ISSN 1996-3343

Asian Journal of Applied Sciences

Knowledgia
SCIENTIFIC
A Place to Publish Outstanding Research

http://knowledgiascientific.com

Asian Journal of Applied Sciences 8 (3): 173-184, 2015
ISSN 1996-3343 / DOI: 10.3923/ajaps.2015.173.184

Money Laundering Identification on Banking Data Using Probabilistic Relational Audit Sequential Pattern

Vikas Jayasree and R.V. Siva Balan
Department of Computer Application, Noorul Islam University, Tamil Nadu, India

Corresponding Author: Vikas Jayasree, Department of Computer Application, Noorul Islam University, Tamil Nadu, India Tel: +971 50 5035529

ABSTRACT

Data mining techniques are the most commonly used techniques for prevention and detection of money laundering frauds. The fraud detected on the financial account using the data mining technique and the existing systems provides the primary solution to fraudulent detection problem. The solution on the fraudulent detection fails to direct the attention towards practical money laundering banking principles. The transaction process through the 'k' banking database is not effective on processing and responding against the money laundering. The money laundering carried out based on the users account information. To direct attention towards the money laundering identification, a Probabilistic Relational Model using the Audit Sequential Pattern (PRM-ASP) Mining is proposed in this study. Association Mapping (AM) algorithm is performed on the preprocessed data set to separate the transactions which are take place from one-to-many and many-to-one accounts. PRM-ASP mining taken for the money laundering identification uses the time series data and identifies one-to-many and many-to-one relationship between transactions to identify the vulnerable accounts. From the separated set of transactions by PRM, the vulnerable banking accounts are identified and collect all the money laundering accounts. Then, PRM-ASP mining based on relational logic uses the audit sequential pattern to identify the pattern of transaction on the vulnerable accounts. In addition to provide a logical money laundering identification in most of the real-world domains, the PRM is effectively used by auditing the sequential patterns. Probabilistic Relational Model (PRM) uses the multiple factors and metrics for the experimental work such as fraud identification accuracy, false positive rate and processing time to identify vulnerable account.

Key words: Money laundering, probabilistic relational models, vulnerable accounts, association mapping, statistical technique, transaction processing

INTRODUCTION

Due to a fast improvement in the electronic commerce technology, the use of banking system is dramatically increased to perform the transaction. As the banking account has become the one of the most popular system to perform the transaction through online and offline. One of the biggest issue occurred on the banking system is the money laundering operation. The key concept on the money laundering is to analyze the behavior of the account users. The inconsistency occurs with respect to the unusual transaction is carried out on the banking account. The user behavior with respect to the banking account varies periodically. The money laundering process is clearly described in Fig. 1.

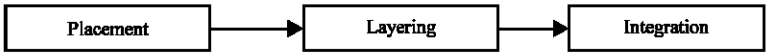


Fig. 1: Money laundering process

Figure 1 clearly describes the money laundering process. At the initial stage, placement performs the depositing of money on the bank account. The deposited money is the illegal money of the users. Then the placement hides the origin of the funds through the series of transaction. The series of financial transaction is carefully carried out in the layering structure. Finally, the integration creates the legal origin to cover the criminal's transactions. Some of the count measures to suspect the bank account behaviors are the variation of billing address, maximum amount of transaction, large transaction done far away from the living place and money transaction to the particular user account repeatedly.

Fraud detection system is detecting fraudulent transactions in an online system. The fraud detection (Olszewski, 2014) on the credit card based transaction is competent of minimizing the unnecessary activities. In Philip and Sherly (2012), unsupervised method vigorously analyzes the profile behavior of the patterns. The unsupervised algorithms are developed for the detection but the verification result does not provide the higher scalability result. Classification models are designed to group data into their various categories by Muhammad (2014) to attain the higher scalability result. Naive Bayes Classifier with input, hidden and output layer is developed to optimize the result. Bayes classifier presumes that the existence of a particular feature is dissimilar to the any other feature.

Reasonably (Pulakkazhy and Balan, 2013; Jayasree and Balan, 2013) financial fraud is becoming an increasingly serious problem in the current trend. Existing Financial Fraud Detection (FFD) framework as described in (Ngai *et al*., 2011; Huang *et al*., 2014) classifies the data mining tasks and provides primary solutions to the fraudulent detection problems. FFD fails to direct attention toward practical money laundering banking principles and solutions. Fraudulent transaction with pattern matching by Tripathi and Ragha (2013) has become very important on all money laundering issues in banks. The fraudulent is avoided in this system using the rule based filtering approach but Bayesian learning still needs the help for improving the system accuracy.

Singh and Singh (2014), cybercrime detection based on Bayesian Learning Approach improved the system accuracy by analyzing the behavior of the customers. Bayesian Learning Approach solved the problem and not effective in identifying the user presented geographical location. Credit card fraud detection system joins the different types of evidences using DempsterBShafer theory by Panigrahi *et al.* (2009). The purpose of aggregation meaningfully summarizes and simplifies the bulk data processing into a single source points. Bayesian learning is used with probabilistic approach to build intelligent learning systems.

Behavior based classification approach using Support Vector Machines in (Dheepa and Dhanapal, 2012) employed a proficient feature extraction method. Any inconsistency happen in the behavior where the transaction prototype is forecast as suspicious and taken for further consideration to find the frauds. The support vector machine consumes the higher cost factor on effective kernel function development. Kamra and Bertino (2011), Joint Threshold Administration (JTA) Model key idea jointly administers the 'k' kernel function based banking databases. Transaction processing and response action against the money laundering based on the DBMS information is not effective.

Based on the aforementioned techniques and methods, in this study, effective money laundering identification technique called as Probabilistic Relational Model using the Audit

Sequential Pattern (PRM-ASP) Mining is designed on German Credit Data set. PRM-ASP is implemented to identify the sequence pattern by minimizing the false positive rate. The contribution of PRM-ASP Mining is:

- To present an Association Mapping (AM) algorithm to separate the transactions from one-to-many and many-to-one accounts
- To compute the vulnerable account AM algorithm based money laundering identification uses the time series data
- To collect all the money laundering accounts, Probabilistic Relational Model based on relational logic is developed
- To categorize the path of vulnerable transfer is identified using the audit sequential pattern.

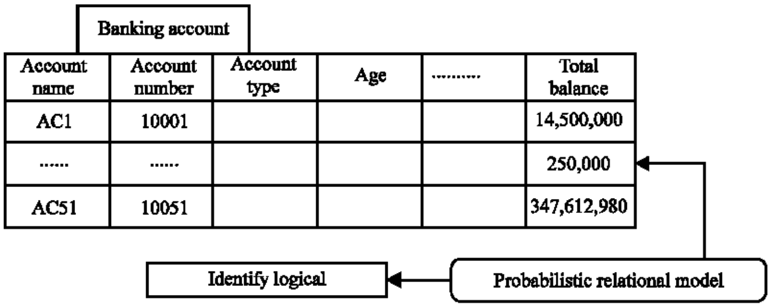
MATERIALS AND METHODS

Development of probabilistic relational model on money laundering identification: Probabilistic Relational Model using the Audit Sequential Pattern (PRM-ASP) Mining main goal is to identify the money laundering accounts on the bank dataset. Money laundering is a criminal activity with serious threat to financial institutions, through which it becomes a major threat to the entire nation, so the PRM-ASP mining is used to identify the faulty bank accounts. Relational logic based auditing identifies the relationship of personal account with bank rules in PRM-ASP mining.

Figure 2 clearly defines the relationship logic between the client information and banking system using the probabilistic relational model to easily identify the money launders. Banks collects thorough personal information from their clients while performing the PRM-ASP mining as well as information collected is used for the relational logic. The relational logic between the client and banking companies are clearly identified and auditing of sequential pattern is carried out. Probabilistic relational model are expressive in describing the relations between the objects.

Auditing sequential pattern mining with PRM is used to extract the valuable information of the clients and to easily identify the money laundering account on larger database. PRM-ASP mining initially identifies the relationship of the client and the accounts. Auditing sequential pattern is intuitive enough to easily mine the client information. The pattern information is summarize with the probabilistic relational to effectively process and recognize the money laundering accounts. Architecture Diagram of PRM using Audit Sequential Pattern Mining is described in Fig. 3.

As illustrated in Fig. 3, PRM-ASP Mining is used to effectively identify the money laundering accounts. The banking dataset (German Credit Dataset) is used for identification of the money launder clients. Initially, in data preprocessing step, the client account information is extracted using the Association Mapping algorithm. The AM algorithm extracts the client information by



Account name	Account number	Account type	Age	....	Total balance
AC1	10001				14,500,000
......	......				250,000
AC51	10051				347,612,980

Fig. 2: Probabilistic relational model on client information

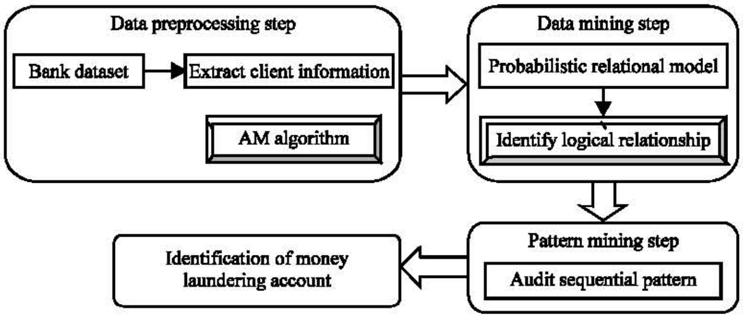

Data preprocessing step
Bank dataset
Extract client information
AM algorithm
Data mining step
Probabilistic relational model
Identify logical relationship
Pattern mining step
Audit sequential pattern
Identification of money laundering account

Fig. 3: Architecture diagram of PRM-ASP mining

identifying the many-to-one and one-to-many mapping accounts. The one-to-many and many-to-one money transaction accounts are grouped as a set to identify the relational logic in PRM-ASP Mining.

After preprocessing in PRM-ASP Mining, it produces the result to the data mining step to identify the relational logic of the system. Probabilistic Relational Model deals with the faulty account to identify the relationship between the clients and the banking system. PRM represent the ambiguity over the banking properties and captures the probabilistic dependence between the client and banking system. The probabilistic relational model then explain the audit sequential pattern mining on the client account to categorize the money launders using the data mining technique. The mining step combines the work with pattern analysis step to audit the fault accounts and identify the money laundering on each time frame. The pattern analysis is carried out using the Audit Sequential Pattern mining.

Association mapping procedure: Association mapping in the PRM-ASP Mining is performed on the preprocessing step. The AM separates the client transaction which is different to the distinctive accounts. From the PRM-ASP mining, the separate set of doubtful (i.e.) faulty accounts are collected and also set of accounts linked to the particular account is also identified. The preprocessing step with association mapping recognizes the one-to-many and many-to-one relation money transactions on the client accounts.

The many-to-one and one-to-many money transaction in PRM-ASP mining is explained through the AM algorithm.

```
Begin
//Many-to-One Transaction
<Account name="Client name">
<generator class="local"/>
<many-to-one name="address" column="addressId" not-null="true"/>
</Account>
//One-to-Many Transaction
<Account name="Client Address">
<generator class="local"/>
<set name="ACC_name" inverse="true" key column="addressId"/>
<one-to-many class=" ACC_name "/>
</set>
</Account>
End
```

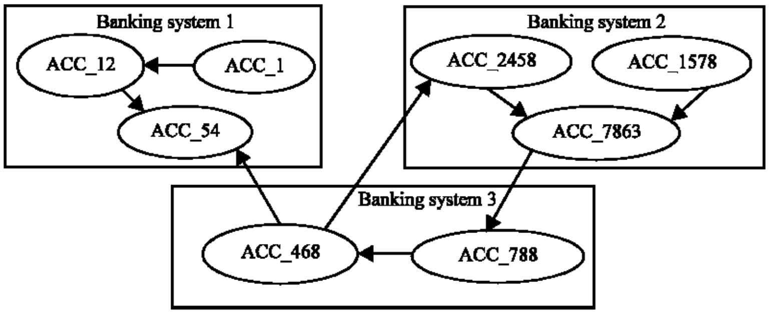


Fig. 4: Probabilistic relational on different time frame

The above AM algorithm used to easily identify the faulty transaction carried out on the many-to-one and one-to-many transactions. The transactions create the 'Account' class and the generator class checks whether the transaction is carried out within the local account. The many-to-one transacts the money to the same account from the varying source accounts. The one-to-many perform the money transaction by setting the account name to the diverse destination accounts. The many-to-one transaction carried and association between the accounts are mapped effectively in PRM-ASP mining.

Probabilistic relational model: The probabilistic relational model identifies the relationship between the number of transactions and the money transferred on the each time frame. The money transferred between the different bank clients are noticed in PRM-ASP mining and the relational logic is analyzed. The association mapping in the preprocessing step are used for the probabilistic relational logic identification in the data mining step. The probabilistic relational model is represented in Fig. 4.

Figure 4 describes the money transaction to the different banking system account on the varying time frame. Transaction relational logic of ACC_15, ACC_12 and ACC_54 are examined using the probabilistic relational model. The overall amount transferred is computed in PRM-ASP mining and the vulnerable account is predicted in the data mining step:

$$\text{MtO Transaction} = \text{Amount of transaction} > \text{Threshold rate} \quad (1)$$

Equation 1 MtO describes the Many-to One transaction process in the probabilistic relational model. On varying time frame (PRM-tf), many-to-one relationship vulnerable is identified, if the amount of transaction exceeds the threshold rate on particular account, then the account is considered as the vulnerable account in PRM-ASP mining. The one–to-many relationship vulnerable is identified in PRM-ASP mining, when the maximum number of transaction is carried out on the particular time frame (tf):

$$\text{MtO Transaction} = \text{Current of transaction} > \text{tf transaction limit} \quad (2)$$

Equation 2 OtM describes the One-to-Many transaction process in the probabilistic relational model. PRM deals in identifying the money laundering on the multiple accounts with varying entities and properties. PRM captures all the probabilistic dependence of the different accounts, thereby offers the efficient system result on the money laundering identification. The sequential pattern auditing is clearly explained in below section.

Audit sequential pattern: Identified money laundering account using the probabilistic relational model, now categorize the path of transfer and money transferred using audit sequential pattern. Audit sequential pattern compute the pattern n (t) number of transmission path using relational logic. 'n' represents the total number of available path in the relation logic system and 't' represents the number of account involved in money laundering. The auditing carried out in the PRM-ASP mining to collect the entire amount transferred paths and available paths of group used to compute the probability of money laundering. The algorithmic step of the audit sequential pattern is described as:

```
Begin
Step 1: Read banking data information of clients, Tm-Money transferred
Step 2: Identify distinctive source account set 'S'
        For each account
Step 3: Compute overall money transferred $S = \sum T_m n(t)$
        Step 3.1: MtO Transaction = Amount of transaction>threshold rate
        Step 3.2: OtM Transaction = Current Transaction>tf Transaction limit
Step 4: Identify set of transfer paths using sequential pattern 'S'
        Step 4.1: Add 'S' to transfer set '$T_m$'
End For
End
```

The above algorithm described for pattern identification with probabilistic relational model easily identifies the money laundering. The source account 'S' computed the money transferred from one-to-many and many-to-one relationship. The 'MtO' or OtM' based transaction is carried out to identify the exact account which performs the money laundering operation. The identified pattern for amount transfer in PRM-ASP mining provides an effective system to identify the money laundering.

Experimental evaluation: Probabilistic Relational Model using the Audit Sequential Pattern (PRM-ASP) Mining is experimented in JAVA platform using Statlog (German Credit Data) Data Set. Statlog German Credit Data from the UCI repository classifies the people by a set of attributes list. For AM algorithm experimentation, numerical attributes from Strathclyde University with numerous pointer variables are added to make it effective algorithm for money laundering identification. The attribute characteristics are categorized as categorical and integer type. Nearly, 17 attributes from the Statlog German Credit Data has been coded as integer type and 3 under the categorical type.

Probabilistic Relational Model using the Audit Sequential Pattern mining is compared with the existing Financial Fraud Detection (FFD) framework and Joint Threshold Administration (JTA) Model key. Statlog German Credit Data contains the 1000 instances on financial area for performing the experimental work to identify the vulnerable accounts. The experiment is conducted on the factors such as fraud identification accuracy level, false positive rate, processing time to identify the vulnerable account, overall system efficiency rate, scalability and sequential pattern auditing rate.

The more accurate identification of fraud is defined as the trueness occurred without any systematic error in the proposed PRM-ASP Mining. The associate trueness defines accurately the trueness and falseness:

$$\text{Fault identification accuracy level} = \left[\frac{\text{Retrieved fault accounts}}{\text{Retrieved overall accounts}} \times 100\right]$$

The fault identification accuracy level in above formulation describes the class of fault account is extracted accurately from the group of user relevant accounts. The false positive rate is when a test result indicates that minimal false result occurred on identifying the money laundering accounts:

$$\text{False positive rate} = \frac{\text{False results}}{\text{False results} + \text{True results}}$$

The false and true results together achieve the ratio of '1', where the experimental results are measured. Processing time on money laundering account identification is defined as the amount of time consumed to perform the overall processing operation such as associate mapping, probabilistic relational model and audit sequential pattern:

$$\text{Processing time} = \text{User bank account monitor start time} - \text{User bank account monitor end time}$$

Scalability is defined as the ability of the system to handle the growing amount of banking accounts without any money laundering operations. The scalability factor is measured in terms of percentage (%). Audit rate is the amount at which the pattern of money laundering process is carried out, measure in terms of percentage.

RESULT AND DISCUSSION

To effective identify the money laundering accounts, Probabilistic Relational Model using the Audit Sequential Pattern (PRM-ASP) Mining experimental results. PRM-ASP Mining is compared against the existing Financial Fraud Detection (FFD) framework (Ngai *et al*., 2011) and Joint Threshold Administration (JTA) Model key (Kamra and Bertino, 2011). Java is used to experiment the factors and analyze the measures of the result percentage with graph. Results are presented for different number of transaction accounts. The experimental work uses the Statlog (German Credit Data) Data Set to measure the percentage of gain result.

Table 1 tabulates the accuracy level of fraud identification in FFD framework (Ngai *et al*., 2011) JTA Model (Kamra and Bertino, 2011) and PRM-ASP Mining. It describes the fraud identification accuracy level based on the transaction account. The transaction account taken from the

Table 1: Tabulation for fraud identification accuracy level

	Fraud identification accuracy level (%)		
No. of transaction accounts	FFD framework	JTA model	PRM-ASP mining
100	17.2	19.1	20.00
200	22.4	23.4	25.00
300	27.6	30.6	33.33
400	25.9	28.4	30.00
500	38.4	41.2	44.80
600	48.2	50.4	56.80
700	50.7	53.4	60.18

Table 2: False positive rate tabulation

	False positive rate (%)		
User counts	FFD framework	JTA model	PRM-ASP mining
50	0.07	0.05	0.04
100	0.06	0.05	0.03
150	0.11	0.09	0.06
200	0.15	0.13	0.11
250	0.16	0.14	0.09
300	0.20	0.17	0.15
350	0.21	0.18	0.14

Table 3: Tabulation on overall system efficiency

	Overall system efficiency rate (Efficiency %)		
Accounts count	FFD framework	JTA model	PRM-ASP mining
30	73	62	86
60	75	64	89
90	74	67	90
120	78	69	92
150	81	70	93
180	83	70	94
210	84	71	95
240	85	72	97

experimental evaluation is from 100-700 accounts. AM algorithm used to easily identify the faulty transaction carried out on the many-to-one and one-to-many transactions. The transactions create the 'Account' class and the generator class and check the fraud level accurately. The accuracy level is raised from 11-20% in PRM-ASP Mining when compared with the existing FFD framework (Ngai *et al*., 2011). The one-to-many perform the money transaction by setting the account name to the diverse destination accounts, so that the fraud is identified accurately with 4-12% improved result in PRM-ASP Mining when compared with existing JTA Model (Kamra and Bertino, 2011).

Table 2 tabulates the false positive rate in FFD framework (Ngai *et al*., 2011) JTA Model (Kamra and Bertino, 2011) and PRMASP Mining. It represents the false positive rate based on the user accounts. As illustrated in the figure, the average false positive rate is measured on the different user counts. The false positive rate is reducing because the probabilistic relational model is introduced in the PRM-ASP mining. The relational logic reduces the false positive rate by 25-50% when compared with the FFD framework (Ngai *et al*., 2011). The association mapping in the preprocessing step are used for the probabilistic relational logic identification, thereby reducing the false positive rate by 11-40% when compared with the existing JTA Model (Kamra and Bertino, 2011). The money transferred between the different bank clients are noticed in PRM-ASP mining and the relational logic is analyzed on the 350 user accounts.

Table 3 tabulates the examined overall system efficiency of the FFD framework (Ngai *et al*., 2011), JTA Model (Kamra and Bertino, 2011) and PRM-ASP Mining are examined. The bank accounts of the different count are taken for identifying the money laundering identification efficiency rate. It describes the overall system efficiency of the system based on the account count. The FFD framework (Ngai *et al*., 2011) and JTA Model (Kamra and Bertino, 2011) versus

Table 4: Tabulation of processing time

	Processing time (sec)		
Size of each user account (KB)	FFD framework	JTA model	PRM-ASP mining
50	438	475	413
100	512	507	465
150	693	687	581
200	777	766	721
250	857	849	734
300	921	959	869
350	967	928	815

increasing number of accounts used to measure the efficiency rate. The count of the account with German Statlog data information improves the efficiency rate by 13-21% when compared with the existing FFD framework (Ngai *et al.*, 2011). PRM deals in identifying the money laundering on the multiple accounts with varying entities and properties ranges. The entities varies when the transaction between the accounts get increased. PRM captures all the probabilistic dependence of the different accounts, thereby offers the efficient system result on the money laundering identification, thereby improving the efficiency rate by 32-39% when compared with existing JTA Model (Kamra and Bertino, 2011). The efficiency rate is measured on analyzing the effectiveness of money laundering accounts. On taking the 60 user accounts, the overall system efficiency is 89% whereas; the JTA model attains only the 64%.

Table 4 tabulates the processing time in FFD framework (Ngai *et al.*, 2011) JTA Model (Kamra and Bertino, 2011) and PRM-ASP Mining. It demonstrates the processing time based on the each user account. The size of user count is used to measure the processing time of the system. The targeting results of the PRM-ASP Mining processing time is compared with two existing state of arts method. The state of arts methods taken for the experimental work is FFD framework (Ngai *et al.*, 2011) and JTA Model (Kamra and Bertino, 2011). Auditing sequential pattern is intuitive enough to easily mine the client information, thereby reducing the processing time by 5-16% in PRM-ASP Mining when compared with existing FFD framework (Ngai *et al.*, 2011). The pattern information is summarize with the probabilistic relational to effectively process and recognize the money laundering accounts, thereby reducing the processing time by 5-15% when compared with JTA Model (Kamra and Bertino, 2011).

Figure 5 represents the scalability in FFD framework (Ngai *et al.*, 2011) JTA Model (Kamra and Bertino, 2011) and PRM-ASP Mining.

The PRM-ASP mining separates the faulty accounts where all the accounts are linked to the database. The removal of faulty account through the PRM-ASP Mining, improves the scalability ratio result. The scalability factor improves by 4% when compared with existing FFD framework (Ngai *et al.*, 2011), where preprocessing step with association mapping recognizes the one-to-many and many-to-one relation money transactions on the client accounts. The scalability factor with the probabilistic relational improves the scalability in PRM-ASP Mining by 9% when compared with JTA Model (Kamra and Bertino, 2011).

Table 5 tabulates the audit rate of sequential pattern in FFD framework (Ngai *et al.*, 2011) JTA Model (Kamra and Bertino, 2011) and PRM-ASP Mining.

It demonstrates the sequential pattern audit rate based on the transaction count. The transaction is collected using the probabilistic relational model and now categorize the path of

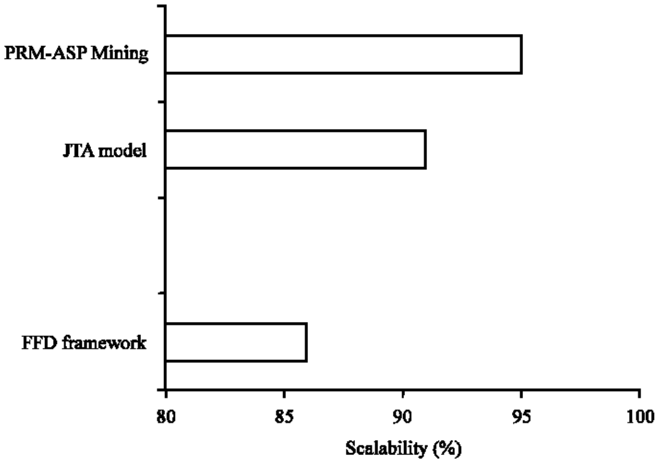


Fig. 5: Measure of scalability

Table 5: Sequential pattern audit rate tabulation

	Sequential pattern audit rate (Audit %)		
No. of transaction	FFD framework	JTA model	PRM-ASP mining
10	73	82	86
100	74	84	87
1000	74	87	91
10000	78	89	93
100000	79	88	93
1000000	82	90	92

transfer and money transferred using audit sequential pattern. The audit sequential pattern is improved by 12-22% in PRM-ASP Mining when compared with the FFD framework (Ngai *et al*., 2011). At the 1000 transaction accounts, PRM-ASP Mining attains 91% higher audit rate whereas the JTA Model attains the 85% result. Audit sequential pattern compute the pattern n (t) number of transmission path using relational logic and produce the result of 2-5% improved result in PRM-ASP Mining when compared with the JTA Model (Kamra and Bertino, 2011).

Finally, PRM-ASP mining identifies the money laundering under the various tie series, thereby identifying the vulnerable accounts. PRM-ASP mining based on relational logic uses the audit sequential pattern to identify the pattern of transaction a logical money laundering identification in most of the real-world domains.

Data mining excel in performing the transaction process monitoring where it is emerge as most effectual fraud detection. In Thiprungsri and Vasarhelyi (2011), clustering technique is employed to perform the anomaly detection. Cluster analysis helps the auditors to points their banking account malpractice and automatically audits the frauds. Cluster analysis recognizes anomalies in accounting systems by the inner auditing operation. The filtering concept is employed but the resulting group does not produce the effective result. In (Sabau, 2012), clustering is an unsupervised data mining technique deal with the difficulty of separating a given position of entities into significant subsets to detect the fraud. Clustering entities surrounded by the same group which helps to easily detect the financial fraud on banking accounts.

Clustering based techniques in (Koupaie *et al.*, 2013), are further extended by proposing the concept of cluster based local outlier, in which a measure for identifying the outlier of each data object is defined. Stream Projected Outlier detector (SPOT) manages the outlier detection problem and new window based time model and degenerations cell summaries get data from the data stream. Sparse Subspace Template (SST) makes it exclusive to differentiate expected outliers. Crime mapping refers to the process of conducting spatial analysis in (Ahmed and Salihu, 2013) within the range of activities of crime analysis. Clustering concept is introduced to group the similar types of clients but not effective on decision making process.

Spatial analysis is defined as a broad range of statistical techniques to perform decision making process. In (Shekhar *et al.*, 2010), many crime activities handle all type of crime activities but do not handle the temporal semantics of crime activities and useful analytical methods. PELARI (Profitability, Efficiency, Liquidity, Asset Quality, Risk Measures and Investor analyses) model in (Sebe-Yeboah and Mensah, 2014) analyze the financial performance with temporal semantics of the bank without looking on the other indicators such as loan coverage, productivity and service quality. Still, a better information technology platform should be developed to boost its competitive strategies for better and appropriate services.

Biometric form of security particularly addresses the robustness and resolves the all type of attacks against synthetic forgeries. Stefan *et al.* (2012), TUBA (Telling hUman and Bot Apart) monitors a user's typing patterns in a client and server architecture and offer the authentication framework. The user is notified a suspicious behavior and fails to provide automatic locked, under the different attacks. Adaptivity of modern malware against synthetic forgeries in TUBA provides the comprehensive evaluation with higher order Markov chains.

CONCLUSION

In this study, Probabilistic Relational Model using the Audit Sequential Pattern (PRM-ASP) Mining is developed to identify the money laundering accounts effectively without any false positive rate. Initially, the Association Mapping (AM) procedure is employed on the German Credit Data from UCI repository to separate the transactions. The transactions of one-to-many and many-to-one accounts are identified effectively through the mapping procedure. Then, the separated transaction set uses the relational logic named Probabilistic Relational Model to identify the vulnerable accounts. Finally, to categorize the path of money transfer, audit sequential pattern is extended in PRM-ASP Mining process. The PRM-ASP mining in addition provides the logical system in most of the real-world domains. Experimental results demonstrate that the proposed PRM-ASP mining not only identifies the money laundering account but also identifies the vulnerable account with the minimal processing time. PRM-ASP mining provides 25.488% lesser false positive rate and 16.744% improved overall system efficiency.

REFERENCES

Ahmed, M. and R.S. Salihu, 2013. Spatiotemporal pattern of crime using Geographic Information System (GIS) approach in dala L.G.A of Kano State, Nigeria. Am. J. Eng. Res., 2: 51-58.

Dheepa, V. and R. Dhanapal, 2012. Behavior based credit card fraud detection using support vector machines. ICTACT J. Soft Comput., 2: 391-397.

Huang, S.Y., R.H. Tsaih and F. Yu, 2014. Topological pattern discovery and feature extraction for fraudulent financial reporting. Expert Syst. Applic., 41: 4360-4372.

Jayasree, V. and R.V.S. Balan, 2013. A review on data mining in banking sector. Am. J. Applied Sci., 10: 1160-1165.

Kamra, A. and E. Bertino, 2011. Design and implementation of an intrusion response system for relational databases. IEEE Trans. Knowledge Data Eng., 23: 875-888.

Koupaie, H.M., S. Ibrahim and J. Hosseinkhani, 2013. Outlier detection in stream data by clustering method. Int. J. Adv. Comput. Sci. Inform. Technol., 2: 25-34.

Muhammad, S.A., 2014. Fraud: The affinity of classification techniques to insurance fraud detection. Int. J. Innov. Technol. Explor. Eng., 3: 62-66.

Ngai, E.W.T., Y. Hu, Y.H. Wong, Y. Chen and X. Sun, 2011. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decis. Support Syst., 50: 559-569.

Olszewski, D., 2014. Fraud detection using self-organizing map visualizing the user profiles. Knowledge-Based Syst., 70: 324-334.

Panigrahi, S., A. Kundu, S. Sural and A.K. Majumdar, 2009. Credit card fraud detection: A fusion approach using dempster-shafer theory and bayesian learning. Inform. Fusion, 10: 354-363.

Philip, N. and K.K. Sherly, 2012. Credit card fraud detection based on behavior mining. TIST Int. J. Sci. Technol. Res., 1: 7-12.

Pulakkazhy, S. and R.V.S. Balan, 2013. Data mining in banking and its applications: A review. J. Comput. Sci., 9: 1252-1259.

Sabau, A.S., 2012. Survey of clustering based financial fraud detection research. Inform. Econ., 16: 110-122.

Sebe-Yeboah, G. and C. Mensah, 2014. A critical analysis of financial performance of agricultural development bank (Adb, Ghana). Eur. J. Account. Audit. Finance Res., 2: 1-23.

Shekhar, S., M. Celik, B. George, P. Mohan, N. Levine, R.E. Wilson and P. Mohanty, 2010. Spatial analysis of crime report datasets. National Science Foundation (NSF), Washington, DC., USA., May 2010.

Singh, M. and P. Singh, 2014. Security mechanism to detect fraud based on customer behavior. Int. J. Sci. Res. Dev., 2: 258-263.

Stefan, D., X. Shu and D. Yao, 2012. Robustness of keystroke-dynamics based biometrics against synthetic forgeries. Comput. Secur., 31: 109-121.

Thiprungsri, S. and M.A. Vasarhelyi, 2011. Cluster analysis for anomaly detection in accounting data: An audit approach. Int. J. Digital Account. Res., 11: 69-84.

Tripathi, K.K. and L. Ragha, 2013. Hybrid approach for credit card fraud detection. Int. J. Soft Comput. Eng., 3: 8-11.