Automated Biometric Voice-Based Access Control in Automatic Teller Machine (ATM)

Yekini N.A.
Department of Computer Technology
Yaba College of Technology, Lagos Nigeria.

Itegboje A.O.
PHD Candidate, SMED Southern university,
Baton Rouge, LA US.

Oyeyinka I.K.
Department of Computer Technology
Yaba College of Technology, Lagos Nigeria

Akinwole A.K.
Department of Computer Technology
Yaba College of Technology, Lagos Nigeria.

***Abstract*— An automatic teller machine requires a user to pass an identity test before any transaction can be granted. The current method available for access control in ATM is based on smartcard. Efforts were made to conduct an interview with structured questions among the ATM users and the result proofed that a lot of problems was associated with ATM smartcard for access control. Among the problems are; it is very difficult to prevent another person from attaining and using a legitimate persons card, also conventional smartcard can be lost, duplicated, stolen or impersonated with accuracy. To address the problems, the paper proposed the use of biometric voice-based access control system in automatic teller machine. In the proposed system, access will be authorized simply by means of an enroll user speaking into a microphone attached to the automatic teller machine. There are 2 phases in implementation of the proposed system: first training phase, second testing or operational phase as discussed in section 4 of this paper.**

Keywords- Automatic Teller Machine (ATM), Biometric, Microphone, Voiced-Based Access Control, Smartcard Access Control, Voiced-Based Verification System

I. INTRODUCTION

The biometric recognition systems, used to identify person on the basis of physical or behavioral characteristics (voice, fingerprints, face, iris, etc.), have gained in popularity during recent years especially in forensic work and law enforcement applications [1]. Automatic Teller Machine was invented to address the following issues in banking system: Long queue in banking hall, Quick access to fund withdrawal, banking at any time, Improvement in the quality of banking services to customers.

Safety of bank customer fund in banking has always been a concern since ATM was introduced. Access control for automatic teller machine represent an important tool for protecting hank customers fund and guarantee that the authentic owner of the ATM card [smartcard] is the one using it for transaction [9]. The most important authentication method for ATM is based *on* smartcard [Njemanze, P.C. 2007). It is very difficult to prevent another person from attaining and using a legitimate person's card.

The conventional smartcard can be lost, duplicated, stolen, forgotten or impersonated with accuracy [7]. This conventional security procedure in ATM cannot guarantee the required security for ATM.

An intelligent voiced-based access control system, which is biometric in nature, will enable automatic verification of identity by electronic assessment of one or more behavior and/or physiological characteristics of a person. Recently biometric methods used for personal authentication utilize such features as face, voice, hand shape, finger print and Iris [4]. In other to overcome the problems of smartcard access control in ATM. This paper proposed an intelligent voice-based access control system which is a biometric technique that offers an ability to provide positive verification of identity from individual voice characteristics to access automatic teller machine. The use of voice as a biometric characteristic offers advantages such as: it is well accepted by the uses, can be recorded by regular microphones, the hardware costs are reduced, etc. The paper discusses; ATM and it model network, drawback in smartcard based access control for ATM based on survey of 1000 users of ATMs, proposed voiced based access control and conclusion that compare the advantages of the system over current: available technology.

II. AUTOMATIC TELLER MACHINE MODEL NETWORK

Automatic teller machine is online with bank, each transaction will be authorized by the bank on demands and it uses real-time online processing technique which directly updated the account from which transaction takes place. Figure I, gives the ATM model network.

The ATM model in figure 1 work as follow; Bank customer inserts the smartcard (smartcard) in the ATM machine. The machine then request for a personal identification Number PIN if the supply PIN is correct, access will be authorized and transaction will continue, the customer then enter the amount to withdrawal, and if the customer has enough money in the account then the amount will he paid.

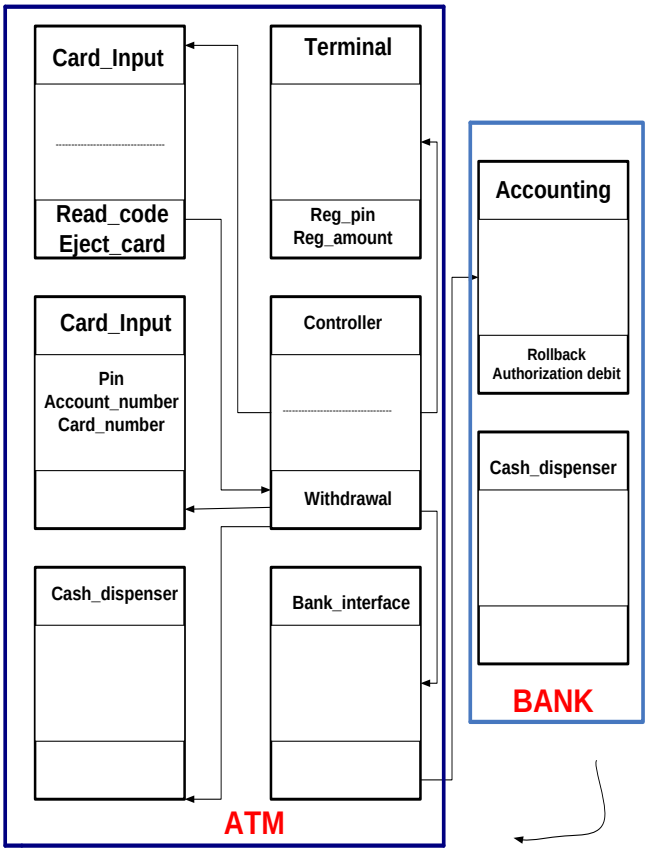


Figure l: ATM Model Network [8].

The whole work is being monitored by the controller class. In principle this is not necessary, but for working with a secure model the controller class is needed as a dispatcher of actions and it would have a log file with the trace of every transaction earned out by ATM.

The class card_input has the methods for reading the code of the client's card and for ejecting the card from machine. It interacts through the controller with the class terminal, where the methods reg_PIN and reg_amount are defined.

In other to verify whether the PIN of a particular users is correct or not, the class card will have the information of the cardholder i.e. card_number, PIN, and Account number. The controller will interact with the bank the bank using the information of the card holder in order to get the authorization to pay (or not) request amount.The bank_interface will send the request to the accounting class, which belongs to the bank package, in other to call the debit method of the accounting class [5].

The accounting class has the methods of rollback, authorization and debit which directly interact with the accounting class. Rollback is for rollback a transaction in case anything is wrong and should leave the account and the teller machine in the original state; authorization will authorize or not an operation and debit will extract the requested amount of money from the account in case the operation is authorized [8].

III. RESEARCH FRAMEWORK AND METHODOLOGY

Research framework and methodology is based on the survey that covered a sample of one thousand ATM users in Lagos state. The choice of the location is based on the fact that Lagos state is the economy nerve center of Nigeria and it has more branches of the banks and ATM location compare to any other state in Nigeria. The following questionnaire was used to get information that prompts us to proposed the voiced based access control

QUESTIONNAIRE

Set A

S/N	Question	Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1.	Banking would have been better if ATM was never invented	817	155	5	10	13
2.	Withdrawal of money from bank using ATM is faster compared to normal banking	836	34	0	156	714
3.	Withdrawal of money from ATM is more secure	619	181	9	101	100
4.	There is need for better security access for ATM that will guarantee only one person to a card.	0	9	11	99	881
5.	Biometric Technique as in face recognition, fingerprint, voice recognition etc for access control in ATM would provide better security	0	11	9	109	871

Set B

		YES	NO
6.	Has there been a time where your card was rejected by ATM card because you enter a wrong PIN	618	382
7.	Have you ever misplaced your ATM card before?	719	281
8.	Have you been a victim of ATM fraud before	699	301
	If yes to question no (8) please give brief detail	Detail vary	

The result was later converted to column charts as shown figure 2a and b.

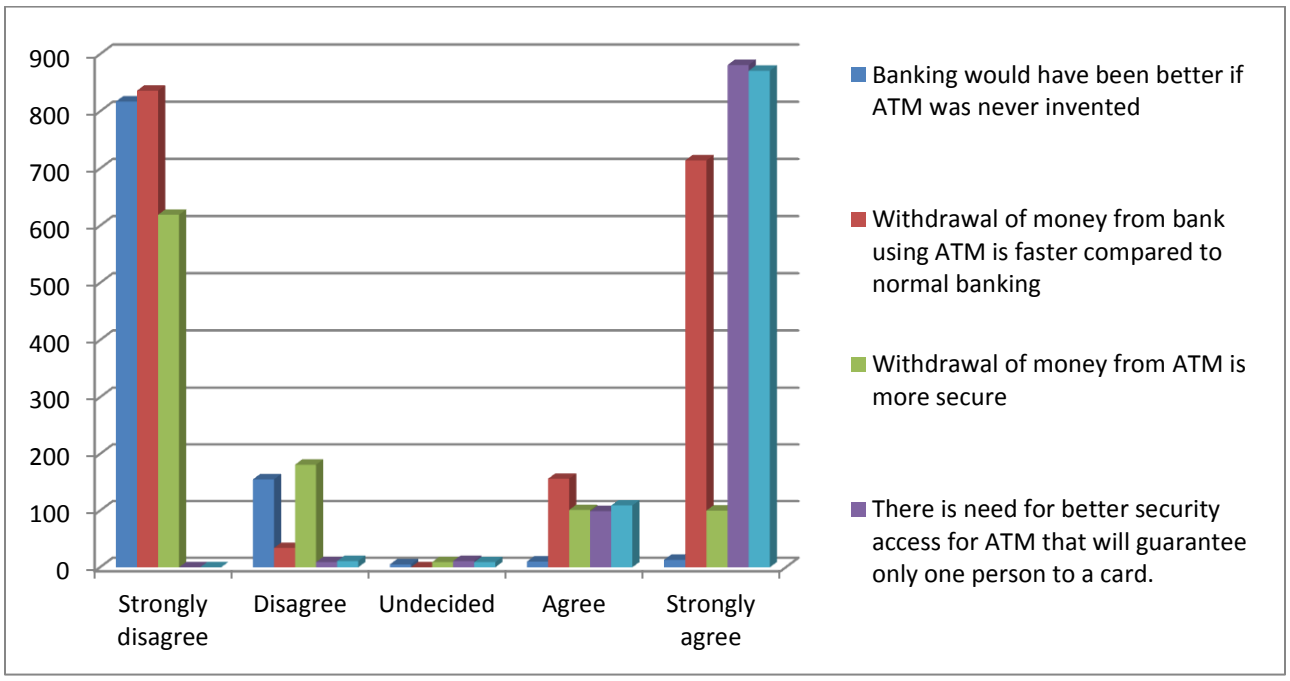


Figure 2a: Column chart for question set A

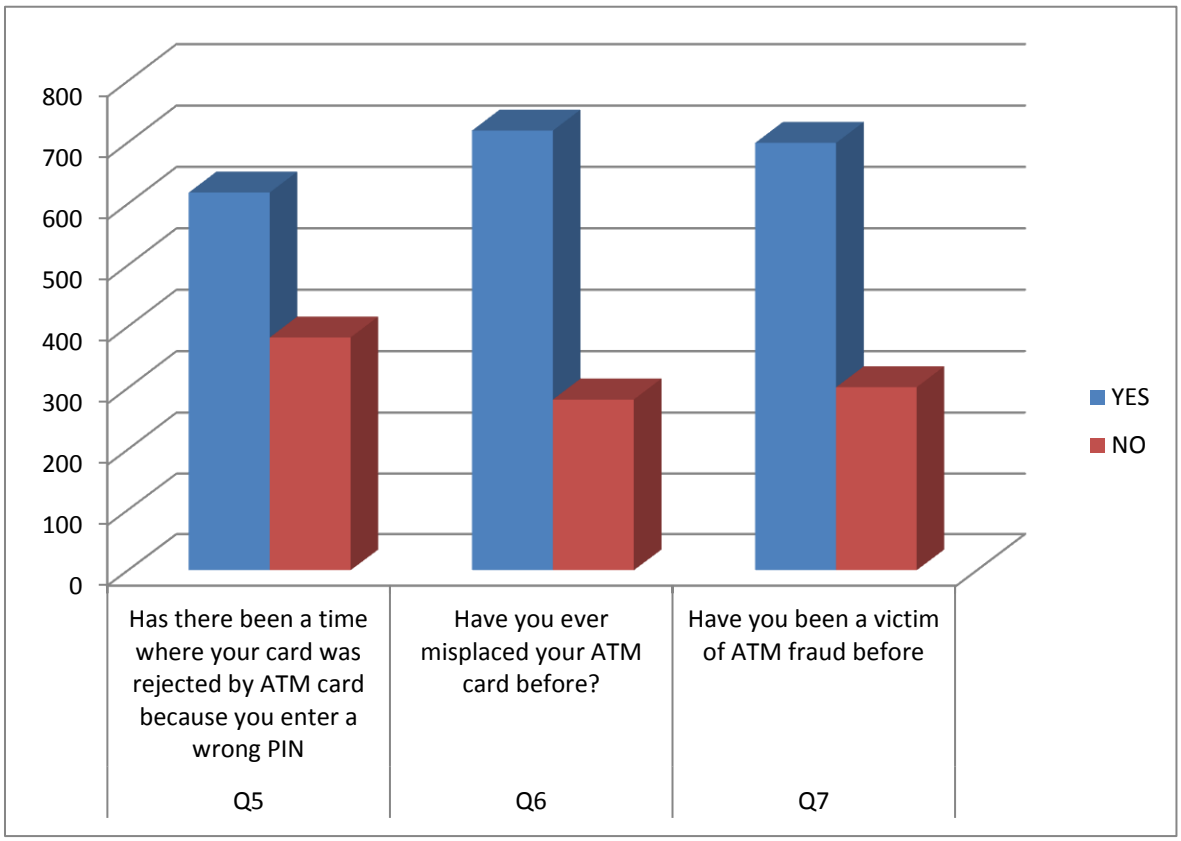


Figure 2b: Column Chart for Question set B

The result obtained from the questionnaire shows that, there is need for better security approaches to ATM access control. The result is analyses as follows:

Question 1: 81.7%, the response to the question implied that invention of ATM is a welcome innovation in banking sector.

Question	Strongly Disagree	%	Disagree	%	Undecided	%	Agree	%	Strongly Agree	%
Q1	817	81.7	155	15.5	5	0.5	10	1	13	13
Q2	336	83. 6	34	3.4	0	0	156	I5.6	714	71.4
Q3	619	61.9	181	18.1	9	0.9	101	10.1	100	10
Q4	0		9	0.9	11	1.1	99	99	881	88.1
Q5	0		11	1.1	9	0.9	109	109	871	87.1

Question 2: the majority of the respondent prefers using ATM because it enables quick access to withdrawal of money.

Question 3: the majority of the respondent strongly agreed that fund withdrawal through ATM is not secure compared to using face-face with cashier.

Question 4: larger percentage of the respondents strongly agreed that there is need for better security that will guarantee one user with one

Question 5: biometric approach to ATM access control would provide better security in ATM.

Question 6: majority of people interview has forgotten their password before and as a result they were unable to use their card to withdraw money from their account.

Question 7: larger percentage of people Intel-viewed has misplaced their ATM card before and as a result they were unable to use their card to withdraw money from their account.

Question 8: 69.9% of the people interviewed were once a victim of ATM fraud. Based on the detail given the approaches use in defraud the users varied and it was not discussed in this write up. The only common thing is that their card was used by another person to withdraw money from their account.

Based on the result analysis, it was discovered that Smart card access control has the following drawbacks;

1) Magnetic stripe or chip distortion: information require for the card to function is stored on the chip or magnetic stripe. There is possibility of magnetic surface being distorted as result of continuous use and improper handling. This distortion can leads to damage and rendered the card useless.

2) Misplacement of the card: theirs is possibility of the card being misplaced and as a result rendered the card useless.

3) Stolen or theft: this card could be stolen by another person even with the password. There have been a case of burglar's forcefully collected ATM card and password from the legitimate owner and even follow such person to the ATM location to confirm that the PIN number given to them is correct.

4) Card fraud: recently, there has been reported case of card fraud. Various methods were use by fraudster in perpetuating this crime; among others are: for a low tech form of fraud, the easiest is to simply steal an ATM card. A later variant is of this is to trap the card inside ATMs card reader [3]. Advance fraud in ATM involve the installation of a magnetic card reader over the real ATMs card slot and use of a wireless surveillance camera or a modified digital camera to observe the user PIN. Card data is then cloned out on a second card and the criminal attempt a standard cash withdrawal [6]. Consequent to the identified drawbacks. The authors of this paper proposed the design of the intelligent voice-based access control in automatic teller machine.

IV. PROPOSED INTELLIGENT VOICE-BASED SYSTEM

Proposed system description, figure 2 shows the schematic diagram of proposed intelligent voiced-based access control for ATMs. The proposed system basically consists of 3 main components:

1) Voice sensor
2) Speaker verification system and
3) ATM access control

A low cost microphone commonly used in computer system is used as voice sensor to record the ATM user voice. The recorded voice is then sent to the voiced-based verification system which will verity the authenticity of the user based on his/her voice.

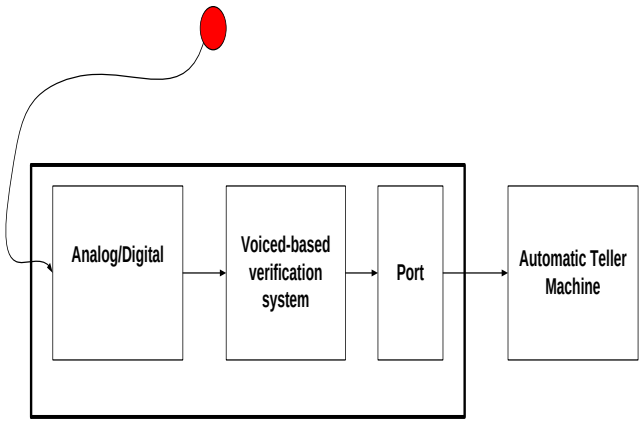


Figure 2: Proposed Intelligent Voice-Based ATM Access Control

Voice base verification, will enable a decision signal which will accept or reject the access that will be sent through the parallel port of the system. The intelligent voice-based access control will generally make possible decision as;

4) Authorized person (ATM user) accepted
5) Unauthorized person (ATM user] rejected

The qualities to measure rate of access control accuracy to reject the authorized person is called false rejection (FRR), and that to measure rate of access control to accept the unauthorized person is called false acceptance rate [FAR].

Mathematically, both rates are expressed as percentage using the following simple calculation [2].

NFR and NFA are the numbers of false rejections and false acceptance respectively, while NFA and NIA are the number of authorized person attempts. To generate high security of the ATM access control system it is expected that the proposed system have both low FRR and low FAR.

A. Voiced-based verification System

The use of voice for biometric measurement becomes more popular due to the following reasons; natural signal generation, convenient to process or distributed, and applicable for remote access. There are 2 kinds of voiced-based recognition or speaker recognition (Campbell J.P. 1997].

1) Speaker identification
2) Speaker recognition

In speaker verification system, the system decodes that a user is who claims to be. On other hand speaker identification decides the person among a group of person. Speaker recognition is further divided into 2 categories which are text dependent arid text independent.

Tex dependent speaker recognition recognizes the phrase that spoken, whereas in text identification the speaker can alter any word. Thy most appropriate method for voice-based ATM access control is based on concept of speaker verification, since the objective in the access control is accept or reject a user to gain access into ATM. Figure 3a and b. show the basic structure of the proposed system. There are 2 phases in the proposed system.

1. Training enrolment as shown in figure 2a, the authorized persons are registered and their voices are recorded. The recorded voices are then extracted. Features extracted from the recorded voices are used to develop models of authorized persons.

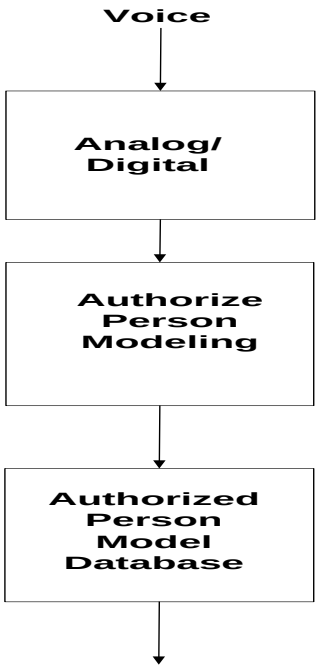


Figure 3a: Training phase

2. Testing or operational phase as shown in figure 3b, in this phase a person who want to access the ATM is required to enter the claimed identity and his/her voice. The entered voice is processed and compared with the claimed person model to verify his/her claim. At this point system decides whether the feature extracted from the given voice matches with the model of claimed person. Threshold is set in order to give a definite answer of access acceptance or rejection. When degree of similarity between a given voice and model is greater than threshold the system will accept the access, otherwise the system will reject the person to access the ATM.

V. Merits of Intelligent Voice-Based Access Control

Precession of classification: voice-based system has low false acceptance rate (FAR] and false rejection rate FRR compared to smartcard, and even other biometric method like fingerprint.

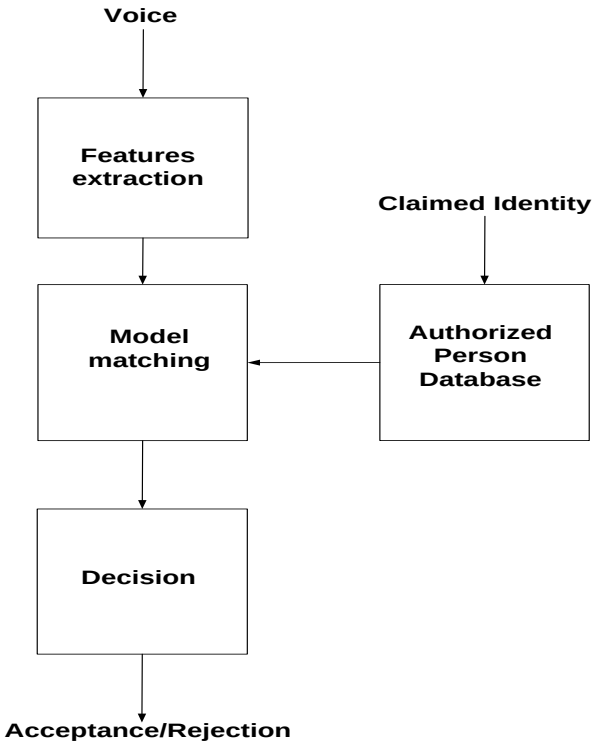


Figure 3b: Testing (operational) Phase

2. **Reliability**: as for other biometric, a test has shown that, spoofing method can be used to bypass finger print check, facial recognition can be broken in by showing a video of someone face or a still image of person. Voice recognition is reliable in the sense that no two people have the same voice signal.

3. **No misplacement**: smartcard can be misplaced or forgotten but a user voice is part of his body, as a result it can be forgotten or misplaced

4. **Economy**: the use of voice recognition will save the banks cost of producing smartcard.

5. **Fraud**: use of this method will reduce fraud discussed earlier.

VI. Conclusion

This paper presents a conceptual framework for use of intelligent voice-based access control in ATMs which is biometric approach. Research has shown that ATM user have encountered several problems in the past which include; chip distortion, card misplacement.

Card fraud, etc. these entire problems are associated with using smartcard access control in ATM. To overcome these problems it is advisable that government should partner with banking sector to implement the use of biometric technique "intelligent voice-based access control" in ATMs, as this will eliminate completely the problems associated with smartcard access control.

REFERENCES

[1] Atkins, W., 2001: A testing for face recognition technology. Biometric Technology Today, vol 147, pp. 195-197.

[2] Campbell, J, P., 1997. Speaker recognition; a tutorial. In Procc. IEEE, pp; 1437-1462.

[3] Dade, L. A. et al. 1998. Human brain function encoding and recognition: Anal of the New York Academy of Sciences, 355, 572 - 574

[4] Kung, S. Y., M W, Mack, and S. H. Lin, 2004. Biometric authentication machine learning approach. Prentice Hall

[5] Njemanze, P. C. 2007. Cerebral lateralization for processing Laterality, 12, 31 -49.

[6] Schoon G. A. A. and deBurn J. C. 1994, Forensic science international, pill.

[7] Wahyudi et al, 2007. Speaker recognition identifies people by their voices. In Proc. Of conference on security in computer application (2007).

[8] Yekini, N. A., and Lawal, 0. N. 2000. 1CT for accountants and Bankers: Hasfem Publication,

[9] Zhang, D, *d.*, 2000. Automated biometric technologies and systems. Kluwer academic Publisher.

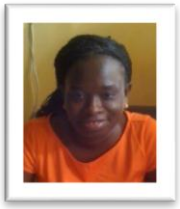
REFERENCES

Yekini Nureni Asafe., majors in Data Communication & Networking, Computer Application, and Computer Architecture. He obtained NCE in Physic from Lagos state college of education, B.Sc. Degree in Electronic and Computer Engineering from Lagos State University and Master Degree in Computer Science from University of Lagos, Nigeria.

He is a member of International association of Engineers (**IAENG**) and Nigeria Computer Society (**NSC**), International association of Computer Science and Information Technology (**IACSIT**). He currently lectures Data Communication and Networking, Assembly Language and Computer architecture in Yaba College of Technology, Lagos, Nigeria.

Itegboje A.O., obtained her B.sc degree in mathematics education, PGD in computer science and MSc in computer science from university of Lagos, former; HOD computer department, Director of MIS center, Yaba College of Technology. Lagos Nigeria. She is currently a PHD research candidate, SMED Southern university, Baton Rouge, LA US.

Oyeyinka I.K., a chief lecturer. Major in network congestion and control. He obtained his B.sc degree in mathematics and PGD in computer science from University of Lagos, and PhD Computer science from university of Abeokuta. He is a chief Lecturer in the department of Computer Technology, and currently the Director Center for Information Technology management center of Yaba College of Technology, Nigeria. He's a member of Computer Professional Council of Nigeria [CPN] and Nigeria Computer Society [NCS].



Akinwole A.K., a principal technologist. Major in Mobile Computing and ADhoc Network Performance. She obtained her academic Higher Diploma degree (HND) from Yaba College of Technology, PGD in Computer Science from Namidi Azikwe University and MTech in Computer Science from Ladoke Akintola University (LAUTECH) Ogbomosho. She is currently and academic staff in the department of Computer Technology, Yaba College of Technology. Lagos Nigeria.