extreme purchasing practice input-III

Fraudulent transactions shouldn't go unnoticed in the same way. In light of these two considerations, the model is flexible. Although 0.8 is the top threshold value used here, it can be altered with further knowledge. The weighting of each characteristic is also determined in accordance with the advice of the credit card company.

Bayesian learning produced one intriguing finding. When a customer uses their card with ID number 8 for their first transaction, it seems suspicious. After a brief interval, he executes a second transaction that is worth $13,500 and is flagged as fraudulent by Bayesian learning.

JSRT JOURNAL

PAGES: 9-31
2/24/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-2 FEBRUARY
Registered under MSME Government of India ISSN: 2583-8660

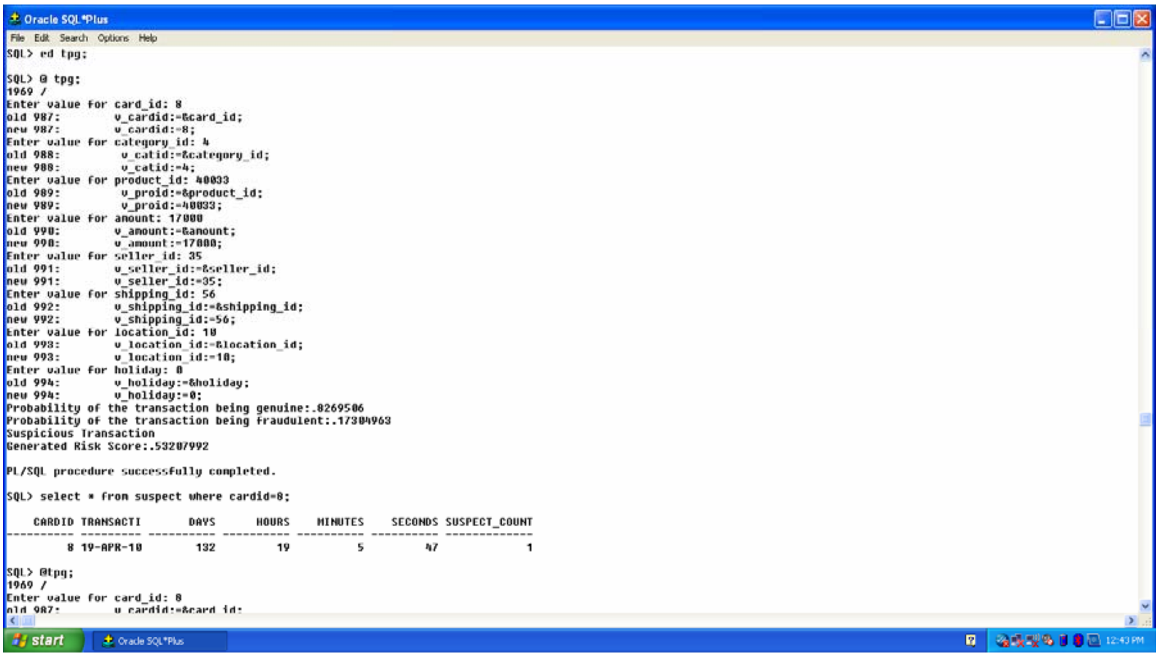

Figure 29 Example output of Data Mining Application for Bayesian Learning - I

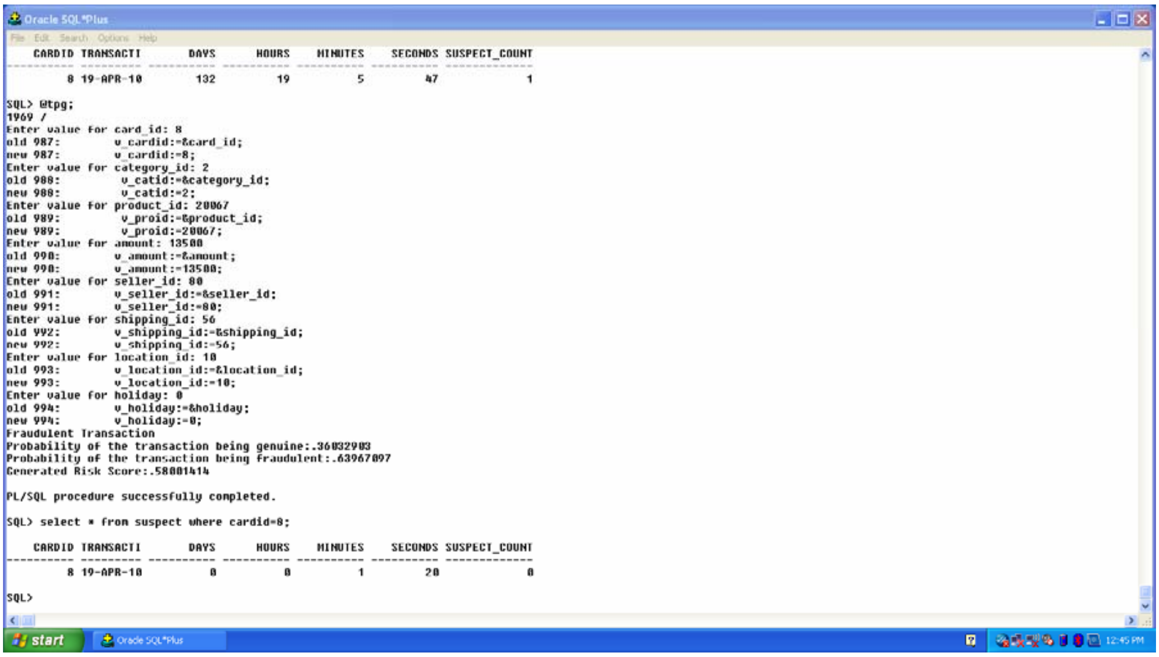

Figure 30 Example output of Data Mining Application for Bayesian Learning-II

IV. CONCLUSION

As we covered in Chapter 1, many techniques, such as First Virtual, Cyber Cash, and SET, are employed to avoid financial cybercrime. Although customers and businesses rarely use these systems, they are very secure. These models protect our online transactions, but they cannot prevent fraud if a customer's credit card information is physically lost or falls into the wrong hands.

An Internet Virtual Credit Card Model has been provided by Anshul Jain et al. [1]. In this scenario, the bank will provide a login name and password. Then A virtual credit card number and expiration date would be provided by bank after classification into the bank's website. In order to complete an online transaction, the customer must provide and remember four pieces of information: their login ID, password, virtual credit card number, virtual card's expiration date. In my perspective, it will cost the customer more and make it harder for them to recall these extra facts.

The Reserve Bank of India recently mandated that all banks in India offer unique passwords to their credit card holders for use during online transactions. This strategy is already being applied in other nations. Although the first transaction is quite safe, in my opinion, this strategy is insufficient to stop fraud since, while the consumer is completing the first transaction, a fraudster might potentially get the password by hacking the computer or using another method.

4.1 PROPOSED FINANCIAL CYBER CRIME PREVENTION MODEL

In this arrangement, the credit card holder receives a unique password for online transactions as well as the ability to choose the length of time the password will remain active. The client must sign onto the bank's website. He can then set his password for the online transaction as well as its expiration date. If it has expired, he cannot finish the transaction. If he is the legitimate cardholder, he must connect onto the bank website, set a password, and specify an expiration date for the password.

As a result, in this paradigm, the password is only active until its expiration date has passed. When the password expires, the customer must request a new password from the bank along with confirmation of its validity. The customer's chosen expiration date needs to fall between the current day and the card's real expiration date.

While in our concept, the user will provide the password, making it a user-defined word that is simple for him to remember. Customers that deal frequently may choose to make their password expiration date very brief in order to prevent falsification. Additionally, he has the option of setting the password expiration date to the following day. As a result, the customer may ensure the security of each of his online transactions. Customers might choose a long expiration date if they don't transact frequently or see of it as overhead. When financial cybercrime spikes significantly in a given month, users can choose a shorter expiration date to prevent fraud.

4.2 SIGNIFICANCE OF THE RESEARCH

The study is distinctive in that it uses data mining, statistics, artificial intelligence on one platform for modeling portion. Work detailed in thesis must be beneficial to researchers; in particular, a literature review of data mining techniques is an effort to offer a roadmap for the researchers to explore, choose the best data mining approach beforehand putting it into practice. Additionally, building additional financial applications benefits from an sympathetic of the role data mining plays in detecting monetary corruption.

Although the programme was developed with online transactions in mind, cardholders can also use it for disconnected dealings.

Although we have created a specific application, we believe, current approach can be successfully applied to prevent infiltration in other database applications with just small application-specific modifications.

We contacted practically all of Gujarat's banks, but none of them are currently utilizing any form of software for detecting financial cybercrime. Consequently, our data mining program has been quite helpful to them.

4.3 LIMITATION OF THE STUDY:

Customers who frequently use their credit cards are the only ones who use the data mining programme that has been built. It is not for people who only deal occasionally throughout the year. The customer's whole purchasing history must be learned by the model in order for it to accurately forecast future transactions. As the customer completes more transactions, perfect gets stronger, studies customer's behaviour, more accurately anticipates the transaction.

Parameter holiday is different for each country, despite the fact that the application is global and was created with consideration for all nations. Therefore, to apply this update, the application needs just modest changes.

4.4 FUTURE SCOPE OF THE RESEARCH:

Present work takes into account the customer's site when they conduct an online transaction. It is not taken into account which machine is used for the online transaction, in future effort IP address may also be taken into account, designs may be developed for this IP address. Only issue is that IP addresses are changeable rather than static. Therefore, it is important to take this element into consideration.

The research has been prepared and carried out with the utmost care to fulfill the research objectives. It is impossible to halt in this sector since it constantly has to be updated to take into account the dynamic changes that have occurred as the genuine issues.

Although the DBSCAN data mining procedure is only used for transaction amounts, it can also be used for additional attributes.

REFERENCES

1. “Securing Big Data Environment from Attacks” by Udhaya Tupakula and Vijay Varadharajan , Advanced Cyber Security Research Centre, Faculty of Science and Engineering, Macquarie Australia in 2016 at IEEE publication[978-1-5090- 2403-2/16] DOI. 10.1109/Bigdatasecurity-HPSC-IDS-2016.
2. ”Cyber Crime Investigation in the Era of Big Data”, by Andrii Shalaginov, Jon William Johnsen, Katrin Franke, NTNU Digital forensics group, Faculty of information technology and electrical engineering, Norwegian University. 2017 IEEE International Conference on Big Data.978-1-5386- 2715-0/17.
3. Crime Analysis and Predictin Using Big Data” by aarthi srinivasnadathur, gayathri narayannan, Indraja ravichandran, srividhya.S,kavalvizhi form department of information technology , SRM Institute of Science and Technology, Kattankulathur,Kancheepuram, Tamilnadu, India. Published in “International Journal of Pure and Applied Mathematics” Volume 119 No. 12, 2018. ISSN: 1314- 3395.
4. Technologies of safety in the bank sphere from cyber attacks”by Nyrkov Anatoliy .P, Abramova Kritstina.V , Koroleva,Gaskarov from Admiral Kakarov State University of Maritime and Inland Shipping, Russia. 978-1-5386-4340-2/18 @IEEE in year 2018.
5. “Crime analysis using K-Means Clustering” by Jyothi Agarwal,Renuka Nagpal, Rajini sehgol form Amity University, Nodia, in the International Journal of Computer Application [0975-8887] volume 83,No 4 December 2013.
6. Priyanka Kulkarni, & Dr. Swaroopa Shastri. (2024). Rice Leaf Diseases Detection Using Machine Learning. Journal of Scientific Research and Technology, 2(1), 17–22. https://doi.org/10.61808/jsrt81
7. A Data Mining Framework To Analyze Road Accident Data Journal Of Big Data, Sachin Kumar and Durga Toshniwal 2015.
8. “Cyber Crime Analysis in Social Media using Data Mining Technique”, by M. Ganesan, P. Mayilvahanan, Department of Computer Science, Vels University. In International Journal of Pure and Applied Mathematics(IJPAM) volume 116 No. 22 [1311-8080] 2017.
9. “Survey of Analysis of crime detection techniques using data mining and Machine Learning”, by S. Prabhakaran, and silpa mitra , in National Conference on Mathematical Techniques and its applications [1742-6596].
10. “Predictive Modelling of Crime Dataset using Data mining”,by prajakta yerpude and Vaishnavi Gudur, Department of Compute science, in International Journal of Data Mining and Knowledge Process. vol-4 - 2017.
11. Shilpa Patil. (2023). Security for Electronic Health Record Based on Attribute using Block-Chain Technology. Journal of Scientific Research and Technology, 1(6), 145–155. https://doi.org/10.5281/zenodo.8330325
12. Mohammed Maaz, Md Akif Ahmed, Md Maqsood, & Dr Shridevi Soma. (2023). Development Of Service Deployment Models In Private Cloud. Journal of Scientific Research and Technology, 1(9), 1–12. https://doi.org/10.61808/jsrt74
13. Antariksh Sharma, Prof. Vibhakar Mansotra, & Kuljeet Singh. (2023). Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning. Journal of Scientific Research and Technology, 1(6), 174–187.
14. Dr. Megha Rani Raigonda, & Shweta. (2024). Signature Verification System Using SSIM In Image Processing. Journal of Scientific Research and Technology, 2(1), 5–11. https://doi.org/10.61808/jsrt79
15. Shri Udayshankar B, Veeraj R Singh, Sampras P, & Aryan Dhage. (2023). Fake Job Post Prediction Using Data Mining. Journal of Scientific Research and Technology, 1(2), 39–47.
16. Gaurav Prajapati, Avinash, Lav Kumar, & Smt. Rekha S Patil. (2023). Road Accident Prediction Using Machine Learning. Journal of Scientific Research and Technology, 1(2), 48–59.

17. Dr. Rekha Patil, Vidya Kumar Katrabad, Mahantappa, & Sunil Kumar. (2023). Image Classification Using CNN Model Based on Deep Learning. Journal of Scientific Research and Technology, 1(2), 60–71.
18. Ambresh Bhadrashetty, & Surekha Patil. (2024). Movie Success and Rating Prediction Using Data Mining. Journal of Scientific Research and Technology, 2(1), 1–4. https://doi.org/10.61808/jsrt78
19. Dr. Megha Rani Raigonda, & Shweta. (2024). Signature Verification System Using SSIM In Image Processing. Journal of Scientific Research and Technology, 2(1), 5–11. https://doi.org/10.61808/jsrt79
20. Priyanka Kulkarni, & Dr. Swaroopa Shastri. (2024). Rice Leaf Diseases Detection Using Machine Learning. Journal of Scientific Research and Technology, 2(1), 17–22. https://doi.org/10.61808/jsrt81