International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 3 Issue 09 September 2017
ISSN (Online): 2455-4723

A REVIEW ON ATM FRAUD DETECTION TECHNIQUE USING IMAGE PROCCESING IN MATLAB

Deepika Khatwa BM College of Science & Technology Indore M.P.*
Mr. Rahul Kaul BM College of Science & Technology Indore M.P
deepikakhatwa16@gmail.com* , rahulcsbmct@gmail.com**

ABSTRACT

We present a novel approach for detecting fraudulent behaviors from automated teller machine (ATM) usage data by analyzing geo-behavioral habits of the customers describe the use of a fuzzy rule-based system capable of classifying suspicious and non-suspicious transactions. We first compute the geographic entropies of ATM cardholders to form customer classes based on these entropies. ATM transactions are spatiotemporal by inclusion of location information. The transition data can be generated by using transaction data from the current location to the next one. Once, the transition data are generated, statistical outlier detection techniques can be utilized. On top of classical methods, we can easily use crisp unsupervised methods to detect outliers in the transition data. We analyze ATM usage dataset which contains around two years' worth of data, provided by a mid-size Turkish bank. We have shown that a significant bulk of ATM users does not leave the vicinity of their living places. We also present some insightful business rules that can be extracted from geo-tagged ATM transaction data by means of using a MATLAB.

Keywords: Location intelligence; fraud detection; ATM fraud; spatiotemporal outlier.

INTRODUCTION

Financial fraud detection and prevention have been receiving increasing attention in the past few years, due to the dramatic increase of losses because of fraud transactions every year. Ensuring the security of transactions carried out by banks and other financial institutions is one of the major factors affecting the reputation and profitability of such organizations. Fraud detection activities involve monitoring the behavior of transactions. Fraud prevention means a proactive approach that involves the analysis of transactions before they are completed and identifying if they are fraud

or not. Automated teller machines (ATMs), which have given the consumers a quality of life by allowing them to access cash and other financial information, occupy an important position in alternative delivery channels of banking. Since the introduction of the first ATM in 1967, perpetrators have been devising various ways to steal the cash inside the ATMs. According to European ATM Security Team's (EAST) report, card skimming, cash trapping and ATM malware incidents are generally increased worldwide. Besides, it is reported by Europol and EAST that, as the European Union (EU) bankingindustry migrates to the Europay, MasterCard and Visa (EMV) environment, losses caused by illegal domestic transactions in the EU have gradually decreased since 2008. However, at the same time, the level of illegal transactions overseas has seen a sharp increase. The United States of America remains the top location for such losses, followed by Indonesia and Thailand. In order to fight with this situation, a short term solution called GeoBlocking, was recommended by Europol and European Central Bank, which limits the possibility to misuse debit cards in regions without Chip and PIN verification. The implementation of GeoBlocking solution depends on static rules that are location based and this type of solution has been extremely positive from a security point of view. Since the main issue with ATM fraud is misusage of card information, the problem of determining the authenticity of card usage becomes the central point.

Fig: Credit Card Fraud Detection

LITERATURE SURVEY:

Aburrous M., Hossain M.A., Dahal K., Thabtah F.(1),Detecting and identifying any phishing websites in real-time, particularly for e-banking, is really a complex and dynamic problem involving many factors and criteria. Because of the subjective considerations and the ambiguities involved in the detection, fuzzy data mining techniques can be an effective

tool in assessing and identifying phishing websites for e-banking since it offers a more natural way of dealing with quality factors rather than exact values. In this paper, we present novel approach to overcome the 'fuzziness' in the e-banking phishing website assessment and propose an intelligent resilient and effective model for detecting e-banking phishing websites. The proposed model is based on fuzzy logic combined with data mining algorithms to characterize the e-banking phishing website factors and to investigate its techniques by classifying the phishing types and defining six e-banking phishing website attack criteria's with a layer structure.

Bentley P. J., Kim J., Jung G., Choi J.(2), Due to a rapid advancement in the electronic commerce technology, the payment method varies from cash to electronic settlement such as credit card, mobile payment and mobile application card. Therefore, financial fraud is increasing notably for a purpose of personal gain. In response, financial companies are building the FDS (Fraud Detection System) to protect consumers from fraudulent transactions. The one of the goals of FDS is identifying the fraudulent transaction with high accuracy by analyzing transaction data and personal information in real-time. Data mining techniques are providing great aid in financial accounting fraud detection, so it have been applied most extensively to provide primary solutions to the problems. In this paper, we try to provide an overview of the research on data mining based fraud detection. Also, we classify researches under few criteria such as data set, data mining algorithm and viewpoint of research.

BEZDEK, James C.; EHRLICH, Robert; FULL, William. FCM: Image Segmentation is one of the important areas of image processing. It helps in getting more focused analysis of targeted area in image. It can be done using many algorithms. FCM is one of the algorithm and is based on clustering method. FCM algorithm is popularized with a lot of modifications. In this paper, we will see the modifications in FCM algorithms.

Shrutanjay Kulkarni, SanketMurkute, PrateekNangare, ATM card fraud was causing many losses for the card payment industry. Now a days most accepted payment mode is Debit card for both online and also for regular purchasing; hence frauds related with it are also growing. To find the fraudulent transaction, we

implement an Advanced Security Model for ATM payment using Hidden Markov Model (HMM), which finds the fraud by using customers behavior. This Security Model is primarily focusing on the normal spending behavior of a cardholder and some advanced securities such as Location, how much money we takes from machine, Time and Sequence of transactions. If the trained Security model identifies any misbehavior in upcoming transaction, then that transaction is permanently blocked until the user enter High Security Alert Password (HSAP).

Pankaj Richhariya Dr. Prashant K Singh,Owing to levitate and rapid escalation of E-Commerce, cases of financial fraud allied with it are also intensifying and which results in trouncing of billions of dollars worldwide each year. Fraud detection involves scrutinizing the behavior of populations of users in order to ballpark figure, detect, or steer clear of objectionable behavior: Undesirable behavior is a extensive term including delinquency: swindle, infringement, and account evasion. Factually, swindle transactions are speckled with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately.

BACKGROUND

A.ATM (Automatic Teller Machine)

It is a computerized machine built over efficienttelecommunication system which enables financial institution along with the combination of financial transactions in a public domain which is primarily responsible for the cash dispense procedure as well as checking of account balance etc .This machines possess different structures in different nations worldwide. USA during 1969 witnessed the first ATM. They contribute nominally towards the positive currency growthwhich do not have a very robust effect. ATMs are considered to be more profitable bank service as it is a prime attraction for most of the non-bank customers. Its main structure comprises of a Central Processing Unit, a Pin pad, Secure Cryptographic processor, magnetic chip card, vault and the function keys.

B. Threats in ATM

Generally ATM frauds can be categorized into 3 main categories: Logical attacks, frauds related to cards and currency and physical attacks. However the crimes and threats corresponds to.

- Personal identification number threats

- Electronic data interception
- Fraudulent electronic transactions
- Theft of money.
- Burglary and vandalism in ATMs
- Multiple access and Physical attacks

RELATED WORKS

Over the recent years human being detection in video surveillance systems is fairly gaining popularity due to its wide range of applications that involves vital processes like detectingabnormal events, characterization of gaits in humans, to countindividuals in crowds, identifying people, classifications based on gender, detection of fall for the elderly people etc. Generally the various scenes that are a result of the video surveillance system is composed of very low resolution. However static camera captures scenes with minimum change in the background scenarios wherein the outdoor surveillance has to detect object that are in a larger scope. Some of the existing systems depend upon the human observers which would perform real time activity detection which leads to limitations like the difficulty related to simultaneous monitoring in the displays of the surveillance systems. This calls for an automation of the video surveillance for analysis of human motion and has creates a research attraction on the field of pattern recognition and computer vision. The entire process comprises of 2 primary processes: Object detection and classification. The former can be carried out by processes like background subtraction, optical flow followed by spatiotemporal filtering. The first process, background subtraction is extremely popular for detection of objects where pixel by pixel or block by block fashion is considered to find the difference between the background and the current frame while detecting moving objects.

Most of the Bank ATM Card Skimming is when the criminals electronically "skim" the Magnetic Stripe which is behind the card in order to steal card details and PIN during ATM transactions. This is done by fitting unseen/unrecognized portable electronic as described aforementioned by using devices on the ATM like portable electronic card reader and mini camera. By capturing data they can easily do the following as suggested in:-

• Potentially clone debit!credit! ATM cards

• Capture the Personal Identification Number (PIN)

• Use the combined information to withdraw funds from accounts.

CONCLUSION

To serve the research goal of detecting ATM Card, various image processing techniques have been applied Texture Segmentation method. To summarize, the proposed algorithm initiated the procedure by aligning the base image with the target image, segment the ROI, perform morphology closingWe introduced a methodology for using a Segment image to detect fraudulent ATM transactions based on location information and derived transition data (such as speed). We showed that coupling entropy values with movement related data can yield valuable information to prevent frauds.

REFERENCES

[1] Aburrous M., Hossain M.A., Dahal K., Thabtah F., "Intelligent Phishing Detection System for E-Banking Using Fuzzy Data Mining", Expert Systems with Applications, 37 (2010), 7913-7921

[2] Bentley P. J., Kim J., Jung G., Choi J., "Fuzzy Darwinian Detection of Credit Card Fraud", Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society, http://www.researchgate.net/publication/228971658

[3] BEZDEK, James C.; EHRLICH, Robert; FULL, William. FCM: The fuzzy C-Means clustering algorithm. *Computers & Geosciences*, 1984, 10.2: 191-203.

[4] Demiriz, A., Ekizoglu, B..Using Location Aware Business Rules for Preventing Retail Banking Frauds.To be published in the Proceedings of First International Conference on Anti-Cybercrime (ICACC-2015) 10- 12 November 2015 - Riyadh, Saudi Arabia.

[5] M. E. Edge and P. R. F. Sampaio, “The design of FFML: A rule-based policy modelling language for proactive fraud management in financial data streams,” Expert Systems with Applications, vol. 39, no. 11, pp. 9966 – 9985, 2012.

[6] Singh, K. ,Choube, Y. , and Goel, " A Proposed Framework to Prevent Financial Fraud through ATM Card Cloning", World Congress on Engineering, vol. 1, July 2011.

[7] Mandai, Ghosh, Alarn, S.S. and Chandra, "The White E Wallet Technology Enabled Money", International Journal of

Advanced Research in Computer Science and Software Engineering, vol. 4, no. 3, March 2014.

[8] Upendar, and Rao, E. , (2013) "An overview of plastic card frauds and solutions for avoiding fraudster transactions", International Journal of Research in Engineering and Technology, vol. 02, no. 08, August 2013.

[9] Meshram, L. , and Yenganti, P. T., "Credit and ATM Card Fraud Prevention Using Cryptographic Algorithm", International Journal of Advanced Researh in Computer Science and Software Engineering, vol. 3, no. 8, August 2013.

[10] Estevez P. A., Held C. M., Perez C. A., "Subscription Fraud Preventionin Telecommunications Using Fuzzy Rules and Neural Networks", Expert Systems with Applications, 31 (2006), 337-344

[11] European ATM Security Team (EAST), "European Fraud Update 3- 2014" https://www.european-atm-security.eu/east-publishes-europeanfraud- update-3-2014/

[12] Europol, Situation Report, "Payment Card Fraud in the European Union", Perspective of Law Enforcement Agencies, 2012 https://www.europol.europa.eu/content/situation-report-payment-cardfraud-european-union.