ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 6, June 2015*

# Reducing Internal Banking Fraud using Smart Cards and Biometrics as Access Control Tools

**Daniel Ugoh[1], Macdonald N. Onyeizu[2], Charles Ugwunna[3], Celestine O. Uwa[4]**

Technologist/Researcher, Computer Science Department, Nnamdi Azikiwe University, Awka, Nigeria[1]

PG Student, Computer Science Department, Nnamdi Azikiwe University, Awka, Nigeria[2,3,4]

**Abstract**: Internal crimes in banking industry are issues that face customers, bank employers and employees. A lot of internal criminal activities have been recorded in banking industry. Securing banking software from unauthorized access, unauthorized modification, unauthorized fund transfer and withdrawal has been a challenge. The researchers in this work responded to this challenge by developing a two-tier authentification system that is to be attached to the main banking software. This system uses magnetic featured staff identity card for identification and fingerprint biometric for authentication. The techniques of the Object Oriented Analysis and Design Methodology (OOADM) and the prototyping methodology were adopted for the systematic study and design of the system. The system was designed and implemented in Microsoft Visual C# development environment. The system was featured to interface with magnetic card and fingerprint readers. The result is a two-tier authentifiation system that would act as access control tool for the main banking software. An employee requesting for access into the banking software is expected to pass magnetic featured staff identity card check and fingerprint matching check. This will go a long way in reducing internal banking fraud.

**Keywords**: Authentification, Banking, Biometrics, Fraud, Internal, Template.

## I. Introduction

The gradual adoption of Information and Communication Technology (ICT) by different fields has brought tremendous development in growth and services rendered by the field. The banking industry has seriously utilized the untapped resources available in ICT to deliver superb services to their customers and enhance work process for their employees. This industry (banking) conducts most of its businesses via electronic means even those banks in the developing countries and this has made the industry vulnerable security breaches – both internally and externally. A security breach at a bank can result in a severe loss of business and reputation [1]. However, banking software developers have instituted some security or access control techniques to minimize fraud and security breaches. But in spite of this, there have been many concerns among the consumers related to security[2], whereby many organizations have suggested the use of Biometrics for authentication but still this has been hardly accepted by the consumers (Trocchian, Ainscough , 2006). This work is therefore aimed at developing supplementary software for banking software to enhance security and reduce internal fraud. We presented the use of magnetic embedded staff Identity card for identification and finger print biometric for authentication. These two access control tools must be passed before access is given into the main banking software.

## II. Review of Causes and protection of fraud

Poor internal control has been identified to be the main cause of fraud. Albrecht (1996) opined that the symptoms of poor internal controls increase the likelihood of frauds. Internal control symptoms include a poor control environment, lack of segregation of duties, lack of physical safeguards, lack of independent checks, lack of proper authorizations, lack of proper documents and records, the overriding of existing controls, and an inadequate accounting system.

Bologna (1994) reviewed that environmental factors could enhance the probability of embezzlement. These factors are: inadequate rewards; inadequate internal controls; no separation of duties or audit trails; ambiguity in job roles, duties, responsibilities, and areas of accountability; failure to counsel and take administrative action when performance levels or personal behaviour fall below acceptable levels; inadequate operational review; lack of timely or periodic review, inspections, and follow-up to assure compliance with company goals, priorities, policies, procedures, and governmental regulations and failure to monitor and enforce policies on honesty and loyalty.

However, Beirstaker, Brody & Pacini (2005) proposed numerous fraud protection and detection techniques. These various techniques include fraud policies, telephone hotlines, employee reference checks, fraud vulnerability reviews, vendor contract reviews and sanctions, analytical reviews (financial ratio analysis), password protection, firewalls, digital analysis and other forms of software technology, and discovery sampling. Furthermore, [7] believed that authentification systems at ATMs, transactions at the point of sale, telephone banking and online banking as well as many other banking applications are vulnerable to fraud and can be secured through biometrics technology. Although customers still have concerns about privacy, the banking sector is increasingly more and more interested in this technology (biometrics) [8].

DOI 10.17148/IJARCCE.2015.46114

## III. Our Proposed Solutions

Having comprehensively studied the internal security challenges facing banking industry, two new approaches are proposed: (a) use of Staff ID Card embedded with magnetic features for identification and (b) fingerprint biometrics for authentication. These two approaches are to be combined before access is granted into the banking software.

### *A. Biometric Solution*

Tabitha, Pirim, Boswell, Reithel and Barkhi (2006) defined *biometric* the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of humans. Such unique biological characteristics relies on individual humane identities such as DNA, voice, retinal and iris, fingerprints, facial images, hand prints, or other unique biological characteristics. Tabitha et al. (2006) noted that *biometric* is "a method of identification that has been growing in popularity" (p. 2). Moreover, Pons (2006) notes that *biometric devices* are technological devices that utilize an individual's unique physical or behavioral characteristic to identify and authenticate the individual precisely. Essentially, biometric technologies operate by scanning a biological characteristic and matching it with the stored data. Jain, Hong, and Pankanti (2000) note that a biometric system is "essentially a pattern recognition system that makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the user" (p. 92).

The use of Biometrics has become a common practice in many areas for the purpose of identification of a human and there are a number of researches related to this aspect whereby the system identifies the human by his individual anatomy such as his fingerprints and voice (Venkatraman and Delpachitra. 2008). The technology such as voice recognition and fingerprints or the iris detection is the most commonly used biometric systems in an application (Venkatraman and Delpachitra. 2008). The biometric system recognizes the various patterns of a system which is related to the acquired set of the stored information in the database. Based on the context of the data it is determined whether the context is in an identification mode or a verification mode.

The main reasons for having a biometric authentication is that biometrics are traits of a person which can be hardly copied or shared thereby it becomes very difficult to forge the identity of a person and even can be recovered easily in case if it is lost and this system are highly reliable than other systems due to its nature (Toledano, Pozo, Trapote, Gomez, 2006). Many research experts personally believe that Biometrics will be the future of the authentication industry (Toledano, Pozo, Trapote, Gomez, 2006).

Pons [20] maintained that fingerprints biometric scans are the most commonly used biometric solution for authentication as they are less expensive compared with other biometric solutions. A fingerprint is a unique pattern of ridges and furrows on the surface of a fingertip, the formation of which is determined during the fetal period. Fingerprints are unique for each individual, where even identical twins have different fingerprints [11]. Several scholars documented the increase popularity of fingerprint biometric-based systems and their decline in costs [11] and [14]. Another advantage of finger print biometric is that the reader is now embedded on some of the peripherals of computer system like mouse, keyboards, etc while some are attached with keypads for easy access and use. A number of affordable and widely available biometric devices that read fingerprints and plug into USB ports [15], as shown in figure 1.

Figure 1: Biometric enabled pad, keyboard and

Meanwhile, biometric authentification has become more and more popular in the banking and finance sector. The use of biometric technologies at ATMs, POS terminals and online-banking is currently only used in very small projects with few users except in Japan. Since August 2005 Japanese banks have had to replace customer losses from improper cash withdrawals by law unless culpable behaviour can be proved against the customer [16].

However, Sarker and Wells (2003) opined that user perception to adopt biometrics in banking is closely related to the security being offered in this form of banking and how it influences the user's perception to accept this technology. This construct is related to the perceptions of the users to adopt the technology of biometrics in the banking activities which suggests that adopting biometrics would make online banking more secure and offer him the best of services at the comfort of his own which again is in turn influenced with the construct of self efficacy [2].

### *B. Combination with Smart Cards*

Few studies have reviewed the importance of combining biometrics with smart cards during authentification

DOI 10.17148/IJARCCE.2015.46114

process. MasterCard estimates that adding smartcard-based biometric authentication to a POS credit card payment will decrease fraud by 80% [7]. The combination with smart cards supports privacy protection and increases security and trust [18]. The use of smart cards in combination with biometric authentication makes the storage of biometric data in a central database obsolete. The use of a central database using identification methods results in higher error rates depending on the number N of biometric templates [19]. Therefore the combination with smart cards using verification decreases the probability of a false identification and gives the user more privacy having his biometric data in his hands, which also increases the trust in the technology [18].

## IV. PROPOSED STAFF ENROLMENT METHOD

The first process in any biometric recognition system is enrolment‘, [20], whereby fingerprints of all users who are supposed to use the system are captured. Each fingerprint template is attached to the corresponding staff's magnetic identity card and is stored in the server database and biometric server database. All the fingerprint scans (templates) will be saved in an encrypted form to avoid any modifications. Figure 2 below shows the proposed staff enrolment method.

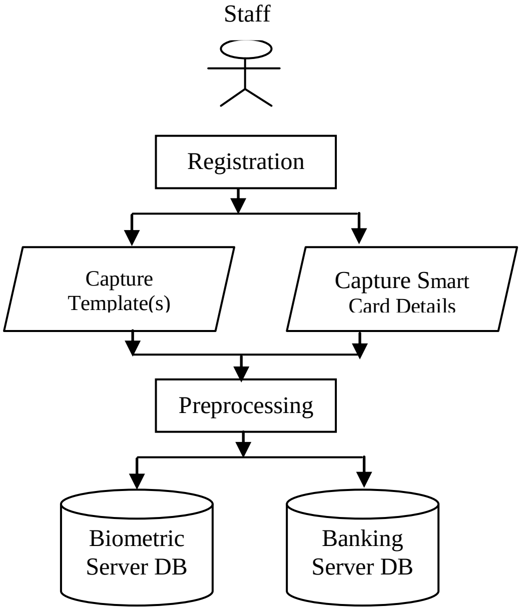

Figure 2: Proposed Enrolment Method

## V. GENERAL AUTHENTICATION PROCESS

The flowchart shown in figure 3 explains the general identification and authentication process. The authorized user is expected to swipe his/her staff identity card through the magnetic card reader (identification) and the system would prompt out fingerprint (authentication). These two processes must be successfully completed before full access is granted into the main banking software. Meanwhile, if an employee's identity card is stolen by a colleague or an intruder, and the person tries to login, the first stage (identification) would be successful while authentication would fail. However, the system is featured to capture the fingerprints of the intruder for fraud check by the management.

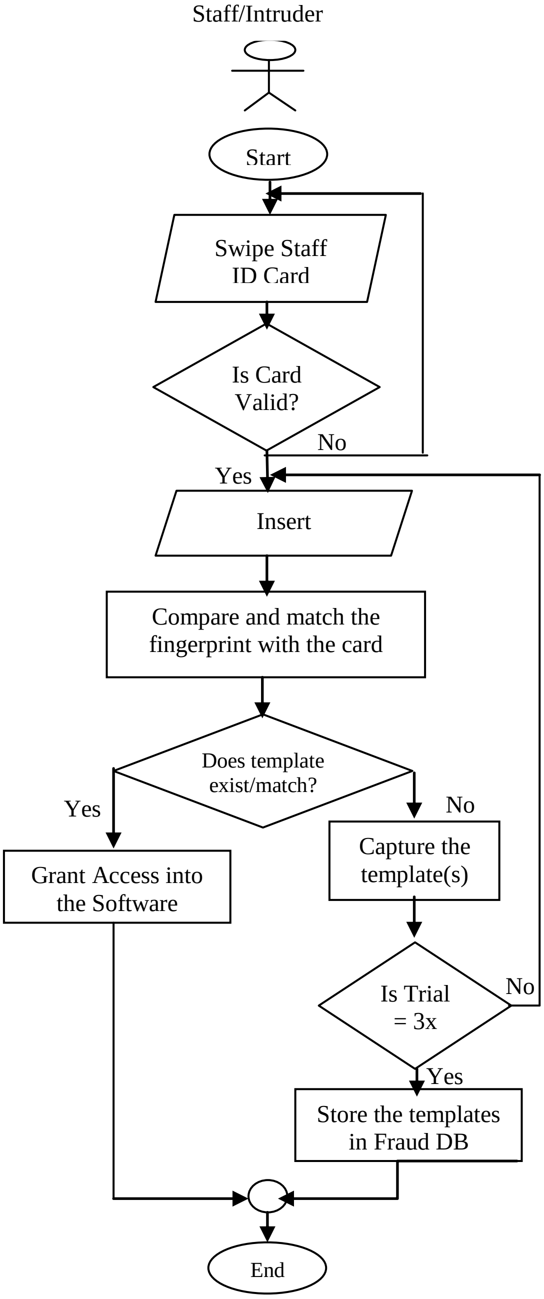
Staff/Intruder
Start
Swipe Staff ID Card
Is Card Valid?
No
Yes
Insert
Compare and match the fingerprint with the card
Does template exist/match?
Yes
No
Grant Access into the Software
Capture the template(s)
Is Trial = 3x
No
Yes
Store the templates in Fraud DB
End

Figure 3: Flowchart of General Authentification Process

## VI. FRAUDSTER DETECTION PROCESS

With this system, management of the bank can decide to run a general check on employee(s) or unauthorized individual(s) that tried to have unauthorized access into the main banking software. This is done by running a fingerprint matching check with templates stored in fraud database. These templates were collected as the unauthorized users attempted to have access into the main banking software. Figure 4 explains this process.

DOI 10.17148/IJARCCE.2015.46114

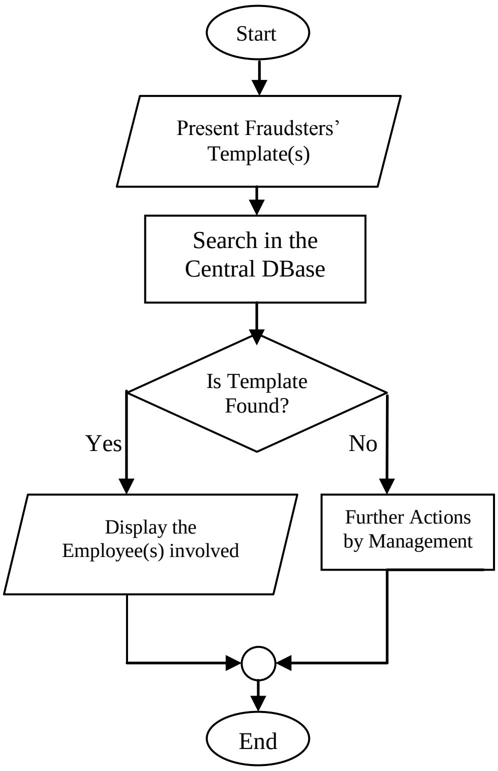
Start
Present Fraudsters' Template(s)
Search in the Central DBase
Is Template Found?
Yes
No
Display the Employee(s) involved
Further Actions by Management
End

Figure 4. Flowchart of Fraudsters Detection Process

## VII. CONCLUSION

We have analyzed and discussed the concept of biometrics and smart card and their usage in reducing internal banking fraud. In this study, biometric authentification is combined with smart cards in order to have better security approach in the banking sector. The system is expected to be attached to the main banking software to take care of access control. User trying to have access into the main banking software would be expected to provide his/her official staff identity card which will be swiped on the magnetic card reader (identification) and after which, demand for fingerprint biometrics (authentication) would be made before full access is given into the main banking software. If these two stages were not successfully completed, access would be denied and this will go a long way in reducing the internal banking fraud and unauthorized access always experienced in the banking industry.

## REFERENCES

[1] K. Mohan, A. Rakhi and C. Dhruv, Safe as a Bank: Iris Scan Biometrics for Secure Data Access, 2013. Available: www.infosys.com.

[2] D. T. Ahmad and M. Hariri, User Acceptance of Biometrics in E-banking to improve Security. Business Management Dynamics Vol.2, No.1, Jul 2012, pp.01-04S.

[3] P.J. Trocchian and T. L. Ainscough, " Characterising consumer concerns about identification technology" International Journal of Retail & Distribution Management, vol.34, no.8, pp609-620, 2006.

[4] W.S. Albrecht, Employee fraud. Internal Auditor, October, 1996, p. 26.

[5] J. Bologna, Handbook on Corporate Fraud, Butterworth-Heinemann, Stoneham, MA, pp. 54-62, 1993.

[6] J. Bierstaker, R. G. Brody and C. Pacini, Accountants' perception regarding fraud detection and prevention methods. Managerial Auditing Journal, Vol. 21, No. 5, pp 520-535, 2006.

[7] D. Zhang and L. Yu, Biometrics for Security in E-Commerce. Springer-Verlag, 2003 ch. 4 pp. 71–92.

[8] Gerik Alexander von Graevenitz, Biometric authentication in relation to payment systems and ATMs. DuD • Datenschutz und Datensicherheit 31, 2007

[9] J. Tabitha, T. Pirim, K. Boswell, B. Reithel and R. Barkhi, Determining the intention to use biometric devices: An application and extension of the technology acceptance model. Journal of Organizational and End User Computing, 18(3), 1-25, 2006.

[10] A. P. Pons, Biometric marketing: Targeting the online consumer. Communications of the ACM, 49(8), 60-65, 2006.

[11] A. Jain, L. Hong and S. Pankanti, Biometric identification. Communications of the ACM, 43(2), 91–98, 2000.

[12] S. Venkatraman and I. Delpachitra, "Biometrics in banking security: a case study". Information Management & Computer Security, vol.16, no.4, pp415-430, 2008.

[13] D. T. Toledano, R. F. Pozo, A. H. Trapote and L. H. Gomez, "Usability evaluation of multi-modal biometric verification systems" Interacting with Computers vol.18, pp1101-1122, 2006.

[14] L. Coventry, A. De Angeli and G. Johnson, Usability of large scale public systems: Usability and biometric verification at the ATM interface. Proceedings of the Conference on Human Factors in Computing Systems. Florida, USA, 153-160, 2003.

[15] M. O. Onyesolu, V. E. Ejiofor, M. N. Onyeizu & D. Ugoh, Enhancing Security in a Distributed Examination Using Biometrics and Distributed Firewall System. International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 9, September 2013. Website: www.ijetae.com

[16] T. Bengs and W. Grudzien "Biometrie in der Kreditwirtschaft" in DuD – Datenschutz und Datensicherheit J. Bizer, D. Fox, and H. Reimer, Eds. vol. 31 no. 3. Wiesbaden: Vieweg Verlag, March 2007 pp. 157–159.

[17] S. Sarker and J. P. Wells, Understanding: mobile handheld device use and adoption, Communications of the ACM vol. 46, no.12, 2003, pp. 35–41.

[18] G. von Graevenitz, "Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren", 1st ed. ser. Management Wissen aktuell G.-M. Hellstern, Ed. Berlin: Lit Verlag, 2006.

[19] M. Bromba "Ein biometrisches Bezahlsystem für Kaufhäuser" in DuD – Datenschutz und Datensicherheit J. Bizer, D. Fox, and H. Reimer, Eds. vol. 31 no. 3. Wiesbaden: Vieweg Verlag, March 2007 pp. 194–198.

[20] V. E. Ejiofor, M. N. Onyeizu, D. Ugoh and A. N. Nwosu, Development of Distributive Architecture for Post-Unified Tertiary Matriculation Examination (UTME) Assessment. International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 9, September 2013. website: www.ijaiem.org

DOI 10.17148/IJARCCE.2015.46114