

Implementation paper on Data Privacy and System Security for Banking and Financial Services

KOLPE YAMUNA, ARCHANA SUDGE, PRIYANKA JADHAV

BE Students, Department of Computer Engineering, HSBPVT'S Parikrama COE Kashti, Ahmednagar.

PROF. DUDHANDE V.N

Asst. Professor, Department of Computer Engineering, HSBPVT'S Parikrama COE Kashti, Ahmednagar.

Abstract

Now a day's online payment gaining popularity because of easy and convenience use of ecommerce. It became very easy mode of payment. People choose online payment and e-shopping; because of time convenience, transport convenience, etc. As the result of huge amount of e-commerce use, there is a vast increment in credit card fraud also. Machine Learning has been successfully applied to finance databases to automate analysis of huge volumes of complex data.

Keywords: Banking Application, Security, Cloud computing, data privacy, Transaction.

Introduction

The banking sector is a very important sector in our present day generation where almost every human has to deal with the bank either physically or online. In dealing with the banks, the customers and the banks face the chances of being trapped by fraudsters. Examples of fraud include insurance fraud, credit card fraud, accounting fraud, etc. Detection of fraudulent activity is thus critical to control these costs. Banks are an essential part of the Indian economy. While the primary responsibility for preventing frauds lies with banks themselves. Banks are dealing with public's money and hence it is imperative that employees should exercise due care and diligence in handling the transactions in banks. With an initial purpose of a mechanism behind crypto currencies, today the block chain technology has stepped far beyond just powering the bit coin or other transactions.

Related Work

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working on and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers. In this section, we briefly review the related work on Banking Security.

In this paper we propose to create a new set of Features based on analyzing the periodic behavior of the time of a transaction using the von Mises distribution. Using a real credit card fraud dataset provided by a large European card processing company, we compare state-of-the-art credit card fraud detection models, and evaluate how the different sets of features have an impact on the results. By including the proposed periodic features into the methods, the results show an average increase in savings of 13%. The aforementioned card processing company is currently incorporating the methodology proposed in this paper into their fraud detection system. [1]

In this paper we address a realistic fraud-detection setting and we show that investigator's feedbacks and delayed labels have to be handled separately. We design two FDSs on the basis of an ensemble and a sliding-window approach and we show that the winning strategy consists in training two separate classifiers (on feed backs and delayed labels, respectively), and then aggregating the outcomes. Experiments on large dataset of real-world transactions show that the alert precision, which is the primary concern of investigators, can be substantially improved by the proposed approach.. [2]

Individual Banks store vast amounts of user sensitive data on their private server. Sharing this data with other banks will provide an efficient way of offering their customers with personalized services and will deliver value-added data services to the entire banking sector. This data is highly sensitive and requires a secure sharing medium. We have described and implemented a Cloud based secure banking application framework that provides data integrity by encrypting the sensitive data during its transfer and storage, it also provides user authentication as only bank with valid access rights can access this data. This framework supports data destruction as data is destroyed when the application closes. As the data is kept in encrypted form we also provide security against semi trusted platform. [3]

Online banking is getting popularity due to location independence, 24/7 services and responsiveness. Financial services through the internet are running under various threats like phishing, pharming (cyber attack intended to redirect a website's traffic to another fake site), malware,

Man-In-The-Middle (MITM) attack and the evolving sophistication of compromise techniques. One time password (OTP) in online banking system alleviate the risk and make it secure. In this paper, we propose dynamic KYC based transaction authorization method to ensure secure and flawless financial access to the actual account holder of the online bank. Analysis and simulation results show that the proposed method provides equal control as existing OTP authorization minimizing some dynamic risk of being stolen and delay delivery of SMS. Our proposed method is costless and does not incur any hurdle to carry an additional hardware. [4]

In this document proposes a new comparative measure of the comparison rules that reasonably represents the profits and losses due to fraud detection. A cost-sensitive method based on the minimum Bayes risk is presented using the proposed cost measure. Improvements of up to 23% are obtained by comparing this method and other latest-generation algorithms. The data set for this document is based on the real-life transactional data of a large European company and personal data in the data is kept confidential. The accuracy of an algorithm is about 50%. The importance of this work was to find an algorithm and reduce the cost measurement. The result was 23% and the algorithm they found was the minimal risk of Bayes. [5]

In Nutan and Suman on review on credit card fraud detection they have supported the theory of what is credit card fraud, types of fraud like telecommunication, bankruptcy fraud etc. and how to detect it, in addition to it they have explained numerous algorithms and methods on how to detect fraud using Glass Algorithm, Bayesian, networks, Hidden Markova model, Decision Tree and 4 more. They have explained in detail about each algorithm and how this algorithm works along with mathematical explanation. Types of machine learning along with classifications have been studied. Pros and cons of each method are listed. [6]

In Several modern techniques based on sequence alignment, machine learning, artificial intelligence, genetic programming, data mining, etc. They have been developed and are still being developed to detect fraudulent credit card transactions. A solid and clear understanding of all these approaches is needed, which will undoubtedly lead to an efficient credit card fraud detection system. This document shows a survey of different techniques used in credit card fraud detection mechanisms and the evaluation of each methodology based on certain design criteria. An analysis of credit card fraud detection methods was performed. The survey in this document was based solely on detecting the efficiency and transparency of each method. The importance of this document was to conduct a survey to compare different credit card fraud detection algorithms to find the most appropriate algorithm to solve the problem. [7]

Problem Statement

Internet has become an important part of human’s life, a person can shop, invest, and perform all the banking task online. Almost, all the organizations have their own website,

where customer can perform all the task like shopping, they only have to provide their credit card details. Online banking and e-commerce organizations have been experiencing the increase in credit card transaction and other modes of on-line transaction. Due to this credit card fraud becomes a very popular issue for credit card.

Proposed Method

The proposed system overcomes the above mentioned issue in an efficient way. By using algorithm the fraud is detected and it produces an optimized result. The fraud is detected based on the customers behavior. A new classification problem which has a variable misclassification cost is introduced. Here the algorithms is made where a set of interval valued parameters are optimized.

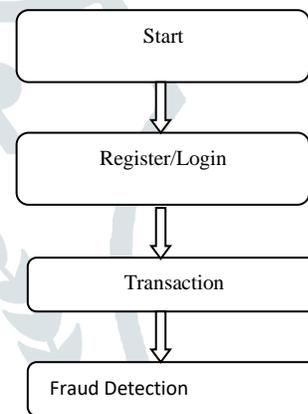


Fig.1 Flow diagram

Architecture

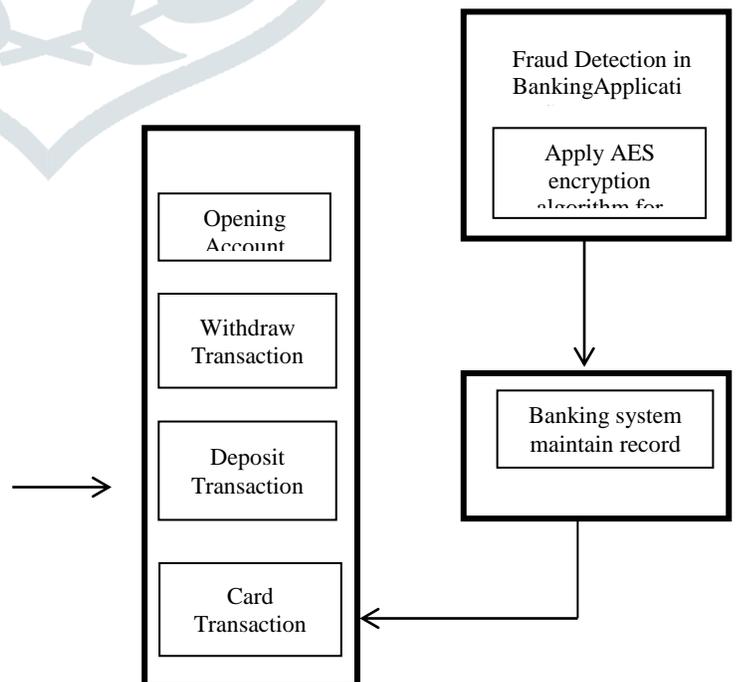


Fig.2 SystemArchitecture

Algorithm

Naive Bayes

Steps:

Given training dataset D which consists of documents belonging to different class say Class A and Class B

Calculate the prior probability of class A=number of objects of class A/total number of objects

Calculate the prior probability of class B=number of objects of class B/total number of objects

Find NI, the total no of frequency of each class

Na=the total no of frequency of class A

Nb=the total no of frequency of class B

Find conditional probability of keyword occurrence given a class:

$P(\text{value1/ClassA}) = \text{count}/n_i(A)$

$P(\text{value1/ClassB}) = \text{count}/n_i(B)$

$P(\text{value2/ClassA}) = \text{count}/n_i(A)$

$P(\text{value2/ClassB}) = \text{count}/n_i(B)$

.....

$P(\text{valuen/ClassB}) = \text{count}/n_i(B)$

Avoid zero frequency problems by applying uniform distribution

Classify Document C based on the probability $p(C/W)$

Find $P(A/W)=P(A)*P(\text{value 1/Class A}) * P(\text{value 2/Class A}) \dots\dots P(\text{value n /Class A})$

Find $P(B/W)=P(B)*P(\text{value 1/Class B}) * P(\text{value 2/Class B}) \dots\dots P(\text{value n /Class B})$

Assign document to class that has higher probability.

Conclusion

Fraud detection is a fascinating domain. From this survey, we analyse that it is the best compared to forecasting and classification. Various techniques are preferred in fraud detection, due to their high accuracy and detection rate.

Even so, researchers find it difficult to achieve greater accuracy and detection speed. In addition, organizations are interested in finding ways to reduce costs and increase profits; you can find and select the method of previous studies. Further, organizations are interested in finding methods that can reduce cost and increase the profit; they can find and select the method from above studies.

References

1. A. C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Detecting credit card fraud using periodic features," in Proc. 14th Int. Conf. Mach. Learn. Appl., Dec. 2015, pp. 208–213.
2. A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection and concept-drift adaptation with delayed supervised information," in Proc. Int. Joint Conf. Neural Netw., 2015, pp. 1–8.
3. Neha RaghobaParab , Louella M. MesquitaColaco, Fiona Coutinho , " Cloud Based Secure Banking Application ".
4. Prakash Chandra Mondal, Rupam Deb,2 and Mohammad Nurul Huda1 , " Transaction Authorization from Know Your Customer (KYC) Information in Online Banking "9th International Conference on Electrical and Computer Engineering 20-22 December, 2016, Dhaka, Bangladesh.
5. Jain R., Gour B., Dubey S., "A hybrid approach for credit card fraud detection using rough set and decision tree technique , " Year: 2016.
6. Bahnsen A.C., Stojanovic A., Aouada D., OtterstenB. , "Cost sensitive credit card fraud detection using Bayes minimum risk." Year: 2013.
7. Dermala N., Agrawal A.N., " Credit card fraud detection using SVM and Reduction of false alarms" Year: 2016.
8. Bilal Ahmad Sheikh, IIDr. P.Rajmohan, " Internet Banking, Security Models and Weakness", International Journal of Research in Management & Business Studies (IJRMBS 2015).
9. Sharaaf N. A., Haamid M.N., Samarawickrama S.S., Gunawardhane C.N., Kuragala K.R.S.C.B, DhishanDhammearatchi, "Improved E-Banking System With Advanced Encryption Standards And Security Models", INTERNATIONAL JOURNAL

OF SCIENTIFIC & TECHNOLOGY RESEARCH
VOLUME 5, ISSUE 10, OCTOBER 2016.

10. ShaliniSoni, Dr. Ravi Verma,” SURVEY PAPER ON ONLINE-BANKING”, International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 02, Issue 05; May - 2016 [ISSN: 2455-1457].
11. JanardanChoubey and BhaskarChoubey,” Secure User Authentication in Internet Banking: A Qualitative Survey” International Journal of Innovation, Management and Technology, Vol. 4, No. 2, April 2013.
12. Ms. Ritu, Ms. Renu,” Research on Online Transaction Protocols for Supporting Credit/ Debit Card Transaction” International Journal of Computer Science and Mobile Computing.
13. Karthik G Menon, MahimaBalan, M. Soumya Krishnan,” An Investigative Research on Fraud Analysis in Digital Banking” Jour of Adv Research in Dynamical & Control Systems, 11-Special Issue, July 2017.

