PREDICTING THE FRAUD VOLUME IN PERSONAL COMPUTER USING DIFFERENT WEB BROWSERS

[1]Z. Nuha, [2]Sh.Asadullah
International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Selangor, Malaysia
For Correspondence; [1]nuha_rose_963@hotmail.com, [2]asadullah@iium.edu.my

ABSTRACT: *Online banking has grown 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. 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 paper presents fraud attack prediction from a new perspective. Adaptive Neuro-Fuzzy Inference System (ANFIS) was utilized for the data collected in the past decade and then used to predict the effect of internet usage rate on the fraud attack volume of different age groups as well as the total fraud volume in the future. Seven different scenarios in this study are considered to be addressing the effect of different web browsers on the fraud volume. Results show that fraud volume would increase with the increasing of using Mozilla, Firefox, Opera, Safari and Chrome and would decrease with the increasing of internet explorer and Netscap.*

1. INTRODUCTION

Technological development has transformed the world to a global village, with the aid of highly interconnected and integrated Internet and its related applications. This has become more important to people's day-to-day activities. Online banking is a part of this achievement, where banking business is performed strictly on the Internet. Nowadays, online banking becomes the preferred choice for individuals, private organizations and government. This could be attributed mostly to saving time and cost effectiveness, which leads to a high demand for online transactions. About 50% of Americans performed online banking transactions starting from 2003 [1-3]. The increases are spread elsewhere around the world [4-9].

The increases of online banking comes along with security obstacles. This has been the major concern for both the stakeholders and researchers. While there are several research attempts to tackle the online fraud growth phenomenon, yet

New attack and fraud tactics are coming up. This problem lies from both technical and social aspects of online issues. Pertaining to the security system that involves technical applications, research studies have provided some possible solutions against some certain types of attacks and those that required more approach [10]. Unfortunately, when it comes to the social aspect of the online banking fraud cases, onward information and perceptions are required. There is a need of understanding different aspects of awareness of online banking fraud. Crucial to this is awareness of detecting the fraud. One of the most important factors affecting the fraud volume growth is also important [11]. Previous studies have revealed that awareness of online banking fraud starts by detecting the fraud and reporting the case through the available channels by individuals [11-13]. Hence, various factors, which influence awareness of online banking fraud is necessary, and need to be understood clearly. Information Security Awareness Portal (ISAP) is one of the major tools used by considering many factors that might provide the necessary security information [14]. However, the drawbacks of such approach is the lack of individual awareness and perceptions with respect to the detecting fraud inceptions and operations time, as well as possible predictions on some signs of attempting fraud while performing online banking transactions.

Various efforts to predict the future of fraud in the era of smart devices are still premature, although, personal computer operating system has been discovered to be more secure than handheld devices in terms of online fraud [15-16], yet. Personal computer operating systems are packages with different web browsers. This is also a crucial avenue to fraud cases. It is worthwhile to mention that the aforesaid works [1-16] still focusing on various aspect of fraud banking case, Nevertheless, how to extract future fraud attempt for practical applications and detecting factors of the current fraud cases has not been greatly discussed. Hence, this paper presents a mathematical model intended to exert fraud volume behavior in relation to the different internet web browsers usage rate. The model is developed by quantitative evaluation of the effect of handheld devices on the fraud growth. Thus, the developed model utilizes ANFIS to establish the required relation as well as the prediction of the future of the fraud volumes.

2. DATA COLLECTION

Fraud volume for USA was used for this research. It was collected via online and it's free, the raw data are the percentages of fraud related reports from smart phone usage and the computer based internet data rates for global scale. The reports reveal that majority of fraud attempt in USA comes from outside the country [17-18]. Hence those reports on the fraud cases related to the global mobile phone usage and computer based internet rates for USA is gathered for analysis. 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 [19]. The raw datasets are being transformed in the Preprocessing stage through, Data mapping; Curve smoothing; and Data scaling suitable for ANFIS training, aimed at modeling predictions of fraud cases.

3. EXPERIMENTAL ANALYSIS

Adaptive Neuro-Fuzzy Inference system (ANFIS) is used in the modelling of the fraud predictions cases. It has the ability to integrate Artificial Neural Networks (ANN) back propagation and Fuzzy logic in representing a system model as a set of rules. This research proposed model is shown in Fig. 1.

Population growth (pop growth), type of internet browser such as Mozilla, Internet explorer, Fire fox, Netscap, Opera, Safari and Chrome are the input of the model. The fraud complains count divided according to the age is the output of this model. For Each scenario, increasing one web browser and keeping the other constant is the exercise. This will study the effect of each web browser on the fraud volume. Apart from population growth as it is increase constantly [19].

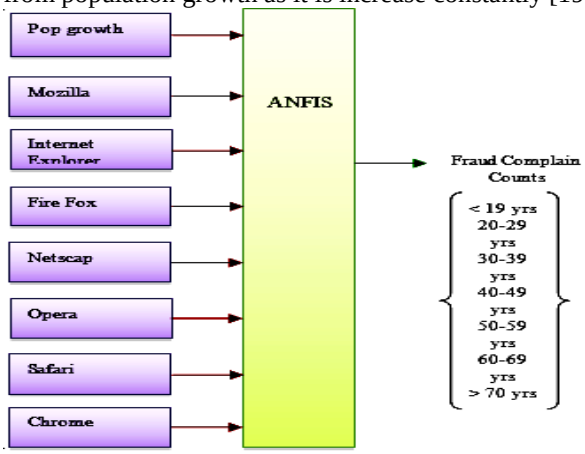

Fig. 1: Proposed system (ANFIS)

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. All types of membership functions (mf) types are used. Then, the training the system was set and.

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. 3.

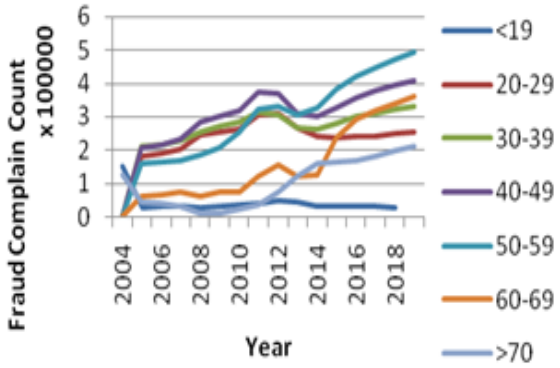

Fig. 2: Membership function training

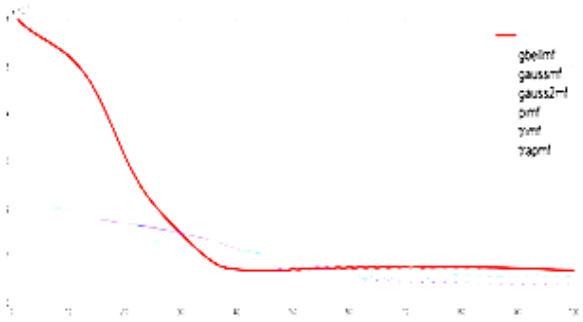

Fig. 3: Membership function training

4. 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:

Scenario 1:

If the population and Mozilla web browser are growing and Internet explorer, Fire fox, Netscap, Opera, Safari and Chrome are still as it is. It is clear that the fraud complain count is increase when the Mozilla usage rate increases in next six years as shown in fig.4.

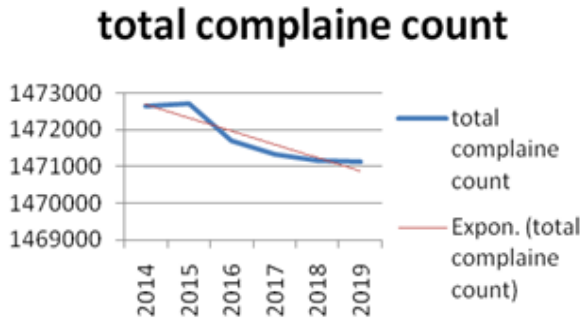

Fig. 4: Trend of estimation result scenario 1 (Mozilla)

Scenario 2:

If the population and Internet explorer web browser are growing and Mozilla, Fire fox, Netscap, Opera, Safari and Chrome are still as it is. It is clear that using internet explorer decrease the fraud complaint as shown in fig 5. This means that using internet explorer is more secure than others.

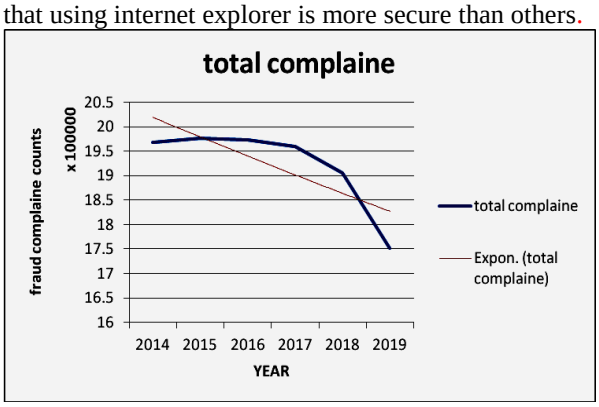

Fig.5: Trend of estimation result for scenario 2 (Internet Explorer)

Scenario 3:

If the population and Fire fox web browser are growing and Mozilla, Internet explorer, Netscap, Opera, Safari and Chrome are still as it is. It is clear that the fraud complain count is increased when the Firefox usage rate increases in next six years as shown in fig.6.

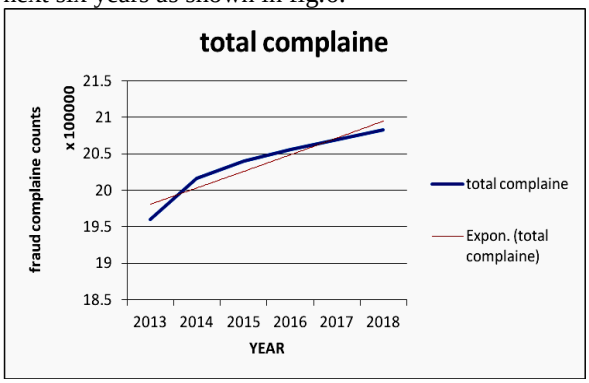

Fig.6: Trend of estimation result scenario 3 (Firefox)

Scenario 4:

If the population and Netscap web browser are growing and Internet explorer, Fire fox, Mozilla, Opera, Safari and Chrome are still as it is. It is clear that the fraud complain count is increase when the Netscap usage rate increases in next six years as shown in fig.7.

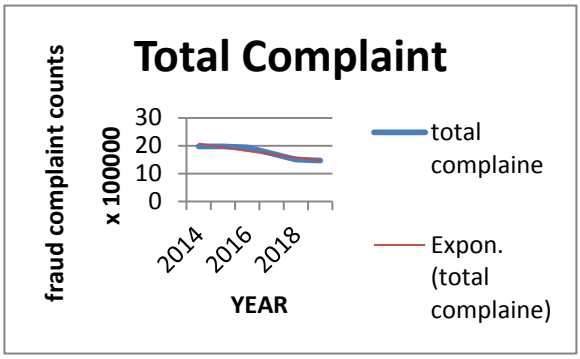

Fig. 7: Trend of estimation result scenario 3

Scenario 5:

If the population and Opera web browser are growing and Internet explorer, Fire fox, Netscap, Mozilla, Safari and Chrome are still as it is. It is clear that the fraud complain count is increase when the Opera usage rate increases in next six years as shown in fig.8.

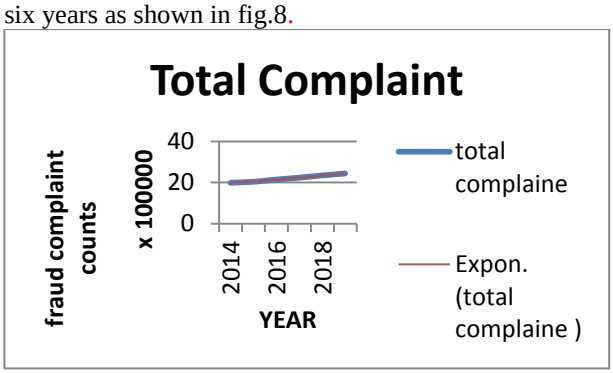

Fig 8: Trend of estimation result for scenario 5 (opera)

Scenario 6:

If the population and Safari web browser are growing and Internet explorer, Fire fox, Netscap, Opera, Mozilla and Chrome are still as it is. It is clear that the fraud complain count is increase when the Safari usage rate increases in next six years as shown in fig.9.

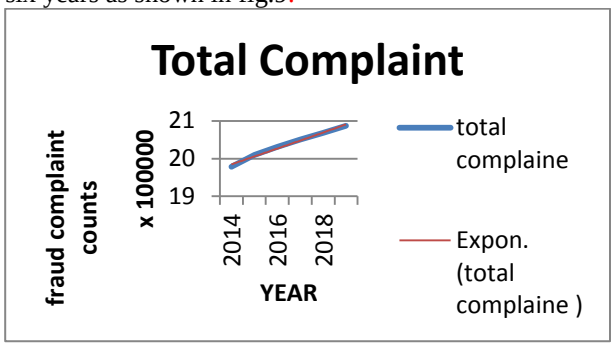

Fig 9: Trend of estimation result scenario 6 (safari)

Scenario 7:

If the population and Chrome web browser are growing and Internet explorer, Fire fox, Netscap, Opera, Safari and Mozilla are still as it is. It is clear that the fraud complain count is increase when the Chrome usage rate increases in next six years as shown in fig.10.

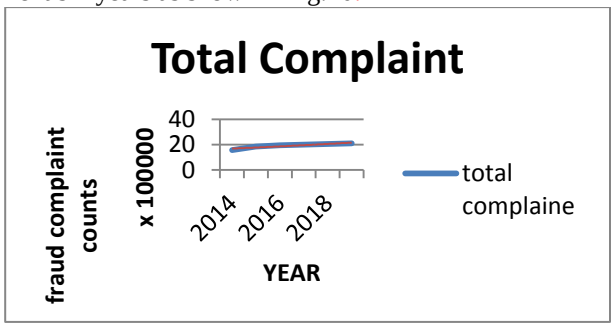

Fig 10: Trend of estimation result scenario 7 (Chrome)

5. CONCLUSION AND RECOMMENDATION

The Online banking is a new technology used by most people recently. However, it is vulnerable to fraud. It has been proofed in previous work that using personal computer operating system is more secure. This paper studied the effect of different web browsers on personal computer operating system on the fraud volume.

ANFIS system has been used to find the relation between different web browsers 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. Seven 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 Internet explorer and Netscap web browsers and fraud volume as the fraud complains decrease when these web browsers usage rate increases. The result also showed that there is a parallel relationship between Mozilla, Fire Fox, Opera, Safari and Chrome web browsers and fraud volume as increasing these web browsers usage rate affect positively on fraud volume.

Based on these results, keep using secure web browser such as internet explorer and Netscap to achieve online banking transaction is a good idea. It is important to be more care when using some web browsers such as Mozilla, Fire Fox, Opera, Safari and Chrome.

6. ACKNOWLEDGEMENTS

I thank Allah, the almighty, for giving me the strength to carry on this paper and for blessing me with many great people who have been my greatest support in both my personal and professional life. I would like to take this opportunity to express my deepest regards and gratitude to my supervisor Professor Asadullah Shah.

7. REFERENCES

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

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

[3] Pewinternet. Online banking. (2009)

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

[5] Mulligan, P. & Gordon, S. 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 (2002)

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

[7] Gerrard, P. & Cunningham, J. The diffusion of internet banking among singapore consumers. International journal of bank marketing, 21(1),PP.16-28. (2003)

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

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

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

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

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

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

[14] Tolnai, A., & Solms, S. Von. Solving security issues using information security awareness portal. IEEE. (2009)

[15] Nuha, Z. and Asadullah, Sh., predicting the financial frauds Using Adaptive Neuro-Fuzzy Inference System", IJCC, AACL 07, pp. 53~54. (2016)

[16] Nuha, Z. and Asadullah, Sh., predicting the fraud volume in the advent of internet enabled handheld devices", ICAESAM, (2015) http://dx.doi.org/10.15242/IIE.E1215039, ISBN: 978-93-84422-47-9.

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

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

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

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