ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Survey On: Fraud Risk Management of E-Commerce Website using Data Mining

Vaibhav Nangare[1], Mayuresh Dhamankar[2], Harshik Gohil[3], Harshal Kuwar[4]

Student, Dept. of Computer Engineering, PVPP, Mumbai University, Mumbai, India[1,2,3,4]

ABSTRACT: With development of finance and mobile Internet, fraud risk comes in all sizes and shapes. The abstract introduces the Fraud Risk Management of E-Commerce website using data mining. A fraud risk monitoring and management system based on intelligent risk models and real-time big data processing has been introduced . It captures fraud signals directly from large amount of data of user behaviors and network, examines them in real-time using machine learning, and precisely predicts the transactions and bad users. To extend the fraud risk prevention capability to external customers. In the Fraud Risk Management of E-Commerce Website, there is a five layer fraud risk prevention system where the five layers like Account Analysis, Device Analysis, Activity Analysis, Risk Analysis and Manual Review are used for the finding of any type of trespassing into the system which is extremely confidential.One fraudster can pass first layer on account check, and then there are still four layers ahead to block the fraudster. When a transaction is initiated, the first layer is Account Analysis, which includes user account information. Several checks on the first layer Account Analysis are studied as questions: Does the user account have bad/untrusting activity before? Is there any expectation that the user account is stolen? Highly suspicious transactions may be declined to protect genuine users, or extra trustworthy methods may be trigged to double confirmation in this situation. The second layer is Device Analysis, which includes the IP address check and operation check on the same device. Similarly, checks on the second layer Device Analysis are studied from passing several questions: Whether there are large quantify of transactions from the identical device? Any transaction is from bad devices? The third layer is Activity Analysis, called as Behaviour Analysis as well, which checks historical records, user's behaviour pattern, linking among devices, accounts and scenarios. Checks on the third layer Activity Analysis layer are studied as questions as well: Whether the user account link to an identified bad account? The fourth layer is Risk Analysis, which makes final opinion and takes suitable action. Checks on the fourth layer Risk Strategy are designed to aggregate all results from early checks according to severity levels. Some transactions are transmitted to auto-decision due to obvious fraud activities. Some grey cases are transmitted to Manual Review. Without powerful evidence, suspicious cases will be manually reviewed in the last layer Manual Review, where many evidences are revealed and some phone calls may be made to confirm or remind or check with users.

KEYWORDS: Fraud detection and prevention, Risk model, Malicious behavior, Risk score, Data analysis

I. INTRODUCTION

Nowadays it is very important to maintain a advanced level security to guarantee safe and trusted communication of information and transactions. But secured data communication over Internet and any other network is always under threat of frauds and misuses. So Fraud Risk Management System is a necessary component in terms of computer and network security. A complete description of all the function and specification of fraud risk management system is provided. Fraud Risk Management System which increase the detection rates of attacks and avoids frauds.

With the rapid development of network technology, the network computer system has become the primary target of hackers, network system security faces a immense threat, and fraud detection technology becomes the hot topic in the field of network security. As a result of the various advantages offered by the Internet, businesses have become more open to supporting Internet-powered initiatives such as e-commerce, customer care and extra-net collaboration. However this presents a new challenge. Many enterprise networks have been broken into by hackers. Fraud Detection is an crucial component of infrastructure protection mechanisms. Given the increasing complexities of today's network environments, more and more hosts are becoming vulnerable to attacks and hence it is important to look at efficient, systematic and automated approaches to Avoid and Detect Frauds.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Online Frauds to computer systems are increasing because of the commercialization of the Internet and local networks. Computer systems are turning out to be more and more susceptible to attack, due to its extended network connectivity. The usual objective of the aforesaid attacks is to undermine the conventional security processes on the systems and perform actions in excess of the attacker‘s permissions. These actions could encompass reading secure or confidential data or just doing vicious destruction to the system or user files. A system security operator can detect possibly malicious behaviors as they take place by setting up intricate tools, which incessantly monitors and informs activities. Fraud Risk Management uses five layer checking to confirm that the ongoing transaction is a verified transaction and has no risk or threats. Capability of discriminating between standard and anomalous user behaviors is present in Fraud Risk Management System. This would comprise of any event, state, content, or behavior that is regarded as abnormal by a predefined criterion.

The Fraud Risk Management of E-Commerce Website applies five layers of security, which maintain the security of the online transactions being done on the system. In Fraud Risk Management of E-Commerce Website, there is a five layer fraud risk prevention system where the five layers like Account Analysis, Device Analysis, Activity Analysis, Risk Analysis and Manual Review are used for the finding of any kind of trespassing into the system which is highly confidential.One fraudster can pass first layer on account check, and then there are still four layers ahead to block the fraudster.

When a transaction is initiated, the first layer is Account Analysis, which includes user account information. Several checks on the first layer Account Check are designed as questions: Does the user account have bad/suspicious activity before? Is there any possibility the user account stolen etc? Extremely suspicious transactions may be declined to protect genuine users, or extra authentic methods may be trigged to double confirmation in this situation. The second layer is Device Analysis, which includes the IP address check and operation check on the same device. Similarly, checks on the second layer Device Check are designed from passing several questions: Whether there are huge quantify of transactions from the same device? Any transaction is from bad devices? The third layer is Activity Analysis, called as Behavior Analysis as well, which checks historical records, user behavior pattern, linking among accounts, devices and scenarios. Checks on the third layer Activity Check are designed as questions as well: Whether the user account link to an identified bad account? The fourth layer is Risk Analysis, which makes final judgment and takes appropriate action. Checks on the fourth layer Risk Strategy are designed to aggregate all results from previous checks according to severity levels. Some transactions are sent to auto-decision due to obvious fraud activities. Some grey cases are sent to Manual Review. Without strong evidence, suspicious cases will be manually reviewed in the last layer Manual Review, where more evidences are revealed and some phone calls may be made to verify or remind or check with user’s.

II. RELATED WORK

A. ***ONLINE PASSWORD:*** The security of a password-protected system depends on several factors. The overall system must, of course, be designed for sound security, with protection against computer viruses and man-in-the-middle attacks. Physical security issues are also a concern, from deterring shoulder surfing to more sophisticated physical threats such as video cameras and keyboard sniffers. And, of course, passwords should be chosen so that they are hard for an attacker to guess and hard for an attacker to discover using any (and all) of the available automatic attack schemes. Nowadays, it is a common practice for computer systems to hide passwords as they are typed. The purpose of this measure is to avoid bystanders reading the password. However, some argue that this practice may lead to mistakes and stress, encouraging users to choose weak passwords.

B. ***PIN NUMBER:*** Financial PINs are often four-digit numbers in the range 0000-9999, resulting in 10,000 possible numbers.Some systems set up default PIN and most allow the customer to set up a PIN or to change the default one, and on some a change of PIN on first access is mandatory. Customers are usually advised not to set up a PIN based on their or their spouse's birthdays, on driver license numbers, consecutive or repetitive numbers, or some other schemes.

C. ***OTP:*** OTP generation algorithms are typically making the use of the pseudorandomness or randomness, making prediction of the successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are given: 1)Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

short period of time). 2)Using a mathematical algorithm to generate a new password based on the previouspassword (OTPs are effectively a chain and must be used in a predefined order). 3)Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter. There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

III. PROBLEM STATEMENT

An effective fraud risk management framework will enable organisations to have controls that first prevent the fraud from occurring, detect as soon as a fraud happens and respond effectively to fraud incidents when they occur. An effective fraud risk management framework will enable organisations to have controls that first prevent the fraud from occurring, detect as soon as a fraud happens and respond effectively to fraud incidents when they occur. Preventive Controls are designed to help reduce the risk of fraud and misconduct from occurring in the first place. Detection controls are designed to uncover fraud and misconduct when it occurs. Response controls are designed to take corrective action and remedy from the harm caused by fraud or misconduct.

With development of mobile internet and finance, fraud risk comes in all shapes and sizes. The Fraud Risk Management of E-Commerce website using data mining is introduced. A fraud risk monitoring and management system based on real-time big data processing and intelligent risk models. The fraud risk monitoring and management system captures fraud signals directly from huge amount data of user behaviors and network, analyzes them in real-time using machine learning, and accurately predicts the bad users and transactions. To extend the fraud risk prevention ability to external customers. In Fraud Risk Management of E-Commerce Website, we have a five layer fraud risk prevention system where the five layers like Account Analysis, Device Analysis, Activity Analysis, Risk Analysis and Manual Review are used for the finding of any kind of security breach created by the attackers who attack or hack the user accounts and create problems in the system.

IV. PROPOSED SYSTEM

The System will have a E-Commerce website as a frontend of the project. There will also be a payment portal of a particular bank for making payment. As it is a Fraud Risk Management of E-Commerce website there will be a lot of users using the website for shopping of all the different products available to them. These users will have accounts which are called as User Accounts for Login and will be Password protected. Their accounts will even hold their banking information and bank account which they use for making payment of the goods or products they purchase from the website. While making payments, if any suspicious activity is detected the Fraud Risk Management tool comes into action and the Five Layers are used in sequence. If the fraud is confirmed after the checking of these five layers, the gateway between the website and the payment portal will be blocked and the Payment Portal will not show. Hence, Payment will not be made and Fraud will be detected as well as Avoided.

The five layers of the Fraud Risk Management System are shown in the Figure.1, as shown in the figure the first layer is the Account Analysis layer, the second layer is the Device Analysis Layer, the third is the Activity Analysis Layer, the fourth layer is Risk Analysis Layer and the last fifth layer is the Manual Review Layer.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

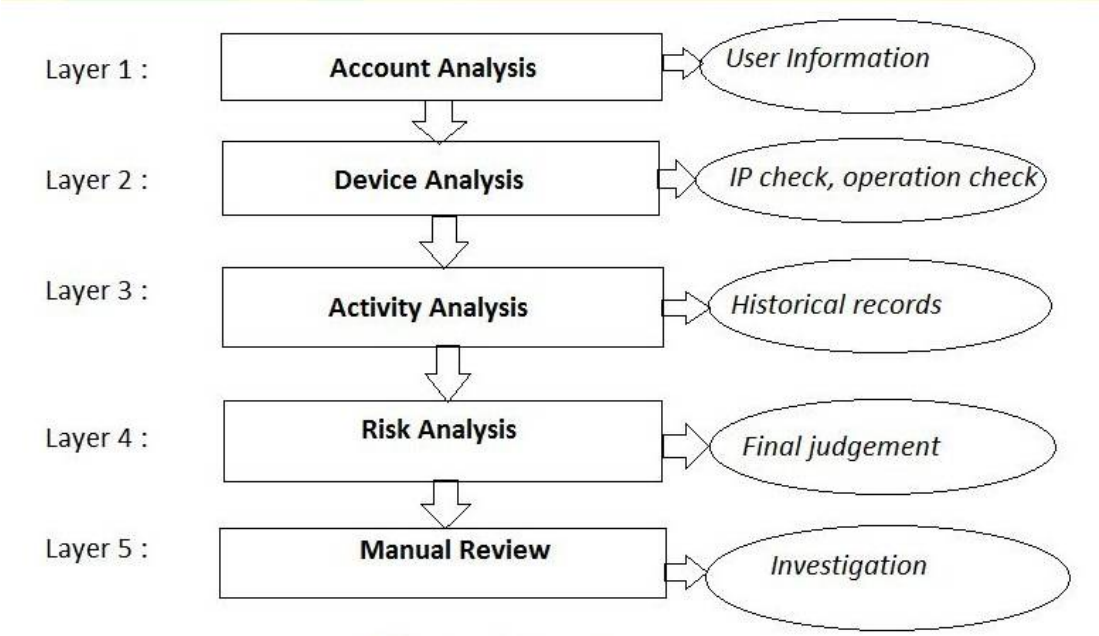

Figure 1: Five Layers Of Fraud Risk Management System

When a transaction is initiated, the first layer is Account Analysis layer, which includes user's account information. Several checks on the first layer Account Analysis are designed. The first layer checks whether the user account have bad/suspicious activity before. Also it verifies if there is any possibility that the user account is stolen? Extremely suspicious transactions may be declined to protect genuine users, or extra authentic methods may be trigged to double confirmation in this situation. The second layer is Device Analysis, which includes the IP address check and operation check on the identical device. Similarly, checks on the second layer Device Check are designed. Whether there are huge quantify of transactions from the identical device? Any transaction is from bad devices? The third layer is Activity Analysis, called as Behavior Analysis as well, which analysis the historical records, user behavior pattern, linking among accounts, devices and scenarios. Checks on the third layer Activity Analysis are designed as questions as well: Whether the user account link to an identified bad account? The fourth layer is Risk Analysis, which makes final judgment and takes appropriate action. Checks on the fourth layer Risk Strategy are designed to aggregate all results from previous checks according to severity levels. Some transactions are sent to auto-decision due to obvious fraud activities. Some grey cases are sent to Manual Review. Without strong evidence, suspicious cases will be manually reviewed in the last layer Manual Review, where more evidences are revealed and some phone calls may be made to verify or remind or check with users.

V. Conclusion and Future Work

A survey on fraud Risk Management of E-Commerce website to Detect and Prevent Frauds on the E-Commerce website is provided. The fraud risk monitoring and management system uses the Five Layer Approach to implement and measure the performance of system. The Payment Portal is Blocked if any threat has been Detected.

Till now, only the user entered OTP was checked. A survey is carried out on how to trace the user's phone location and then cross check with the IP address he/she is using for accessing the website for shopping. Due to this implementation in future, the fraud risk monitoring and management system will remain updated and can be proven more useful and helpful in detecting frauds.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

ACKNOWLEDGEMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends and family members.

REFERENCES

1. Iyer, N. and Samociuk, M., "Fraud and Corruption: Prevention and Detection", 2006.
2. Ernst & Young, "Fraud, the Unmanaged Risk", www.ey.com, 2003.
3. Iyer, N. and Samociuk, M., "Rotten to the Core", Excellence in Leadership Issue 2, SPG Media, 2007.
4. Collier, P.M. and Agyei-Ampomah S., "CIMA Official Learning System Management Accounting Risk and Control Strategy", 2007.
5. An Oracle White Paper. Or ACLE Real Application Clusters (RAC) ; 2013.
6. EMC Inc. Greenplum Database, "Critical Mass Innovation, Architecture" White Paper , 2010.
7. Freeman LC, "Centrality in social networks I: conceptual clarification", Soc Netw, 1979.
8. Wasserman Stanley, Faust Katherine, "Social Network Analysis: Methods and Applications (Structural Analysis in the Social Sciences)", Combridge Unviversity Press, 1994.
9. BDO Stoy Hayward LLP, "BDO Fraudtrack 5: A global challenge", www.bdo.co.uk/fraudtrack, January 2008.
10. White Tom., "Hadoop: the Definitive Guide", O'Reilly Press, 2012.
11. Finn, J. and Cafferty, D., "Defence Mechanism, Financial Management", September 2002.
12. Fraud Advisory Panel, "Ethical behaviour is the best defence against fraud", Ninth Annual Review 2006-2007.

BIOGRAPHY

Vaibhav Ashok Nangare pursuing BE in Computer Engineering from University of Mumbai at Padmabhushan Vasantdada Patil Pratishthan's College Of Engineering.

Harshal Ravikant Kuwar pursuing BE in Computer Engineering from University of Mumbai at Padmabhushan Vasantdada Patil Pratishthan's College Of Engineering.

Gohil Harshik Vinod pursuing BE in Computer Engineering from University of Mumbai at Padmabhushan Vasantdada Patil Pratishthan's College Of Engineering.

Mayuresh Mahendra Dhamankar pursuing BE in Computer Engineering from University of Mumbai at Padmabhushan Vasantdada Patil Pratishthan's College Of Engineering.