Investigation and Development of a Biometric e-Fraud Prevention System

CONFERENCE PAPER · SEPTEMBER 2013

DOI: 10.13140/2.1.1847.1042

3 AUTHORS:

Kazembe Tr

Fort Hare University

1 PUBLICATION **0** CITATIONS

SEE PROFILE

Mfundo Shakes Scott

Fort Hare University

22 PUBLICATIONS **1** CITATION

SEE PROFILE

Nobert Jere

Polytechnic of Namibia

23 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Investigation and Development of a Biometric e-Fraud Prevention System

Kazembe T.R., Scott M.S. and Jere N.R.
Telkom Centre of Excellence, Computer Science Department,
University of Fort Hare, P/Bag X1314, Alice, 5700, South Africa
Cell: 0794548694, Tel: 0406022746, Fax: 0862489404
Email: tkazembe@ufh.ac.za, sscott@ufh.ac.za, njere@ufh.ac.za

ABSTRACT- Online Fraud remains a single colossal form of modern day crime with trickery ploys that seem to increase at a pace faster than technology is changing. No doubt online fraud is the cause of concern not only in developing countries but the world at large. Relying only on User ID and User Password as well as case based online Fraud analytics adapters is neither practical nor efficient at stopping the stealing of user name and password. The work paper explores biometrics as a better option to introduce Fraud prevention efforts. It is the prelude to the development of an online fraud prevention framework targeted at improving the plight of marginalised communities specifically Dwesa in the Eastern Cape province of South Africa This is a rural location in which our research team has an ICT infrastructure deployed and villagers from this community make use of such a facility for their various daily operations.

Keywords: e-Fraud; biometrics; online fraud; identity theft; Banking Security Framework; BEFP; Fingerprint; ICT.

I. INTRODUCTION

The pervasiveness of ICT (Information and Communication Technology) has made us all users of computing devices both at business and individual level while it reduces costs of standing in bank queues and travelling to shops [1].There is an e-Fraud (electronic fraud) side effect that according to a survey conducted by United Kingdom (UK) information Security Breach and the UK National High-Tech Crime Unit. Online Fraud is the single biggest serious e-Crime and takes over 60% of e-Crime [2]. Fraud occurswhen a userID and a password are stolen resulting in lossof money from a bank account and hence Fraud prevention efforts are targeted at making financial information systems secure to fight against Fraud. Biometrics Fraud Prevention is based on distinctiveness, permanence and non-repudiation and it also suggests the use of any physiological features such as face, fingerprint, Iris, Palm print, hand geometry, voice, signature, DNA, hand veins and keystroke dynamics on online transactions to minimise the fraud risk [1] .

II. OVERVIEW OF BIOMETRICS FRAMEWORK

Primarily the system is targeted at online fraud prevention through biometric features and can only work as part of a financial institution's security framework, because all fraud efforts are aimed at faking or pilfering an ID to claim financial assets that are not your own. The system will require that a user produces their password as well as a Biometric ID for both ATM (Automated Teller machine) and Internet transactions. This will improve existent systems that rely on credit card information that can easily be stolen and abused.Biometric featureshave beenused over time to capture criminals (fingerprint), Forensic Investigation (DNA (deoxyribonucleic acid) andFingerprint), Voice recognition system (anti-terrorism) [5].The Fraud gap existing in South Africa and all over the world may be closed or minimised by Biometrics because they make online transactions resemble face to face scenarios where people can shake hands.

III. THE BIOMETRICS E-FRAUD PREVENTION SYSTEM

The biometric fraud prevention application is designed to stop purveyors of e-Fraud from accessing bank accounts other than theirs. However before committing an online transaction the system will ask for a biometric feature to be entered on a relevant device such as a face scanner, hand pattern scanner, finger print reader or any biometric feature reader. Once entered the data will be matched with a template in the database and the result can be a rejection or acceptance of the transaction. The key advantage with biometrics is no two people share common biometric features and it takes a lot of effort for example to steal a finger print. Biometrics have been reliably used in the world at large in forensic investigations and every law enforcement agency uses the fingerprint and once detected their verity is irrefutable [3]. Sensor hardware such as finger print scanners, iris scanners and face scanners from different vendors shall be tested to improve system interoperability.

IV. BIOMETRIC FRAMEWORK METHODOLOGY

For successful development it is imperative to unit test and consult every step of the biometric system development process to ensure conformance to known, best practices taking note that the system will behave differently under different circumstances that include; composition of user population (age, size, gender, profession etc.),size of database, and variations in operating environment(temperature and humidity)[3]. The following steps shall be followed in the design process; requirements analysis, architecture design, detailed design, extensive coding, system integration and maintenance. The design process will among other things; ensure relevance, accuracy and assurance through tests on false rejects and false accepts. The entire development process shall be done

with the highest security expectations in mind hence SQL SERVER 2012 shall be used as the database application. This is because the application has built in predictive programming tools with the ability to flag anonymous data, predict values that are missing, perform text mining on data flows [6].

V. WORK DONE AND FUTURE WORK

Development of a BEFP (Biometric e-Fraud Prevention) system is imperative considering the losses suffered by banks especially in South Africa [4] and many efforts have been put towards fraud prevention. The latest breakthrough is case based systems that are able to learn and adapt to changes using artificial intelligence and powerful algorithms;an example is the fraud analytics adapter from IBM [9]. The proposed system as shown in figure 1 checks user information against stolen cards, credit card number, security code, expiry date and etc. however before a decision is made the system will prompt for a biometric feature. An obvious issue arising is the lack of standardised biometric feature accepting devices. Binarisation converts the grey scale image into a black and white image this is because systems generally process binary images better. Skeletonisation will transform the digital binary pattern into a connected skeleton of unit width with minimised bifurcations. Matching an input image with a template involves computing the sum of the squared differences and if they are below a given threshold then there is a match. A sum of the squared errors E is calculated with K which is the number of pairs in any set B. The equation is shown below:

$$E_{ms} = \frac{1}{k}\sum_{i=1}^{k} e_i^T e_i = e_1^T e_2^T \ldots e_k^T \begin{bmatrix} e_1 \\ e_2 \\ \cdot \\ \cdot \\ \cdot \\ e_k \end{bmatrix} \frac{1}{k}$$

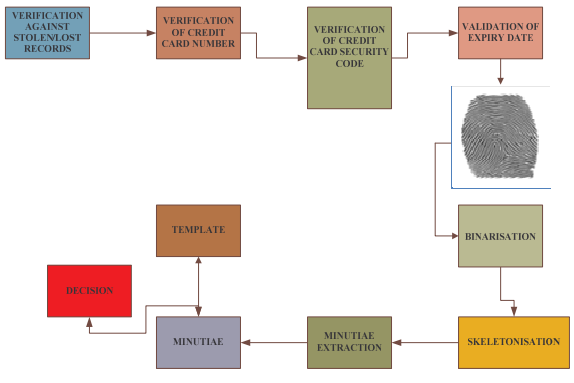

Figure 1: Proposed Biometric Framework

VI. CONCLUSION

Online crime is constantly changing increasing in magnitude and methods; phishing, pharming and Trojans represent some of the most organized and sophisticated technological crime waves worldwide. Successful development and deployment of an online fraud prevention application will help make our world a better place and improve everyone's confidence including rural communities when transacting online. Biometrics are the key to bringing about this change and the BEFP will vastly reduce online crime statistics.

VII. ACKNOWLEDGEMENTS

This work is based on the research undertaken within the Telkom CoE in ICTD supported in part by Telkom SA, Tellabs, Saab Grintek Technologies, Easttel, Khula Holdings, THRIP and National Research Foundation of South Africa (UID : 84006). The opinions, findings and conclusions or recommendations expressed here are those of the authors and none of the above sponsors accepts no liability whatsoever in this regard.

VIII. REFERENCES

[1] **Danish Jamil et al**, Keystroke pattern recognition preventing online fraud, 03 March2011http://www.Connections.ebscohost.com/c/articles/66134831/keystroke-pattern-recognition

[2] **C.Corzo,F .Corzo; N Zhang and A Carpenter**; Using automated banking certificates to detect unauthorised financial transactions; Computer science volume

[3] **Anil.K.Jain,Ajay.Kumar**; Biometrics of Next generation: An Overview, 2010,

[4] **Siya Boya, businessman charged for tax fraud,(2012).**http://www.sowetanlive.co.za/

[5] **Micci-Barreca, Daniele**, Security Management, Electronic Commerce, Sept, 2003.

[6] **Microsoft Corporation,** SQL Server Data Mining Data sheet, (Mar 2012).Available at: http://www.mcirosoft.com/sqlserver

[7] **Oversight Systems**, Forensic Auditing: Structural requirements for fraud monitoring, (2009). http://www.oversight systems.com

[8] **RSA Anti-Fraud Command Centre**: RSA Online fraud report,

[9] **IBM**, Real-time fraud detection analytics on system z, August 2011

Kazembe T.R is a Zimbabwean born at Mutare in the Manicaland province. He completed his BSc (Hons) Information systems in 2006 at Midlands State University and is presently pursuing an MSc in Computer Science at Fort Hare.