Fraud detection and mitigation in secure e-payment transaction.

Mrs.T.K.George, Dr.(Prof)Paulose Jacob

Abstract: Fraudulent entries in the e-payment are quite common in most of the e-commerce transaction. In most of the E-commerce transaction, prevention and detection of fraudulent entries are given much importance as part of risk management strategies. There should be an appropriate technique or procedure to detect and respond to fraudulent entries. In order to detect fraudulent entries, the behavioral pattern of the fraudsters is to be monitored and controlled. Well-structured detective and preventive measures can mitigate the frauds in e-payment transaction and can increase the reliability of e-transaction.

Keywords: Fraud, prevention, detection, e-commerce, mitigation, fraudulent entries.

1 Introduction

The increase in e-transaction and utilization of internet technology has in turn force the customers to face number of risk to personal information and breach of security policies. One of the major problems in the E-Payment system is the management of fraudulent entries [1]. As there is high demand and user preference from e-transaction, the chance of new fraudulent methods trying out by the fraudsters are also increasing in a tremendous speed. One of the research study reported that, every year there are millions of consumer complaints related to fraud [2], and some of the merchants lost almost 1.0% of their online revenue due to fraudulent entries. Since e-payment fraud is a global issue, which has to be tackled with a correct measures globally. Strategic risk is function, which is assessed by comparing it with the current business strategy and the resources deployed to achieve this goal. It includes all the related hardware and software facilities and its impacts in the business transaction. In the Internet, the fraudsters can be anonymous, by hiding their actual identity. e-payment fraud gives lots of negative impact to the economy and it is badly affecting the confidence level of customers[3].

2 Fraudulent entries in e-payment

The e-payment fraud can be categorized into Online and offline frauds. Stealing and miss-using, the important credentials such as personal identification number and credit card details are generally falls under the category of online frauds. Phishing and spoofing attacks are also considered as the serious cases of online fraud. Some of the common examples of off-line frauds are phone solicitation and mail frauds [4]. Detecting fraud seems to be very difficult because of its sophistication. Preventing the fraud on time is next to impossible, while comparing the growth rate of transaction in every year. Gaining illegal entry and hijacking the important credentials from the customers computer by account hacking and Identity theft and later misusing this sensitive information for a credit transfer seems to be dangerous unless it is managed with due importance. In one of the fraud management approaches, reports that in a linear fraud management Life cycle there are eight different phases, such as Deterrence, Prevention, Detection, Mitigation, Analysis, Policy setting, Investigation and Prosecution, which are directly associated with Information Technology[5].

3 Limitations in the existing fraud management:

In the old method of using a transaction monitoring process for fraud management ,by making use of internally developed software with manual intervention will be effective in small real time system within a local network, but within a bigger system with a global application will be difficult to manage as a whole ,since the fraud management process itself is fragmented and are viewed as separate activities[6]. The major authentication issue faced by the traditional system with a PIN & a password is lack of security, but most of the higher end e-payment transaction, it has been addressed by making use of biometric technology (using finger print)[7].

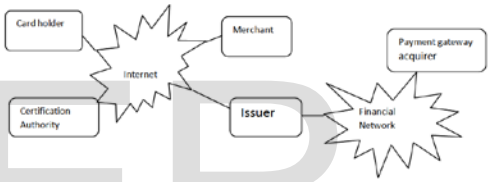


Fig 1 System Architecture for Electronic Payment (ATM)

4 Risk management process in banking transaction

Risk identification and risk control are the two important areas to be focused on .Deploying appropriate technology is the responsibility of the bank. With the support of an effective strategy, the bank can identify measure and control the risk involved in the transactions and provide the required security measures to conduct secure transaction. Risk in e-payment will affect the earning capabilities of the consumers and the bank and unable to extend the services to the right customers [8]. To control the risk most of the banks are getting technological support such as use of biometrics for authentication process.

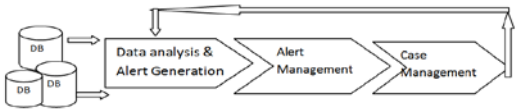


Fig 2: General fraud management approaches in the organization

In order to reduce the risk and to mitigate the loss of revenue, most of the financial institutions or banks are concentrating on the following major areas, during the electronic
Transactions [9]:

- Detecting unknown pattern for financial fraud
- Keep track of new fraud scheme
- Unsure about the exactly what to look for

To reduce the fraudulent entries and controls and reduce the risk, there are many approaches available, which can be implemented based on the type of e-transactions. But some approaches are suitable only for particular patterns as mentioned below[10]:

- Known pattern : Set up rules to filter fraudulent transaction is suitable .

- Unknown pattern: Anomaly detection is suitable
- Complex pattern: Advanced Analytics are Suitable
- Associate link pattern :Social Network Analysis is Suitable

Generally to deal with the fraudulent entries, it is ideal to go for a hybrid (combinational) approach, which can effectively support the fraud management system.

5 Proactive Rule-based Fraud management

In this approach as mentioned in the Figure: 3, there are many software components available which are connected with a strong Relational database [11]. The modules which support the effective handling of fraudulent entries are:

- Web interface for adding and configuring rules(WIAC):Main activity is adding, deleting and modifying rules and for changing configuration parameters.
- Run-time module(RM):It has the ability to generate, manage and implement rules according to the requirement.
- Fraud reporting module (FRM):It has the facility for generating various reports, which may be printed on the screen or SMS to mobile phones of responsible people.

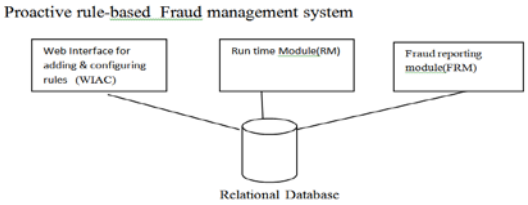


Fig3: Rule-based Fraud management

6 Run time Fraud Management Module.

The ideal solution for fraud management is use all possible combination of technologies rather than using a single tool and validate it with all possible policies and procedures then based on the outcome and the business requirement adopt the best possible option[12].

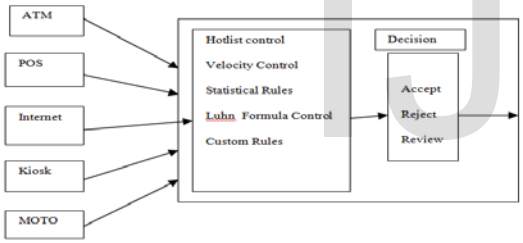


Fig4 :Run time Fraud Management Module

7 Factors Influencing the Fraud Prevention strategies:

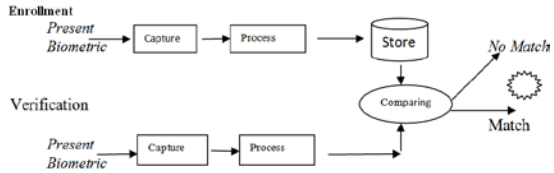
One of the major areas to be concentrated on is improved authentication systems, which can play a significant role in e-payment fraud prevention. There should be an additional security measure is required to confirm the user identity, rather than using common pass word identities [13]. The traditional ,way of authenticating the usernames and passwords are not going to be effective in the modern system ,which require an advanced technology support such as , biometric technology to provide a better authentication procedure and to improve the security]. As per the literature survey some of the existing Fraud Prevention Measures are usually focused on Biometric Authentication, Fraud Prevention Software, One Time Passwords, Smart Card Authentication, and Multi-Layer Passwords [14].

8 The major strategic factors for Fraud Prevention in e-payment can be:

- Communication & Timely access to information to empower management decision making [13].
- Mitigation of consumer vulnerability to fraud by providing adequate Consumer Education and awareness of Socio-Economic climate
- Engaging Consultants/Specialists.
- Organization learning for fraud prevention, include adaptive Policies and Controls
- Use of specialist third parties for online transactions to enhance confidentiality.

9 Biometrics Concepts:

It is an enabling technology with the potential of recognizing people based on their Physical and behavioral characteristic to reduce fraud. It has the important characteristics such as Uniqueness, Universality, permanence, collectability, performance and Acceptability. It is convenient and more accurate than the traditional system for positive authentication. Biometric process are fast and easy to process Dealing with this type of technology is gives less of burden to its users [12]. Most of the physical biometrics is grouped based on Finger print recognition, Facial recognition, Iris recognition, Vascular Patterns (by analyzing vein patterns) and Retinal Scan. The behavioral biometrics is using the features such as Speaker Recognition (vocal behavior Analysis) and Signature- (signature dynamics analysis). Biometric devices are equipped with a scanning device & software to deal with it along with a strong database to record the details. Authentication is done by comparing the stored details with the newly captured biometric samples. There are two major steps such as Enrollment and Verification have to perform, In order to complete the authentication procedure. The following diagram gives the details about the steps. Authentication is performed based on the matching values found during the comparison. The adoption of the effective authentication process can be finalized in the e-payment, based on the output derived from various biometric technologies in terms of their characteristics [15].



One of the most common fraudulent entries in e-Payment transaction is ATM skimming .Due to this issue there is a huge revenue loss occur, even after supporting with lots of counter measures. There should be appropriate validation checking using a technological tool, by the ATM providers as part of security measure [14]. Other major areas to be focused on are Credit card payment and e-cash Internet payment system, which are also prone to malware vulnerabilities.

10 Tools for Fraud Prevention and detection:

There is a requirement of sophisticated and intelligent tool for e-payment transaction as there is a high volume of data transactions taking place in every day with huge change in the behaviours of customers and fraudsters and non-uniform distribution of fraudulent data within the transaction. Some of the tools can be focused on the behaviour patterns of the users and others on transaction process and reporting techniques. Most of the cases these tools can be e used for reporting the fraudulent entries, since the prevention is merely impossible with a simple tool. One of the research studies indicate that an intelligent tool based on fuzzy logic can support the user behaviours, which can proactively mitigate the fraud. There is Address verification Service (AVS), developed to help MOTO merchants to reduce the fraud by verifying numeric field of the address given by the consumer, but these types of verification was possible only in some region [16]. One of the effective fraud prevention tools was the Risk scoring .This model is based on the statistical data from card holders current data compared it with the historical data, by comparing against dozens of fraud indicators available in the system.

11 Security measures for Fraud detection.

In order to detect Frauds in the e-payment, appropriate security measures can be implemented by monitoring the possible threats during the e-transaction. Universal Payment Identification Code (UPIC) and Auto Clearing House (ACH) are the known fraud detection tools. Address Verification Services (AVS), card verification Code (CVC) are known for checking the validity of data. According to Cyber Source [17][18], proper authentication can be done and the server details can be verified by using an IP Address locator. To

support the e-payment procedures there should be an appropriate implementation of Secure Socket layer (SSL) and Secured Electronic Transaction (SET).Secured connection can be provided by SSL with the support of a strong RSA algorithm [19] . Web based security solution are available, which can analyzes suspicious behavior and provide a detailed report on security and risk mitigation procedures. This type of solution can give an indication on threat before it turns out to be a fraud. The users can focus on, Phishing detection, Audit trail, Proactive prevention and detailed log analysis. In general, using an effective fraud management tool, it is possible to accurately consider different incidents from different areas of transaction management, and gives a structured outlook to deal with those fraudulent entries as per the business requirements on time. Anti-fraud software modules are required to automate processes if it is possible, and adapt to the changing patterns fraudulent entries and behaviour of the customers.

12 Findings and Recommendations:

- By analyzing various studies conducted by researchers, it has been proved that biometric technology can contribute significantly to decrease e-banking fraud and biometric ATM has already been deployed in some banks. But due to cost of implementing this technology, it seems to be a rare option for many banks[20]
- Keystroke dynamics, a behavioral biometric, is another option for better security. Keystroke dynamic can analyze the way a user type at a terminal and identify them based on habitual rhythm patterns.
- Administrative support has been identified a Critical success factors for Fraud prevention ,because to implement security measures such as encryption and One time password wouldn't be possible without the guidance and support from Top management. Emphasis must be given to consumer education to protect their personal information and to prevent consumer vulnerability e-payment card fraud.
- An effective defense mechanism for fraud is that there should be a strict internal control by the employees of the banks, and they should not exploit the break downs in internal controls.
- There should be internal audits to ensure whether the policies are set and followed p with due importance. One of the research studies indicates that the business organizations with internal audit procedures are more effective in detecting and reporting fraud than those that don't have internal audit procedures.
- One of the research studies [21] reports that it is very important to protect customer data by using encryption and he suggest that introduction of hybrid cryptosystem can be a better option for both encryption and decryption processes.

13 Conclusion:

One of the important goals in the e-payment system is to mitigate the fraudulent entries and ensure the better security. There are different strategies and technological support is required to achieve this objective. Recent years there is huge increase in the number of on line shoppers and the digital transactions, in proportion to this increase of e-payment, new fraudulent and sophisticated techniques are being developed by the fraudster are also in progress. There should be an appropriate preventive or detection measure to mitigate the fraudulent entries in E-transaction. The research analysis indicates that most of the fraud detection techniques are trying to maximize accuracy rate and minimize frauds at a minimum cost[22]. There should be an ongoing research to give relevant support to reduce risk and protect the entire system of e-payment .It is not an easy job to detect the fraud in real-time transaction. There is no single tool can Identify all type of fraudulent entries. But if there is a combination of strategically designed policies and strong technological support and right kind of fraud management can provide an ideal support for Fraud mitigation. Fraud prevention and detection techniques have to be proactive and always be ready to mitigate fraudulent entries in the e-payment system [23]. It is the need of the hour to develop a mechanism with the combination of different techniques and strategies to mitigate the occurrence of fraudulent entries in the e-transaction by which the revenue loss can be controlled.

Author 1: Mrs.T.K.George
Research scholar, Department of computer science
Cochin University of Science & Technology
Susan@hct.edu.om

Author 2 : Dr.(Prof)Paulose Jacob
Professor, Dept.of Computer Science
Cochin University of Science & Technology
kpj0101@gmail.com

References

[1] Manning, R. (1998); "Electronic Commerce on the Internet" in Olumide, S. A and Falaki, S. O (2001): Electronic Commerce – Promises, Treats, Trust and payment Systems.

[2] Consumer Sentinel Network Data Book for January-December 2011, *Federal Trade Commission*, http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf CyberSource (2012), :

[3]Commission of European Committee (2008) Report, *"Fraud on non-cash means of payment in EU, Brussels"*.

[4].www.cybersource/product_and_sevices/fraud_management/ DOJ (2001),Former Cisco Systems, Inc.

[5].http://definitions.uslegal.com/c/computer-crime/ Graycar, A & Smith, R (2002), *"Identifying and Responding to Electronic Fraud Risks"*, Australian Institute of Criminology.

[6]. Nelsestuen, Rodney. TowerGroup. *Surrounded by the Enemy: The Case for Enterprise Fraud Management*.

[7]. Jain, A., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. Pattern Analysis and Machine Intelligence.

[8]. Nelsestuen, Rodney. TowerGroup. *Surrounded by the Enemy: The Case for Enterprise Fraud Management*.

[9].McAfee Report (2012) *" Financial Fraud and Internet Banking: Threats and countermeasures"*, By François Paget, http://www.mcafee.com/in/resources/reports/rp-financial-fraud-int-banking.pdf.

[10].Cahill M. H., Lambert D., Pinheiro J. C., Sun D. X. (2000), .Detecting fraud in the real world., Handbook of Massive Datasets, Kluwer Academic Publishers.

[11].Bergman B. (2005), ISRN: LITH-IDA-EX-05/029-SE, *"E-fraud – State of art and countermeasures"*

[12].Revett, K. (2009). A Bioinformatics Based Approach to user Authentication via Keystroke Dynamics, International Journal of Control, Automation, and Systems.

[13]. Kim, Rachel and Monahan, Mary. Javelin Strategy and Research. *2008 Identity Fraud Survey Report.*

[14]. Chan K. Philip, Fan W., Prodromidis A., and Stolfo S. (1999), .Distributed data mining in credit card fraud detection.

[15]. Monrose, F., and Rubin, AD., (1999), 'Keystroke Dynamic as a biometric authentication'.

[16]. Hosseini, S., Mohammadi, S. (2012). Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System.

[17].Innoypay (2010) *"Online payment r 2010"* report on the current state of affairs in the global landscape of Internet payments by Wijnand Jongen.

[18].Association for Financial Professionals(AFP) 2011, 2012, *Payments Fraud and Control Survey Report* by J.P. Morgan, San Diego, USA.

[19]. Murdoch, S. & Anderson, R. (2010), "Verified by Visa and MasterCard SecureCode: Or, How Not to
Design Authentication," In Financial Cryptography and Data Security.

[20]. Zhang Jian, “Analyzes based on the SET agreement electronic commerce safety mechanism”, Netinfo
Security.
[21]. Bleha, S., Slivinsky, C., Hussain, B.(1990). “Computer-Access Security Systems Using Keystroke

[22]. Cao Juan, “The electronic commerce security architecture and the safety technology apply”, Net Security
Technologies and Application.
[23]. Jain, A., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. Pattern Analysis and Machine Intelligence.