Predicting the Fraud Volume in the Advent of Internet Enabled Handheld Devices

Nuha Zammarah and Asadullah Shah

***Abstract*—** Online banking has been growing tremendously in the recent years due to the vast development of internet applications on both computer and handheld devices. However, this advancement is faced by equally growing fraud attacks over the last decade. Customer awareness and vendor awareness are considered important factors in the study of fraud attacks volume increase. Moreover, more stringent security standards and multiple defensive security lines have been proposed to reduce the fraud attack cases. Nevertheless, fraud attack cases are showing a relentless increase in the past decade. This increase is attributed to the development of new attack methods and the evolution of new technologies which form new channels for fraudulent to attack. This paper addresses the fraud attack from a new perspective. In this paper, Adaptive Neuro-Fuzzy Inference System (ANFIS) is used to associate the increase in both computers based and handheld devices based internet usage and the fraud attack volume. The system will be trained from data collected in the past decade and then used to predict the effect of internet usage rate on the fraud attack volume for different age groups as well as the total fraud volume in the future. Three different scenarios in this study are considered to be addressing the effect of personal computer operating system, mobile operating system and android attack rate on the fraud volume. Results show that fraud volume would increase with the increase of android attack rate and would decrease with the increase of personal computer and mobile operating system usage rate. Therefore, the main focus on the awareness about fraud should be given to the mobile operating system users who are aged between 20-39 years old and above 70 years old as they cause increasing in the fraud.

***Keywords*—** Online banking, fraud, ANFIS, handheld devices.

I. Introduction

IN this era of globalization, the world is becoming highly interconnected and integrated with the Internet and its related applications. Therefore, Internet is becoming more important in people's day to day activities. Internet-based electronic banking, is also called online banking, is a new channel for the banking business development. Nowadays, online banking becomes the preferred choice for many customers and some providers; this could be attributed for many reasons, to mention some;

1. Time saving of customers. Nowadays, e-banking system provides fast and easy to use platforms which allow customers to perform their banking activities without physically attending any bank branch.

Nuha Zammarah, PhD Student, Ministry of Higher Education, Saudi Arabia.

2. Bank management perspective: online banking is a cost effective alternative to regular banking activities. For such reasons the demand for online banking has increased and the number of people who rely on online transactions has tremendously increased.

The first appearance of the concept of online banking was in the 1980's. In 1995, the first online banking in the world founded in U.S and called Security First Network Bank (SFNB). By 2005, it is reported that one out of every 4 adults of US's residents used online banking. Moreover, by the end of 2002 about 30% of Americans performed their banking transactions using online banking and this figure jumped to 50% in 2003 [1], [2], [3]. Similar trends can be noticed in Singapore, Germany, Sweden, India and Norway [4], [5] [6] [7], [8]. The first appearance of online banking in china lags USA by 3 years. Between 2001 and 2006 in UK, the number of people using Internet or online banking has increased by 174% [9].

This rapid increase in online banking usage raises the need of ensuring the security of the transactions because of the volume of sensitive data carried on the net. This security awareness led to the development of different security standards to improve the security system reliability. Though, records collected in the last decade shows that the fraud volume is increasing rapidly despite all the efforts spent to reduce its growth.

Many researchers studied the fraud growth phenomenon and highlighted different factors that influence its volume increase. The factors can be classified into three main categories:

1. Security systems technical limitations.
2. Customer awareness, and
3. Security system Vendor awareness.

Technically, the security system is required to be affordable and provides high security level within acceptable response. Nonetheless, achieving such attributes proved to be difficult. Some technical solutions show reliability against certain types of attacks and exhibits failure against other forms [10].

On the other hand, customer awareness is considered one of the most important factors affecting the fraud volume growth because detection of fraud cases start from the customers [11]. Therefore, online banking security is not sole organization responsibility; it is shared between customer and organization. The organizational responsibility, represented as vendor awareness, is to update their compliance and data legislation to improve data security along with providing fraud prevention education to the employees. The customer awareness starts by

detecting the fraud and reporting the case through the available channels [11], [12], [13].

Increasing the customer awareness is a challenge because of the diversity of customers dealing with online banking applications. These varieties of customers are exhibiting a wide range of technical knowledge of internet usage which further complicates the customer awareness efforts. Tolnai & Solms [14] developed Information Security Awareness Portal (ISAP) to provide the necessary security information to the customers. However, the questions remain are how many customers are aware of the availability of this portal and how many of them addressed its information?.

Recently, internet usage is no more restricted to personal computers. The advent of handheld devices equipped with internet facilities occupies a major share of internet data usage. The advantage of handheld devices over personal computers is allowing the customers to stay online by providing them multiple channels of communications. Moreover, handheld devices help to increase the diversity of customers who are able to access online applications which increases their vulnerability to fraud attacks.

As handheld devices are new technology, mobile internet guidance absence may confuse banking leaders and customers as well. This technology may complicate the fight against the fraud and increases the vagueness of understanding the fraud rate behavior in the near future. Mobile internet usage is showing a sharp increase since the advent of smart devices which might encourage the fraudsters to migrate to mobile internet hacking. Therefore, more stringent application control strategies are recommended to prevent hacking on mobile internet compared to personal computer based internet [11], [12].

In general, from the trends of fraud data, the impact of all the efforts spent to reduce the fraud growth is limited. Furthermore, a comprehensive understanding of the influence of migration to the smart devices technology on the fraud growth is not thoroughly investigated in literature. Moreover, efforts to predict the future of fraud in the era of smart devices are still premature.

The contribution of this work is developing a mathematical model of the fraud volume behavior in relation to the internet and smart phone usage rates and personal computer based internet usage rate. This model will provide a quantitative evaluation of the effect of handheld devices on the fraud growth. The proposed model is used to predict the future of fraud when the handheld devices usage dominates other technology. The developed system is utilizing ANFIS to establish the required relation and then it will be used to predict the future of the fraud volumes.

The next section of this paper discusses the data collection and preprocessing. The third section demonstrates the system development followed by the results and discussion section. The last section concludes the work and provides the recommendations based on the results.

II. Data Collection

This work is aiming to model the fraud behavior in relation to the smart phone and computer based internet usage rates. However, in many countries fraud volume data is considered classified and governed by regulations controlling the data online availability. Therefore, fraud volume in USA is collected and considered as a case study in this work. In addition, the percentage of smart phone usage and the computer based internet data rates in global scale are collected. Using global rates of internet usage with fraud volume for USA in this study is justified by noting that most of the fraud in USA is sourced from outside the country [15], [16]. Therefore, the increase in the global mobile phone usage and computer based internet rates affect the fraud in USA.

The smart phone usage and computer internet data rates are presented in percentages of the global population, while the fraud volume is presented as number of cases per year [17]. Preprocessing stage is used to prepare the collected data for ANFIS training. The preprocessing involves the following steps:

1. Data mapping stage which maps the smart phone and computer based internet usage rates to represent the volume.
2. Curve smoothing is implemented to extract the data trend.
3. Data scaling stage to limit the domain of the data in the interval [-1, 1] to be suitable for ANFIS training.

III. System Development

To model the relation between the fraud cases and the parameters, Adaptive Neuro-Fuzzy Inference system (ANFIS) is used. The choice of ANFIS is due to its integration between the power of learning of Artificial Neural Networks (ANN) back propagation and the power of Fuzzy in representing the system model as a set of rules. Moreover, ANFIS shows faster learning compared to ANN since it utilizes the gradient descent combined with least square method in the learning algorithm. The system is shown in Fig. 1.

Population growth (pop growth), personal computer operating system usage rate (PC O/S usage rate), usage rate in mobile operating system (Mobile O/S usage rate) and android attack rate are the input in this model. Windows operating system is the one that used in this paper as it is the most common PCs' operating system based on collected data. Moreover, the most popular operating systems in mobile are Iphone Operating System (IOS) and android. Therefore, this paper used the usage rate of them. According to collected data, the biggest percentage of attacks was targeting android operating system devices [18]. So, using the percentage of attack on android will help to find the required result. The fraud complains count divided according to the age is the output of this model. Results will be addressed based on three different scenarios. Each scenario increasing one factor and keep the other constant to study the effect of each factor on the fraud volume. Apart from population growth as it is increase constantly [17].

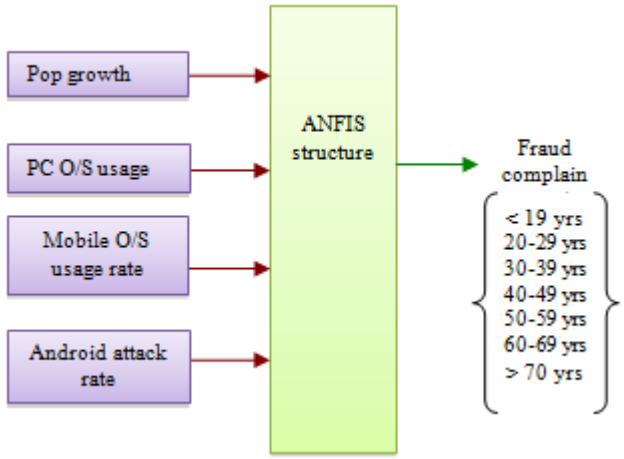

Fig. 1 Proposed system (ANFIS)

IV. System Model

Each single output needs to create ANFIS and for each input there are two membership functions. The system decides how to establish connection between membership function and rules using back propagation. Each rule create linear equation so, least square method is used to get the output. The structure of this system is showing in Fig. 2. This structure for one single output (here using the fraud complain count for age rate as an example).

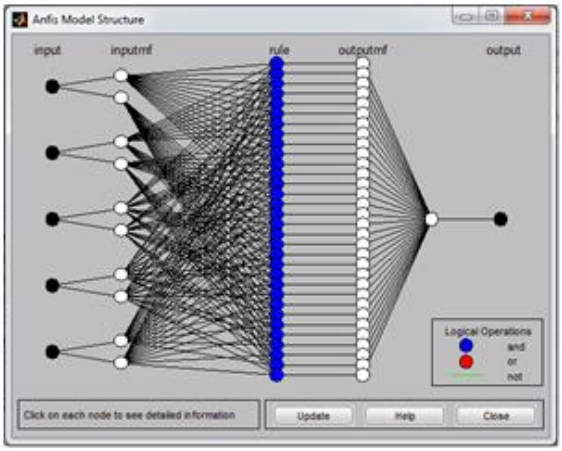

Fig. 2 Structure of proposed system (Internal Operational)

V. System Validation

A. Training ANFIS

The membership functions have many types. The different types have been investigated with same set of input data. Sigmoid Membership Functions (psigmf) gives more stable result. This paper used psigmf as it is most suitable type with the available data. Fig. 3 show all types of membership functions (mf) types. By training the system, finding that it is work very well as showing in Fig. 3.

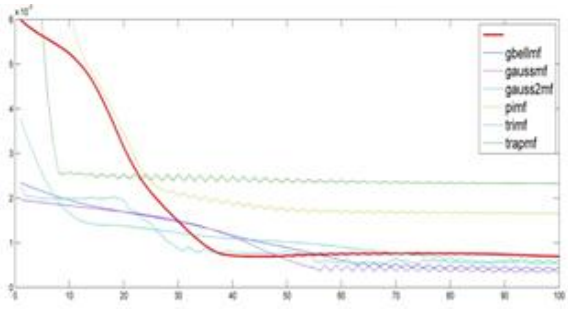

Fig. 3 Membership function training

B. Estimation

It is possible to choose a number of years to forecast the result as training ANFIS is a success. For example the estimated result for the next six years will get this result as shown in Fig. 4.

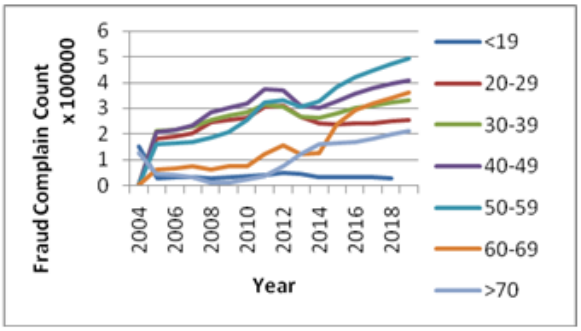

Fig. 4 Estimated result for next six years

VI. Prediction Results

The model after training is ready to estimate the result for future. The estimation results have been done for six coming years in the future. This work is divided into three different scenarios:

A. Scenario 1:

If the population and personal computer operating system usage rate are growing and usage rate in mobile operating system and android attack rate are still as it is. It is clear that the fraud complain count is decreased when the personal computer operating system usage rate increase in next six years as shown in fig.5. This is because using the personal computer is more secure than using handheld devices as the anti-virus programs need large space of memory which is not available easily in handheld devices.

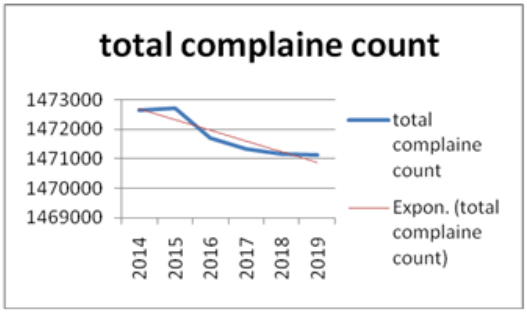

Fig. 5 Trend of estimation result (scenario 1)

B. Scenario 2:

If the population and usage rate in mobile operating system are growing. However, personal computer operating system usage rate in addition to android attack rate are still as it is. It is clear that the usage rate in mobile operating system such as IOS and android will increase the fraud complain count from the people especially who are between 20-39 years old and above 70 years old as shown in fig. 6, fig. 7 and fig. 8. However, people in other age groups cause decreasing in the fraud complain count as shown in Fig. 9. This is because the people who are between 20-39 years are using the new technology such as handheld devices more than the others in different age categories. Therefore, they faced the fraud problems by using handheld devices. The people who are above 70 years old are not aware enough about the fraud. Therefore, these people cause increasing number of fraud complains.

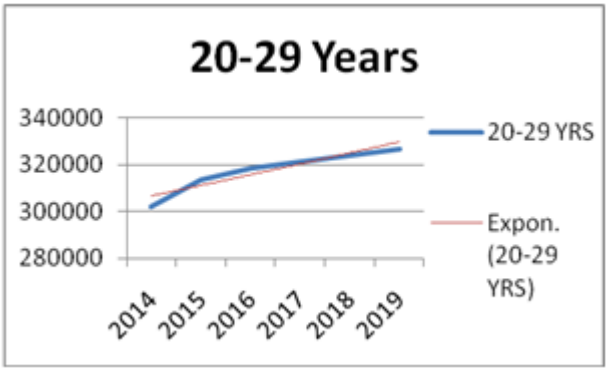

Fig. 6 Trend of estimation result for 20-29 yrs

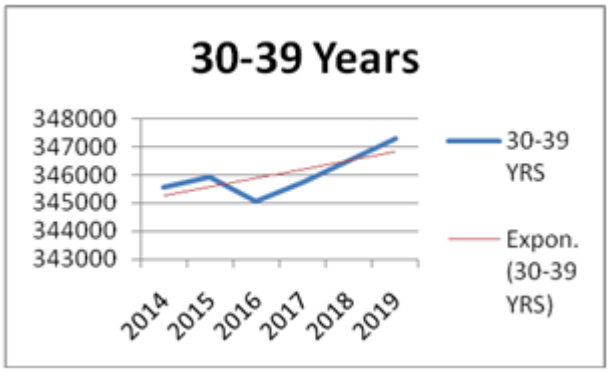

Fig. 7 Trend of estimation result for 30-39 yrs

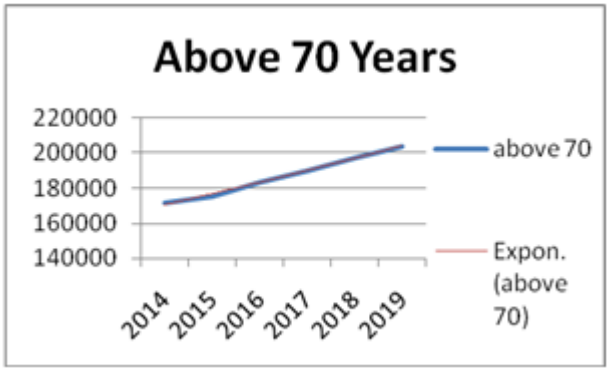

Fig. 8 Trend of estimation result for above 70 yrs

C. Scenario 3:

If the population and android attack rate are growing. However, personal computer operating system usage rate in addition to usage rate in mobile operating system are still as it is as shown in Fig. 9. It is clear that the android attack rate increase the complain count. So, there is a parallel relationship between the android attack rate and the complain count. In other words, when the android attack rate increase the complain count increase also from all different ages which is expected as shown in fig. 10.

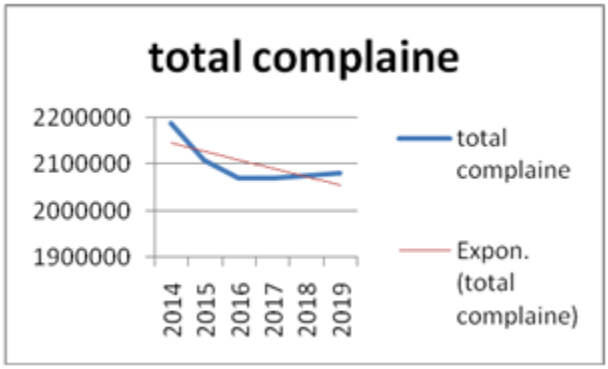

Fig. 9 Trend of estimation result (scenario 2)

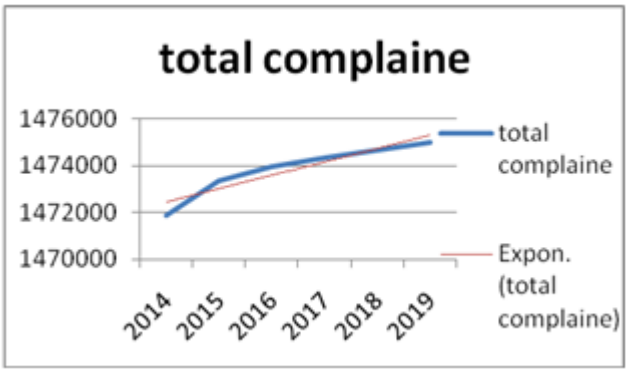

Fig. 10 Trend of estimation result (scenario 3)

VII. Conclusion and Recommendations

The Online banking is a new technology used by most people recently. However, it is vulnerable to fraud. This paper studied the effect of personal computer operating system, mobile operating system and android attack rate on the fraud volume.

ANFIS system has been used to find the relation between personal computer operating system, mobile operating system and android attack rate with fraud volume in addition to estimation result in the next six years. This system was training data and then used to predict the effect of the different factors on the fraud volume. Three different scenarios have been addressed to find the effect of each factor. Each scenario is increasing one factor and keeping the others constant.

Results showed that there is an inverse relationship between the personal computer operating system and fraud volume as the fraud complains decrease when the personal computer operating system usage rate increases. The same relation is also there between the mobile operating system and fraud volume. However, there is some age groups affecting

positively on the fraud volume which are 20-29, 30-39 and above 70 years old as the fraud increasing with the increasing of the mobile operating system usage rate from these age groups. The result also showed that there is a parallel relationship between android attack rate and fraud volume as the android attack rate affect positively on fraud volume.

Based on these results, keep using personal computer to achieve online banking transaction is a good idea. This is because personal computer is a more secure channel as it has a large space that make the antivirus program work efficiently. Using online banking through the handheld devices should be limit especially for the users who are between 20-39 years old. The awareness should be given especially for the users who are above 70 years old. The Android operating system is targeted as it is easily attacked so, it is better to be banned, especially for online banking transactions.

REFERENCES

[1] Bruno, m.a.(2003). Bofa's climb to the top of the online world. Us banker, 113(6), PP.24-25.

[2] Ramasan, C. (2003). Online banking comes of age. Bank systems and technology, 40(11), P.29.

[3] Pewinternet. (2009). Online banking.

[4] Burto, G. (1999). E-Banking 1999: New Model of Banking Emerges. Stamford, CT: Gartner Group.

[5] Mulligan, P. & Gordon, S. (2002). The impact of information technology on customer and suppliers relations in the financial services. International journal of service industry management, 13(1), pp.29-46. http://dx.doi.org/10.1108/09564230210421146

[6] Mattila, M., Karjaluoto, H. & Pento, T. (2003). Internet banking adoption among mature customers: early majority or laggards? Journal of services marketing, 17(5),PP.514-528.

[7] Gerrard, P. & Cunningham, J. (2003). The diffusion of internet banking among singapore consumers. International journal of bank marketing, 21(1),PP.16-28. http://dx.doi.org/10.1108/02652320310457776

[8] Srivastava, R. (2007). Customer's Perception on usage of Internet Banking. Innovative Marketing, 3(4), pp.66-72.

[9] APACS. (2009). Online banking usage among over 55s up fourfold in five years.Pewinternet.

[10] Hisamatsu, A., Pishva, D., & Nishantha, G. G. D. (2010). Online banking and modem approaches toward its enhanced security, 1459–1463.

[11] Inscoe, S., Litan, A., Speare, M., & Tubin, G. (2012). Faces of Fraud Insights and Recommendations from Top Fraud Experts : From the Editor.

[12] Ponemon Institute Report. (2012). 2012 Business Banking Trust Trends Study Sponsored by Guardian Analytics. Retrieved from: http://www.ponemon.org/library/2012-business-banking-trust-trends-study

[13] Karim, Z., Rezaul, K. M., & Hossain, A. (2009). Towards secure information systems in online banking.

[14] Tolnai, A., & Solms, S. Von. (2009). Solving security issues using information security awareness portal. IEEE. http://dx.doi.org/10.1109/icitst.2009.5402560

[15] APWG report. (2013). Phishing activity trends report 3 quarter. USA. Retrieved from http://www.antiphishing.org/

[16] CSN report. (2013). Consumer sentinel network data book january – december 2012. Usa. Retrieved from http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf

[17] Geohive, (2013). Population of the entire world, yearly, 1950 - 2100, http://www.geohive.com/earth/his_history3.aspx

[18] Kaspersky Lab Global Research And Analysis Team (GREAT). (2013). Kaspersky security bulletin 2013, (c). Retrieved from http://www.securelist.com