Credit Card Fraud Detection System using Visual Analytics through the Data Mining

Julapati Gayathri[1], Mylapoor Madhu[2]
[1]*Student, Master of Computer Applications, SKIIMS, Srikalahasti, Andhra Pradesh India*
[2] *Asst.Professsor, Master of Computer Applications, SKIIMS, Srikalahasti, India*

***Abstract*- Financial institutions are interested in ensuring security and quality for their customers. Banks, for instance, need to identify and stop harmful transactions in a timely manner. In order to detect fraudulent operations, data mining techniques and customer profile analysis are commonly used. Thus, we propose EVA, a Visual Analytics approach for supporting fraud investigation, fine-tuning fraud detection algorithms, and thus, reducing false positive alarms. Due to the theatrical increases of fraud which results in loss of dollars worldwide each year, several modern techniques in detecting fraud are persistently evolved and applied to many business fields. The goal of this paper is to provide a security in credit card transaction using EVA technique to detect fraud. The credit card fraud detection features uses user behavior and location scanning to check for unusual patterns.**

***Index Terms*- Visual Knowledge Discovery, Data Mining, Financial Visualization, Financial Fraud Detection.**

1. INTRODUCTION

Credit card fraud can be defined as "unauthorized account activity by a person for whom the account was not intended. Operationally this is an event for detect the fraud in credit card. Now a days in online shopping increases the credit card fraud. Different types of fraud associated with debit and credit card transactions.

Event detection is an important task in many domains such as finding interesting changes in stock markets, spotting problems in health parameters, or detecting financial fraud. Besides its challenging nature, FFD has also a strong social and financial importance. For instance, fraudulent schemes such as 'money laundering', 'unauthorized transaction', or 'straw person' should be detected and fought as fast as possible by financial systems, since the negative economical and social impact increases with time. Thus, governments, banks, and other financial institutions that provide credit and money transaction services have a strong interest in improving operation monitoring and fraud detection. Types of Frauds:

Lost or stolen cards- Is a relatively common one, and should be reported immediately to minimize any damages.

Account takeover- when a cardholder unwittingly gives personal information (such as home address, mother's maiden name, etc.) to a fraudster, who then contacts the cardholder's bank, reports a lost card and change of address, and obtains a new card in the soon-to-be victim's name.

Counterfeit cards- when a card is "cloned" from another and then used to make purchases. In Asia Pacific, 10% to 15% of fraud results from malpractices such as card skimming but this number has significantly dropped from what it was a couple of years prior, largely due to the many safety features put in place for payment cards, such as EMV chip.

Never received- when a new or replacement card is stolen from the email, never reaching its rightful owner.

Fraudulent application- when a fraudster uses another person's name and information to apply for and obtain a credit card.

Multiple imprint- when a single transaction is recorded multiple times on old-fashioned credit card imprint machines known as "knuckle busters".

Collusive merchants- when merchant employees work with fraudsters to defraud banks.

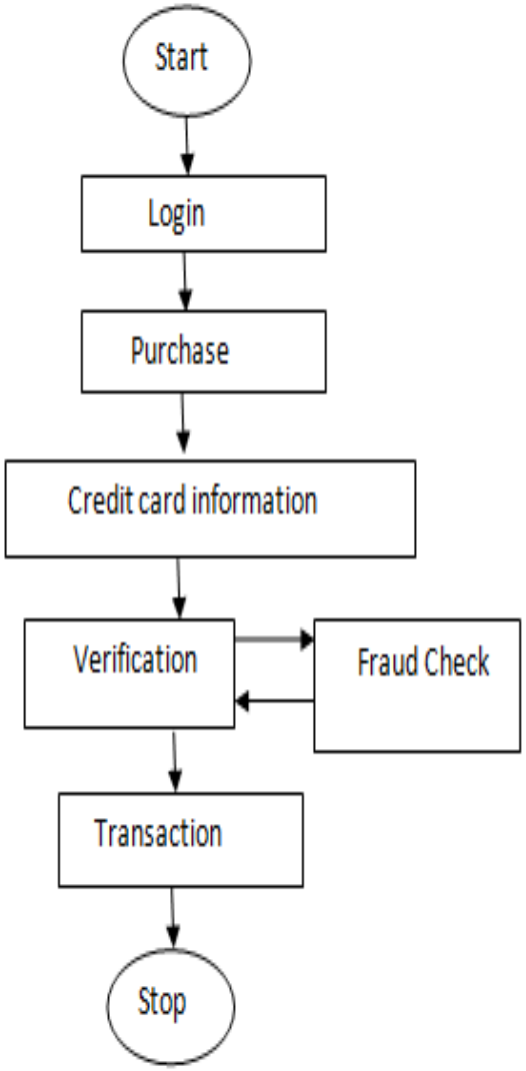
Email order/telephone order (MO/TO) fraud- which now includes e-commerce, and is the largest category of total payment card fraud in Asia-Pacific, amounting to nearly three-quarters of all fraud cases.

2. RELATED WORK

There are a number of surveys that focus on fraud detection. In 2002, Bolton and Hand [32] published a review about fraud detection approaches. They described the available tools for statistical fraud detection and identified the most used technologies in four areas: credit card fraud, money laundering, telecommunication fraud, and computer intrusion. Kou et al. [20] presented a survey of techniques for identifying the same types of fraud as described in . The different approaches are broadly classified into two categories: misuse and anomaly detection. Both categories present techniques such as: outlier detection, neural networks, expert systems, model-based reasoning, data mining, state transition analysis, and information visualization. These works helped us to understand diverse fraud domains and how they are normally tackled. In the health domain, Rind et al. [33] conducted a survey study focusing on information visualization systems for exploring and querying electronic health records. Moreover, Wagner et al. [36] presented a systematic overview and categorization of malware visualization systems from a VA perspective. Both domains of these studies are similar to FFD, since they both involve multivariate and temporal aspects. However, the FFD domain demands for special consideration due to the complexity of the involved tasks

3. PROPOSED SYSTEM

The aim of proposed system is to develop a system of improved facilities. The proposed system can overcome all the limitations of the existing system. The system provides proper security and reduces the manual work and easily maintains the payments information. The existing system has several disadvantages and many more difficulties to work well. The proposed system will help the user to reduce the workload and mental conflict. The proposed system helps the user to work user friendly and he can easily do his jobs without time lagging.



Flowchart of HMM model for credit card fraud detection

In proposed system, we present a EVA (Event detection with Visual Analytics) in tight collaboration with a national bank institution Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. Card transaction processing sequence by the stochastic process of an HMM. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc.

4. FINANCIAL FRAUD DETECTION

We developed our prototype called EVA (Event detection with Visual Analytics) in tight

collaboration with a national bank institution [8] with the aim to improve and support their current FFD techniques. In this section, we
(1) Describe the characteristics of transaction data
(2) Discuss the complexity of the problem at hand
(3) present the currently used methodology for FFD at the bank,

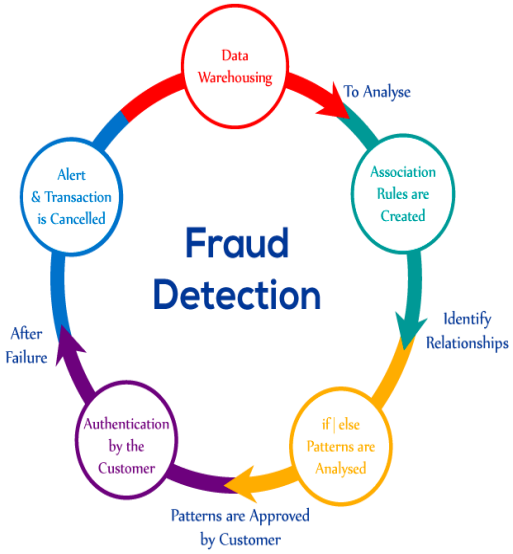
4.1 Methodology for FFD
In this subsection we give an overview of the methodology that is used for FFD by our collaborating bank. Since we are using real data that is quite sensitive, we need to respect privacy and security regulations. Thus, we are not allowed to get into details about the actual algorithms. However, we roughly sketch the four phases of the FFD methodology applied: Profile Generation System, Scoring System, Results Interpretation, and Fraud Validation. Profile Generation System.

Profile Generation System For each customer account the automatic system for FFD generates profiles based on this account‘s transaction history. A single account can have several profiles which reflect different aspects, for instance, separate sender and receiver profiles for one account.

Scoring System The system compares each of the incoming transactions with the corresponding customer‘s profile. To this end, it uses metrics to compute several different scores that are summarized in one overall score

Results Interpretation After calculating the scores, the non automatic part of the investigation takes place. In this phase, investigators analyze multiple transactions simultaneously, due to time constraints. Transactions whose scores exceed a given threshold are further filtered by predefined rules.

Fraud Validation Once investigators have decided that a suspicious transaction is possibly fraudulent, they call the account owner to ask him/her about the transaction‘s veracity. The bank stops the transaction in case the account owner did not authorize it. We incorporated a VA component into the described work flow.



5. EVA’S DESIGN IMPLEMENTATION

In the design phase of EVA we collaborated with two domain experts from the bank institution. Following the design triangle , to generate interactive VA methods we designed EVA with respect to the data, users, and tasks at hand.

Data Financial transaction events constitute multivariate and time oriented data which include details about the transactions such as amount, time, receiver, etc.
Users Investigators from financial institutions that investigate and validate transactions alerts.

Task The overall tasks are fraud detection by means of profile analysis. This task includes the reduction of false negative and false positive alarms, history comparison, as well as the manual investigation

5.1 Requirements
When looking at currently used FFD solutions, there are still many opportunities for improvements. Instead of running queries in spreadsheets and judging alarms by a single overall score value, we propose EVA to support investigators during their decision-making process. From the study of related work and in collaboration with our project partners, we derived the follow requirements

Reasoning about Frauds:

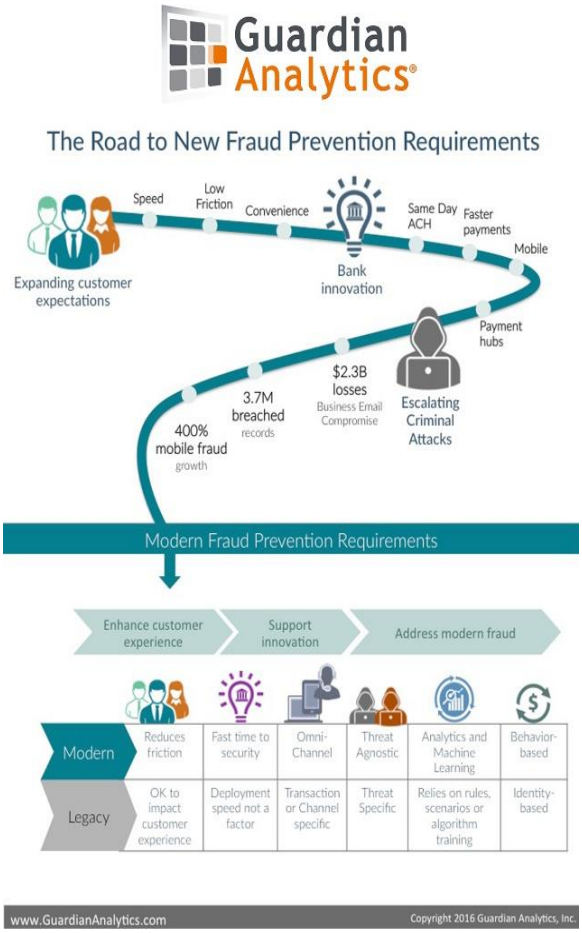
During the fraud validation phase (see Section 3.3), the investigator has to decide if a transaction flagged as suspicious is going to be confirmed as being fraud or not.

Identification of Hidden Frauds

After completing reasoning next phase is identifying the frauds. How it will occur what can do for reduce this frauds. This can lead investigators to overlook fraudulent transactions that were not detected by the automatic system.

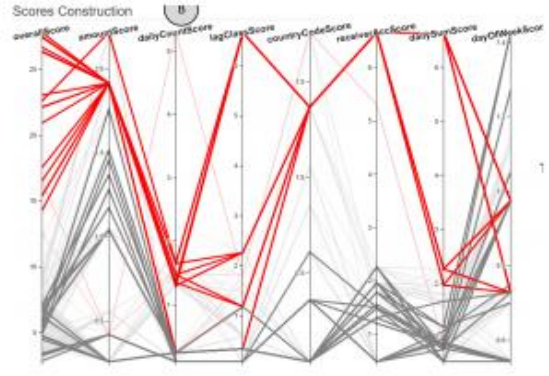
Visual Support for Scoring System

Considering the constantly changing fraudulent behavior, the scoring system and the profiling systems should be in constant evaluation. They should be frequently updated in order to stay effective. . Moreover, investigators should be able to compare single transactions and their scores with the client‘s history of transactions.



5.2 Event Detection with Visual Analytics (EVA)

e. EVA is composed of six views displaying different aspects of the data. All views are connected via brushing and linking. The visualization techniques were chosen with respect to the suitability of their visual attributes (e.g., element position, length, angle, color) to effectively and accurately encode the data types at hand [24]. In particular, we chose different visual encodings to achieve the best possible balance between distinguishability, separability, and pop-out of important information.



Score construction view

Transaction amount and frequencies And ranks dynamic table

Score Construction View

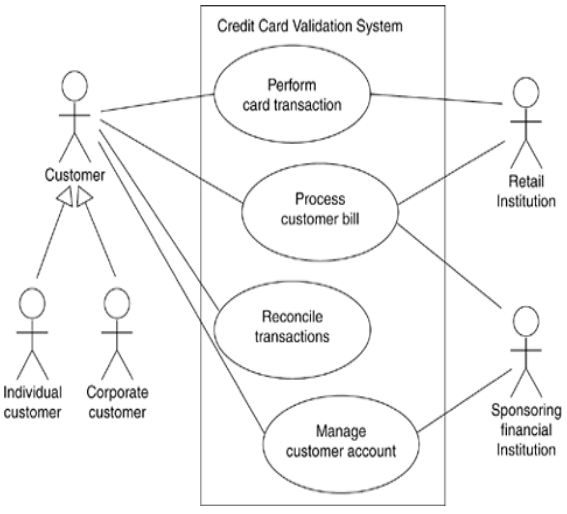
We use parallel coordinates to present a visual history of transactions where each line represents a transaction of the selected account. The Score Construction view B highlights the selected data

while graying out other transactions. This feature allows investigators to keep the context of filtered transactions.

Dynamic table:
Each row represents one transaction and each column one of its dimensions. Filters and selections in other views are automatically reflected by the table view and the other way around. Moreover, it is possible to sort rows by column values and to execute manual search queries.

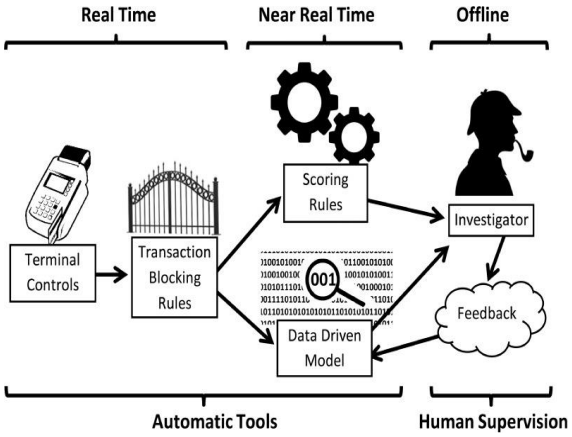
Temporal Views
Both views represent the temporal dimension of transactions. In both views, time is laid out on the x-axis, while the y-axis represents the total amount of money transacted per day. Thus, in A.1 (see Figure 4), each bar represents a day. Days that contain at least one suspicious transaction are highlighted in red. A.2 (see Figure 4) serves as an overview visualization of the inspected time period and as an interactive temporal filter.

Accounts Selector
Accounts Selector. When investigating more than one account, this view facilitates comparison and switching between accounts. The bar length represents the amount of transactions that each account executed, which already facilitates the selection of accounts of interest.
Event detection with visual analytics this used reduced the fraud in financial transaction. Before transactions are maintained the data. Using dynamic table data and account selector.



6. EVALUATION

To assess the usefulness of EVA, we conducted a qualitative evaluation which aimed to address the following research questions (RQ):
Comparison:



What are the advantages and disadvantages of EVA compared to the tools which users usually use. Comparison. The investigators stated that they typically use visualizations for presentation tasks which they typically generate with Microsoft Office tools (e.g., Excel and PowerPoint). Therefore, they argued that it is difficult to compare EVA with these tools.

Insights
What kind of insights can be generated with EVA. Insights In total we found 77 insights. Most of these insights were connection insights (53.2%). Coincidence insights contributed 26%. Curiosity insights (6.5%) and contradiction insights (9.1%) played a marginal role. Creative desperation insights also only showed up in 5.2% of the cases

Improvements
Do users miss any features or have suggestions for improvement. Improvements The investigators made useful suggestions for possible new features and improvements. One suggestion was to expand the filter and selection functionality. For example, all investigators noted that filter options especially for the table representation (e.g., only to show transactions with a certain amount) would be helpful. One expert highlighted that he would also like to directly select suspicious cases in the Time Panel by selecting bars instead of using the temporal filter.

. Data Analysis

The collected qualitative data were analyzed in order to find out what works well, what needs further improvement, and what are possible missing features (cf. research questions comparison and insights). However, we were also interested in which kinds of insights they gained with EVA while they solved the tasks (cf. insights). EVA supports processes of exploration and sense making. There are two well-known approaches explaining sense making with visualization - the model by Pirolli and Card [30] and Klein‘s sense making model. The model by Pirolli and Card has been criticized because it applies only to a very narrow range of activities of intelligence analysis, while Klein‘s model is much broader.

7. CONCLUSION

During the development of EVA we followed an iterative design over a period of 1.5 years in close collaboration with domain experts from a national bank. EVA follows the VA principles of interweaving intuitive interactive visualizations and analytical techniques in a seamless way. We evaluated EVA with real world data and could demonstrate that EVA was able to scale well even for extreme cases and to perform the required tasks in a suitable and appropriate way. Using EVA technique to reduce the fraud in financial transaction in credit cards. Implemented EVA methodology can easily reduce the fraud. Now day’s day by day increasing fraud in world wide. This technique used to reduce the fraud.

REFERENCES

[1] W. Aigner, S. Miksch, H. Schumann, and C. Tominski. Visualization of time-oriented data. Springer Science & Business Media, 2011.

[2] N. Andrienko and G. Andrienko. Exploratory Analysis of Spatial and Temporal Data: A Systematic Approach. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006. doi: 10.1007/3-540-31190-4 3

[3] M. Carminati, R. Caron, F. Maggi, I. Epifani, and S. Zanero. Banksealer: an online banking fraud analysis and decision support system. In IFIP International Information Security Conference

[4] W. S. Cleveland. Graphical methods for data presentation: Full scale breaks, dot charts, and multibased logging. The American Statistician, 38(4):270–280, 1984.

[5] W. N. Dilla and R. L. Raschke. Data visualization for fraud detection: Practice implications and a call for future research. International Journal of Accounting Information Systems,16:1–22,2015.