Two-Factor Authentication Based Automobile Keyless Entry System

O. Akinsanmi, A.D. Usman, A. Abdulraheem, G.D. Obikoya, B.G. Bajoga

Abstract—**Mechanical keys have traditionally been used to restrict unauthorized access to automobiles. In recent times, microcontrollers were embedded into cars for various applications such as passive keyless entry systems and vehicle immobilizer systems to prevent circumventing the mechanical lock to open the door and then start the engine via short-circuiting the ignition. The embedded electronic systems are very convenient to users but the security of the system can be easily breached for unauthorized access either through theft or lost and found of the car key fob, relay attacks by impostors or if the embedded code is revealed through the wireless interface scanning. In this paper, the development of an Automobile Keyless Entry System using Two-Factor Authentication is described where, the automobile would autonomously verify the users' alongside the conventional mono-factor (i.e., device-based) automobile key fob authentication framework, thus achieving a two-factor authentication system. In addition, the new framework can prevent the three kinds of security breach scenarios. Furthermore, the car owner may allow new persons to drive the car using their voiceprints. The significance of this new framework is that it has provided high level of comfort and convenience and has eliminated the probability of theft. This paper will provide the understanding of the system to the designer of key-less systems. It will also provide designers with some ideas of how to make vehicle more secure. This paper will also benefit many people in terms of saving time and effort that would be required for them to collect the information presented in this paper by reading many published papers.**

***Index Terms*— Keyless Entry System, Voice Biometrics, Vehicle Immobilizer System, Relay Attacks, Key Fob, SmartVR Module.**

I. INTRODUCTION

The aim of this work is the design and development of a Two-Factor Authentication based Automobile Keyless Entry System. This is essential to checkmate the current security problems associated with the electronic embedded systems. For example, in a typical passive keyless entry system, if the key fob is lost and found, stolen or cloned, the car can easily be unlocked. This is due to the fact that, instead of the car validating that the legitimate user is with the authentic key fob, the system only verifies if the car can communicate with the key fob, assuming that the ability to communicate implies that the key fob is genuine and its assumed legitimate user (holding the key fob) is physically close to the car. However, most automobile keyless-entry systems are complemented with vehicle immobilizer systems such that illegal access does not mean that a thief will successfully drive away the vehicle. Nevertheless, both systems have been confirmed to be vulnerable to another type of key fob and vehicle "man-in-the-middle" attack called relay attacks [1]. In practice, the adversary consists of two parties, a leech (RA1), which impersonates the verifier, to the prover, and a ghost (RA2), which impersonates the prover to the verifier [2].

The current car theft problem is so enormous such that about 2,916 (i.e., 33%) vehicles were stolen from the home address or in the vicinity where the owner claimed to have the keys (i.e., as illustrated in the pie chart of Fig. 1) from a 36 day statistics as generated from the UK Police National Computer between 1 January 2011 and 5 February 2011 [1].

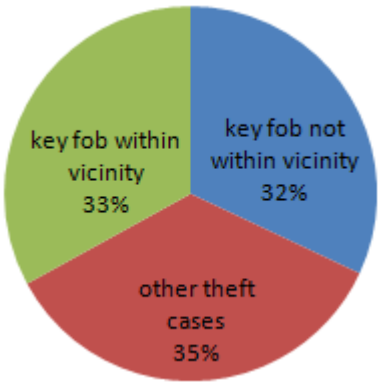

Fig. 1: Statistics of vehicle stolen without using the original key in the UK.

The challenge for car manufacturers now is that any secure automobile keyless entry system should open only when the legitimate user (in possession of the key fob) intends to open the car because, the verification of the vehicle's key only does not guarantee that the key fob holder is really the owner.

Biometric systems can address the problems of security breaches such as the relay attacks and other security issues associated with the traditional passive keyless entry and vehicle immobilizer system due to poor legitimate user verification techniques. Biometrics refers to automatic identification and verification of an individual based on certain behavioral and physiological characteristics

Manuscript received .
Olaitan Akinsanmi, [1]Department of Electrical and Electronics Engineering, Federal University Oye-Ekiti, Nigeria .
(e-mail: akinsanmi2013@gmail.com).
A.D. Usman, [2]Department of Electrical and Electronics Engineering Kaduna Polytechnic, Kaduna, Nigeria.
(e-mail: aliyuusman@gmail.com).
A. Abdulraheem, [3]Department of Electrical and Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.
(e-mail: abiabdirrahman@ gmail.com).
Gbenga Daniel Obikoya, [1]Department of Electrical and Electronics Engineering, Federal University Oye-Ekiti, Nigeria
(e-mail: gbenga.obikoya@fuoye.edu.ng).
B.G. Bajoga, [3]Department of Electrical and Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

associated with the person such as fingerprints, voiceprint, face, etc. This automobile keyless entry user identification and authentication system is based on voice biometric (human recognition through voiceprints). The integration of the voice biometric technology will help to achieve higher security needs and it is more suitable to implement on the existing keyless entry system operational framework.

II. THE SYSTEM DESIGN AND IMPLEMENTATION

The new system framework involves the development and implementation of the hardware and software of the new framework. The h-PKE hardware comprises the key fob and an on-vehicle module. As for the key fob, users have to possess a standard keyless entry transponder key fob. In this work, the design and development of a new keyless entry framework does not involve any structural modification to the existing keyless entry system key fob. Therefore, the key fob can be any software reconfigurable type that can be in-circuit programmed to accommodate 128 bit advance encryption scheme (AES) for encrypting the wireless communication transmitted data for better security as opposed to proprietary stream cipher with 48-bit keys commonly used for authentication [3]. However, the on-vehicle module was designed and implemented around three different microcontrollers supporting the dynamic operations of the new keyless entry system. These microcontrollers include the embedded RSC-4128 microcontroller based speech processing module (i.e., in the SmartVR module), the PIC16F886 and the PIC18F4680. The SmartVR module is configured as the Biometric Certifying Authority (BCA), the PIC16F886 is the main access controller while, the PIC18F4680 is configured as the base station controller. Fig. 2 shows the system architecture of the developed system hardware.

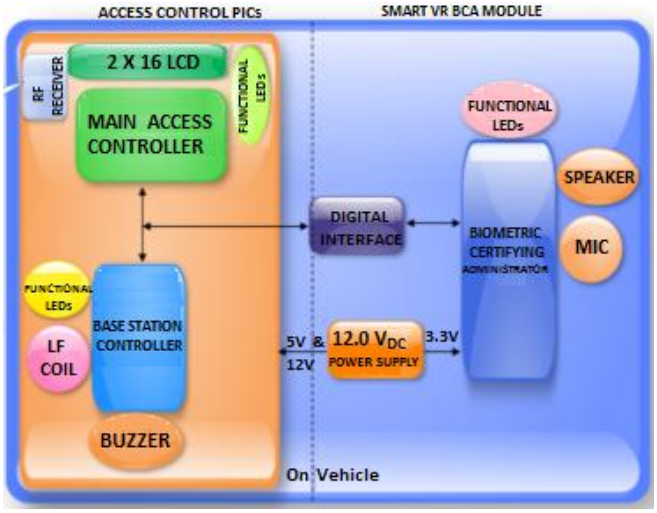

Fig. 2: System Architecture of the Developed System

A description of the on-vehicle module hardware components (shown in Fig. 2) with their specifications as well as the software driving the microcontrollers is presented in the following sub-sections.

A. Hardware Subsystem Components

(1) The Smart VR Module: The SmartVR module (termed as BCA in Fig. 4) from TIGAL KG Inc., Austria is the core component of the user verification hardware interface. It contains an embedded RSC-4128 mixed signal processor which is a state-of-the-art speech processing microcontroller (from Sensory Inc., USA). The SmartVR module is packed into a 56-pin dual-in-line package (DIP) module of 42 x 72 mm size having an upgradeable Virtual Machine firmware located onboard its electrically erasable programmable read-only memory (EEPROM). This can be erased and re-programmed any time. The embedded voice recognition RSC processor in the SmartVR module has connected to it other on-chip peripheral components like the analog to digital converter which serve as the omni-microphone interface to the processor. A program firmware for the SmartVR module has been written in such a way that only the main system user (i.e., the system administrator) can control all the SmartVR system functionalities.

(2) The Main Access Controller: The main access controller coordinates the entire keyless entry system having interfaces with all other modules including the SmartVR module. The circuit is built around a PIC16F886 microcontroller. The PIC16F886 is an 8-bit microcontroller which belongs to the midrange family of the PIC microcontroller devices (from Microchip Technology Inc., Chandler, AZ, USA). It has 28-pins and there are a total of 25 input and output (I/O) pins (on PORTA, PORTB and PORTC) that are user-configurable on a pin-to-pin basis. It has a Random Access Memory (RAM) space that can contain 368 bytes of data while it's EEPROM can contain 256 bytes of data. The PIC16F886 software program for this work was developed in C language to decode Microchips KEELOQ code hopping RF signal messages from the key fob which is further encrypted with 128 bit Advance Encryption Standard (AES). Besides, it coordinates the door lock/unlock process. It also has valid user access trigger input from the SmartVR module that is used to decide whether or not to initiate an unlock process after validating the key fob signal. The inputs and outputs from the SmartVR module's circuit and the key fob LF base station controller unit are configured to the main access microcontroller. Other configured input and output ports are the door lock/unlock and door open/close detection inputs, learn/delete key fob serial number input, door lock/open actuator's signal output and bi-directional communication link with the Low Frequency (LF) Base Station and the SmartVR module.

(3) The Base Station Controller: An independent LF base station controller is needed as opposed to implementing its functions on the same main access microcontroller because there is the need to cater for the simultaneous transmission and reception of an LF signal during the challenge and response wireless key fob authentication. Hence, the need for PIC18F4680 microcontroller which was selected for the implementation of the LF Base controller due to its availability and the wide range of specific automobile compliant peripherals available on the chip. For example, it

has a controller area network (CAN) and a local interconnect network (LIN) compatible Enhanced Universal Synchronous Asynchronous Receiver Transmitter (EUSART) which can seamlessly be interfaced with standard in-vehicle CAN or LIN networks.

The Base Station transmits LF plain text to the key fob using the challenge and response protocol after receiving a trigger pulse from the SmartVR module and also transmits and receives acknowledgement messages from the central access microcontroller via bi-directional link.

A. Final Stage

In order to achieve a comprehensive embedded system solution, software was written and programmed into each of the microcontroller unit of the system. Furthermore, the operation of each module was synchronized to achieve a seamless software system as in [4].

The software subsystem was designed such that users would have to for once or periodically register securely their vocal identity with the Smart VR module which is termed the biometric certifying administrator (BCA) and the user voiceprint will be stored on-board the Smart VR memory. This enables the BCA to dedicatedly manage the integrated user verification process.

The BCA is responsible for the comparison and management of voiceprint feature of pre-registered users. For access to be granted, it matches the features of user's voiceprints with those saved in the memory and calculates the matching scores between all the voice print features in its database with the current user's voiceprints using a specialized C language program developed and programmed into it. Then, if there is a match the BCA communicates with the base station controller to initiate the 125 kHz low frequency (LF) signal to wake up and activate the key fob transponder which in turn responds to the car through a 433 MHz ultra-high frequency (UHF) based transmitter. The AES encrypted response from the key fob transponder is simultaneously received and decoded by the main access controller. The main access controller will then communicate with the user through speech synthesis capability of the BCA for operation validation. The main access controller waits for the user's BCA authenticated voice acknowledgement before a secure access is permitted. As soon as the user gains access, the door relocks automatically.

III. PROTOTYPES SYSTEM RESULTS AND DISCUSSION

The system's hardware and software described in the previously had been successfully implemented into a fully functional prototype system by interfacing all the hardware components. Thereafter, the software programs running in each of the microcontrollers were synchronized thereby, achieving the aim of the new design. Nevertheless, the human/user voice biometrics recognition aspect of the system was specifically tested to evaluate the prototype system performance in a real life environment.

The simulation test illustrated by an experimental setup in Fig. 3 was performed in a noise controlled office room setting by carrying out a speaker dependent and speaker independent system recognition experiments by combining the password/SI command voiceprints and a busy high way noise sample at various signal-to-noise ratios using the COLEAMATLAB toolbox reported in [5].

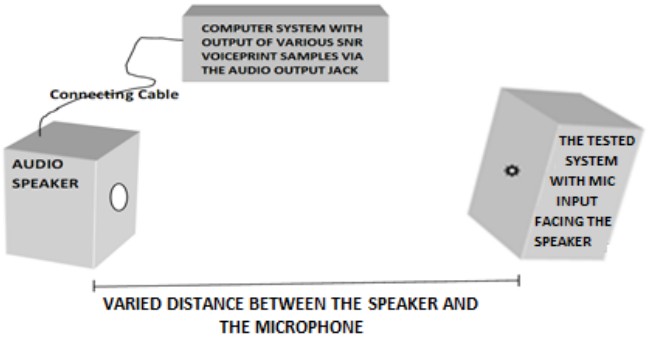

Fig. 3: Voice Recognition Experimental Setup

Table 1: Experimental Results

Output Parameters / Input Samples		0.5m Experimental Results						1.0m Experimental Results					
		FAR (Acceptance Score) (%)			FRR (100%-Acceptance Score)			FAR (Acceptance Score) (%)			FRR (100%-Acceptance Score)		
SNR (dB) / Case Studies		10	15	Mean	20	Clean	Mean	10	15	Mean	20	Clean	Mean
1	User Password 1	20	20	20	20	0	10	0	20	10	40	0	20
2	User Password 2	0	40	20	40	0	20	0	20	10	60	0	30
3	My Vocal Car (Phrase)	0	40	20	20	0	10	0	40	20	20	0	10
4	Settings (Word)	0	20	10	20	0	10	0	20	10	40	0	20
Final Mean Values				**17.5**			**12.5**			**12.5**			**20.0**
Standard Deviation				**4.33**			**4.33**			**4.33**			**7.07**

A 19dB SNR threshold standard as reported in [6], [7] for voice samples generated using the electret microphone was adopted to distinguish the system's FAR and FRR error rates. The test result for five trial cases recognition for the two cases of 0.5m and 1.0m distance is shown in Tables 1.

The MATLAB function evaluation toolbox for biometric systems released as "DET wareversion 2.1" by NIST was used to analyze the experimental results by plotting the DET curve based on the measured FAR and FRR error ratios of the prototype system using the US National Institute of Standards and Technology (NIST) Speaker Recognition Evaluation (SRE) 2008 protocols. Table 2 shows the precise MATLAB output values of the EER, HTER and the minimum detection cost function (minDCF) for the system when the DCF parameters were set as CMiss = 10, CFA = 1 and PTarget = 0.01 respectively.

Table 2: Performance Evaluation Results

PARAMETERS:	EER	HTER	minDCF	THRESHOLD VALUE	TOTAL SYSTEM ERROR (%)
@ 0.5 m	0.7710	0.5135	0.0848	1.5159	21.9
@ 1.0 m	0.7665	0.4975	0.0635	1.4874	23.0
MEAN VALUES:	0.7688	0.5055	0.0742	1.517	22.45

Fig 4 shows the system EER for both experimental cases in respect of the two distances. Such graph is known as the Receiver Operating Characteristic (ROC) curve.

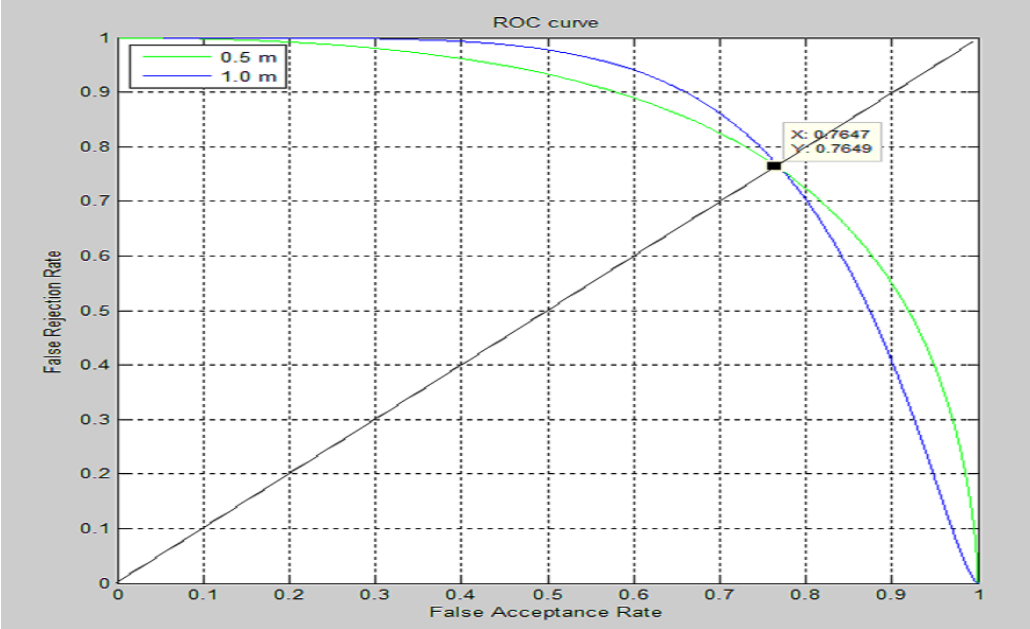

Fig. 4: ROC Curve Showing Same EER for both Distances

Fig. 4 shows that both curves have a similar EER at a value of 0.765 which implies that the system had a stable performance over both distances. It represents the error at the threshold that gives equal false acceptance and false rejection which serves as a reference indication of the system performance. In addition, the mean equal error rate of the system is 22.45 per cent (from Table 2) which is slightly lower and better than the 23.9 per cent of a high performance HMM machine recognizer with microphone channel adaptation for an omni-microphone reported in [6]. The significant of this result is that the system should properly distinguish between an Imposter and the genuine speaker in 76.9 per cent cases if the threshold is set at 1.5 since the rates of FAR and FRR, define the operating point of the system. However, the system can be adjusted for tighter security but this would consequently decrease the user conveniences.

Similarly, the time taken to perform these operations was measured by initializing the application and measuring operational period using a stop watch. The time taken for the administrative user is within 3s whilst a proxy user takes about 5s. The administrative setting domain log-in procedure takes 10s for execution because of the intelligent genuine user verification procedure implemented by answering a set of randomized challenge and response questions using the interactive voice response. The remote keyless entry operation from the key fob (with the new user authorization acknowledgments) takes only 3s to execute under the demonstration room condition. The administrative user also has the ability to gain access into the vehicle and start the engine without using the conventional mechanical key backup in the event that the key fob malfunctioned or missing. This would be achieved through an alternate unlock mode using one of the three pre-programmed one-time-useable speaker independent phrase (i.e., "foolish lion", "intelligent goat") having passed the challenge and response user probity questions. This alternative is also available when the system

system requesting for the user password prior access authorization and deactivation of vehicle immobilizer system. Also, during the functionality test performed, the interactive voice response capability of the system was explored and fond to suit the different aspect of the speech recognition application and the users' audio feedback mechanism of the system. fails to recognize the user due to cold, tiredness, low SNR, and so on.

The RKE mode was also tested successfully with the system requesting for the user password prior access authorization and deactivation of vehicle immobilizer system. Also, during the functionality test performed, the interactive voice response capability of the system was explored and fond to suit the different aspect of the speech recognition application and the users' audio feedback mechanism of the system.

IV. CONCLUSION

This paper explained how the development of a new two-factor keyless-entry access authentication system framework through combination of a secure wireless communication and legitimate user authorization was achieved with an implemented functional prototype validating the concept. Finally, a two-factor authentication based keyless entry system prototype has been implemented by integrating a multi-modal speaker verification system to identify the legitimate users in addition to the challenge and response protocol of the conventional key fob (that must be in possession of a legitimate user) thus, providing a more reliable interdependent security system. The system would put the success rate of stealing vehicles with the replay, relay and other key fob cryptographical attack at approximated 1 out of every 500 attempts based on the GAR experimental results. The limitation of this system is that the driver (or the intruder) will still require the use of car key (or by short-circuiting the ignition system) to start the engine. Therefore, any attempt to compromise the security of the door by the intruder may led to theft. However, it is recommended that customer identification device should be built into ignition system for improvement and further development of the prototype system into a full functional commercial product.

REFERENCES

[1] S. Mason , "Vehicle remote keyless entry systems and engine immobilizers: Do not believe the insurer that this technology is perfect [Online]," Retrieved March 14, 2014, from http://dx.doi.org/doi:10.1016/j.clsr.2012.01.004, 2012.

[2] C. Onete, "Security Aspects of Distance-bounding Protocols [Online]," Retrieved March 14, 2014, from http://tuprints.ulb.tu-darmstadt.de/3040/7/ThesisMain-final.pdf, 2012.

[3] R. Verdul, F.D. Garcia, , & J. Balasch, , " Gone in 360 Seconds: Hijacking with Hitag2. USENIX_2012 [Online]," Retrieved March 19, 2014, from http://www.cs.ru.nl/~rverdult/Gone_in_360_Seconds_Hijacking_with_Hitag2-USENIX_2012.pdf, 2012.

[4] J. Valvano & R. Yerraballi, "Embedded Systems - Shape The World [Online]," University of Texas Online Course E-book, RetrievedMay09, 2014 from http://users.ece.utexas.edu/~valvano/Volume1/E-Book/C2_FundamentalConcepts.htm, 2013.

[5] P. Loizou, "COLEA: A MATLAB Software Tool for Speech Analysis," Department of Applied Science, University of Arkansas at Little Rock [Online], Retrieved May 13, 2014, from http://ecs.utdallas.edu/loizou/speech/manual.pdf, 1998.

[6] R.P. Lippmann , "Speech recognition by machines and human," ELSEVIER Speech Communication, RetrievedJune04,2014,from http://www.utdallas.edu/~assmann/hcs6367/lippmann97.pdf 1997, pp. 1 – 15.

[7] N. Deshmukh, A. Ganapathiraju, R. J. Duncan, & J. Picone, "Human speech recognition performance on the 1995 CSR HUB-3 CORPUS," Institute for Signal and Information Processing, Mississippi State University," Retrieved June 04,2014, from http://www.isip.piconepress.com/publications/conference_proceedings/1996/arpa_srw/human_benchmarks/paper.pdf

Engr. Dr. Olaitan Akinsanmi is an Associate Professor. He holds a Bachelor of Engineering (BEng, 1997) degree from the University of Ado-Ekiti, Master of Science (MSc, 2005) degree and Doctor of Philosophy (PhD, 2012) degree from Ahmadu Bello University, Zaria, Nigeria. Professionally, he is a registered Engineer with the Council for The Regulation of Engineering in Nigeria (COREN), Professional Member, Institute of Electrical and Electronics Engineers (IEEE), and Corporate Member of The Nigerian Society of Engineers (NSE), Associate Member, The Nigerian Institute for Biomedical Engineering (NIBE), Fellow of the Nigerian Institute of Natural Resources and Human Development, Associate Member: Nigerian Institute of Management Chartered (NIM), and National Association of Educational Managers and Planners (MNAEMP) among others. Engr. Dr. Akinsanmi is a recipient of Award of The Pillar of Nation Builder in the Academics from The Nigerian Strategic Institute for Natural Resources and Human Development in 2013. He has acquired over Seventeen year of research and development with different organizations and over 15 years of effective teaching and administrative experience at the University level. He is a specialist in Computational Electromagnetics, Neural Network Soft Computing in Artificial Intelligence and Reliability of Engineering systems. He is the present Head of Dept Electrical and Electronics Engineering Federal University Oye-Ekiti,Ekiti State, Nigeria.

Dr. Aliyu D. Usman obtained his Doctor of Philosophy (Ph.D.) in the Department of Electrical and Electronics Engineering, Faculty of Engineering, University Putra Malaysia, Selangor, Malaysia. He is currently the Head of Department of the Department of Electrical and Electronics Engineering, College of Engineering, Kaduna Polytechnic, Kaduna, Nigeria. His major field is electromagnetic, RF safety, antenna and propagation.

Engr. A. Abdulraheem obtained a Bachelor of Engineering (B. Eng.) from University of Ilorin and Master of Science (M.Sc.) from Ahmadu Bello University. He is registered Engineer with the Council for The Regulation of Engineering in Nigeria (COREN). His keen interest is in Computer communication network and security.

Engr. Gbenga D. Obikoya obtained a Bachelor of Technology in Electrical and Electronics Engineering from Ladoke Akintola University of Technology (2006) and proceeded to University of Lagos where he obtained Master of Science in Electrical and Electronics Engineering (2012). He is certified and registered by Council for The Regulation of Engineering in Nigeria (COREN), he is a Corporate Member of The Nigerian Society of Engineers (NSE) and a also a Member of The Institute of Electrical and Electronics Engineers (IEEE). He is a Lecturer and a Researcher in the Department of Electrical and Electronics Engineering with interest in Telecommunication Systems and Network, Antenna and Propagation, Information Technology, Nano-Antenna and Nano- Communication. He is presently the Departmental Examination Officer.

Engr. Prof. Buba Garery Bajoga is a Professor of Electrical Engineering at the Ahmadu Bello University, Zaria, Nigeria. He obtained his Bachelor of Science (B.Sc., 1968) in Electrical Engineering from Ahmadu Bello University, Zaria, Nigeria and a Doctor of Philosophy (Ph.D., 1972) in Electrical and Electronics Engineering from the State University of New York. He served as two-term Vice-Chancellor covering the period 1984-1994 during which, he also served as Chairman of Committee of Vice-Chancellors. At various times, he was a member of Board of Directors of NITEL (1985); member, the Technical Sub-Committee on NITEL (1988) and member of Board of Directors of Nigerian Communications Commission (NCC) (1993). Prof. Bajoga has served on the Council of COREN as well as on several Committees of NSE. He is currently the Managing Director of NITEL, and a Foundation Fellow of the Academy.