



FRAUD ANALYSIS AND PREVENTION OF E- BUSINESS

Neha Banu* Rasika Sv**

Student, Mount Carmel College (Affiliated to Bangalore University), Bangalore.

Student, Mount Carmel College (Affiliated to Bangalore University), Bangalore.

Abstract

The magnitude of electronic business transaction has raised outstandingly in last few decades, mainly due to mass market appeal of electronic business retailers. Due to which there is increase in fraud cases, which relates in resulting of losses each year throughout the world. Therefore it is mandatory to develop and apply new prevention techniques that can accommodate in detecting the fraud and fraud prevention. The main ultimate aim is to identify and prevent the fraud occurrence in electronic transaction, more precisely in various forms (credit card and paytm, Google pay) operation performed by electronically. In order to judge the various techniques which used to analyze the fraud occurrences. Another area of fraud happening in the e- business transaction is basically on the seller side which is popularly known as merchant fraud. This paper is intensively the implication towards the framework to detect such fraudulent seller and the buyer with the help of various prevention techniques.

Keywords: E-Commerce, Fraud Detection, Techniques, E-Business, E- Payments.

Introduction

Recently we have remarked impressively increase in the volume of electronic business Transaction mainly due to the familiarized of World Wide Web and electronic transaction or Business as online retailers. (E.g. Amazon, flipchart,). It also indicate that they is a huge Increase in the number of online frauds, which in turn results in million dollars of losses each Year the countries suffered worldwide. Therefore it is important and necessary to developed And apply the techniques that will help to assist in fraud detection. Fraud in electronic business transaction comes in numerous distinct flavors that is it first Involves unauthorized purchases. Most storefront provides their customers with a mean of Storing personal information such as purchase history and delivery details. Hackers who gain Contact to these accounts can hijack them to net some unrestricted material

Further more, many fraud detection problems which occurs in huge amount of data loss. For Cases like credit card Company in UK has loss of 350 billion, the processing of these datasets Looking for fraudulent operation requires fast and efficient techniques. Thus, safeguarding and protecting all the electronic data is a very important task to all the Retailer and traders. Keeping all the customer data, business data safe from hacking is very important so that there is no outflow of confidential data. This study is conducted to understand the type of frauds and better ways to prevent these Frauds.

Statement of the Problem

In recent years serious of frauds have been committed both in public as well as private sector Of the economy. Due to which there is a deficiency in the growth of the economy, Business Fraud consists of dishonest and illegal activities perpetrated by individuals or companies in Order to provide an advantageous financial outcome to those persons or establishments. Fraud Detection in today's world involves a comprehensive approach to match data points with Activities to find what is abnormal. Fraudsters have developed sophisticated tactics, so it's Essential to stay on top of these changing approaches of gaming the system. Consequently there is a requirement to develop fraud detection techniques which will have the ability to cover the small risk through shrewd companies which have huge potential in the Indian Market.

Objectives of the Study

1. To understand the volume and intensity of frauds in electronic business transaction
2. To analyze the applicability of the fraud prevention techniques in this field.
3. To suggest improvised prevention techniques.



4. To study issues and challenges in dispersion and suggest ways for the improvement of Fraud detection and fraud prevention.

Review of the Literature

- Chau et al. (2006) - propose a methodology called 2-Level Fraud Spotting (2LFS) to mode the techniques that fraudsters often use to carry out fraudulent activities and to detect offenders preventively. This methodology is used to characterize the auction users on-line a honest, dishonest, and accomplices. Methodologies that characterize fraud are essential for the first phase of the process, since they are the starting point to create a model of the problem and define the best technique for its solution.
- Thomas et al. (2004) - propose a very simple decision tree that is used to identify general fraud classes. They also propose a first step towards fraud taxonomy.
- VasIU and VasIU (2004) - propose taxonomy for computer fraud and, to build it, employ a five-phase methodology. According to the authors, the taxonomy presented was prepared from a fraud preventing perspective and may be used in various ways.
- Phua et al - conducted an exploratory study of numerous articles related to fraud detection using data mining and explained these methods and techniques. These algorithms are based on some approaches such as supervised strategy with labeled data, unsupervised strategy with unlabeled data and hybrid approach.
- Akazune, M.I (2015) – in this paper, the incorporation of CMRR component into the e-commerce transaction model has addressed the problem of fake web merchant and will invariably that are involved in electronic transaction.

Findings of the Paper

Fraud is an intentional false representation of a fact. The purpose of fraud is to deceive another party in order to obtain a profit

- Fraud analysis often leads to chargeback which includes operational costs.
- E- Business fraud is an illegal or false transaction made in a web shop.
- Hackers either use the data themselves or sell it to cyber thieves, to make fraudulent transactions.
- According to a Nilson Report from 2015 and another from 2016, worldwide card Fraud:
 - Has increased every year since 1993
 - Has increased especially since 2010
 - Will keep increasing until 2019
 - With a large amount of card information stored and transferred online, it has been become easier for the hackers to get access to this information.
 - They are various techniques used in order to detect fraud , yet the techniques need to be improvised
 - In the payment industry they should be priorities the customer account which in turn lead to account theft.

Interpretation

1. The focus on fraud detection and prevention of techniques need to shift progressively in the internal audit department of the organization.
2. Develop fraud risk profiles as a part of an overall risk assessment of potential frauds.
3. Need to test 100 percentage of the data for possible indicators of frauds, not just random samples.
4. Improve the control by implementing continuous auditing and monitoring.
5. A big part of the fraud prevention is communicating the monitoring activity throughout the organization.
6. Segregation of duties it is important to be flexible in fixing broken control immediately.
7. Provide management with immediate notification when things are going wrong.
8. Re-evaluate your fraud profile, taking into account both the common fraud schemes and those related to the risks that are unique to your organization.



Conclusion

As all the transaction in today's world is getting electronic there is high risk of losing confidential data and financial loss. There is constant increase in the number of the transactions going digital, most of the consumers are opting for electronic media as a mode of transaction. But along with transactional increase there is increase in the way of fraud. Thus, there must be a straighten rules and regulations for all electronic transactions and the first way to preventing fraud is keen supervision and then there must be strict action taken to control fraud. They should be improvised techniques to detect and prevent fraud activities and fraudster at the commencement stage of fraud itself.

References

1. researchgate.net/publication/287299598_Fraud_Analysis_and_Prevention_in_e-Commerce Transaction
2. C. Mind ware Research Group, 2011 Online Fraud Report, 12th ed., 2011 [Online]. Available: <http://www.cybersource.com>.
3. S. Bhattacharyya, S. Jha, K. Tharakunnel, Westland, and J. Christopher, "Data mining for credit card fraud: A comparative study," *Decis. Support Syst.*, vol. 50, pp. 602–613, February 2011.
4. R. J. B P. Ravisankar, V. Ravi, G. R. Rao, and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques, *Decision Support Systems*, vol. 50, no. 2, pp. 491–500, 2011
5. D. H. Chau, S. P, and C. Faloutsos, "Detecting fraudulent personalities in networks of online auctioneers," in *In Proc. ECML/PKDD*, 2006, pp. 103–114.