

# A FRAMEWORK FOR THE ADOPTION OF BIOMETRIC ATM PERFORMANCE AND SCALABILITY EVALUATION

**\*OMOGBHEMHE, I.M. AND MOMODU, I.B.**

Department of Computer Science, Ambrose Alli University, Ekpoma

## Abstract

*The increase fraud within Automatic Teller Machine (ATM) today has become a global threat to the survival of the electronic banking system and its services. This is as a result of the traditional method (Personal Identification Number) used in securing the services of this system (ATM). This traditional security mechanism has failed, since fraud is still on the increase through this medium. As a result, a better model was proposed by the author called Biometric ATM Model suitable for achieving better security within ATM services. However, in order to authenticate the real life environment performance of this model, this paper presents the performance analysis of the biometric ATM model. This analysis helps to predict the behaviour of the biometric ATM in achieving its scalability when fully deployed in real life environment. The conclusion whether to accept this model or not was made based on the performance analysis outcome of the False Acceptance Rate (FAR) and False Rejection Rate (FRR) as presented in this paper. After the evaluation using some data, the FAR was lower than the FRR. Consequently, the biometric ATM software will not accept an unauthorized user. This paper therefore recommends the use of biometric in securing ATM services in the banking sectors.*

**Keywords:** Framework, Biometric, Automatic Teller Machine, Evaluation, Performance, Model

## INTRODUCTION

Software scalability and performance is of optimal importance to every software that must be used to deliver good services to the user. In today's world of computing, there exists a lot of software for performing the same task. These

software were developed using different style, methodologies, algorithms, languages and platforms. Thus, in choosing a particular software for a particular operation, and task, scalability and performance of such software must be highly considered. Software performance evaluation is used to uncover

performance problems that can result in lack of server side resources, inadequate database capabilities, inadequate coding style, poor design functionality etc. The intent of software performance evaluation is to understand how the system responds to loading. It is design to simulate real world loading.

Meanwhile, software scalability is of general importance to software development community. Ekuobase and Onibere (2011) pointed out that the poor scalability of web services if not properly addressed, may not only pose a serious threat to its survivability but may also lead the Information Technology (IT) community into shambles. They further show while scalability and software performance measurement is highly important before the deployment of such software. Consequently, developing service oriented biometric Automated Teller Machine (ATM) software, need such evaluation.

In order to improve the security features of ATM, Omogbhemhe (2018) developed an ATM using biometric as its security mechanism. Hence, validating the performance of such system (ATM with biometric features) is the need for this paper. As a result of ATM fraud, it is obvious that the conventional security mechanism has been violated. Jain et.al (1997) stressed that the traditional security measures are no longer considered reliable to satisfy the security requirements of electronic transaction. The fraud within the use of ATM is a global threat to

the financial body or institutions. This made Krishnamurthy and Reddy (2012) to develop a GSM model on ATM as its embedded security feature. Similarly, Omogbhemhe (2018) provided a novel security model of the ATM that show the entire ATM feature and a new module that act as the end-service security mechanism using biometric of the owner of a particular account. This will guarantee improved security within ATM transaction as supported by Onyesolu and Ezeani (2012). This kind of mechanism in ATM, will not allow third party transaction and thereby eliminating ATM fraud. This new biometric ATM model is as given in figure 1 in this paper as adapted from (Omogbhemhe 2018).

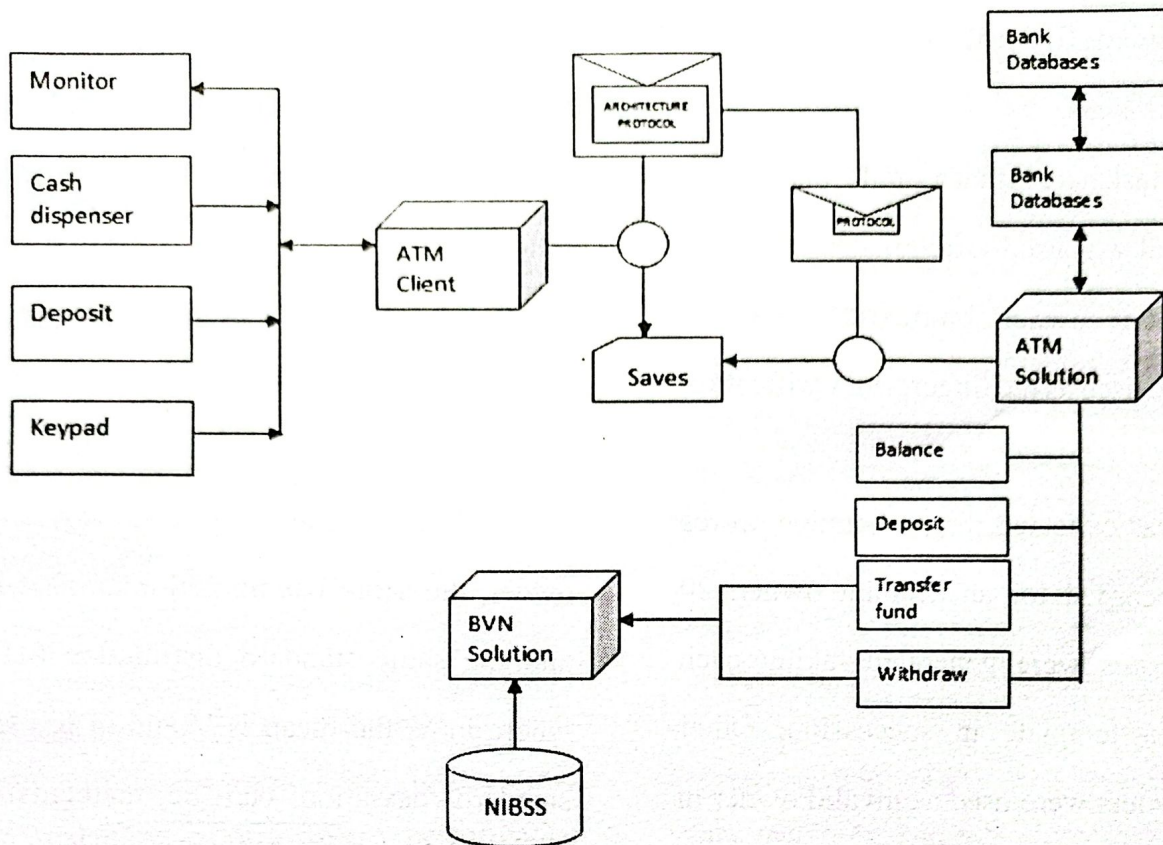


**Figure 1: Biometric ATM Model (Source: Omogbhemhe 2018)**

## EVALUATION

In looking at the software scalability or general performance, Marcells (2013) pointed out three main types of biometric performance evaluation as measured in terms of the number of uncontrolled variables which are terminology, scenario and operational. However, other contributing factors to the system are like application, the environment, the biometric sensor and the user. Practically, scores are used to measure biometric

performance, and threshold values are used to differentiate between the groups of scores and to differentiate between genuine clients and non-genuine clients. In measuring biometric performance and how they can be scalable, False Acceptance Rate (FAR) and False Rejection Rate (FRR) are used. After the development of the software (i.e. biometric ATM software), to evaluate its performance and scalability, a database consisting of 5 account owners was generated. Each account owner

provided five (5) fingerprint images given us 25 images.

The task here is that a single image from an individual was used as templates while the other account owner biometric/fingerprint images were used as the fingerprint verification tool.

It was expected that, 4 genuine scores must be recorded for an account owner. 20 genuine scores were generated taking each image as a template in succession. Other account owners were used as invalid owner in relation to the genuine owner. 100 invalid scores were expected each. Hence, the total number of valid scores is 100 while the one for invalid scores are 500 as shown in table 1.

**Table 1: Total number of Scores**

| Account Owner | Template | Valid scores | Invalid Scores |
|---------------|----------|--------------|----------------|
| 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)          |

Meanwhile in analyzing the threshold (i.e a set used to differentiate between the group of scores and also used to differentiate between valid owners and non-valid owners of account). In this analysis, two different people were considered; V = Valid owner and I = Invalid owner. Each owner is related with a score 'a'.

Assuming in each of the two account owner, the score has normal distribution ( , ), and the same standard distribution SD or , where in V, the mean is V and in I is I. The standard deviation can be mathematically shown as:  $\sigma = \sqrt{1/N \left( \sum_{i=1}^N (x_i - \mu)^2 \right)}$

Where N = Number of Account owners

$x$  = Individual Scores

$\mu$  = Mean scores

Ideally, an account owner that has his/her scores greater than threshold  $t$ , will be accepted as valid. If the score from unacceptable owner is greater than  $t$ , it is false acceptance or if the score from the acceptable owner is below  $t$ , it is false rejection. These two scenarios can be mathematically shown using the probabilities of their occurrence as:

$$\text{Err\_of\_False\_Acceptance} = P(N(\mu, \sigma) > t)$$

$$\text{Err\_of\_False\_Rejection} = P(N(v, ) < t)$$

In using the above, if the classification threshold selected is too high, some client patterns will be falsely rejected and if it is too low, some invalid owner will be falsely accepted. Hence, 50 was chosen for the threshold  $t$ . The error and its rate of occurrence can be calculated using the above probability equations for the error occurrence.

Consequently, choosing a threshold of 50%, 15 invalid scores exceeded the threshold and 5 valid scores fell below the threshold. Calculating the FAR and FRR of the outcome, we have

$$FAR = \frac{\text{Invalid scores exceeded threshold}}{\text{All invalid scores recorded}}$$

$$= \frac{15}{500} = 0.03$$

$$FRR = \frac{\text{Valid Scores falling below threshold}}{\text{All valid scores recorded}}$$

$$= \frac{5}{100} = 0.05$$

Analyzing this in percentage, in order to generate the percentage occurrence of the FAR using the tested parameters we have, FAR = 30% and FRR = 50%

Hence, since from the evaluation and analysis, we have a low FAR and a higher FRR,

it is obvious that any unauthorized person will not be allowed access to the biometric ATM system services. In practical scenario, a low FAR and high FRR would ensure that any unauthorized person will not be allow access to the biometric ATM system services. Therefore, it is good to have a low FAR, but the low FAR must not come at the cost of the high FRR (Danny 2018).

## CONCLUSION

This paper has demonstrated and evaluated the performance of the biometric ATM. This is necessitated in order to ascertain the operation performance of this model before its full deployment and implementation in real life environment. As a result of the large amount of resources required in the development of software, it is necessary to carry out the performance analysis of a novel model of software before committing such resource to its full implementation. In this paper, the FAR and FRR analysis was carried out on the biometric ATM software and the results were highly promising. Hence, the

deployment and full implementation of this kind of software in real life environment will have a better and scalable performance.

## REFERENCES

- Danny, T (2018): False Acceptance Rate and False Recognition Rate in Biometric. [www.bayometric.com](http://www.bayometric.com)
- Ekuobase, G. and Onibere, E (2011): Architecture for Scalable Web Service Solution. Canadian Journal of Pure and Applied Sciences 5(1): 1449–1453.
- Jain A.K, Hong L, Pankati S and Bolle R, (1997): An Identity-authentication Fingerprints. Proceedings of the IEEE, 85(9), 1365-1388
- Krishnamurthy P and Reddy M.M (2012): Implementation of ATM security by using fingerprint recognition and GSM. International Journal of Electronic Communication and Computer Engineering, 3(1).
- Omogbhemhe, M. (2018): Service Oriented Biometric Model Suitable for Securing ATM System. International Journal of Scientific and Engineering Research. 9(8). 97-101.
- 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.
- Marcel S (2013): BEAT – Biometrics Evaluation and Testing. Biometric Technology today, (1), 5-7