On Securing Automatic Teller Machine Transactions Using Bank Verification Number

Ojulari Hakeem, Oke Alice

Abstract— Automatic Teller Machine (ATM) fraud is a global threat and has been on increase in Nigeria. Conventional security system to protect customer's accounts on ATM has been debased. This paper presents an empirical model of securing Nigerian ATMs using Bank Verification Number (BVN) indicating technical ATM integration. Two integration models namely BIO and BIO-PIN were developed with ATM state flows. The models were integrated with biometric application and connected to a BVN emulator. Each model requires a biometric state and was integrated into the ATM state flow. The biometric state was used as an exit state to the biometric application which is exclusively different from ATM application. The whole unit was linked through a web service to a BVN emulator for verification process; customer primary account number (PAN) was used as a query parameter to retrieve fingerprint image from BVN proxy server which was connected to the main server.

Index Terms— Automatic Teller Machine (ATM) , Bank Verification Number (BVN), BIO and BIO-PIN models , Biometirc application, BVN emulator, NCR ATM, fingerprint image.

1 Introduction

THE term biometric refers to identifying human based on physiological features such as irises, faces, fingerprints, signatures etc. Biometrics industry was established in the early 1990s [1], and deployed live in controlled environments. Biometric system is being used where authentication is needed in a real time to enhance system operations and security. The usual practice of securing sensitive information is by the use of Personal Identification Number (PIN) and Password. This conventional security system was adopted on ATM cards but has been violated leading to ATM frauds due to identity theft. ATM fraud is a global treat to financial institutions and is exponentially growing. Jain, *el al*, [7] stressed that traditional security methods such as PIN are no longer considered reliable to satisfy the security requirements of electronic transactions. Implementing biometric technology on ATM has been a better improvement over conventional security system [5] because bio-data cannot be stolen, lost or forgotten.

The banking industry biometric 'know your customer' (KYC) project was initiated as a result of lack of a central and standardized identity database with associated infrastructure for identification and verification of bank customers in Nigeria. Consequently, central bank of Nigeria (CBN) in collaboration with Nigerian banks launched a centralized biometric identification system in February 14, 2014 which is referred to as Bank Verification Number (BVN) project. Charms Plc (Nigerian Company) and Dermalog (German Company) entered a technical partnership to implement BVN project with the single central database for all banks data residing at the Nigeria Inter-Bank Settlement System (NIBSS). This involves biometric captures (fingerprints and facial images) of bank customers for unique identification during bank transactions which are stored in a database. With the BVN project which has been concluded successfully in all banks, NCR Nigeria aims at providing a biometric security solution on NCR ATMs in order to protect bank customers from ATM frauds through system integration to BVN server for authentication. Due to the fact gathered that numerous researches believe that fingerprint implementation is easier on ATM [5], this work adopts fingerprint of the two biometrics features (facial and fingerprint) available at NIBSS.

Relatively all researches on ATM biometric systems in Nigeria have never been put to a real practice. It could be as a result of lack of full understanding of ATM technology or not having the opportunity to carry the empirical tests in any ATM laboratory. NCR research team [1] investigated all possible physiological biometrics techniques in the laboratory and pointed out that the approaches followed a similar operation since the verification process involves comparing with stored data. It was concluded that fingerprint has a preferential advantage over other biometric features like facial and iris. Global research investigated that fingerprint is the widely used biometric identification [5] as shown in Fig. 1. NCR in 2003 suggested that a verification process of matching (one-one) rather than identification (one-many)

- *Ojulari Hakeem O is currently pursuing masters degree program in Computer Science and Engineering in Ladoke Akintola University of Technology, Oyo State, Nigeria, and also a Professional Service Consultant in NCR Nigeria E-mail: update_ak47@yahoo.com, Ojulari.Olusegun@ncr.com*
- *Oke Alice O. is currently a Senior Lecturer in the department of Computer Science and Engineering, Ladoke Akintola University of Technology, Oyo State Nigeria. A Registered Engineer with The Council for the Regulation of Engineering in Nigeria (COREN), full member of Computer Professional (Registration) Council of Nigeria, (MCPN), the National Computer Society (NCS) and Nigerian Society of Engineers (NSE). E-mail: aooke@lautech.edu.ng*

which requires a form of unique identifier to verify user is the better option to adopt on ATM.

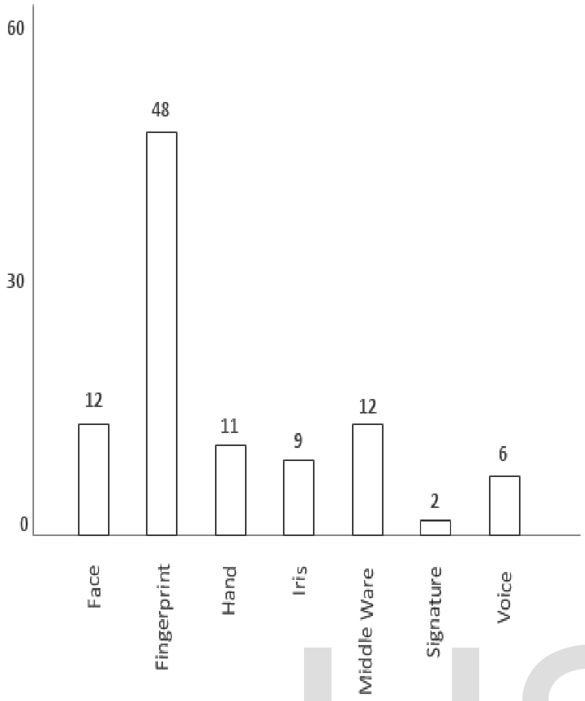

Fig. 1: Comparative survey on the wide use of fingerprint

Mohammed [3] proposed a model that captured customer fingerprint and used PIN as an encryption key to store the image in the ATM card. The model still requires customers to enter PIN as part of authentication. The enrollment stage involves the use of the actual ATM card for data storage. Krishnamurthy and Reddy [2] implemented a GSM modem on ATM as an embedded security system to send an auto generated PIN (after verification) as an SMS message to the customer whenever a finger swipe is observed on the biometric device. The customer uses the PIN to continue the transaction and the customer mobile number is required during enrollment process.

2 SYSTEM DESIGN

This paper presents two models that were simulated in the ATM laboratory to implement fingerprint biometric on NCR ATMs. The research work is dependent on BVN project as the central biometric database. Identifier as the application was called is an ATM Biometric client that was developed and deployed on ATM together with an authorized bio scanner device from Dermalog. The client-server application involves four stages these are:

- Capturing module
- Validation module
- ATM integrating module
- BVN server integrating module

2.1 CAPTURING MODULE

The client application captures fingerprint image from bio-scanner (Dermalog device); and verifies against existing BVN repository through an exposed web service. The web service interacts directly with bio-database. The validation is a one to one process; this means that the captured image is verified against an existing customer bio-data. The use of ATM card is still required. A preliminary search is performed on the bio-database using customer's account which is linked with the card number, and primary account number (PAN), which is indirectly linked to BVN. This will narrow the verification process down to 1:1 and speed up the matching process.

2.2 VALIDATION MODULE

The validation module interacts with BVN database through a proxy connection for verification. ATM is a finite state machine (FSM) which operates on a state flow; this state flow in ATM industry is referred to as download. However, a new state *(referred to as BIO)* can be created and added to the download. Hence, BIO state was created as shown in Fig. 2 indicating interoperability of the modules. The BIO state is added immediately after a PIN state which is an exit from NCR direct connect (NDC) application software. Both PIN and Next states are part of NDC platform. An actuating switch is used to handle both entering and exiting NDC in order to manage the integration process. While exiting NDC

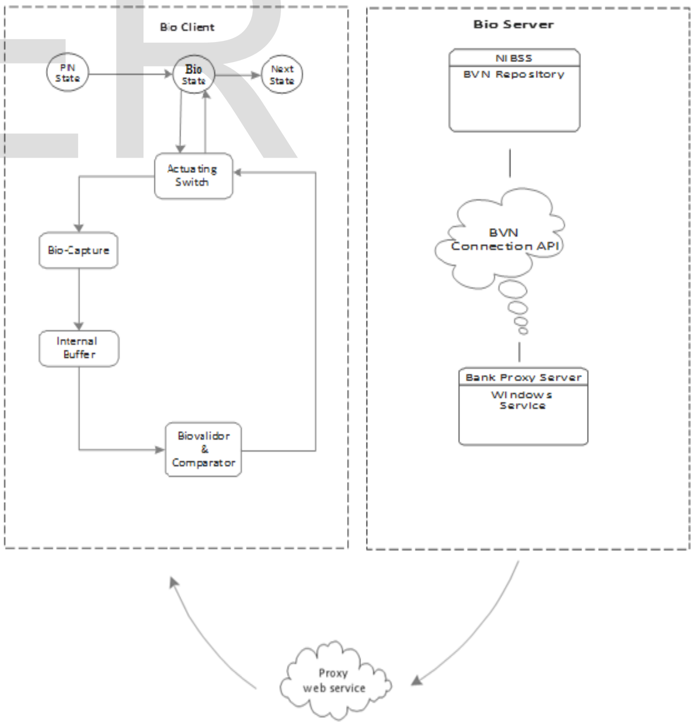

Fig. 2: An overview of the Application design

platform, the actuating switch initializes biometric device to scan the customer finger by indicating a prompt on the ATM screen and save the image in the internal buffer. BioValidator and comparator perform the validation process, and the process takes place as soon as image is captured. The validation/verification result is passed to the actuating switch to determine the next state. The next state is a composite of bad next state and good next state. If the verification is successful, a good next state is initiated which means the customer can proceed the transaction, otherwise a bad next state is initiated and the ATM comes to a close state which ejects the ATM card.

2.3 ATM Integration Module

NCR ATM integration needs real expertise in NDC protocol or ATM download. The two models under consideration are described as BIO-PIN and BIO models of which both require bio-state to be created on ATM download.

(a) BIO-PIN Model

In this model, the BIO state is integrated after the PIN state as shown in Fig. 3. This model still requires PIN entry state first before capturing fingerprint for customer verification. Normal transaction state flow is allowed to continue after successful validation. Hence, both BIO and PIN are required for authentication. However, if the captured bio-data is invalid (after 3 retries) the ATM is taken to a close state (final state) and card is ejected. This model is referred to as BIO-PIN model.

(b) BIO Model

This model is similar to model (a) but with the absence of PIN entry state. Normal transaction flow is allowed only after successful validation of captured bio-data as shown in Fig. 4 Thus, it is only BIO that is required for authentication.

2.4 BVN Server Integration Module

The server side of the biometric system requires a proxy that connects to BVN server through a BVN application programming interface (API) called BVN connection API. The proxy handles all requests from the bank ATMs and provides connection to the BVN server in order to reduce overloading of BVN server network bandwidth. There is a windows service that runs on the proxy that manages the BVN connection. ATM sends a request for BVN fingerprints via a proxy web service handler using customer account detail as a parameter to retrieve customer fingerprint from BVN server.

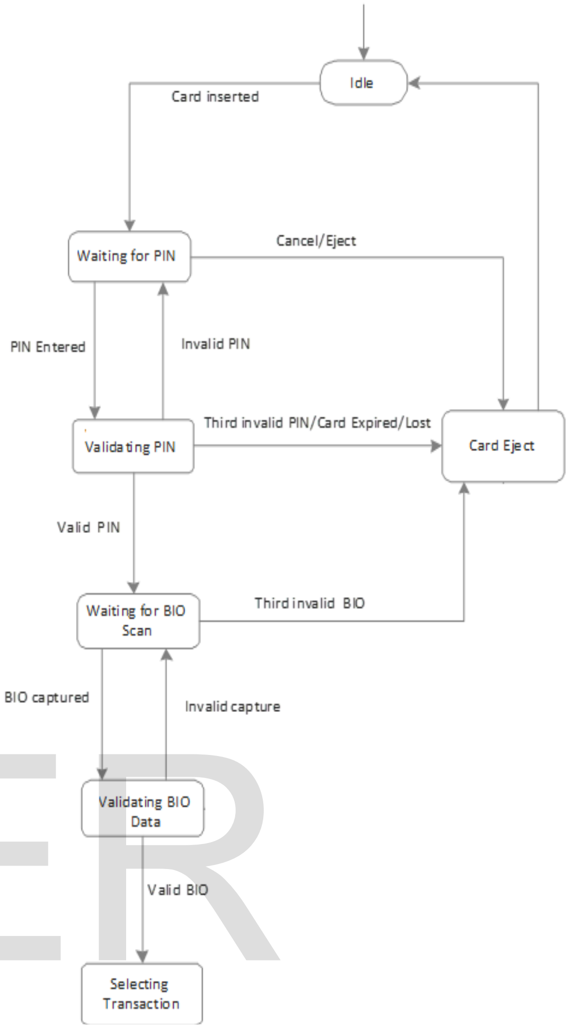

Fig. 3: BIO-PIN Model state chart

3 Performance Evaluation

Marcel [4] pointed out three main types of biometric performance evaluation as measured in terms of the number of uncontrolled variables which are technology, scenario, and operational. The biometric sensor, the application, the environment and the users are contributing factors to system. In practice, score is used to measure biometric performance, and threshold value is used to differentiate between the groups of scores and to differentiate between genuine clients and impostors. Generally, false acceptance rate (FAR) and false rejection rate (FRR) are used to measure biometric performance.

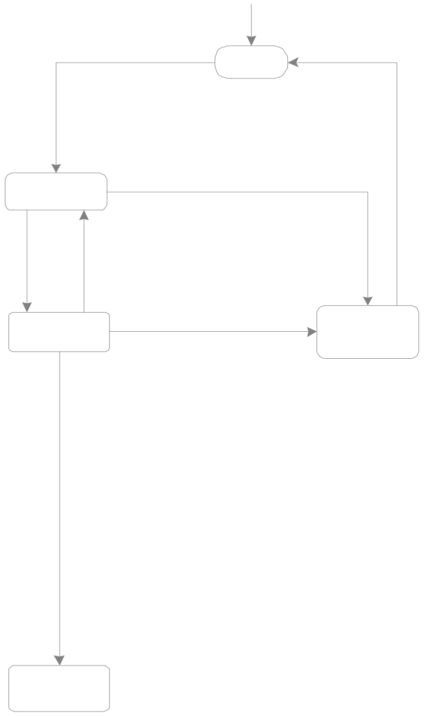

Fig. 4: BIO model state chart

Fig. 5 shows the FAR for a varying threshold over the score distribution. Typically, FAR and FRR are used to generate Receiver Operating Characteristic (ROC) curve, this is as shown in Fig. 6 which is a plot of true acceptance rate (TAR = 1 - FRR) against FAR. The closer the curve is to the top left corner, the better it is (this corresponds to maximizing the so-called area under the curve or AUC). Generally, such curves are generated from a database of bio records.

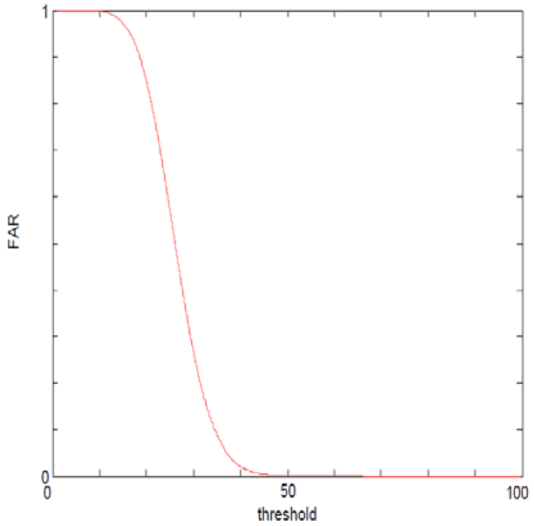

Fig. 5 Typical plot of FAR against threshold

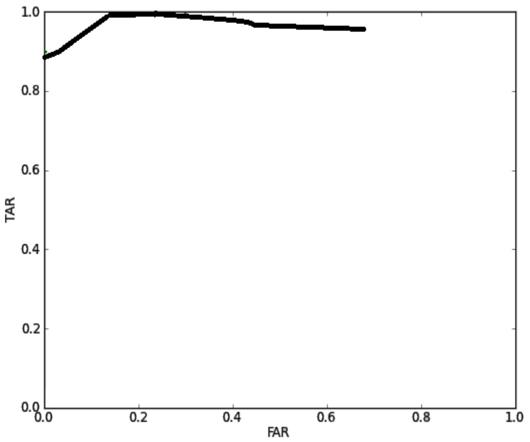

Fig. 6 ROC Curve

In order to evaluate performance of the biometric system deployed on a test ATM, a database consisting of 5 NCR staff was generated as a test. Each staff provided 5 fingerprint images giving 25 images in total. A single image from individual was used as a template while the rest of the individual images were used to verify the fingerprint. Ideally, the expectation was to have 4 genuine scores on individual. 20 genuine scores were derived taking each image as a template in succession. Consequently, other staffs were used as impostors and 100 impostor scores were expected each. In all, total number of genuine scores and impostor scores are 100 and 500 respectively as shown in Table 1. These scores are usually used to generate the ROC curve in order to choose the best threshold suiting the live implementation for verification or matching.

Table 1 Score distribution

Staff	Template	Genuine Score	Impostor Score
1	1 (5)	4(5)	20(5)
2	1 (5)	4(5)	20(5)
3	1 (5)	4(5)	20(5)
4	1 (5)	4(5)	20(5)
5	1 (5)	4(5)	20(5)
		100	500

However, the choice of threshold becomes a problem. A threshold is set to differentiate between the groups of scores and used to differentiate between clients and impostors. There are two populations of individuals that were considered; A = acceptable individuals and U = unacceptable individuals. Each individual is related with a 'score' X. Suppose in each of the two populations, the scores have normal distributions, (μ, σ), and the same standard deviation, SD or σ, where in A, the mean is μA and in U is μU. The standard deviation, σ, is given mathematically as shown in (1)

$$\sigma = \sqrt{1/N(\sum_{i=1}^{N}(x_i - \mu)^2)} \qquad (1)$$

where N = number of individuals,
x = individual score,
μ = mean score

An individual that has its score greater than threshold t will be accepted. However, if the score from unacceptable individuals is greater than t, it is false acceptance or if the score from the acceptable individuals is below t, it is false rejection. The probabilities of the two scenarios are shown mathematically;

$$Err_{falseAcc} = P(N(\mu_U, \sigma) > t) \qquad (2)$$

$$Err_{falseRej} = P(N(\mu_A, \sigma) < t) \qquad (3)$$

If the classification threshold selected is too high some client patterns will be falsely rejected and if it is too low some impostors will be accepted. The threshold, t, was chosen moderately around 50. The error rates calculation is as shown in (2) and (3) respectively. FAR and FRR were determined to plot ROC curve. Choosing a threshold of 50%, 15 impostor scores exceeded the threshold and 5 genuine scores fell below the threshold. Calculating FAR and FRR:

$$\text{FAR} = \frac{\text{impostor scores exceeding threshold}}{\text{all impostor scores}} = \frac{15}{500} = 3\%$$

$$\text{FRR} = \frac{\text{genuine scores falling below threshold}}{\text{all genuine scores}} = \frac{5}{100} = 5\%$$

Performance was also evaluated using confusion matrix as shown in Table 2 to calculate specificity and sensitivity.

Table 2: Confusion matrix with threshold of 50%

		Class	
		Client	Impostor
Match	Client	95 (TP)	5 (FP)
	Impostor	15 (FN)	485 (TN)

Calculating specificity and sensitivity;

$$\text{Sensitivity} = \frac{\text{TP}}{(\text{TP} + \text{FN})} = \frac{95}{95 + 15} = 0.863 = 86.3\%$$

$$\text{Specificity} = \frac{\text{TN}}{(\text{TN} + \text{FP})} = \frac{485}{485 + 5} = 0.989 = 98.9\%$$

4 Conclusion

This paper has demonstrated a practical method of integrating a biometric system on ATM with existing BVN biometric database, and performance evaluated mathematically. Biometric is a very secure system which has been extended to ATM environment. A better performance can be achieved if the threshold is considerably adjusted to increase sensitivity or to reduce FRR. Nonetheless, the performance will definitely be different when deployed in a live environment where there are heterogeneous set of users of large number compared to what was tested in the laboratory with homogenous set of users of small number. The user experience on every new technology is a contributing factor that will affect the performance of the system, and thus will increase the failure rate. However, it predisposes a risk of customers being kidnaped in order to get fingerprint access to customer accounts on ATM. In addition to this, customers will not be able to give their ATM cards to either friends or family anymore. Despite the shortcomings, it is expected that ATM biometric system will reduce ATM frauds to a great extent in Nigeria when fully implemented in live environment.

References

[1] Coventry, L., De Angeli, A., and Johnson, G. (2003). Usability and biometric verification at the ATM interface. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 153-160). ACM.

[2] Krishnamurthy, P., and Redddy, M. M. (2012). Implementation of ATM Security by Using Fingerprint recognition and GSM. *International Journal of Electronics Communication and Computer Engineering*, *3*(1).

[3] Mohammed, L. A. (2011). Use of biometrics to tackle ATM fraud. In *Proc. 2010 International Conference on Business and Economics Research* (Vol. 1).

[4] Marcel, S. (2013). BEAT–biometrics evaluation and testing. *Biometric technology today*, (1), 5-7.

[5] Onyesolu, M. O., and Ezeani, I. M. (2012). ATM Security Using Fingerprint Biometric Identifier: An Investigative

Study. *International Journal of Advanced Computer Science and Applications*, *3*(4), 68-72.

[6] Pare Jr, D. F., Hoffman, N., & Lee, J. A. (2000). *U.S. Patent No. 6,154,879*. Washington, DC: U.S. Patent and Trademark Office.

[7] Jain, A. K., Hong, L., Pankanti, S., and Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, *85*(9), 1365-1388.