IMPLEMENTATION OF CREDIT CARD FRAUD DETECTION SYSTEM

Shilpashree.N, Swati Maurya, Mrs.K.S.Shwetha, Dr. Jitendranath Mungara
B.E Students, Department of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India
Asst. Professor, Department of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India
HOD, Department of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT: Credit card fraud detection is a relevant problem that draws attention of machine learning. In the fraud detection task, there are some peculiarities present, such as the unavoidable condition of a strong class imbalance, the existence of unlabelled transaction, and the large number of records that must be processed. The present paper aims to propose a methodology for automatic detection of fraudulent transactions that tackle all these problems. The methodology is based on Balanced Random Forest that can be used in supervised and semi-supervised scenarios through a co-training approach, which allows to compensate the class imbalance problem. In FDS, it has described the alert feedback interaction, which is a mechanism of providing recent supervised samples to train or update the classifiers. The main objective of FDS is to identify the fraud as soon as possible in order to take the necessary actions to revert it. Feedbacks play a central role in the proposed learning strategy.

KEYWORDS: Fraud Detection, Machine Learning, Random Forest, Semi-Supervised Learning, Class Imbalance.

INTRODUCTION:

Credit fraud is a term used to refer to the family of frauds which are perpetrated in credit industry. Card fraud begins either with the theft of the physical card or with the compromise of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction. The objective of the Credit Card Fraud Detection Systems is to extract transactions from dataset which contains all the transactions of each user and group the legal transaction pattern and fraudulent transaction pattern of each user. Analyze whether their coming transaction is matching more with legal transaction pattern or fraudulent transaction pattern.

Whenever a new product comes into the market the admin updates it in the database. The admin can also view all the products and also the customers. The admin has also provision to update the product stock and product rate. The user can buy any product which is provided in the website. The product will be delivered within three days. By this we can maintain the customer satisfaction**.** Every time when a customer buys products, his/her credit card details are verified to check the amount. Whenever a customer buys product, his credit card is verified each time to see only valid user buys the product. The users are allowed to change their personal details whenever it is necessary.

LITERATURE SURVEY:

Credit card is foremost well liked mode of payment. And nowadays fraudsters are increasing day by day. There are multiple approaches for fraud detection. To improve merchants risk management level in an automatic and effective way, building an accurate and easy handling credit card risk monitoring system is one of the key tasks for the merchant banks. Frauds are happened based on instance and incidents, but they are repeated offensives using some methods. The

traditional methods of fraud detection is based on simple comparisons, but also based on association, good based on time complexities and heterogeneous data bases, different syntax and needs domain experts. Our aim of this study is to identify the user model that best identifies the fraud cases.

TYPES OF FRAUD

Different types of fraud are credit card fraud, financial fraud, mortgage fraud, insurance fraud, telecommunication fraud.

Credit card fraud: This fraud is defined as the method of purchasing and marketing goods without having money. It is a small plastic card to provide the credit service to the customer. Nowadays credit card plays a important role in automated business and online money transaction area which is increasing every year. With the growth of usage of the credit card, fraudsters are finding more opportunities to commit the fraud which causes huge loss to cardholders and banks.

Credit card fraud is classified into two types:

• Offline credit card fraud:

This kind of fraud is done physically which means that the plastic card is stolen by fraudsters and using the card in stocks or supplies or stores or for different purposes as an actual owner. It is an unusual type of fraud because financial organizations will immediately block the card immediately when the card holders report about the theft.

• Online credit card fraud:

This kind of fraud is popular and it is very dangerous, the credit card's information is stolen by the fraudsters to be used in future online transactions by internet or by phone. This kind of fraud is also called as "cardholder not existing" fraud. The card holders can be obtained by the fraudsters through the skimming, phishing or credit card generators. There is another classification for credit card fraud they are application fraud and behavioral fraud. This classification is based on fraudster's strategy on compelling the fraud. Application fraud occurs when the user enters any wrong evidence and wrong details in to the presentation for opening a new credit card. Fraudsters may use other persons information to obtain credit cards or get their new credit cards by using false information with the intention of the never repaying the purchases. Behavioral fraud occurs when fraudsters obtain credit card holder details to use them later for sales which are made on a cardholder present basis.

SYSTEM DESIGN: Here we describe the main specialty and the operating condition of a real-world FDS. Fig 1 illustrates the five layers of control typically employed in an FDS:

1. The terminal.
2. The transaction-blocking rules.
3. The scoring rules.
4. The data-driven model(DDM) and
5. The investigators.

Layers from 1 to 4 are fully implementing automatic controls, while layer 5 is the only one requiring human intervention.

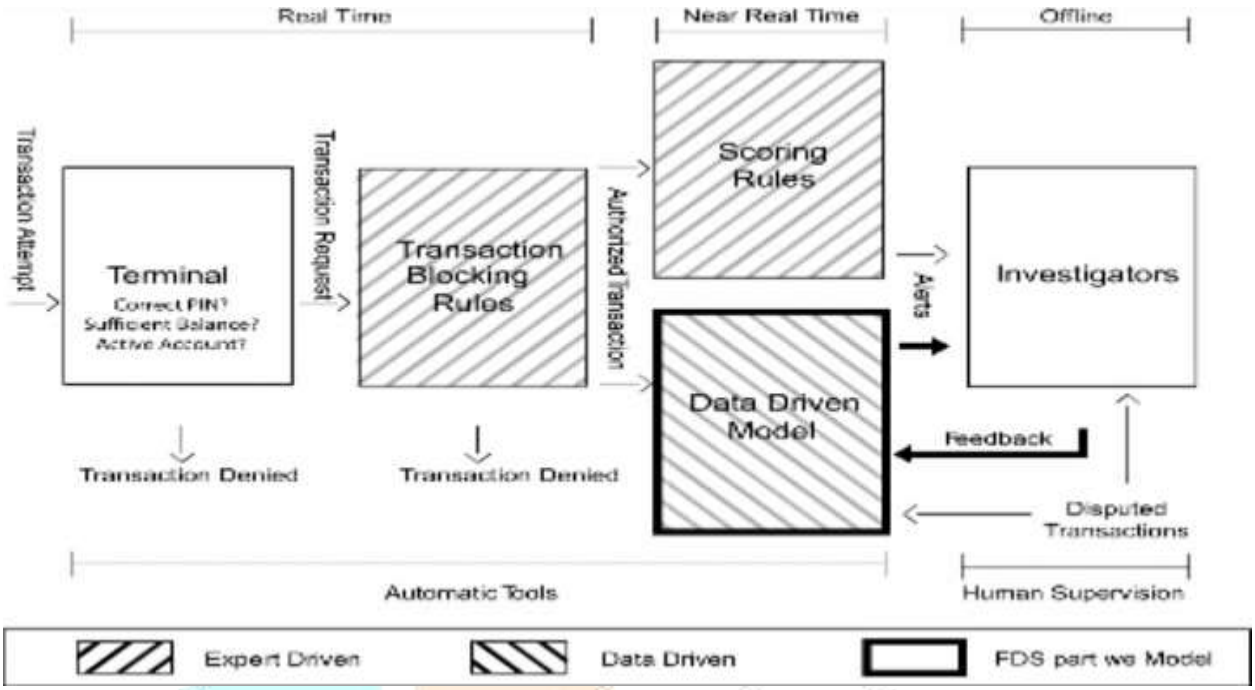

FIG 1: Illustrating the layers of control in FDS

A. Layers of controls in an FDS

1. Terminal: The first control layer is represented by terminal in an FDS which performs conventional security checks on all the payment request. Security checks include controlling the pin code, number of attempts, the card status (either active or blocked), the balance available and the expenditure limit. These controls are denied when the requests which do not pass any of these controls, while the others become transaction requests that are processed by the second layer of control.
2. Transaction-Blocking Rules: These rules are if-then (-else) statements which are meant to block transaction requests that are clearly perceived as fraud. When the payment is requested, these rules use the few information available without analyzing the historical records or card holder profile. These rules are manually designed by investigator and, as such, are expert-driven components of FDS. Blocking rule should be 1. Quick to compute and 2. Very precise, namely, should raise very few false alarms.
3. Scoring rules: Scoring rules are expressed as if-then (-else) statements and are also expert-driven model. However, these operate on vectors and assign a score to each authorized transaction: larger the score, more likely the transaction to be fraud. Scoring rules are designed by investigators which define their associated scores.
4. Data Driven Model (DDM): DDM is trained from a set of labeled transactions and cannot be interrupted or manually modified by investigators. An effective DDM is expected to detect fraudulent patterns by simultaneously analyzing multiple components of the feature vector, possibly throw non-linear expressions. Therefore, the DDM is expected to find frauds according to the rules that go beyond investigator and experience, and that do not necessarily correspond to interpretable rules.

5. Investigators: Investigators are responsible of the expert driven layers of the FDS and are professionals experienced in analyzing credit card transactions. Investigators design transaction-blocking and scoring rules.

B. Features Augmentation

Any transaction request is described by few variables such as the merchant ID, card holder ID, purchase amount, date, and time. All transaction requests passing the blocking rules are entered in a database containing all recent authorized transactions, where the feature- augmentation process starts. During feature augmentation, a specific set of aggregated features associated with each authorized transaction is computed, to provide additional information about the purchase and better discriminate frauds from genuine transactions.

Aggregated features are very informative as they, summarize the recent card holder activities. Thus, they allow to alert transactions that are not suspicious by themselves but might be unusual compared with shopping habits of card holder. This can be computationally expensive, and aggregated features are often pre-computed offline for each card holder on the basis of historical transactions. Aggregated features are stacked with the transaction data in the feature vector.

C. Supervised Information

Investigators' feedbacks are the most recent supervised information made available to the FDS, but only a small fraction of the transactions is processed every day.

There are two types of supervised information:
1) Feedbacks provided by investigators that are limited in number but refer to recent transactions and
2) Delayed supervised transactions, which are the vast majority for which the labels become available after several days (e.g., one month). This latter includes both disputed and non-disputed transactions.

D. System Update

Customers' spending behavior evolves and fraudsters continuously design new attacks, and thus their strategies also change over time. It is then necessary to constantly update the FDS to guarantee satisfactory performance. Expert-driven systems are regularly updated by investigators who add *ad hoc* (transaction-blocking or scoring) rules to counteract the onset of new fraudulent activities and remove those rules liable of too many false alerts.

RESULTS AND DISCUSSION:

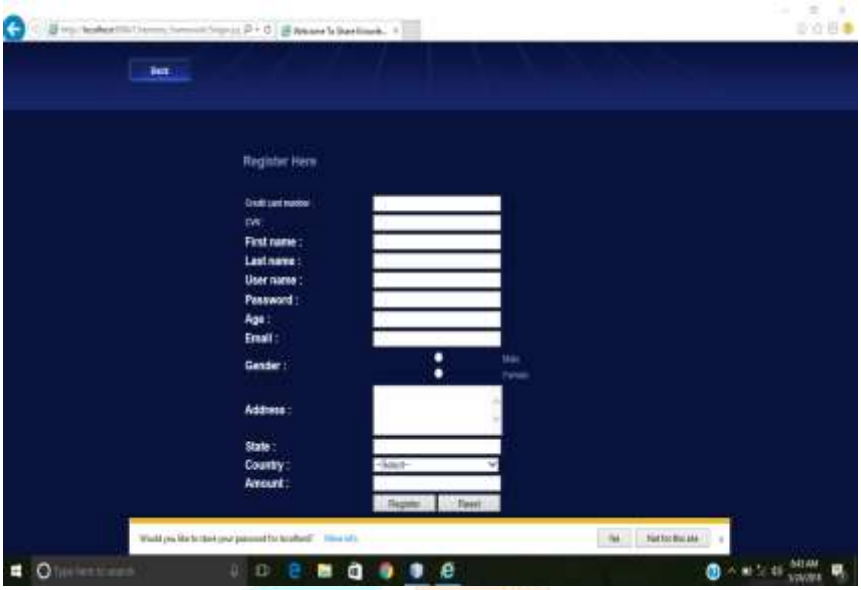

FIG 1: Screenshot of the Registration Page

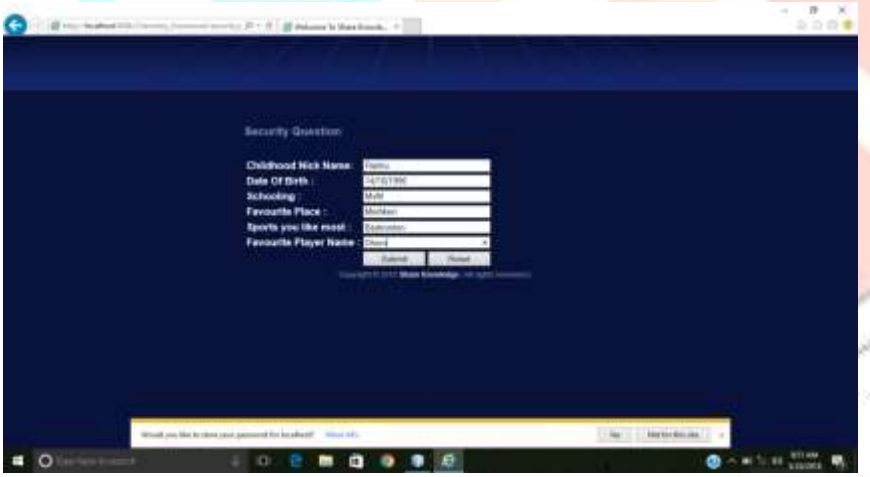

FIG 2: Screenshot of the Security Question Page

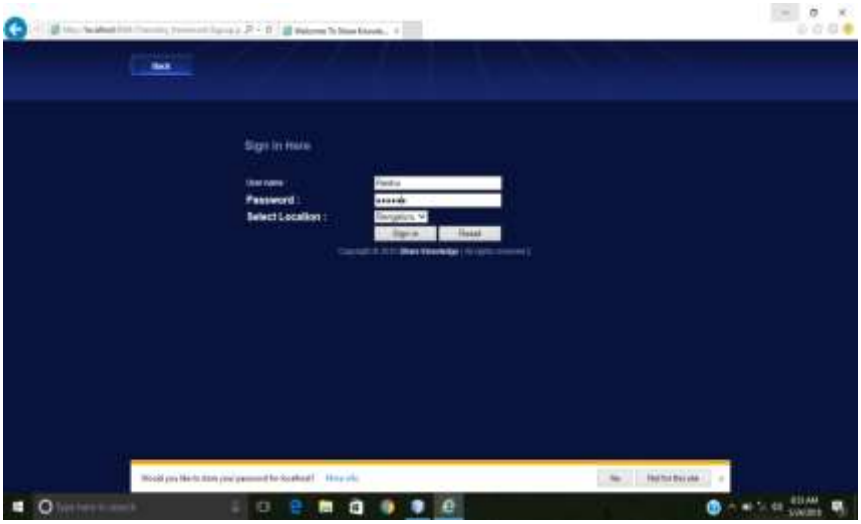

FIG 3: Screenshot of the Login Page

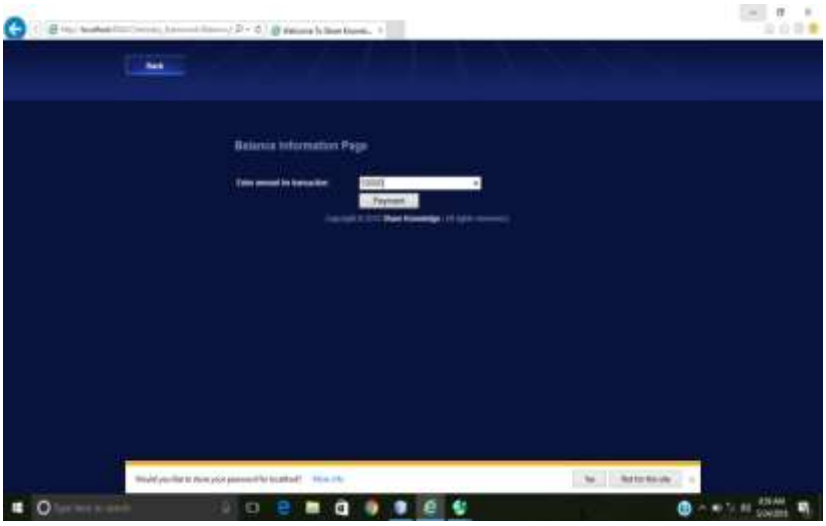

FIG 4: Screenshot of the Balance Information Page

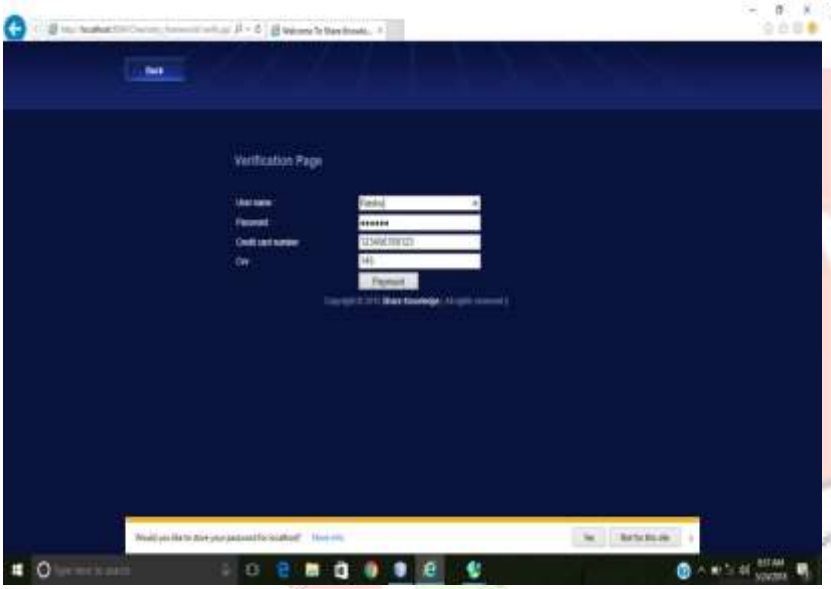

FIG 5: Screenshot of the Verification Page

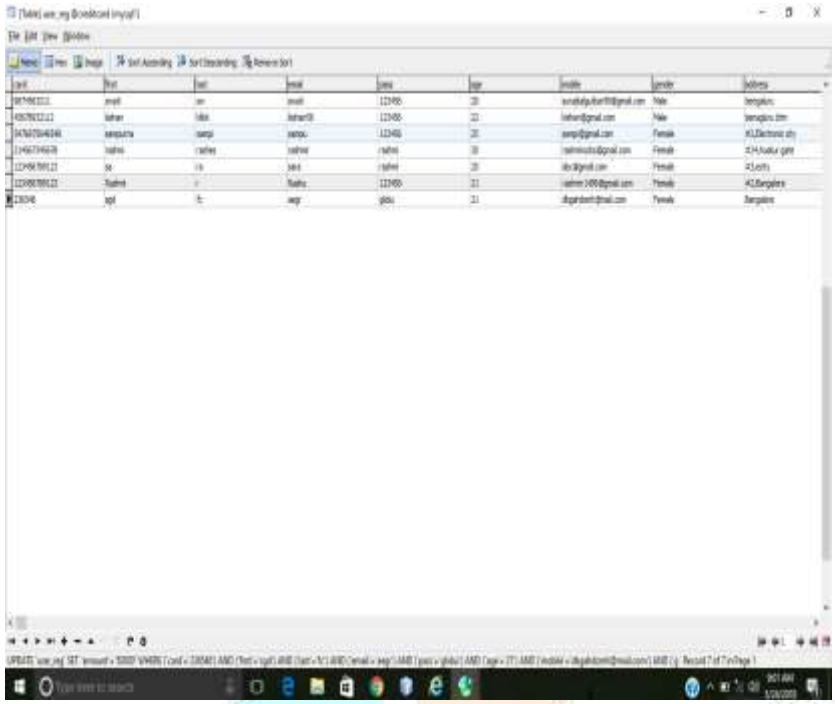

FIG 6: Database of Registration

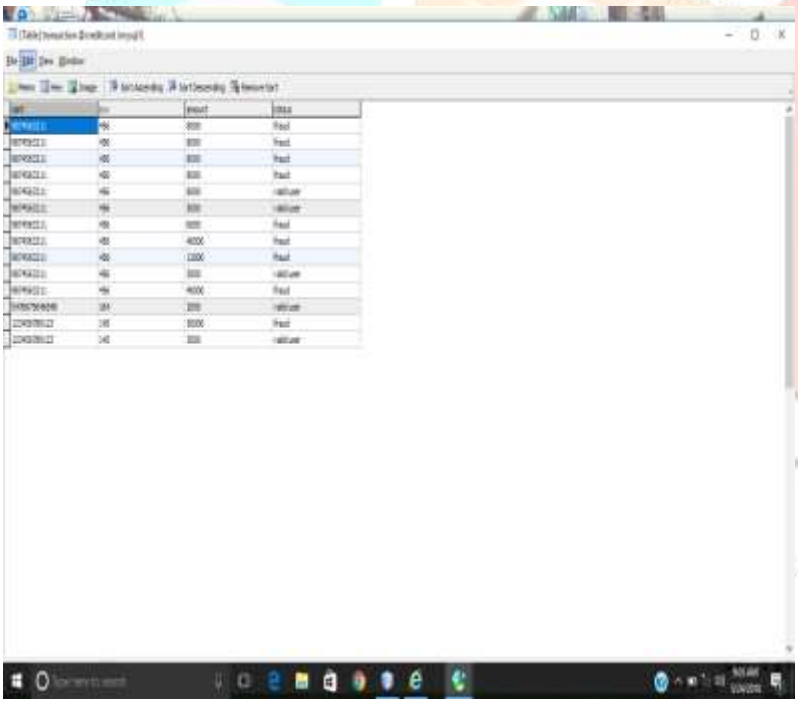

FIG 7: Database of Transaction

CONCLUSION

A fraud detection system for credit card transactions was presented. The system was designed to tackle the three challenges related with fraud detection data sets, namely a strong class imbalance, the inclusion of labeled and unlabeled samples, and the ability to process a large number of transactions.

The result showed that the proposed successfully overcome all the challenges. A BRF based on the Spark RF model was implemented, in order to compensate the class imbalance of the dataset and the unlabeled samples were used trough a co-training approach using the BRF model. Moreover, a proposed strategy based on a meta-classification approach that combines BRF and Co-Trained BRFs achieved the best

performance. All the different strategies evaluated were implemented guaranteeing the scalability of the proposed approach.

FUTURE WORK

Future work concerns the study of adaptive and possibly nonlinear aggregation methods for the classifiers trained on feedbacks and delayed supervised samples. We also expect to further increase the alert precision by implementing a *learning to rank* approach that would be specifically designed to replace the linear aggregation of the posterior probabilities.

Finally, a very promising research direction concerns semi-supervised learning methods for exploiting in the learning process of few recent unlabeled transactions.

REFERENCES

1. Mohammad Behdad, Luigi Barone, Mohammed Bennamoun, and Tim French. Nature-Inspired Techniques in the Context of Fraud Detection,IEEE TRANSACTIONS ON SYSTEMS,MAN,AND CYBERNETICS-PART C:APPLICATIONS AND REVIEWS,VOL.42,NO.6,NOVEMBER-2012.

2. Ayushi Agrawal,ShivKumar,Amit Kumar Mishra,M-Tech-Scholar, Department of Information Technology, Technocrats Institute of Technology, Bhopal, M.P..2015 IEEE.Implementation of Novel Approach for Credit card fraud detection.978-9-3805-4416-8/15/$31.00 2015 IEEE.

3. John O. Awoyemi, Department of Computer Science, Federal University of Technology, Nigeria, johntoba online Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis, **2017 IEEE.**

4. N.Malini, M.Phil student, PG & Research department of Computer Science, Dr.M.Pushpa, Assistant Professor PG & Research department of Computer Science, Quaid-E-Millath Government College For Women(A), Annasalai, Chennai, India."Analysis on credit card fraud identification techniques based on KNN and outlier detection",3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEEICB17).978-1-5090-5434-3c 2017 IEEE.

5. Dr.R.Jayabrabu Associate Professor,Dr.N.G.P.Institute of Technology,Coimbatore,India,Dr.V.Saravanan Professor and Dean, Dept of Computer Application, Dr.J.Jebamalar Tamil selvi, Associate Professor, Dept of Computer Application, Chennai, India. A Framework for Fraud Detection System using Intelligent Agent for better decision making process.

6. Aihua Shen: Rencheng Tong: Yaochen Deng."Application of Classification Models On Credit Card Fraud Detection" Service Systems and Service Management, International Conference on Volume,Issue,9-11 June page(s):1-4,2007.