International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-01, Apr 2018

Fraud Risk Detection & Management For Online Banking

[1]Irfan Shaikh, [2]Yogita Pol, [3]Manoj Nikam, [4]Rohan Shetye, [5]Prof. Dipashri Sonawale

[1,2,3,4,5]Dept. of Information Technology, M.G.M. College Of Engineering and Technology, Kamothe, Navi Mumbai, Maharashtra, India.

Abstract - With development of mobile internet and finance, fraud risk comes in all shapes and sizes. This abstract is to introduce the Fraud Risk Management of Online Banking using data mining. It is a fraud risk monitoring and management system based on real-time big data processing and intelligent risk models. It 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. Here in Fraud Risk Management of Online Banking, it has a five layer fraud risk prevention system where the five layers like Account Check, Device Check, Activity Check, Risk Strategy and Manual Review are used for the finding of any kind of trespassing into the system which is highly confidential.

Keywords:- Online Banking Risk, OTP, Five level Verification, User Behaviour.

I. INTRODUCTION

With the rapid development of network technology, the network computer system has become the main target of hackers, network system security faces a huge 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 customer care, e-commerce, and extranet collaboration. However this presents a new challenge. Many enterprise networks have been broken into by hackers. Fraud Detection is an important 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 systematic, efficient and automated approaches to Detect and Avoid Frauds. 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 behaviours 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 behaviours is present in Fraud Risk Management System. This would comprise of any event, state, content, or behaviour that is regarded as abnormal by a pre-defined criterion.

II. 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. 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. This abstract is to introduce the Fraud Risk Management of E-Commerce website using data mining. We have built a fraud risk monitoring and management system based on real-time big data processing and intelligent risk models. It 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. Here in Fraud Risk Management of E-Commerce Website, we have a five layer fraud risk prevention system where the five layers like Account Check, Device Check, Activity Check, Risk Strategy and

 DOI : 10.18231/2454-9150.2018.0086

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.

III. LITERATURE SURVEY

3.1 Existing Methods

3.1.1 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.

3.1.2 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 PINs 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.

3.1.3 OTP:

OTP generation algorithms are typically making 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 listed below:

• Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)

• Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).

• 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.

3.2 Existing Systems

I. "Sunil S Mhamane and L.M.R.J Lobo" [1] This paper discusses the various types of online banking attacks and preventive measure to minimize the risk and to deal with these attacks. The bank can implement prevention techniques, tools and policies. Review of information security policy and procedure on regular basis. Upgrade existing password single-factor authentication systems to two-factor systems. Implement adequate network security to block unnecessary network traffic to the systems.

II. "Pankaj Richhariya" [2] proposed the hierarchical structure of e-commerce risk, and build the Trust-Based whole process e-commerce credit risk management model.In accordance with the concept of the whole process of transaction, we can divide the transaction process into three parts, respectively pre-transaction, transaction and posttransaction. If further refined, the pre-transaction process contains identifying requirements, information searching and selection comparing. The latter flag has a better reflection of the information flow changes, where e-commerce trust mechanism plays a very important role presenting important significance in e-commerce credit risk management. Through the analysis of credit, trust, reputation and credit risk, present the basic connotation of e-commerce credit risk management meanwhile analyze the relationship among credit.

III. " Shailesh S. Dhok" [3] This work aims to apply and evaluate computational intelligence techniques (e.g., data mining and machine learning) to identify fraud in electronic transactions, more specifically in credit card operations performed by Web payment gateways.

IV. " Anshul Singh, Devesh Narayan " [4] This paper presents a survey of various techniques used in credit card fraud detection mechanisms and evaluates each methodology based on certain design criteria. In the rule-based component, the suspicion level of each incoming transaction based on the extent of its

 DOI : 10.18231/2454-9150.2018.0086

deviation from good pattern is determined. Dempster–Shafer's theory is used to combine multiple such evidences and an initial belief is computed. Sequence alignment becomes an efficient technique for analyzing the spending behavior of customers. Fuzzy Darwinian Detection system [4] uses genetic programming to evolve fuzzy logic rules capable of classifying credit card transactions into "suspicious" and "non-suspicious" classes.

V. "Raghavendra Patidar, Lokesh Sharma " [5] In this paper implemented of hidden markov model in credit card fraud detection. It has also explained the hidden markov model how can detect whether an incoming transaction is fraudulent or not dividing the transaction amount in three categories that is grouping high, medium & low used on different ranges of transaction amount, each group show aberration symbols. Propose the mean distribution probability of observation sequence.

VI. "K. Rama Kalyani, D.UmaDevi " [6] The hypothesis is to design a technique which is the combination of Hidden Markov Model, Behavior Based Technique and Genetic Algorithm. Behavior Based Technique- In this technique model can detect fraud by bearing in mind cardholders spending habit. Genetic Algorithm- It helps to obtain better solution and is used for calculating threshold value.

VII. [7]The aim of this paper is to detect and prevent fraud in case of internet banking using Hidden Markov Model algorithm. This paper explains Architecture and design part of proposed system. Customer Behavior pattern is used for fraud detection. Transaction amount was taken as Observation symbol. An HMM defmes a probability distribution over sequences of observations.

IV. PROPOSED SYSTEM

We present Fraud Risk Management of Online Banking, by applying five layers of security, which maintain the security of the online transactions being done on the system. Here in Fraud Risk Management of Online Banking, we have a five layer fraud risk prevention system where the five layers like Account Check, Device Check, Activity Check, Risk Strategy 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 Check, which includes buyer account information and seller account information. Several checks on the first layer Account Check are designed as questions: does the buyer or seller account have bad/suspicious activity before? Is there any possibility the buyer account stolen etc? Extremely suspicious transactions may be declined to protect genuine buyers, or extra authentic methods may be trigged to double confirmation in this situation. The second layer is Device Check, 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 Check, called as Behavior Check as well, which checks historical records, buyer and seller behavior pattern, linking among accounts, devices and scenarios. Checks on the third layer Activity Check are designed as questions as well: whether the buyer or seller account link to an identified bad account? The fourth layer is Risk Strategy, 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 buyers or sellers.

V. DESIGN

Architecture Block Diagram

1. Run Project
2. Register/Login
3. Browse and Select Products to purchase
4. Add to cart
5. Proceed to checkout
6. Enter details, and valid email id and phone no.
7. A verification mail is sent to the mail id
8. After verification, an OTP is sent to the registered phone no.

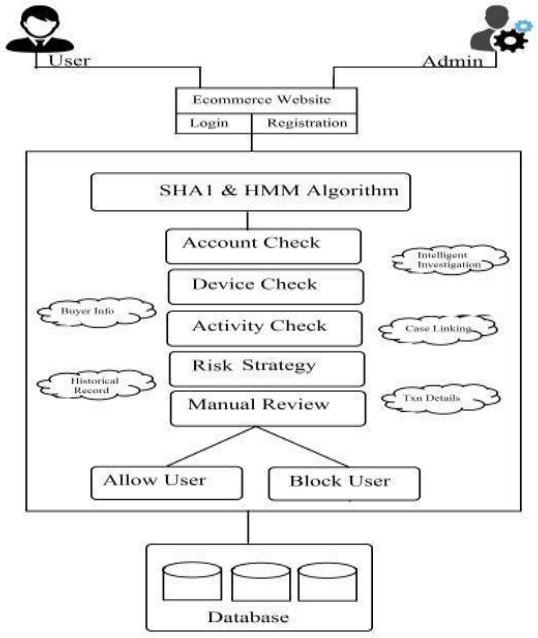

Fig.1 Architecture Block Diagram

 DOI : 10.18231/2454-9150.2018.0086

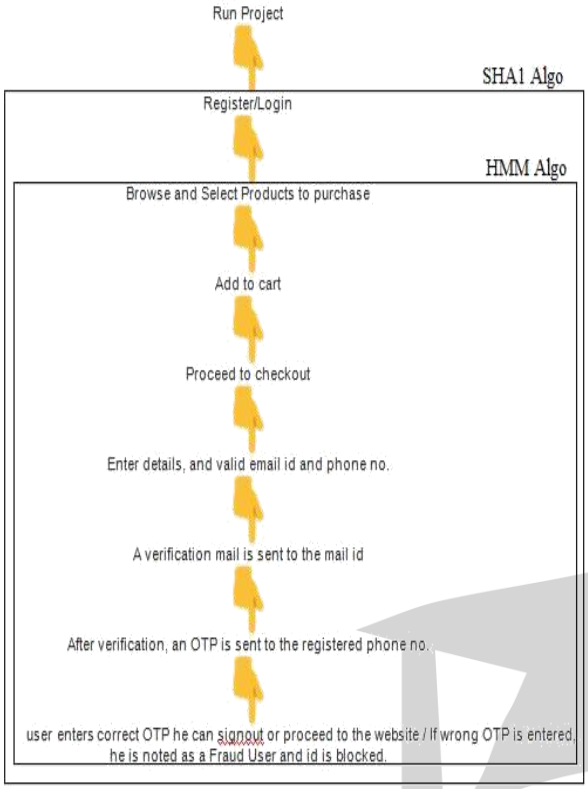

Fig. 2 Work Flow Diagram

VI. METHODOLOGIES

SHA1 Algorithm:

SHA1, one of the Internet's most crucial cryptographic algorithms, is used in our project in order to keep the passwords safe into the database. Whenever a user creates a new account or sets a new password, the system converts his/her password into a cryptograph which uses SHA 1 Algorithm for checking whether the user has entered a correct password or not. These passwords are saved in the form of cryptographs which need to be encoded and decoded by the system whenever the user enters his/her password.

SHA 1 is what's known as a cryptographic hash function. Like all hash functions, it takes a collection of text, computer code, or other message input and generates a long string of letters and numbers that serve as a cryptographic fingerprint for that message. Even a tiny change, such as the addition or deletion of a single comma in a 5,000-word e- mail, will cause a vastly different hash to be produced. Like all fingerprints, the resulting hash is useful only as long as it's unique. The moment two different message inputs produce the same hash, the so-called collision can open the door to signature forgeries that can be disastrous for the security of banking transactions, etc.

Hidden Markov Model:

A hidden Markov model can be considered a generalization of a mixture model where the hidden variables (or latent variables), which control the mixture component to be selected for each observation, are related through a Markov process rather than independent of each other. Recently, hidden Markov models have been generalized to pairwise Markov models and triplet Markov models which allow consideration of more complex data structures and the modelling of nonstationary data.

A hidden Markov model (HMM) is a statistical Markov model in which the system being modeled is assumed to be a Markov process with unobserved (hidden) states. An HMM can be presented as the simplest dynamic Bayesian network. The mathematics behind the HMM were developed by L. E. Baum and coworkers. It is closely related to an earlier work on the optimal nonlinear filtering problem by Ruslan L. Stratonovich, who was the first to describe the forward-backward procedure.

In simpler Markov models (like a Markov chain), the state is directly visible to the observer, and therefore the state transition probabilities are the only parameters. In a hidden Markov model, the state is not directly visible, but the output, dependent on the state, is visible. Each state has a probability distribution over the possible output tokens. Therefore, the sequence of tokens generated by an HMM gives some information about the sequence of states. The adjective 'hidden' refers to the state sequence through which the model passes, not to the parameters of the model; the model is still referred to as a 'hidden' Markov model even if these parameters are known exactly.

Hidden Markov models are especially known for their application in temporal pattern recognition such as speech, handwriting, gesture recognition, part-of-speech tagging, musical score following, partial discharges and bioinformatics.

Hidden Markov models (HMMs) are a formal foundation for making probabilistic models of linear sequence 'labeling' problems. They provide a conceptual toolkit for building complex models just by drawing an intuitive picture. They are at the heart of a diverse range of programs, including genefinding, profile searches, multiple sequence alignment and regulatory site identification. HMMs are the Legos of computational sequence analysis.

VII. CONCLUSION

Fraud Risk Detection & Management is mainly designed to Detect and Prevent Frauds on the E-Commerce website. To implement and measure the performance of the system a Five Layer Approach is used. The Payment Portal is Blocked if any threat has been Detected. The system can also check the location of the user making transaction iffound suspicious, in order to trace the location via OTP message and check whether the user is a genuine user.

ACKNOWLEDGEMENT

We would like to express our sincere and whole hearted thanks to our respected project guide Prof. Dipashri Sonawale for the valuable guidance, which enabled us to compare this project in a systematic manner and stipulated

 DOI : 10.18231/2454-9150.2018.0086

time.We would like to express our sincere thanks to Mr. Venkat

Raman Head of Department of Information Technology Engineering for his encouragement for the completion of project. We would like to express our gratitude to Dr. S. K. Narayankhedkar for his needful assistance in completion of project work. Our sincere thanks also go to staff members of the faculty of Mahatma Gandhi Mission's College Of Engineering And Technology, Kamothe, Navi Mumbai for their co-operation, which helped us a lot in a completion of the project. Sincere appreciation and warmest thanks are extended to many individuals who in their own ways have inspired us in the completion of project.

REFERENCES

[1] Sunil S Mhamane and L.M.R.J Lobo "Use of Hidden Markov Model as Internet Banking Fraud Detection" International Journal of Computer Applications (0975 – 8887) Volume 45– No.21, May 2012

[2] Pankaj Richhariya et al "A Survey on Financial Fraud Detection Methodologies" BITS, Bhopal," International Journal of Computer Applications (0975 – 8887) Volume 45 No.22, May 2012

[3] "Credit Card Fraud Detection Using Hidden Markov Model Shailesh S. Dhok (2012).

[4] A Survey on Hidden Markov Model for Credit Card Fraud Detection Anshul Singh, Devesh Narayan.

[5] Raghavendra Patidar, Lokesh Sharma Credit Card Fraud Detection using Neural Network(2011).

[6] Fraud Detection of Credit Card Payment System by Genetic Algorithm K. Rama Kalyani, D.UmaDevi (2012).

[7] An Oracle White Paper. Oracle Real Application Clusters (RAC) ; 2013.

[8] EMC INC. Geenplum Database: Critical Mass Innovation, Architecture White Paper ; 2010.

 DOI : 10.18231/2454-9150.2018.0086