INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue1)
Available online at: www.ijariit.com

An Intelligent System for Detection of User Behavior in Internet Banking

Manish Bendale
ME-1 year
Department of Computer Engineering
Maharashtra Institute of Technology, Pune, Maharashtra
manishbendale85@gmail.com

Saurabh Dorle
ME-1 Year
Department of Computer Engineering
Maharashtra Institute of Technology, Pune, Maharashtra
sdd.saurabhd@gmail.com

Dr. Nitin N. Pise
Department of Computer Engineering
Maharashtra Institute of Technology, Pune, Maharashtra
nitin.pise@mitpune.edu.in

Abstract- Security and making trust is the first step toward development in both real and virtual societies. Internet-based development is inevitable. Increasing penetration of technology in the internet banking and its effectiveness in contributing to banking profitability and prosperity requires that satisfied customers turn into loyal customers. Currently, a large number of cyber attacks have been focused on online banking systems, and these attacks are considered as a significant security threat. Banks or customers might become the victim of the most complicated financial crime, namely internet fraud. This study has developed an intelligent system that enables detecting the user's abnormal behavior in online banking. Since the user's behavior is associated with uncertainty, the system has been developed based on the fuzzy theory, this enables it to identify user behaviors and categorize suspicious behaviors with various levels of intensity. The performance of the fuzzy expert system has been evaluated using a receiver operating characteristic curve, which provides the accuracy of 94%. This expert system is optimistic to be used for improving e-banking services security and quality.

Keywords – ***Fuzzy Expert System; Suspicious Financial Transactions; Anti-Money Laundering.***

I. INTRODUCTION

Electronic commerce is the main achievement of the information and communications technology in various economic fields. This technology has contributed to commercial development, facilitated communication between economic elements, paved the way for the operation of small and medium enterprises, promoted productivity, and saved time and money. Information and communications technology has increased compatibility among businesses and led to the creation of new job opportunities. Opening new accounts and transferring money "anytime and anywhere"
through the internet banking is a new method of offering banking services. The availability of the internet to a large number of customers coupled with the expansion of electronic communications between various people and organizations has paved the way for commercial transactions and transformed customer's consumption pattern. Customer's attitude toward the internet banking and their acceptance of this phenomenon is one concern of information technology management, especially the internet banking management.

II. RELATED WORK

Financial institutes across the world have reported suspicious activities in their financial systems. To deal with these problems, various methods for detecting suspicious activities have been suggested, including activities identified by employees as daily activities, law enforcement questions, and checking customer records [1]. Therefore, an independent expert system is needed that could detect suspicious transactions and be updated immediately based on basic rules [2]. In the past decade, researchers have actively used a system for demonstrating knowledge in the fields of databases, information integration, cooperative information systems, information marketing, electronic commerce, investment in integration software, knowledge management, etc [3]. Recently, several methods for detecting suspicious transactions have been developed based on machine learning, including dynamic Bayesian networks [4]. Various methods for dealing with fraudulent behavior in the internet banking have drawn the attention of researchers some of which are briefly explained here. Those banks that provide internet-banking services employ

different methods to identify crime and screen customer's transactions. Some of the methods that are currently used include transaction observation, credit card verification, personal ID number, and biometrics. Biometrics includes identification and verification of customer's signature and fingerprint. Recording the log of good customers and bad customers, and categorizing these customers according to different geographical areas are among the other information that has been used to detect crime. Data-mining methods are among the other methods used for detecting crimes. These methods focus on statistical analyses, customer behavior detection, and crime detection patterns [5]. Data- mining methods are based on specific learning rules and can detect fraudulent behavior criteria in large transaction databases. These criteria are used in monitoring systems to register customer's abnormal behaviors and detect suspicious behaviors. The output of these systems could ultimately be used for sending alarms on wrongdoing users [6]. Association rule mining is also one of the best data-mining methods for developing such models. This method utilizes data related to credit cards to extract knowledge, find unconventional behavioral patterns among customer's transactions, and identify and prevent crime. Artificial neural networks are another method that has so far been used for identifying and detecting crime. This method is capable of extracting patterns from databases containing the previous transactions of customers. Artificial neural networks are educable and could adapt to new forms of crime [7].
The current study chiefly seeks to identify and categorize customer's suspicious behaviors in the internet banking through the use of the fuzzy theory.

III. CATEGORIZATION OF CUSTOMER BEHAVIOR

To reach a clear definition of "user behavior", first it is necessary to provide specific definitions for various behaviors of the internet banking users as well as various categories of these behaviors. It is clear that such a categorization greatly contributes to adopting proper approaches toward each category. Therefore, two behavior categories are defined as follows:

A. Normal behavior

Including the behavior of users whose transactions are conducted normally, completely, and without any errors [9] .

B. Suspicious behavior

Including the behavior of users who face frequent errors when logging into the system, are suspicious of illegal entry, show suspicious behavior, log in repeatedly, or conduct suspicious transactions [9] .

The fuzzy expert system has been developed through the use of MTLAB 2012 software.

IV. DETERMINANT OF INPUT PARAMETERS

In the first phase, the user interface receives information related to input variables in the form of absolute values. This information was examined in order to determine input parameters. Then, the viewpoints of banking experts were used so as to extract information items used in designing the fuzzy system. It resulted in the elimination or addition of some of the parameters. In most articles, factors of "mistake numbers at entrance time", "sum and number of orders" and "user dossier in system" have always been parts of entrance factors. The input parameters of the proposed system is in agreement with the study reported in [9] But in this article, factors of "inactive account" and "the interval between transfers" has replaced "IP numbers" and "sort of browser". Since with accomplished analysis this result came out that the normal user because of different reasons (using anti-filter and...) has probably used several IPs .There was also this chance that the user make use of a less known browser and thus increased the error percentage. Therefore with considering the most factors of calculation , the interval between transferred prices and order price was selected which has too much effect on recognizing dangerous behaviors. Following the final analysis, eight parameters involved in determining user behavior in the internet banking were selected as input variables, while one parameter (user behavior) was selected as output variable. Table 1 contains the name and concept of each parameter.

No	Variable Name	Symbol	Unit	Concept
1	Error count	Missing	Times	User error upon logging in system
2	Transfer count	Order count	Times	Number of Internet transfers
3	Transferred amount	Amount	Hundred Thousand	Amount of Internet transfers
4	Dormant account	Dormant	Month	Six month Interval between previous And current use of The account
5	User records	Type user	Month	Time of the user's familiarity with The system
6	Transfer interval	Immediately	Day	Transfer interval is seven days normally
7	Input time	Input Time	O'clock	Time of using the system by the user
8	Output	Result	-	Behavior that Is allocated to the user

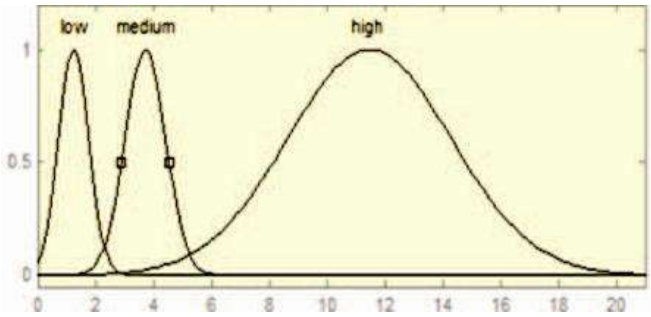

Fig. 1. Membership functions related to the Missing between 0 and 9 times

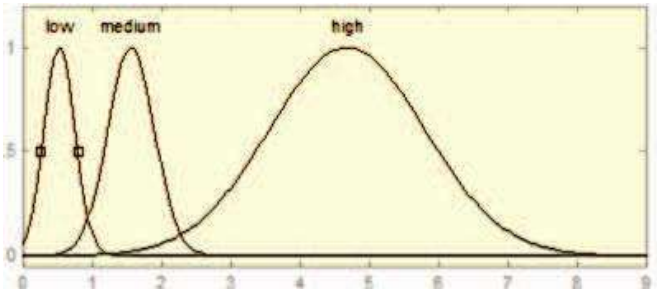

Fig. 2. Membership functions related to the Order Count between 0 and 21 times

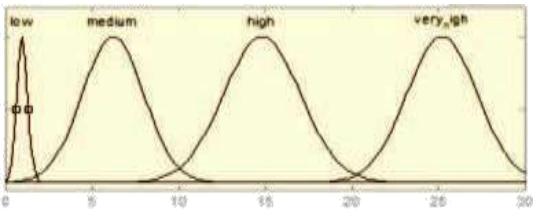

Fig. 3. Membership functions related to the amount between 0 and 30 Hundred Thousand

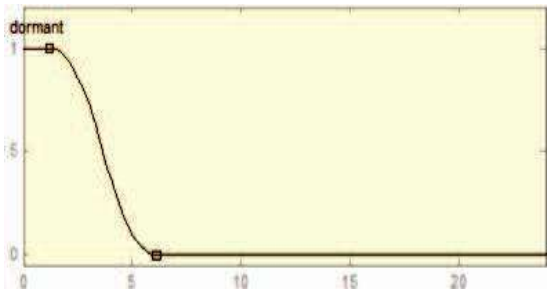

Fig. 4. Membership functions related to the dormant between 0 and 24 Month

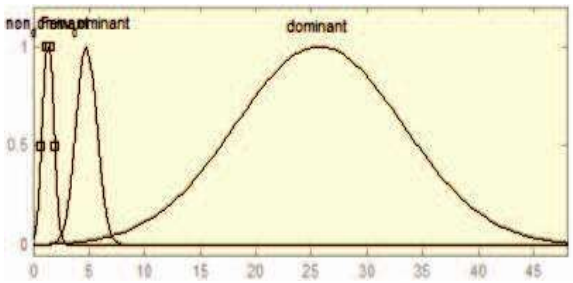

Fig. 5. Membership functions related to the user type between 0 and 48 Month

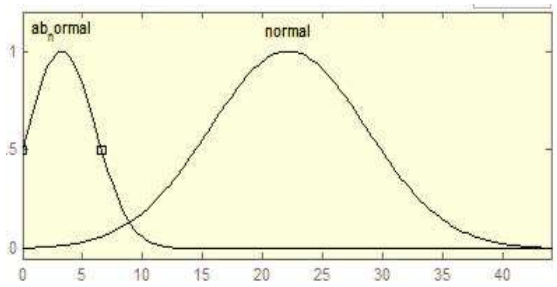

Fig. 6. Membership functions related to the immediately between 0 and 44 Days.

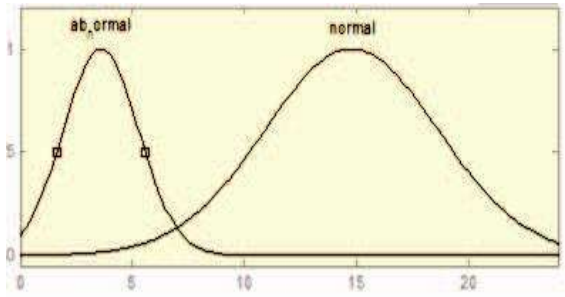

Fig. 7. Membership functions related to the input time between 0 and 24 O'clock

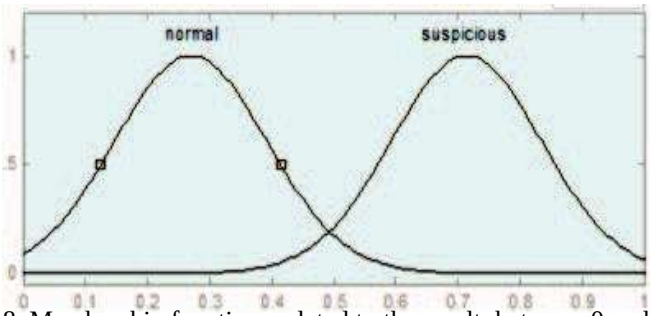

Fig. 8. Membership functions related to the result: between 0 and 1

V. DEVELOPMENT OF THE FUZZY RULE BASE

In this phase, the fuzzy rule base was developed through the use of input variables and expert views, with 120 "if- then" rules based on what has been expressed in last section. This table is similar to the work presented [9]. However, all the rules and membership functions are computed based on new factors have been obtained.

TABLE II. THE RULESET OF FUZZY EXPERT SYSTEM.

No	Rule
1	IF (missing = low) & (OrderCount = medium) & (amount = medium) & (dormant = dormant) & (type = NonDominat) & (immediately = AbNormal) & (time = AbNormal) => (Output = Suspicious)
2	IF (missing = low) & (OrderCount = medium) & (amount = medium) & (dormant = dormant) & (type = NonDominat) & (immediately = Normal) & (time = Normal) => (Output = Normal)
3	IF (missing = low) & (OrderCount = medium) & (amount = medium) & (dormant = dormant) & (type = NonDominat) &

	(immediately = Normal) & (time = AbNormal) => (Output = Suspicious)
No	**Rule**
4	IF (missing = low) & (OrderCount = medium) & (amount = medium) & (dormant = dormant) &(type = FewDominat) & (immediately = Normal) & (time = Normal) => (Output = Normal)
5	IF (missing = low) & (OrderCount = medium) & (amount = medium) & (dormant < > dormant) & (type = FewDominat) & (immediately = AbNormal) & (time = AbNormal) => (Output = Suspicious)
6	IF (missing = low) & (OrderCount = medium) & (amount = medium) & (dormant < > dormant) & (type=NonDominat) & (immediately = Normal) & (time = Normal) => (Output = Normal)
7	IF (missing = low) & (OrderCount = medium) & (amount = medium) & (dormant = dormant) & (type = Dominat) & (immediately = Normal) & (time = AbNormal) => (Output = Suspicious)

TABLE III. THE RESULT OF IMPLEMENTING THE SYSTEM WITH THE EXPERTS.

Error	Transfer Count	Transferred Amount	Dormant Account	User Type	Transfer Interval	Time	Output Report	Expert View
1	1	19	4	11	0	2	0.70	Suspicious
1	6	11	24	46	14	14	0.48	Normal
0	1	14	24	40	1	1	0.59	Suspicious
0	8	17	7	17	8	16	0.59	Normal
5	11	22	4	21	9	24	0.71	Suspicious
2	4	4	10	12	11	6	0.67	Suspicious
1	1	14	24	40	13	1	0.70	Suspicious
3	3	19	24	42	12	21	0.70	Suspicious
2	3	19	21	19	14	24	0.69	Suspicious
1	8	12	14	29	11	1	0.70	Suspicious
4	1	5	13	17	0	17	0.71	Suspicious

VI. FUZZY LOGIC

In this phase, the fuzzy expert system was implemented using information gained from the real environment of the system. To analyze the system, thirty information items related to users, which existed in the databases of the internet banking, were added to the system. Two samples of these information items have been explained in detail below.

1) A user, one day at 2:00, has tried to enter the system. After entering, this user has done an order payment with the price of one hundred ninety thousand rials. The kind of account is inactive and user's dossier in system is 11 months. After entering the information of this user, the designed system finds the user's behavior "suspicious "that is approved by the expert opinion.

2) The user who have been using internet banking more than six months, after fourteen days, at 14:00 , after one mistake at entering password, has entered the system and has done 6 orders with very low prices. After entering this user's information, the designed system recognizes user's behavior "normal "which is approved by the expert.

VII. PERFORMANCE EVALUATION USING RECEIVER OPERATING CHARACTERISTIC ANALYSIS

Having completed all the phases, an receiver operating characteristic (ROC) analysis is employed to examine and assess the implementation of the system. Number of data in this article for 30 users, each user includes seven factors as input, the system is designed. After receiving the output of the system implementation and system output with the actual output by receiver operating characteristic curve will be reviewed and evaluated. receiver operating characteristic curves were developed in 1950, and were used to identify An receiver operating characteristic curve demonstrates the trade-off between system benefits and its cost as the observer changes the decision threshold . For the categorization process, threshold values are applied in the range of [0,1] to determine output. True positive rate and false positive rate are calculated for each threshold. In this connection, the fuzzy output extracted from the system is considered as input, and results examined by experts is put in as target to receive the output. The performance of the fuzzy expert system was evaluated using an receiver operating characteristic curve, which provides the accuracy of 94%. This expert system is optimistic to be used for improving e-banking services security and quality.

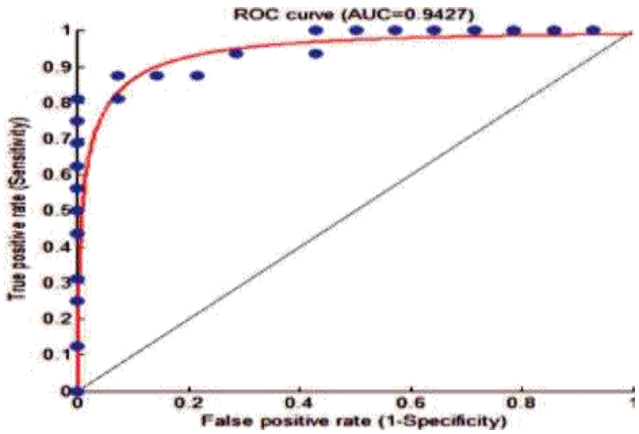

Fig. 10. Receiver operating characteristic (ROC) curve of the fuzzy expert system

CONCLUSION

In this paper, a fuzzy expert system was proposed to identify the user behavior in Internet Banking. ROC curve = 0.9427 , max sensitivity cut-off point= 0.30 , max specificity cut-off point= 0.69 , cost effective Cut-off point= 0.67 , max efficiency cut-off point= 0.67 .Having examined receiver operating characteristic results, it is understood that a system that combines several important factors as input and examines those factors simultaneously can determine if certain banking transactions are dangerous. Given the quick growth of cyber attacks and technologies used by cyber criminals, securing electronic banking has turned into one of the main concerns of banks. Therefore, the higher security of information technology structures in electronic banking contributes to customer's higher trust and loyalty. Given the findings of this study, it is recommended that more attention be paid to activities aimed at creating trust in the banking industry. Winning the trust of customers through activities such as the safe processing and transmission of highly confidential information could be a useful step toward preserving electronic customers.

REFERENCES

[1] S. P. Ketkar, R. Shankar , & D. K. Banwet, "Telecom KYC and mobile banking regulation", An exploratory study. Journal of Banking Regulation Advance online publication, 2013 . http://dx.doi.org/10.1057/jbr.2013.

[2] L. Wong, "Money-laundering in Southeast Asia", liberalism and govern mentality at work. Contemporary Politics, 19(2), 221-233 , 2013. http://dx.doi.org/10.1080/13569775.2013.785832

[3] M. Hepp, P. Leenheer, , A. de Moor, & Y. Sure, "Ontology management" semantic web, semantic web services, and business applications", Semantic Web and Beyond, Vol. 7. Springer, 2008. http://dx.doi.org/10.1007/978-0-387-69900-4

[4]S. Raza,, & S. Haider, "Suspicious activity reporting using dynamic bayesian networks", ProcediaComputer Science, 3, 987-991 , 2011. http://dx.doi.org/10.1016/j.procs.2010.12.162

[5]J. T. S. Quah and M. Sriganesh, "Real-time credit card fraud detection using computational intelligence, Expert Systems with Applications,3112, pp.17-9

[6] L. Fang, M. Cai, H. Fu, and J. Dong, "Ontology-Based Fraud Detection," in Computational Science – ICCS 3112, pp.1048-1055, 2013.

[7] D. Sanchez, M. A. Vila, L. Cerda, and J. M. Serrano, "Association rules applied to credit card fraud detection," Expert Systems with Applications, 2008, pp.1-14 , 2008.

[8] A. A Ramaki, R Asgari ,R.E Atani , "Credit card fraud detection based onontology graph ", International Journal of Security, Privacy and Trust Management(IJSPTM), Vol. 1, No 5, October 2012.

[9] G. Montazer and L Saroukhani , "Design and implementation of a fuzzy expert system for suspicious behavior detection in e-banking system" . 3.; 1 (1 and 2) :9-18 , 2009.

[10] Q Rajput, N.S Khan, A Larik , S Haider,"Ontology Based Expert-System for Suspicious Transactions Detection" , Computer and Information Science; Vol. 7, No. 1; 2014ISSN 1913-8989 E-ISSN 1913-8997.

