UNIVERSITY OF ILORIN

THE TWO HUNDRED AND SEVENTIETH (270TH) INAUGURAL LECTURE

"INVISIBLE BOUNCERS IN THE WORLD OF INFORMATION SECURITY"

By

PROFESSOR OLUWAKEMI CHRISTIANA ABIKOYE

B.Sc. (Ilorin), M.Sc. (Ibadan), Ph.D. (Ilorin), PGD (Education) (NOUN); MNCS, MCPN, MNIWIT, MAITP, MPAIDF

DEPARTMENT OF COMPUTER SCIENCE,

FACULTY OF COMMUNICATION AND INFORMATION SCIENCES,

UNIVERSITY OF ILORIN, NIGERIA

THURSDAY, 28TH NOVEMBER, 2024

This 270th Inaugural Lecture was delivered under the Chairmanship of:

The Vice-Chancellor

Professor Wahab Olasupo Egbewole, SAN
LL.B (Hons) (Ife); B.L (Lagos); LL.M (Ife); Ph.D. (Ilorin); FCArb; Fspsp

28th November, 2024

ISBN: 978-978-8556-91-6

Published by:

The Library and Publications Committee,
University of Ilorin, Ilorin, Nigeria

Printed by
Unilorin Press, Ilorin, Nigeria

PROFESSOR OLUWAKEMI CHRISTIANA ABIKOYE

B.Sc. (Ilorin), M.Sc. (Ibadan), Ph.D. (Ilorin), PGD (Education) (NOUN); MNCS, MCPN, MNIWIT, MAITP, MPAIDF

DEPARTMENT OF COMPUTER SCIENCE,

FACULTY OF COMMUNICATION AND INFORMATION SCIENCES,

UNIVERSITY OF ILORIN, NIGERIA

BLANK

Courtesies

The Vice-Chancellor,
The Deputy Vice-Chancellor (Academic),
The Deputy Vice-Chancellor (Management Services),
The Deputy Vice-Chancellor (Research, Technology and Innovation),
The University Registrar,
The University Bursar,
The University Librarian,
The Provost, College of Health Sciences,
Dean, Faculty of Communication and Information Sciences,
Deans of other Faculties, Postgraduate School, and Student Affairs,
Professors and other members of Senate,
Directors and Heads of various Centres and Units,
Head of the Department of Computer Science,
Heads of other Academic Departments,
Members of the Academic, Administrative and Technical Staff,
My Lords Spiritual and Temporal,
Greatest Computer Science students,
Great students of the University of Ilorin,
Gentlemen of the Print and Electronic Media,
Distinguished Invited Guests,
Ladies and Gentlemen.

Preamble

I give God all the glory, honour, and adoration for the opportunity and privilege given to me to stand in front of this great audience to deliver this inaugural lecture. This is the first to be presented by a female professor of Computer Science at the University of Ilorin. My Lord and God, you are my source, inspiration, sustenance, guide, light, and salvation. As the Bible says in Romans 9: 15-16 (NIV): **For he says to Moses, I will have mercy on whom I will have mercy, and I will have compassion on whom I have compassion. It does not, therefore, depend on man's desire or effort, but on God's mercy".** This implies that true success is not solely dependent on man's desire or effort but on God's mercy. So, it is your mercy, oh Lord, that I receive that made today a reality.

My journey to becoming a professor of computer science was not as straightforward as it seemed. Initially, I wanted to study medicine, but due to my fear of biological jargon while in secondary school, I opted to study pharmacy at Ahmadu Bello University (ABU), Zaria. Back then, applying to higher education required separate applications for each institution, whereas today, a single application allows you to apply to multiple institutions. I was not seriously interested in going to the polytechnic, but I had to pick up the application form as a norm. I initially chose Banking and Finance as a course of study based on my good performance in Accounts as a subject in secondary school and also the lack of health science-related courses at the polytechnic at the time.

One day, my elder brother, then a computer science student at the University of Ilorin, looked through my application form and asked me why I chose Banking and Finance, given my science background. I told him there were no health sciences programs at the polytechnic. He then advised me to pick computer science instead, as he was also studying the course at the University of Ilorin at the time. I decided to follow his advice, and that marks the beginning of my career pursuit in the field of computer science. Eventually, I got admission to Kwara Polytechnic to study computer science. The application to ABU was not successful. I decided to resume for the National Diploma in order not to sit at home for a whole year while I prepare to write another JAMB to study Pharmacy at the University of Ibadan and also collected a University of Ilorin remedial form to study medicine. I put in these applications at the same time to ensure that I got admission into higher institution the following year. All efforts to get admission into the University of Ibadan in the following year proved abortive because of my scores, so the only option left was the Unilorin remedial programme.

Surprisingly and disappointedly, when Unilorin released the remedial admission list, I was offered Agriculture instead of Medicine-*nibo la lo, nibo la jasi*. At this point, I had to seek guidance from a Professor in the Faculty of Health Sciences in the University of Ilorin. He suggested I continue with Agriculture in the remedial programmme while aiming to transfer to Medicine if I performed excellently well in the remedial exams. I took his advice and registered while I was still on the National Diploma Programme in computer at the Polytechnic. On the verge of resuming the remedial programme, during my second year at the polytechnic, ASUU went on a nationwide strike, leading to the closure of all the federal universities, and as such, I had to continue my programme at the polytechnic. When the strike ended, I pondered deeply about going for the remedial programme or completing my national diploma programme; I earnestly did not want to study Agriculture, and I was almost done with the programme at that time. I weighed my options and decided to continue studying Computer Science at Kwara State Polytechnic, with the intention to seek direct entry admission into the computer science programme of the University of Ilorin.

After my National Diploma in Computer Science in Kwara State Polytechnic, I applied for the Unilorin Computer Science programme as a direct entry student and was offered admission. This marked the beginning of where I am today as a Professor of Computer Science. Years later, I found myself returning to the very walls of the University of Ilorin, not as a student seeking knowledge but as a lecturer ready to impart knowledge and conduct research in computing. I started my academic career as a Graduate Assistant in 2004 and I diligently climbed the academic ladder, eventually earning the prestigious title of Professor of Computer Science. Looking back on the twists and turns of my path, I cannot help but see every setback in this journey as a stepping stone that ultimately led me to this fulfilling destiny. This is a reality I would not have foreseen back then. Since then, I have been unravelling the mystery of Information Security using different invisible bouncers.

Introduction

An inaugural lecture is an opportunity for a professor to highlight his or her teaching and research expertise, contributions, and achievements in his or her chosen field of study. Consequently, I feel honoured to stand before this august gathering today to deliver the 270thinaugural lecture in its series. This is the second in the Department of Computer Science and the 5th in the Faculty of Communication and Information Sciences titled ”**Invisible Bouncers in the World of Information Security”.** The first inaugural lecture in the Department of Computer Science titled, “Deconstructing the Crawling Mindset: Combatting Security Challenges of the Net-Centric Computing” was delivered by Professor Rasheed

Gbenga Jimoh on 23rd August, 2023. In the course of this lecture, I will be showcasing my academic expertise (stewardship and scholarly oversight) and achievements using various invisible bouncers to unravel the mystery of information security. Information security uses a variety of techniques, such as encryption, access restrictions, authentication, intrusion detection and prevention systems, and cyber security procedures, to protect data against unauthorised access, disclosure, change, or destruction. However, information security often operates secretly, making its presence known but concealing its operations, much like an invisible guard positioned at the entrance, this complex aspect of information security highlights the challenges and importance of safeguarding digital assets in today's world.

Mr. Vice-Chancellor, it is important that sensitive information is protected in an increasingly interconnected digital world due to the dynamic nature of threats, such as cyber-attacks, malware, phishing, insider threats, and social engineering. By understanding the concept of the invisible bouncer in information security, knowledge of the unseen threats that can affect our digital lives and the techniques required to safeguard against them will be gained.

In this lecture, the mysteries surrounding information security will be unravelled looking into the different aspects of its challenges, implications and solutions such as cryptography, steganography, encryption, intrusion detection systems, spam detection, and malware detection.

In the field of information security, the concept of the "invisible bouncers" is comparable to the role of security measures that silently but effectively operate to protect digital assets. It implies the presence of protective measures that may not be readily evident but play a crucial and important role in protecting networks and sensitive data. In the same way that a bouncer monitors and controls access to a venue or location, these invisible security mechanisms operate silently in the background, scrutinising incoming traffic, verifying user identities, detecting and averting any potential threats. They serve as the first line of defense, actively preventing malicious activities and unauthorised access and making sure that only authorised users have access to sensitive data. This could include intrusion detection systems, firewalls, steganography tools, biometric traits, cryptographic and encryption protocols and other security measures that work behind the scenes to protect against cyber threats.

General Overview of Information Security

The advancements in the Internet and Intranet technologies have brought about their proliferation into various types of businesses such as e-commerce, banking and finance and even government operations. This has created enticing opportunity for attackers to exploit businesses through the Internet for malicious gains. Hence, the need for information and cyber security has become very essential in today's cyberspace.

Information security is also known as cybersecurity, digital security, or Information Technology (IT) security, encompasses measures and controls that safeguard computer systems' confidentiality, integrity, and availability of information in storage, under processing, and on transmission (Soomro et al., 2016). Van Oorschot (2021) defines information security as an IT discipline that merges various disciplines such as art, science, and engineering to secure computer-related assets against unauthorised activities or users. It includes the proactive prevention of unauthorised actions, as well as the detection and subsequent recovery from such incidents. The primary objective of information security is to protect valuable assets such as data, computer hardware and software, communication networks, and physical devices from being manipulated by unauthorised agents. Figure 1 shows the difference between information and cyber security.

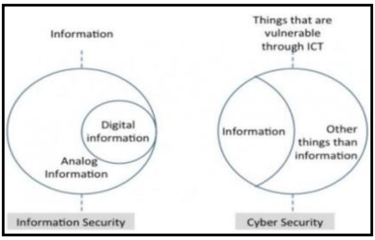

Fig. 1: Difference between information and Cyber Security (Kabanda, 2018)

Goals of Information Security

Every security-based system should have three basic key security elements: confidentiality, integrity, and availability. They are commonly referred to as the CIA of security which are the primary goals that every security system must aim to achieve. Other secondary goals include authentication, utility, and accountability (Chong et al., 2019; Kabanda, 2018; Samonas & Coss, 2014). Figure 2 illustrates the essential security features of an information system:

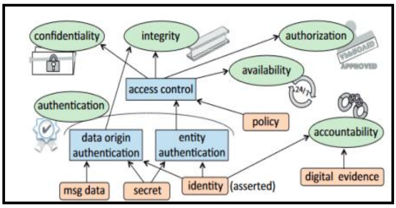

Fig. 2: Security System goals (Kabanda, 2018)

1. **Confidentiality**

Technically, confidentiality deals with the security schemes that conceal data and information to ensure they are not accessible to unauthorised users (Chong *et al*., 2019). Moreover, some researchers claim that confidentiality extends to traffic analysis, where unauthorised users try to take advantage of sophisticated network analysis tools to uncover and read data sent across network channels (Samonas & Coss, 2014).

2. **Integrity**

The integrity of an information or security system is related to its ability to maintain the trustworthiness of the data it retains. In other words, data at rest or in transit does not undergo unauthorised and unintended modification (Liang, 2020). The integrity of an information or security system is said to be compromised when the information it holds is exposed to unauthorised modification (Samonas & Coss, 2014).

3. **Availability**

Availability in information security refers to the ability of an authorised user to access and use data-based systems as intended. It is one of the three core principles of the CIA triad, along with confidentiality and integrity (Samonas & Coss, 2014). Thus, it is when information or confidential data is easily accessible in a timely manner within a digital space. In addition, Rafli *et al*., (2024) revealed that information security is essential and key to company and organisation that deal with confidential information, and availability of those information at the right time ensure trust and easy accessibility to data. Without availability, critical assets and information will not be available to authorised user/system. Hence, availability contributes immensely to information security objective.

My Research Contribution in Information Security

Mr. Vice-Chancellor, my research contribution in unravelling the mystery of Information Security spans Biometrics Security, Cryptography and Steganography, Phishing, Spam Detection, Intrusion Detection Systems (IDS), Web and Network Security, and Android Malware detection.

(1) Biometrics Security

The signature of a person is an important biometric attribute of a human being that can be used to authenticate human identity. However, human signatures can be handled as an image and recognised using computer vision and neural network techniques. An offline signature recognition and verification using a neural network was proposed by **Abikoye**, Mabayoje, and Ajibade (2011), where the signature is captured and presented to the user in an image format. In this study, the signature recognition and verification system was based on image processing, moment invariants, some global properties, and neural networks. Both systems employed a three-step procedure; in the first step, the signature was separated from its image background. The second step performs normalisation and digitisation of the original signature. Moment invariants and some global properties that are used as input features for the neural network (NN) were obtained in the third step. The system was implemented using C# (C-sharp). Our recognition system exhibited a 100% success rate by correctly identifying all the signatures that it was trained for. However, it exhibited poor performance when it was presented with signatures that it was not trained for earlier. Generally, the failure to recognise or verify a signature was due to poor image quality and the high similarity between two signatures. This study aims to reduce the cases of forgery in business transactions.

The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. It has many interlacing features such as stripes, freckles, coronas, radial furrows, crypts, zigzag collarettes, rings, etc., collectively referred to as the texture of the iris. This texture is well known to provide a signature that is unique to each subject. All these features are extracted using different algorithms, i.e., feature extraction is the process of extracting information from the iris image. Iris recognition is one of the newer biometric recognition technologies used for personal identification because it is reliable and widely used.

As part of my contribution to developing an iris recognition system for personal identification, **Abikoye,** Omolehin, and Sadiku (2012) proposed an efficient algorithm for iris localisation. Iris localisation is one of the important steps in iris recognition systems, which relates to the detection of the exact location and contour of the iris in an image. (i.e., it defines the inner and outer boundaries of the iris region.) Obviously, the performance of the identification system is closely related to the precision of the iris localisation step. In this research, images were acquired from pre-collected images from the Chinese Academy of Sciences' Institute of Automation (CASIA) database, and then the iris was localised in the eye image. In localising the iris, we developed an algorithm that captures the Cartesian coordinates of the center of the eye image and two other points for each of the boundaries (inner and outer). These points were used to compute the radii of the boundaries and then used to localise the iris by drawing a perfect geometry that fits the boundaries. The centre points and the computed radii serve as the parameters, which are stored as objects, one for the inner boundary and another for the outer boundary. The algorithm developed can accurately define both the inner and outer boundaries of the iris, irrespective of the geometry it may be (circle or eclipse), by capturing the parameters that represent the geometry. The study was further extended by extracting the features of the iris. The significant features of the iris must be encoded so that comparisons between templates can be made. In this study, the localised iris was converted from a Cartesian coordinate system to a polar coordinate system using the existing Daugman Rubber Sheet Model. Then, a novel feature extraction technique known as Fast Wavelet Transform (FWT) was used to extract the features of the iris and encode the features to generate its 2048-bit iris feature codes. The algorithm is fast and has a low complexity rate (**Abikoye**, Sadiku, Adewole, & Jimoh, 2014).

To deduce the effectiveness of some feature extraction methods used in iris recognition system, **Abikoye**, Aro, Ogundokun and Akande (2018) carried out a comparative analysis of three feature extraction techniques which are Gabor Wavelet Transform, Scale Invariant Feature Transform (SIFT), and Haar Wavelet Transform. We acquired the iris images from the CASIA database and the acquired images were segmented and normalised using Daugman's Integro-differential operator and Daugman's rubber sheet model respectively. The processed iris images were passed separately to the three feature extraction techniques and the extracted features were matched using Hamming distance measure with a threshold value set to ≤0.3732. A comparative performance analysis was conducted on each feature extraction methods and the results revealed that Gabor wavelet Transform performs better than the other two feature extraction methods based on precision, sensitivity and accuracy.

Mr. Vice-Chancellor, cardholders encountered several problems at the point of sale (POS) terminal, these include inadequate security of automated teller machine (ATM) card through theft, not remembering personal identity number (PIN), and the problem of identifying cardholder as the owner of the card. The existing POS machine uses only PIN as a form of authentication which the security can be easily breached. In this study, we proffered a solution to reduce the identified problems by developing a biometric-based POS through the introduction of iris scan at the authentication level of the existing POS machine. A system prototype was designed to imitate a typical PIN-card-based POS system that used iris recognition to improve the security of the POS. The developed system demonstrated a two-tier architectural structure for recognition: the identification and verification module. The verification module focused on the enrolment, normalisation, localisation, extraction of features and matching of iris images obtained from CASIA database. The experimental results showed that the developed system could significantly minimise cardholder fraud at the POS machine if not eradicated (**Abikoye**, Afolabi & Aro, 2019).

Fingerprint recognition is one of the oldest and most reliable biometrics used for personal identification, and it has come a long way from tedious manual fingerprint matching. Adewole, Jimoh, and **Abikoye** (2014), reviewed the algorithms for the various stages involved in fingerprint recognition, such as fingerprint image acquisition, segmentation, normalization, ridge orientation estimation, ridge frequency, Gabor filtering, binarization, thinning, minutiae extraction, template generation, and template matching. Hence, a stepwise biometric procedure for managing students' attendance in higher institutions of learning for both lectures and examinations was presented. We simulated all the various stages involved in the student attendance management system, which include enrolment, fingerprint matching, and attendance management. The results showed that the system is able to identify those students who are qualified to sit for an examination (Adewole, Jimoh, **Abikoye,** & Ajiboye, 2014).

As biometrics becomes the most promising authentication technology, the world is faced with the challenge of choosing the best among the biometric traits for security purposes. **Abikoye**, Adewole, and Salahdeen (2014) applied a fuzzy logic model to determine the security level of fifteen (15) biometric traits. Biometrics characteristics categorised by previous researchers in the field of biometrics were used as a knowledge base. We simulated the model using Qtfuzzylite 4.0 (a fuzzy logic control library in C++), and the results show that fingerprint, hand geometry, hand veins, iris, ear canal, and palm print have a medium security level among the fifteen (15) biometric traits considered based on the following metrics: universality, uniqueness, permanence, collectability, performance, and circumvention. The results of this simulation further revealed that the fuzzy logic approach provides a simple way of drawing definite conclusions from vague and imprecise information.

Despite the fact that biometrics techniques have been recording a high level of security when compared with other forms of authentication, they still come with challenges in terms of speed and accuracy. In this regard, **Abikoye**, Chukwu and

Babatunde (2016) developed an improved palm vein-based recognition system. The development procedure was divided into four stages, which are image enhancement, image segmentation, image thinning, and pattern matching. The image was enhanced using histogram equalisation, after which it was passed to the segmentation stage using K- means algorithm. The binarised image obtained from K-means was then thinned using the Zhang-Suen algorithm and pattern matching was done using Euclidean distance. The inter-distances of the intersections in the thinned image were stored in a database for subsequent matching. The system was successfully tested using the CASIA database and demonstrated high accuracy and speed in recognition, having a very low dependency rate with the Region of Interest (ROI) size extracted. The system was equally tested with an ROI of 100 * 100 and showed increased accuracy when the region was between 150 and 220.

Vice-Chancellor, sir, the importance of security in any financial sector cannot be overemphasized because single-factor authentication (username and password) is no longer sufficient. Therefore, multifactor authentication is required to address security in financial systems. To solve this problem, **Abikoye** and Sanni (2017) proposed keystroke dynamics, a behavioural biometric, as an additional security measure. Keystroke dynamics measures an individual’s typing style. The key press (the time in which the key is held down), key release (the time in which the key is released), the latency (the time between two consecutive keys), and the password length (the total keys of the password) of each user (staff) are produced while typing each character of user password for the registration. The password was further analysed using the statistical method to find the keystroke time and stored in the database for future verification of each registered user. This was achieved using a static keystroke approach on passwords, a statistical feature extraction method to analyse the keystroke time from hold time and latency, and a direct comparison with thresholds based on password length for user verification and authorization. This system provides a stronger security measure than conventional password authentication and can be used in a web-based small and medium scale enterprises (SMEs) sales and stock solution.

An efficient recognition algorithm for the human face is a technique discovered to be based on good facial feature representation. Gabor filters have been employed greatly and are highly considered to be one of the best performing techniques for feature extraction in face recognition owing to their invariance against local distortion initiated by changes in expression, lighting, and pose. In view of this, Aro, Oluwade, **Abikoye,** and Bajeh (2017) conducted a survey on two-dimensional Gabor filters for face recognition. The findings revealed that Gabor filters suffer from high feature dimensionality. In order to solve this problem, a nature-inspired meta-heuristics optimisation algorithm, known as Ant Colony Optimisation (ACO), was applied to obtain relevant and optimal features from the huge Gabor features. We used two face image databases, the Olivetti Research Laboratory (ORL) Database and the Locally Acquired Face Image Database (LAFI), to evaluate the performance of the facial recognition system. Furthermore, three distance classifiers—Malahanobis, Euclidean, and Chebyshev—were used to classify the face images as either matched or mismatched. The results from the experimental study showed that Mahalanobis has the highest classification accuracy of 97.14% and 95.71% for both LAFI and ORL databases, respectively. The lowest False Acceptance Rate (FAR) of 0.1000 was obtained in Mahalanobis, Euclidean, and Chebyshev for LAFI, while the same FAR of 0.1000 was obtained in Mahalanobis and Euclidean for the ORL database. (Aro, **Abikoye**, Bajeh, 2018; Aro, **Abikoye**, Oladipo, & Awotunde, 2019).

Principle Component Analysis (PCA) is an appearance-based technique for feature extraction that is commonly used in computer vision and image processing which suffers from illumination variations; thus, knowing which illumination control method to use in a PCA-based face recognition system is very important. **Abikoye**, Shoyemi, and Aro (2019) performed a comparative analysis of illumination normalisations based on principal component analysis-based feature extraction for face recognition. In this study, face images were acquired from two publicly available face image datasets: the ORL Database and the Face Recognition Technology (FERET Database). After which, three selected normalisation techniques—Discrete Cosine Transform (DCT), Adaptive Histogram Equalization (AHE), and

Contrast Limited Adaptive Histogram Equalization (CLAHE)—were applied to normalise the acquired face images. PCA was further used to extract features from the normalized face images, and Euclidean distance was used to classify the extracted features. The best recognition accuracy of 91.84% was obtained in DCT for the ORL database, while the best accuracy of 76% was achieved in DCT for the FERET database. The highest FAR of 0.9 was achieved in DCT for the ORL database, while the highest FAR of 0.5 was obtained in DCT and AHE for the FERET database. The highest FRR of 0.2821 was achieved in CLAHE for the ORL database, while 0.3000 was obtained in AHE for the FERET database. It was concluded that illumination control approaches have a predominant effect on PCA-based facial recognition systems

Diabetic Retinopathy (DR) is a micro-vascular complication (Hendrick, Gibson, & Kulshreshtha, 2015) of diabetes that results in the alteration or total damage of retinal blood vessels. Early examination of retinal blood vessels could help in the detection and diagnosis of the symptoms of DR, thereby curtailing its effects. In this regard, a Dempster-Shafer (D-S) edge-based detector was used to segment the retinal blood vessels of DR patients from retinal images sourced from the Digital Retinal Image for Vessel Extraction (DRIVE) database. Before the segmentation, median filter, CLAHE, and Mahalanobis distance algorithms were used to preprocess the raw retinal images so that accurate blood vessel detection and segmentation could be achieved. A segmentation accuracy of 0.9765 was recorded when the receiver operating characteristics of the technique were computed. This showed that an acceptable degree of blood vessel segmentation was achieved. The Dempster-Shafer edge-based detector has been further shown to be an effective algorithm for blood vessel segmentation in healthy as well as DR retinal images (Akande, **Abikoye**, & Kayode, 2018).

Furthermore, a framework for Healthy and Diabetic Retinopathy Retinal Image Recognition was implemented. In the study, a framework with two different approaches was presented. The first approach employed structural features for healthy retinal image recognition, while the second employed vascular and lesion-based features for DR retinal image recognition. Any input retinal image was first examined for the presence of DR symptoms before the appropriate feature extraction technique was adopted. Recognition rates of 100% and 97.23% were achieved for the healthy and DR retinal images, respectively, and a false acceptance rate of 0.0444 and a false rejection rate of 0.0133 were also achieved. The findings revealed that if features extracted from healthy and DR retinal images were used to train a retinal recognition system, then such a biometric system should be able to accommodate any possible future changes in the features of the healthy retinal images used to train the retinal recognition system (Akande, **Abikoye**, Kayode & Lamari, 2020).

Mr. Vice- Chancellor, Hypertensive Retinopathy (HR) and glaucoma are also two of the most common and leading eye problems responsible for human vision loss and blindness. Both cases cause alteration of the vascular structures of the retina, thereby initiating gradual vision loss and eventual blindness. It is relieving to know that early detection of the changes in the vascular structure of the retina can help detect these diseases before the eventual collapse of the eye. This prompted Akande, **Abikoye**, Gbadamosi, Ayoola, Ayegba, Ogundokun, and Asani (2020) to present a dataset that contains high-resolution biomedical image files of vascular structures extracted from retinal images of HR and glaucoma from the Digital Retinal Images for Optic Nerve Segmentation Database (DRIONS-DB). The database contains 110 retinal images that were captured with an HP-Photo Smart-S20 high-resolution scanner and are of 600×400 resolution. 23.1% of the raw retinal images belong to patients with chronic glaucoma, while the remaining 76.9% are from patients with HR. The blood vessel segmentation was also carried out using a Dempster-Shafer (D-S) edge-based detector, while the MATLAB R2015a programming environment was used for the implementation. The 110 blood vessels extracted from DRIONS-DB are publicly available at http://doi.org/10.5281/zenodo.1409114 for academic and research purposes.

The iris recognition system is one of the most widely used and acceptable means of personal recognition and authentication. It has recently become an official means of national identification in India. The Unique Identification Authority of India (UIDAI) has successfully captured 1.5 billion irises from Indian citizens for identification and recognition purposes. (The Indian national identity programme tops one billion enrollees.) https://www.irisid.com/indian-national-identity-program-tops-one-billion-enrollees-2/.Therefore, the new publicly available database of human iris images (Omelina, Goga, Pavlovicova, Oravec, & Jansen, 2021) is important. In the field of iris biometric research, the iris dataset produced by the Chinese Academy of Sciences (CASIA) is the first, most popular, and widely used publicly available iris dataset. There are existing publicly available human iris datasets that are collected from non-African subjects, hence the need for an African human iris database. In the words of (Daugman, n.d.).

> There is a more urgent need for an African FACE image database because researchers into face recognition have famously (or infamously) used primarily non-African face images, leading to high levels of bias in algorithms and disastrous classification performance when they are tested on African face images.

Vice-Chancellor, sir, I am glad to let you know that I am among the team that collected the first human iris dataset of African descent, named the African Human Iris dataset (AFHIRIS). The AFHIRIS database is the first of its kind, and it was made freely and publicly available in 2022 at https:// data.mendeley.com/datasets/r3ypmmp2gs/1. It was collected from 1,028 student and staff volunteers (58% male, 42% female) at Ladoke Akintola University of Technology, Oyo State, Nigeria, and at Landmark University in Omu-Aran, Kwara State, Nigeria. About half of the subjects were under 21 years old, with the remainder aged 21–45 years old. They originated from 34 of the 36 states in Nigeria. Images were captured using a Corvus VistaEY2H handheld dual-iris camera.

Three categories of images were collected from 1,028 volunteers. The first category was made up of four iris images that were captured when the volunteers used spectacles as shown in figure 3, while the second category includes four iris images that were captured when the volunteers wore no spectacles as shown in figure 4. However, the third category of iris images was obtained from eight volunteers that used print-patterned contact lenses as shown in figure 5 . Only four images were captured from volunteers in this category as they were not asked to put on spectacles. It is strongly believed that this unique collection of iris datasets of African descent will open up new research in the study of the human iris (Akande, Ojimba, Oghenekaro, **Abikoye**, Ogundokun & Akindele, 2022) which it does eventually.

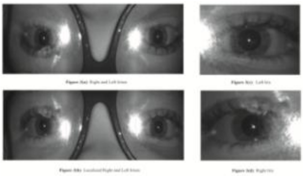

Fig. 3: Irises extracted with spectacles (Akande, Ojimba, Oghenekaro, **Abikoye**, Ogundokun & Akindele, 2022)

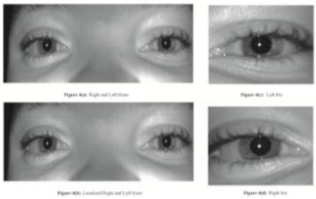

Fig. 4: Irises extracted without spectacles (Akande, Ojimba, Oghenekaro, **Abikoye**, Ogundokun & Akindele, 2022)

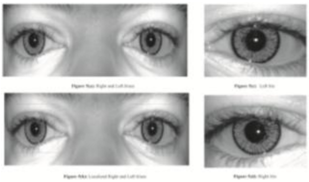

Fig. 5: Irises extracted with print- patterned contact(Akande, Ojimba, Oghenekaro, **Abikoye,** Ogundokun & Akindele, 2022)

To study the ethnicity and biometric uniqueness of individual iris patterns in a West African database, Daugman, Downing, Akande, and **Abikoye** (2024**)** conducted more than 1.3 million comparisons of iris patterns encoded from images in the newly available African Human Iris (AFHIRIS) database. The purpose was to discover whether ethnic differences in iris structure and appearance, such as the textural feature size, as contrasted with an all-Chinese image database or an American database in which only 1.53% were of African-American heritage, made a significant difference for iris discrimination. We measured a reduction in entropy for the AFHIRIS database due to the coarser iris features created by the thick anterior layer of melanocytes and found stochastic parameters that accurately model the relevant empirical distributions.

Quantile-Quantile analysis revealed that a very small change in operational decision thresholds for the African database would compensate for the reduced entropy and generate the same performance in terms of resistance to false matches. We concluded that individuality can be accurately distinguished by comparison of iris patterns in this West African population, despite demographic differences.

2. Cryptography and Steganography

To carry along the Yoruba-speaking people in the advancement taking place in the world of information technology and in linguistics and data security, **Abikoye**, Akintola, and Ibrahim (2014) developed a Yoruba language cryptosystem that involves the encryption and decryption of information written in Yoruba as text using the Caesar Cipher Algorithm and was implemented using Java programming tools. We adopted a symmetric encryption algorithm that uses one key for both encryption and decryption and uses digits as its ciphertext, which is a novel means of ensuring difficulty in breaking the codes as patterns with digits are not easily recognizable. Firstly, we established the letters in the Yoruba alphabet, which are a total of 25 (7 vowels and 18 consonants). These vowels carry diacritics to indicate the tone of the language: an acute accent (`) for the high tone commonly called "Do," a grave accent (′) for the low tone, which is also known as "Mi," and a macron accent (¯) for the middle tone, which is often left blank and is called "Re," which gives a total of 14 additional letters. Finally, we have 39 letters in all for the plain text (i.e., text to be encoded) and the digits 1-39 as the ciphertext (encoded text). The system maintained the integrity of the information, as nothing new was added to the message aside from transcription as a form of security.

As a result of the swift development in efficient video compression techniques and internet technologies. Babatunde, Jimoh, **Abikoye** and Isiaka (2017) provided an overview of existing video encryption techniques with an explanation on the concept of video compression. The review also explored the performance metrics used in the evaluation and comparison of the performance of video encryption algorithms. We concluded that all the encryption algorithms provided the most secured form of video security but it is computationally expensive and not applicable in real-time applications.

Abikoye and Nwokolo (2015) designed an Object-oriented paradigm that can be used to implement a public-key elgamal cryptosystem using the Java programming language. The main goal of this paper is to enable people who do not have full knowledge of programming languages to understand how the proposed system will work and also to enable programmers to implement the algorithm using an object-oriented approach for handling text data. Since the Elgamal cryptosystem relies on a primitive root of a large prime, it is employed in message encryption. This proposed system showed how secure messages are sent over the network and how the generation of public keys is done in an encapsulated way.

The increased use of electronic means of data transfer from one point to another, coupled with growth in networking and the internet, has really called for vital security. Considering this, Omolehin, **Abikoye,** and Jimoh (2008) developed a data encryption and decryption algorithm using a 4-row rail fence cipher. The encryption key depends on the number of rows used to break down the message into a row and column arrangement that resembles a fence rail. We designed the algorithm to illustrate the feasibility of developing a cryptosystem to ensure data reliability, confidentiality, and integrity. In addition, Omolehin, **Abikoye,** and Jimoh (2009) analysed the time complexity of the 4-row rail fence encryption algorithm, and it was shown that the time complexity of the algorithm is quadratic, i.e. $T(n) = O(n^2)$. The research was extended by modifying the Rail Fence Cipher; this was done by the inclusion of a subroutine that re-encrypts the data at a set time interval so that after the first use of a known key, the subsequent key(s) that will be used will be internally determined by the algorithm (Omolehin, **Abikoye,** & Jimoh, 2009) to increase the confidentiality of the key. This will prevent unauthorised access to the encrypted data, ensuring overall security.

To ensure message security before transmission within a messaging system over the internet, Mr. Vice-Chancellor, **Abikoye,** and Ademarati (2016) developed an information security model using the Two Fish algorithm with a single private key of 16 bits in character length for both encryption and decryption. We implemented the algorithm using the Java programming language. The result showed that the system gives a different cipher text each time encryption is performed, which makes it efficient.

Due to the increasing security concerns related to data communication over the internet and the importance of cryptography in securing data, the Advanced Encryption Standard (AES) is an effective encryption algorithm that can be used to ensure data security. In AES encryption, the data to be encrypted and the encryption key to be used are of different lengths, which are 128, 192, or 256 bits (Kumar & Rana, 2016). Due to the complexities involved in implementing AES in 192 and 256 bits, most literature has focused on the implementation of the AES algorithm using 128 bits. However, **Abikoye,** Garba and Akande (2017) implemented the AES data encryption algorithm using 128, 192, and 256 bits for textual information. Results obtained demonstrated that the AES encryption technique could be used to effectively make textual information meaningless to intruders while still being meaningful to the target receiver.

In symmetric cryptography, secret key distribution can create a performance bottleneck, while asymmetric ciphers consume significant computational resources. Leveraging on this, **Abikoye,** Dokoro and Abdullahi (2019) developed a symmetric and asymmetric based encryption model so as to achieve robust security and faster processing speed, by employing AES as symmetric algorithm and Rivest Shamir-Adleman (RSA) as asymmetric algorithm. In this model, RSA is used to encrypt AES secret key in order to secure the exchange of the key, while the rest of the sensitive data is encrypted using AES. We implemented the model using Java programming language and evaluated the performance of the proposed model in terms of encryption/decryption time and the results showed that the proposed model takes a little longer time than the RSA algorithm. This is as a result of the AES key encryption being introduced into the model. It is, therefore, recommended that the model can be implemented as an added layer of security in order to ensure confidentiality while exchanging sensitive financial and personal information in a mobile commerce environment.

The wide acceptability of AES as the most efficient of all of the symmetric cryptographic techniques has further opened it up to more attacks. This has further necessitated the need for **Abikoye**, Ahmed, Abdullahi, Akande, and Asani (2019) to present a modified AES algorithm that was achieved by modifying its SubBytes and ShiftRows transformations. The SubBytes transformation is modified to be round-key dependent, while the ShiftRows transformation is randomised. The rationale behind the modification is to make the two transformations round-key dependent, so that a single bit change in the key will produce a significant change in the cipher text. The conventional and modified AES algorithms are both implemented and evaluated in terms of avalanche effect and execution time. The modified AES algorithm achieved an avalanche effect of 57.81% as compared to 50.78% recorded with the conventional AES. However, with 16, 32, 64, and 128 plain text bytes, the modified AES recorded an execution time of 0.18, 0.31, 0.46, and 0.59 ms, respectively, which is slightly higher than the results obtained with the conventional AES. Though the modified AES recorded a slightly higher execution time with about 0.01ms, the improved encryption and decryption strength via the avalanche effects measured is a desirable feat.

Among the several existing cryptographic techniques, the Data Encryption Standard (DES) has been widely employed; however, it suffers from key and differential attacks. To overcome these attacks, we proposed a DES cryptographic technique whose number of rounds is dynamic, whereby users are expected to specify the number of encryption and decryption rounds to be employed at run time. Moreover, a predefined number of shifting operations, which is a left circular shift 2, was chosen for each encryption round. As a form of trade-off in complexity, the number of substitution boxes (S-boxes) was also reduced to 4, so that the input to the S-boxes would be arranged in four 12-bit blocks for the Exclusive OR (XOR) operation and not six 8-bit blocks as in the traditional DES. Finally, three keys were used to encrypt, decrypt, and encrypt the plaintext ciphertext, as in triple DES. The modified DES yielded a better avalanche effect for rounds greater than 16, though its encryption and decryption time were greater than those of the traditional DES (Akande, **Abikoye**, Kayode, Aro & Ogundokun, 2020).

Vice-Chancellor, sir, the knowledge-based authentication technique uses what a user knows, such as graphical or text-based passwords. Both graphic and static passwords could be forgotten by the user, willingly divulged to a trusted person, or accidentally divulged under pressure. Similarly, they could be easily guessed by a hacker, which has made them prone to dictionary attacks as well as shoulder surfing (Prabhu & Shah, 2015). These limitations led to the introduction of dynamic passwords, aptly called One Time Passwords (OTP), a system-generated password that could only be used once and within a short period of time, therefore providing a smaller window of time for an intruder to operate. Considering this, **Abikoye**, Akande, Garuba, and Ogundokun (2019) presented a (3, 3) Visual Cryptographic Scheme (VCS) technique for OTP security. The technique secures the generated OTP image by dividing it into three shares; one of these shares will be made available to the user, while the remaining shares will be stored at different locations on the server. Before the original OTP image can be recovered, all the shares must be retrieved and stacked together. To avoid the pixel expansion problem and loss of image quality that have characterised the existing VCS technique, progressive visual cryptography was adopted to decrypt the retrieved OTP shares. A high-quality OTP image was recovered, as revealed by the peak signal-to-noise ratio values, and there was no change in the size of the OTP images.

Mr. Vice-Chancellor, the security and privacy of patients' information remain a major issue of concern among health practitioners. In putting up measures to ensure that unauthorised individuals do not have access to this information, Akande, **Abikoye**, Adebiyi, Kayode, Adegun, and Ogundokun (2019) developed a modified blowfish algorithm for securing textual and graphical medical information. The F-function used in generating round sub-keys was strengthened to produce a strong key that could resist differential attacks. Number of Pixel

Change Rate (NPCR) and Unified Average Changing Intensity (UACI) of 98.85% and 33.65% revealed that the modified algorithm is sensitive to changes in its key and also resistive to differential attacks. Furthermore, the modified algorithm demonstrated better encryption and decryption times than the existing blowfish algorithm. Also, Gbolagade, Jimoh, and **Abikoye** (2022) developed an enhanced Blowfish algorithm with reduced computational speed for encrypting and decrypting information. In enhancing the Blowfish algorithm, a 128-bit block size and 128-bit key were used to derive a new F-function; the original structure was also altered by employing the # function to boost the security strength by replacing XOR. The performance of the algorithm was evaluated based on time and avalanche, and due to differences in block sizes, the modified Blowfish was slower with an average of 26.99 ms, 1651.83 ms, and 2765.04 ms based on key generation, encryption, and decryption times, respectively, compared to Blowfish with 21.65 ms, 1297.76 ms, and 2176.59 ms. The 128-bit block size applied enhances security strength by reducing the chances of having duplicate blocks that may reveal the information being transmitted**.** The study was further compared with the Two Fish algorithm, and the enhanced Blowfish was faster with encryption and decryption average times of 2418.08 ms and 4002.70 ms.

Oladipupo and **Abikoye** (2022a) developed a Modified Playfair (MPF) cryptosystem that is capable of handling different block sizes with high diffusion and confusion properties. We introduced permutation during encryption and decryption processes at both character and bit levels as a measure to introduce confusion and diffusion in MPF. Cryptanalysis attacks in the likes of primitive security attacks such as known plaintext attacks (KPA), chosen-plaintext attacks (CPA), chosen-ciphertext attacks (CCA), Spectra frequency analysis, differential cryptanalysis, information entropy analysis, autocorrelation analysis, and brute-force attacks were carried out on the MPF to verify its vulnerability to cryptanalysis attacks. The results showed that the developed MPF cryptosystem is resistant to various cryptographic attacks as 100% and 96.875% of the ciphertext characters changed as a result of a change of one character of the plaintext.

The world is increasingly moving towards the use of resource-constrained applications where computational speed, storage, and bandwidth are limited. With Elliptic Curve Cryptography (ECC), security features such as public key encryption, digital signatures, non-interactive key exchange, and a host of others can be offered with high speed, small space consumption, and bandwidth savings. However, most of the existing ECC implementations suffer from implementation flaws that make them vulnerable to cryptanalysis attacks. As a measure to reduce flaws in ECC implementations, Oladipupo and **Abikoye** (2022b) identified the flaws in the existing ECC implementation that made it vulnerable to Man-in-the-Middle attacks (MIMA), CPA, and CCA. A new ECC scheme tagged Improved Authenticated Elliptic Cryptography (IAECC), where a non-interactive sharing of the initialisation vector (IV) was introduced to solve the MIMA problem, was developed. The problems of vulnerability to CPA and CCA were also addressed in the IAECC scheme by introducing Cipher Block Chaining (CBC) mode into its implementation. We carried out a security analysis of the IAECC to present proof of its resistance against specific encryption attacks. In addition, the study conducted a performance evaluation to compare the impact of the security enhancements in IAECC on encryption and decryption times, throughput, and power consumption with the existing ECC scheme. The experimental results of the security analysis showed that IAECC is resistant to the security flaws that the existing systems are vulnerable to. A further modification was made to the existing ECC by optimizing it for parallel execution of the encryption and decryption processes and security against primitive attacks in the design of the Wireless Sensor Network (WSN) model that employs clustering of multicore Wireless Sensors (WS). An ECC-based encryption/decryption scheme for parallelizing encryption/decryption operations within a node was developed. The Elliptic Curve Diffie-Helman (ECDH) was used for the key exchange algorithm and the Elliptic Curve Digital Signature Algorithm (ECDSA) for authentication among the communicating nodes. Security analysis of the model and comparative performance analysis with the existing ones were demonstrated, and the results revealed that the proposed model meets the security requirements and resists various security attacks. The results of the comparative performance analysis showed that the developed WSN model can efficiently leverage multiprocessors and/or many cores for quicker execution and conserve power usage (Oladipupo, **Abikoye** *et al*., 2023).

The Internet of Things (IoT) is a recent paradigm in the wireless communication field that comprises smart appliances with a digital entity that can universally connect to a network and the Internet. The amalgamation of IoT technology into medical systems gave birth to the Internet of Medical Things (IoMT). The IoMT has made activities such as real-time drug prescription, patient monitoring, real-time diagnosis of patients, and a host of other services in the healthcare system, which otherwise require the physical presence of healthcare workers and patients, possible remotely. However, the wide acceptability of IoMT has met with strict resistance, as people are still reluctant to provide critical user data or authorization to a server where such data could be accessed because the confidentiality of the data is at stake.

As a way to put up a secure, privacy-preserving, and less computationally intensive scheme for securing and preserving the privacy of sensitive medical information on the cloud, **Abikoye** *et al*. (2023) developed a secure IoMT model with an efficient cloud data privacy-preserving technique for securing critical user information over the Internet of Medical Things Platforms using a hybrid cryptography scheme. We modified the existing stream Caesar cipher into a symmetric block cipher for improved security, and a B+ File Organization technique, an efficient technique that searches through encrypted files stored on the cloud without decrypting the file was used. The Elliptic Curve Diffie–Hellman technique was employed to exchange shared secret keys to form the Hybrid Modified Caesar Cryptosystem (HMCC). The developed IoMT model, leveraging the hybrid cryptography algorithm, was analyzed and compared against different security attacks. The analysis results revealed that the model is secure, preserves the privacy of critical user information, and shows robust resistance against different cryptanalysis attacks. Existing lightweight cryptosystems have proven to be very efficient in terms of memory size and energy consumption required for their implementation, they are more suitable for text and binary data than for multimedia data. As IoT applications are pivoting towards multimedia-oriented data, such as videoconferencing, surveillance sensors in the environment or military fields, and medical sensors and applications, a lightweight cryptosystem capable of securing multimedia data will be more appropriate. The thought along the line above inspired Oladipupo, **Abikoye,** and Awotunde (2024) to develop a new lightweight image cryptosystem tagged Hash XOR Permutation (HXP) for Cloud-Assisted Internet of Things that does not make use of Substitution Box (S-Box) to achieve diffusion, confusion, and non-linearity. An algorithm termed *Enc* that accepts a block of size n divides the block into Ln R bits of equal length and outputs the encrypted block as follows: $E = (L \otimes R) \oplus R$,where $\otimes$and$\oplus$ are exclusive-or and concatenation operators, respectively, was created. A hash result, $hasR = SHA256(P \oplus K)$, was obtained, where SHA256, P, and K are the Secure Hash algorithm (SHA−256), the encryption key, and plain image, respectively. A seed, S, generated from$enchash = Enc(hashenc, K)$, where $hashenc$ is the first $n$bits of $hasR$, was used to generate a random image, Rim. An intermediate image, $intimage = Rim \otimes P$, and a cipher image, $C = Enc(intimage, K)$were obtained. We carried out security analysis, and the result shows that HXP is more secure than the existing schemes in terms of its encryption quality (EQ), entropy, normalized cross-correlation (NCC), resistance to known plaintext, known ciphertext, chosen plaintext, chosen ciphertext, and differential cryptanalysis attacks. It was concluded that the security of a cryptosystem can still be maintained without the use of S-Box in its design.

The increase in the number of attacks recorded during the electronic exchange of information between the source and intended destination has called for a more robust method for securing data transfer. Taking this into account**, Abikoye**, Adewole, and Oladipupo (2012) introduced a system for concealing data, leveraging audio steganography and cryptography, with the objective of securing data transfer between the source and destination. Audio medium was used for the steganography, and the least significant bit (LSB) algorithm was employed to encode the message inside the audio file. The result showed that the encryption and decryption methods used for developing the system make its security more efficient in securing data from unauthorised access.

To solve the problem of attacking or hacking a biometric template for a malicious act, which has become a huge problem in the iris recognition system, **Abikoye**, Ojo, Awotunde, and Ogundokun (2020) combined two cryptography algorithms and steganography to secure the iris template and make it safe. In this work, the Hough transform, Daugman rubber-sheet model, and Log Gabor filter were used for iris image segmentation, normalisation, and feature extraction, respectively, and the iris template generated was encrypted using the Triple Data Encryption Standard (3DES) and Twofish cryptography algorithms to obtain a cipher image. The cipher image was then embedded into a cover image to produce a stego image using the LSB steganography algorithm. The result of this work slightly changed the master file after embedding the secret image (stego file), making it unrecognizable to the human eye. Only a JPEG image was used as the master or cover file. The dual-level security technique provided high embedded capacity and produced high-quality stego images that would be able to withstand attacks.

Vice-Chancellor, sir, the development of the medical field has led to the transformation of communication from paper information into digital form. Medical information security has become a great concern as the medical field is moving towards the digital world, and hence patient information, disease diagnosis, and so on are all being stored in the digital image. Therefore, to improve medical information security, the safe conveyance of medical data across unsecured networks nowadays is an essential issue in telemedicine. A comprehensive review of the research trends on LSB steganography that can be used in securing medical information such as text, image, audio, video, and graphics was done, and its efficiency and effectiveness were also evaluated.

The survey findings showed that the LSB steganography approach can effectively safeguard medical information from unauthorised access and intruders. Therefore, a modified and improved LSB technique called circular shift LSB was used to protect and hide both medical images of different formats, such as png, bmp, and jpeg, and data being transmitted over the internet from being accessed by the intruder. The modified LSB algorithm was implemented on a MATLAB 2018a programming environment, and three metrics, which are Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index Measure (SSIM), were used to evaluate the performance of the system. The results showed the PSNR value is higher and the MSE value is lower when compared with existing systems. This approach effectively enhances the security, reliability, and imperceptibility of transmitting both medical images and textual information, ensuring that communication remains undetectable to potential intruders or attackers (Ogundokun, **Abikoye,** Misra & Awotunde, 2020; **Abikoye** & Ogundokun, 2021; Ogundokun & **Abikoye**, 2021; **Abikoye,** Ogundokun, Misra, & Agrawal, 2022).

3. Phishing, Spam Detection and Intrusion Detection System (IDS)

Mr. Vice-Chancellor, with the multitude of security challenges facing the online community, malicious websites play a critical role in today's cybersecurity threats. Indeed malicious Uniform Resource Locators (URLs) can be delivered to users via emails, text messages, pop-ups, or advertisements. To recognise these malicious websites, blacklisting services have been created by the web security community, which have proven to be inefficient. In addressing this problem, Adewole, Raheem, **Abikoye,** Ajiboye, Oladele, Jimoh, and Aremu (2021) proposed a meta-heuristic optimization method for malicious URL detection based on Genetic Algorithms (GA) and Wolf Optimization Algorithm (WOA). Support Vector Machines (SVM) as well as Random Forest (RF) was used for the classification of phishing web pages. Experimental results showed that WOA reduced model complexity with comparable classification results without feature subset selection. The RF classifier outperforms SVM based on the evaluation conducted. The RF model without feature selection produced accuracy and Receiver Operating Characteristic (ROC) of 0.972 and 0.993, respectively, while the RF model based on the WOA optimization algorithm produced an accuracy of 0.944 and ROC of 0.987. Hence, given the experiments conducted using two well-known phishing datasets, this research showed that WOA can yield promising results for detecting phishing URLs.

The use of Machine Learning (ML) approaches for phishing attack classification is an active research area in the field of cyber security. These ML techniques can be categorised as single or ensemble learners. Ensemble learners have been identified as more promising than single classifiers. However, some of the ways to achieve improved ML-based detection models are through feature selection and dimensionality reduction as well as hyperparameter tuning. In this regard, Jimoh, Oyelakin, **Abikoye**, Akanbi, Gbolagade, Akanni, Jibrin, and Ogundele (2023) used Ensemble Learning Algorithms, which are RF and Extra Trees ensembles, for the classification of phishing websites. The models built from the algorithms are optimized by applying feature-importance attribute selection and hyperparameter tuning approaches. The RF-based phishing classification model achieved 99.3% accuracy, 0.996 recall, 0.983 f1-score, 0.996 precision, and 1.000 as an AUC score. Similarly, the Extra Trees-based model attained 99.1% accuracy, 0.990 as recall, an F1-score of 0.981, a precision of 0.990, and an AUC score of 1.000. Thus, the RF-based phishing classification model slightly achieved better classification results when compared with Extra Trees own. The study concluded that the attribute selection and hyperparameter tuning approaches employed are very promising.

Twitter microblogging social network has become a data stream communication environment where millions of tweets are distributed daily. To date, existing approaches for spam detection on Twitter focused primarily on batch-learning approaches and categorized tweets as spam or non-spam. Due to the streaming nature of tweets, Adewole, Jimoh, Akintola, and **Abikoye** (2018) deviated from the existing batch-learning approach and proposed an ensemble-based streaming framework for both spam detection and risk assessment on the Twitter network. The proposed framework incorporated both classification and clustering methods. The classification stage employed a combination of Multinomial Naive Bayes (Multinomial NB) and modified K-Nearest Neighbour (KNN) algorithms for spam detection and risk assessment. The risk assessment function is formulated to compute the risk score from the outputs of two stream-based classifiers. The streaming K-means algorithm was used at the clustering stage to detect spam campaigns. Experimental results demonstrated the accuracy and scalability of the proposed ensemble framework.

Due to the obvious importance of accuracy in the performance of intrusion detection systems, in addition to the algorithms used, there is an increasing need for more activities to be carried out, aiming for improved accuracy and reduced real-time detection. Therefore, **Abikoye**, Balogun, Olarewaju, and Bajeh (2016) investigated the use of filtered datasets on the performance of the J48 Decision Tree classifier to classify a connection as either normal or an attack. Gain Ratio attribute evaluation technique (entropy) was employed for performing feature selection (removal of redundant attributes), and the filtered dataset was fed into a J48 Decision Tree algorithm for classification. We used a 10-fold cross-validation technique for the performance evaluation of the J48 Decision Tree classifier on the KDD Cup 1999 dataset and simulated it in WEKA tool. The results showed that J48 decision tree algorithm performed better in terms of accuracy and false positive report on the reduced dataset than the full dataset (probing full dataset: 97.8%, probing reduced dataset: 99.5%, U2R full dataset: 75%, reduced dataset: 76.9%, R2L full dataset: 98.0%, reduced dataset: 98.3%).

In the quest for an efficient Intrusion Detection System (IDS), **Abikoye**, Aro, Obisesan, and Babatunde (2017) developed a hybridized Intrusion Detection System using Genetic and Tabu Search algorithms. The result of the evaluation revealed that the hybridized IDS performs better than Genetic algorithm with a classification accuracy of 83.56%, which can significantly detect almost all anomaly data in the computer network.

Short Message Service (SMS) has been identified as a fast communication approach due to its low cost and stress-free nature. The general acceptability of SMS has exposed it to many threats, and one of these is spamming. In SMS spam detection, feature extraction plays a vital role. The extraction of features in SMS involves a process of reducing an initial set of raw features into more manageable forms for processing. **Abikoye,** Taofeek-Ibrahim, and Aro (2020) developed an optimized one-dimensional ternary pattern (1D TP) for SMS feature extraction. 1D-TP is a statistical feature extraction method that is based on the comparisons of characters with their neighbours according to their UTF-8 values. It was used to extract the SMS features, and the extracted features were optimized by introducing a nature-inspired optimization algorithm known as Simulated Annealing to select the most relevant and discriminant features. Subsequently, Taofeek-Ibrahim, **Abikoye,** and Toye (2020) extended the research by classifying the optimised features using seven ML algorithms; Bayesian Network (BN), Naïve Bayes (NB), Radial Basic Artificial Neural Network (RBFN), RF, KNN, Logistic Regression (LR), and SVM. The developed system was evaluated using the Kaggle SMS Spam Dataset, and experimental results showed that the highest accuracy of 86.56% was obtained in LR for non-optimized upper features and the highest accuracy of 92.56% was recorded in RF for optimized upper features. The highest precision of 0.95 was achieved in BN for non-optimized upper features of 1D-TP, and the highest precision of 0.94 was obtained in optimized upper features of 1D-TP. The highest recall of 1.00 was obtained in NB, SVM, and LR for non-optimized lower and upper features, and the highest recall of 1.00 was recorded in NB and RF for lower and upper features of 1D-TP. SVM emerged as the best-performing algorithm for both non-optimized and optimized systems, achieving an accuracy of 94.61722% and 98.44498%, respectively. In addition, the optimised system demonstrated superior performance across various metrics, indicating the effectiveness of the simulated annealing optimisation algorithm. The study offered valuable insights for data scientists to enhance SMS spam detection accuracy, presenting a potential solution to mitigate the growing issue of unwanted SMS messages.

Furthermore, to prevent the act of smishing rather than detecting and separating spam SMS from ham messages Akande, Gbenle, **Abikoye**, Jimoh, Akande, Balogun, and Fatokun (2022) developed a mobile application called SMSPROTEST that used a rule-based SMS service to detect and prevent smishing attacks. RIPPER and C4.5 were used as the rule-based learning model, and a mobile service was developed to intercept and forward incoming SMS to the rule-based model. The developed model selects rules to analyze the retrieved message and assert if it was spam or ham. The result of the analysis is sent as a notification to the users through the developed mobile application. However, the final decision to retain or discard the message depends on the user after receiving the notification.

4. **Web and Network Security**

The development of the A3 and A8 algorithms is considered a matter for individual GSM network operators. **Abikoye** and Bajeh (2008) presented a computer model for the A3 algorithm, and the model was implemented using Visual Basic 6.0 programming language. The concept of a 2 by 2 matrix was used to develop the A3 algorithm model, the 2 by 2 matrix was formed with the two inputs, Random Challenge and the subscriber's authentication key (RAND and KI), both of 128 bits, to get the output signal response (SRES) of 32 bits. We simulated the model using two platforms: the network platform and the SIM platform. To perform the authentication process, the network platform generates a 128-bit RAND and sends it to the SIM platform. On receiving the RAND, the SIM platform used the ki that is already stored on its platform together with the RAND received from the network platform to calculate the 32 SRESSIM using the model developed. The SRESSIM is sent back to the network platform for comparison with the SRESHLR, which is also calculated on the network platform using the 128-bit ki, which is stored in the HLR, and the 128-bit RAND. If SRESHLR = SRESSIM, then the SIM is authenticated and allowed access to the network; otherwise, an authentication signal is sent to the SIM and access to the network is denied. The A3 and A8 algorithms are similar in functionality and are commonly implemented as a single algorithm called COMP128.

Furthermore, Vice-Chancellor, sir, **Abikoye** and Oluwade (2008) performed a computational time complexity analysis of COMP 128. It was shown that the running time of the user authentication algorithm COMP128 is constant, $T (n) = \Theta (k)$, meaning that the number of executions of basic operations in the COMP128 algorithm is fixed and so the total time is bounded by a constant. In conclusion, GSM has experienced a lot of security breaches, and despite all the breaches, GSM is by far more secure than previous analog cellular systems and continues to be the most secure public wireless standard in the world.

Due to the increasing threat of Structured Query Language (SQL) injection and Cross-Site Scripting (XSS) attacks on data-driven web applications, measures must be put in place to curtail the growing threats of these attacks. With this understanding, **Abikoye**, Abdullahi, Ahmed, Akande, and Kayode (2020) presented a novel technique to prevent these attacks using the Knuth-Morris-Pratt (KMP) string match algorithm. In this study, the various types and patterns of the attacks were first studied, and then a parse tree was designed to represent the patterns. Based on the identified patterns, a filter() function was formulated using the KMP string matching algorithm to match the user's input string with the stored pattern of the injection string in order to detect any malicious code. The formulated filter() function detects and prevents any form of SQL injection or XSS attack. Every input string is expected to pass through this filter() function. If at least one function returns True, then the filter() function will block that user, reset the HTTP request, and display a corresponding warning message. The implementation was carried out using the PHP scripting language and Apache XAMPP Server. To measure the security level of the technique, it was tested using a test plan that consisted of different forms of boolean-based, union-based, error-based, batch query, like-based, encoded SQL injections, and cross-site scripting attacks. Results obtained revealed that the technique can successfully detect and prevent attacks, log the attack entry in the database, block the system using its Mac address to prevent further attacks and issue a blocked message. A comparison of the proposed technique with existing techniques revealed that the proposed technique is more efficient because it is not limited to a particular form of attack and can handle different forms of SQL injection and XSS attacks.

5. Android Malware Detection

Mr. Vice-Chancellor, truly, humans are the weakest link of security (Mitnick, Simon, & L., 2011) and (GBC-DELL Survey, 2015). Human cyber security behaviours have created serious vulnerabilities that attackers exploit using social engineering attack techniques, and findings revealed that human factors are responsible for 95% of all security incidences. Therefore, Aruwa and **Abikoye** (2017) critically analysed the human factors or behaviours as major threats to cybersecurity, using the anonymous attack on Hbgary as a case study. We placed focus on the usual roles played by both attackers and defenders (the targets of the attacker) in cyber threats' pervasiveness and the potential impacts of such actions on critical security infrastructures. To facilitate an effective and practical analysis, the Anonymous attack against HBGary Federal (A security firm in the United States) was used as a case study to reveal the huge damaging impacts of human errors and attitudes against the security of organisations and individuals. The findings revealed that the powerful security firm was compromised and overtaken through simple SQL injection techniques and a very crafty social engineering attack, which succeeded because of sheer personnel negligence and unwitting utterances.

Android smart phones and tablets are massively proliferating in every sector of national economies. The developed economies are well advanced in making preparations against any eventualities and security challenges that might arise with the adoption of these technologies. Developing economies, on the other hand, are not well prepared to face the different devastating challenges. To address this pertinent issue, **Abikoye** and Aruwa (2018) seek to critically evaluate the security threats associated with Android malware, especially the awareness rate of Android users to the existence of Android malware and the associated cyber threats to growing economies. We carried out a survey, and secondary literature was analysed. It was revealed that there is a very low rate of Android malware and cyber threat awareness among users in developing economies. The evasive and sophisticated nature of malware, such as split-personality malware, low or zero awareness rates of malware threats, and acceptable cybersecurity behaviours and practices can have a huge negative impact on the growth of any economy.

Vice-Chancellor, sir, this informs **Abikoye**, Gyunka, and Akande (2020a) to carry out a comprehensive review of ML techniques and their applications in Android malware detection as found in contemporary literature. Furthermore, **Abikoye**, Gyunka, and Akande (2020b) identified that traditional signature-based malware detection techniques have been proven to be less effective in detecting new and unknown malware. Therefore, ML techniques are taking the lead for timely zero-day anomaly detections. To evaluate the performance of four different machine learning algorithms in detecting malware in

Android devices, Salihu, Quadri and **Abikoye** (2020) conducted a study where some machine learning algorithms namely SVM, K-means, NB, and Decision Tree (DT) were used in the detection of malware in Android devices. The study experimented with 558 APK applications with 279 malware samples from MalGenome and 279 benign samples from the Google Play store. SVM, K-means, and DT achieved an accuracy of 94% while NB had 90% accuracy. This study demonstrated that ML techniques can detect Android malware successfully. Because of this, we introduced an optimsied Android malware detection model using ensemble learning techniques. Random Forest, Support Vector Machine, and KNN were used to develop three distinct base models, and their predictive results were further combined using the majority vote combination function to produce an ensemble model. A reverse engineering procedure was used to extract static features from a large repository of malware samples and benign applications. WEKA 3.8.2 data mining suite was used to perform all the learning experiments. The results revealed that Random Forest had a better sensitivity of 97.9% and a classification accuracy of 98.00% among the other base classifiers, indicating that it is a strong base model. However, the ensemble model achieved a sensitivity of 98.1% and a classification accuracy of 98.16%. The finding showed that, although the base learners had good detection results, the ensemble learners produced a better result. To further confirm the best performing ML classification algorithm for anomaly Android malware detection, Gyunka, **Abikoye**, and Adekeye (2021) conducted a performance comparative analysis between six different classification algorithms, namely: Naïve Bayes, Simple Logistics, Random Forest, Partial Decision Tree (PART), k-Nearest Neighbours (k-NN), and SVM, leveraging permission-based feature sets. The findings of the study showed that Random Forest had the best detection result with a false alarm rate of 2.2%, an accuracy of 97.4%, an error rate of 2.6%, and a ROC area of 99.6%. The study concluded that, using Android permission features, Random Forest and k-Nearest Neighbours recorded the best performances in Android malware detection, followed by Support Vector Machine and Simple Logistics classification algorithms. PART performed relatively well, while Naïve Bayes recorded the least performance. Consequently, the deployment of the Random Forest model and KNN model is recommended for the development of an anomaly Android malware detection paradigm.

Internet users have been faced with a lot of threats with the growth of malware around the world. Ransomware, one of the most significant types of malware, encrypts sensitive information and will not release the files until the user pays a ransom. The Internet of Things (IoT) structure is an extensive area of Internet-associated instruments with additional computational capabilities and storage capacities that have the potential to be harmed by ransomware developers. To solve this problem, Ogundokun, Awotunde, Misra, **Abikoye**, and Folarin (2021) presented a ML model capable of detecting ransomware attacks on IoT devices. We used Power—to track and review the power consumption in 500 ms internals of all operating processes and also three devices to perform the experiments, namely: an Android device, Laptop computer, and a projector. The proposed model adopts a recurrent Long Short-Term Memory (LSTM) classifier for the neural network, equipped with an improved version of the back propagation algorithm. The ML model was used to monitor the power consumption of IoT devices using various procedures to categorize ransomware outside of non-malicious operations. The results of the experiments showed that the LSTM model achieved a 96.42% detection rate and a 91.07% accuracy rate. Findings revealed that the proposed model is efficient in improving ransomware detection in IoT systems.

Due to the rise of Artificial Intelligence (AI) and ML, which have prompted concerns regarding the Intellectual Property (IP) protection of Neural Networks (NNs), Ogundokun, **Abikoye**, Sahu, Akinrotimi, Babatunde, Sadiku, and Olabode (2024) Ogundokun et al. (2024) conducted a systematic literature review using PRISMA to evaluate the efficacy of watermarking techniques such as digital watermarking (DW), reversible watermarking (REW), and robust watermarking (ROW) for enhancing the security and ownership protection (SOP) of NNs. Twenty research articles were analysed using various performance indicators, such as detection rate (DR), robustness, and distortion, to evaluate the applicability of the different watermarking techniques. The results demonstrate that watermarking approaches successfully improve security without substantially impacting the performance of NNs. Researchers, professionals, and policymakers should consider watermarking to safeguard the intellectual property of NNs in several domains, including finance, healthcare, and national security.

Human-Computer Interaction (Human Factor) is described as an approach in which individuals communicate with facts, news, computers, and tasks mainly in the areas of the profession, administrative, legislative, and cultural contexts. With a particular emphasis on speech recognition (SR) as an audio-based HCI method, Ogundokun, **Abikoye**, Adegun, and Awotunde (2020) presented a summary and survey on the concept of human-computer interaction (HCI). The historical context of human-computer interaction (HCI) and contemporary research trends and HCI procedures, theories, principles, models, and architecture were investigated in the study. We also discussed the overview of speech recognition (SR), and a table showing the comparative study of the speech recognition system approaches was presented which provided insights on SR and HCI.

Special Research Grant Award

Consequently, Mr. Vice-Chancellor, as a collaborator in AI, I have attracted the Artificial Intelligence for Females in Science, Technology, Engineering and Mathematics (STEM) (AI4FS) Project grant. Permit me sir to elaborate on this grant because it provides gender inclusiveness in Nigeria to solve the problem of high gender inequality in STEM.

AI4FS Project

The Artificial Intelligence for Females in STEM (AI4FS) grant was awarded by the Royal Academy of Engineers (RAENG) (Higher Education Partnerships in sub-Saharan Africa (HEP SSA) 22/24) HEPSSA-2224-4-100184, United Kingdom to a Consortium of Nine Institutions namely Summit University, Offa; University of Ilorin, Ilorin; Federal University of Technology Minna ; Kwara State University Malete; Olabisi Onabanjo University, Ago-Iwoye; Ladoke Akintola University, Ogbomosho; Obafemi Awolowo University, Ile-Ife; Federal Polytechnic, Offa and Manchester Metropolitan University, UK and 4 Industrial partners (AI4CE Nig. Ltd., SUSEJ Nig. Ltd., BASIC Electronic, Nig. Ltd. and Eclipse Power Nig., Ltd.) partners.

Vice-Chancellor, sir, it is my great pleasure to tell you that I am the lead partner for University of Ilorin. The project aims at developing innovation and inventions that would change the way we gain knowledge, acquire skills, work in the industry, develop our curriculum, and provide gender inclusiveness in Nigeria to solve the problem of high gender inequality in STEM which has prevented females from accessing government initiatives, leading to high poverty rate, low entrepreneurial drive, low educational enrolment, and poor access to social infrastructures.

The project had its commencement meeting on the 20th - 23rd November, 2022 at the Summit University, Offa, and has achieved 100% of its objectives. We are currently working on its sustainability.

Mr. Vice-Chancellor, the 2nd Annual workshop of the project was organized by the Unilorin team, led by yours truly, in the Faculty of Communication and Information Sciences Lecture Theatre on the 29th - 31st of October, 2023. The workshop was tagged **"Empowering Tomorrow: Transforming Lives with Gender-Inclusive AI and STEM"**. The workshop is one of the objectives of the AI4FS project to create awareness and create a network for efficient collaboration of females in STEM.

Fig. 6: Participants at the AI4FS 2nd Annual Workshop held at UNILORIN on the 29th-31st of October, 2023- from the 5th to the right mySelf, Unilorin Lead partner, Prof Bamidele (Lead partner, Mancheter Metropolitan University), Prof. Abiodun Musa Aibinu (Principal Investigator), Dr Shekinat Folorunsho (Lead partner, Olabisi Onabanjo University, Ago-Iwoye)

The Hub-Spoke University (HSU) was saddled with organization of the training and capacity development workshops whereby Unilorin team has been playing a vital role. The Unilorin team organized a free 2-day Hands-on training/workshop on AI and Robotics on the 29th -30th January, 2024 convened by me. The training has a total of 60 participants from all the corners of the university. Students, senior lecturers and non-academic staff were in attendance. Participants from sisters universities; the HUB University (Summit University, Offa), Al-Hikmah, University, Ilorin, Kwara state University, Malete, and Obafemi Awolowo University, Ile-Ife, Osun state also grace the occasion. We also had in our midst, the Kwara State Commissioner for Business and Innovation Technology, Honourable Damilola Yusuf Adelodun, she encouraged and inspired women who are pursuing their career in AI and Robotics.

Fig. 7: Participants at the AI and Robotics Workshops with the facilitators

Mr. Vice- Chancellor, two of our students, one female and one male benefitted from the project immersion programme. They had their 6 month SIWES from April 2024 – September 2024 under this project with monthly allowance of Sixteen Thousand Naira (₦16,000:00) and Fifteen Thousand Naira (₦15,000:00) for the female and male beneficiaries respectively. Key indicators for the initiative's success include the number of student and lecturer beneficiaries, the number of industry partners scouted, and the number of post-immersion training activities conducted.

The project has sponsored a female Ph.D. student to the United Kingdom in January, 2024 for her research benchwork and also enhances her capacity on research. Vice- Chancellor, sir, I am happy and excited to let you know that the beneficiary is a postgraduate student of the University of Ilorin and one of my current Ph.D. supervisees. It is worthy of note also that the student had both her 1st and 2nd degrees here at the University of Ilorin, Ilorin, Nigeria. She graduated with First Class Honours in Computer Science in the year 2014.

In conclusion, the AI4FS project stands as a beacon of progress in bridging the gender gap within STEM fields, particularly in Nigeria. As it is in its sustainability phase, the AI4FS project sets a promising precedent for future endeavors aimed at empowering women in technology and fostering a more inclusive and prosperous society.

My Contribution to the University
Departmental Level:

(i) I have successfully supervised eighteen (18) masters and nine (9) Ph.D. theses, mostly in the area of information security, and I am currently supervising two (2) masters and two (3) Ph.D. theses.

(ii) Ist Female Ag, Head of Department, May, 2020 – July 31st 2022.

(iii) Departmental Postgraduate (Ph.D.) Coordinator, 2015-2017.

(iv) Departmental Examination Officer. 2009/2010 - 2014/2015 sessions.

(v) Chairpersons and members of various departmental committees (Accreditation, Postgraduate, Finance, procurement etc.).

Mr. Vice-Chancellor, I must say at this junction that the Lord has always used me as a pacesetters and driving force for all other females in the department.

Faculty Level:

(i) Secretary, Faculty Examination Malpractices Panel, 2010/2011, 2015-2017, 2019-2021 sessions.

(ii) Chairperson, Local organizing Committee, 3rd Faculty International Conference on ICT for National Development and Sustainability (ICT4DS2024).

University Level

(i) Deputy Director (Research), Centre for Research, Development and In-House Training (CREDIT), Sept. 2020 – Nov. 2022.

(ii) Faculty Representative, University Convocation & Ceremonial Committee, 2010 - 2012 session, 2014-2017 session, 2019 – 2020 session.

(iii) Faculty Representative, Business Committee of Senate (BCOS), 2016- 2017, 2019 – 2021.

(iv) Member, University of Ilorin 50th Year Anniversary, 2024.

(v) Alternate Chairman, Technical Committee on developing and implementing innovative entrepreneurship Certification, August, 2024.

Community Service

(i) Pastor at the Potters Porch Int'l Churches

(ii) Member, Success for Ladies (SFL) Ministry. This is a ministry that is committed to liberating ladies for all round success, convened by Pastor Oluseyi Aboyeji.

Professional Service

Current coordinator, Nigerian Women in Information Technology (NIWIIT), Kwara State Chapter.

Conclusion

In conclusion, "Invisible Bouncers in the World of Information Security" reveals several critical details that highlight the significance of data security. Information security is much like a bouncer at the door, and in the background, it guards against both the visible and invisible threats. Through unraveling this mystery, we realise that proactive measures, constant vigilance, and an in-depth knowledge of evolving risks are necessary for effective information security. By these ongoing and continuous research explorations, the confidentiality, integrity, and availability of our digital assets in this highly interconnected world can be guaranteed. By leveraging AI powered technologies, real-time protection, autonomous response and enhanced security will be enabled.

Recommendations

Due to the sensitivity of Information Security, I want to make the following recommendations:

1. Passwords must be changed once every 3 months.
2. Consistent training, retraining, and organisation of cybersecurity awareness programme for the workforce to prevent social engineering targeting the government, organisations, and individuals.
3. Establishment of incident response plans, conducting routine security assessments and audits, and promoting a culture of security awareness within organisations.
4. Application of cutting-edge technologies such as ML, AI and behavioural analytics to detect and reduce security risks.
5. Organisational planning, cyber hygiene, and healthy cybersecurity work behaviour should all be maintained by organisations.
6. Increase focus on privacy regulations, compliance frameworks, and data governance to ensure responsible handling of sensitive information.
7. Researchers, professionals, and policymakers should consider watermarking to safeguard the intellectual property of NNs in various domains, including finance, healthcare, and national security.
8. The government should adopt biometric traits such as the human iris for national identification and recognition systems.
9. Introduction of liveliness detection as part of measures to enhance the security of information and improve the biometrics system in all agencies, parastatals, and organisations.
10. The use of both biometrics and cryptography systems to prevent biometric vulnerabilities
11. Information Security expert should raise public awareness regarding the risks of submitting personal data to websites and the General Data Protection Regulation (GDPR), outlining its usage and consequences for violators.
12. The government should introduce a voice recognition system to the “Am Alive” verification programme for pensioners.

Acknowledgments

I praise my God and Father, from whom all blessings flow; the giver of life, strength, and wisdom; without Him, I am nothing. My Invisible bouncer(bouncing away all forms of evil seen and unseen), the Omnipotent, Omniscience, Lilly of the Valley, I am that I am, The one who was, who is, and is to come, Kings of all kings, Lords of all lords, Greater than the greatest, stronger than the strongest, Richer than the richest, Wiser than the wisest, Faithful father, Jehovah-Shammah, Jehovah-Jireh, Jehovah-Nissi, Jehovah-Shalom, El Roi, reliable Father. If the hairs on my head are tongues, they are not enough to praise you for how far you have brought me. I will bless the Lord at all times, His praises shall continually be in my mouth (Psalm 34:1).

To my father and knight in shining armour and the 1st man I ever admired, Elder (Dr.) Ayodele Oladele Adeoye (of blessed memory), who instilled in me hard work, trust in God, punctuality, diligence, and the qualities of a frontliner. Daddy, you loved me and my siblings, sent us to the best schools around at the time, and generally gave us the best of all you have. It is painful that you are not here today to witness this landmark in my academic pursuits. I know that you are in paradise with the Lord and that you are overjoyed and proud to see me achieve this milestone, which was your dream for me, a status you would have attained when you started your career in academics at the ABU in 1972 before moving down to the civil service in Kwara State in 1973. According to the words of Thomas Campell, *"To live, in hearts we leave behind, is not to die"*. To my amiable, energetic, industrious, supportive, and ever-caring mother and my first teacher, Mrs. Felicia Omowumi Adeoye (of blessed memory). You were my primary 1 teacher, and today's achievement is the result of the solid academic foundation you laid for me. Thank you for your prayers and encouragement all these years. I am equally grateful to you for the inspiration you have given me to always believe in myself and have a can-do spirit. You are my gold, and I cannot trade you for anything. How I wish you stay to witness today, a milestone I once shared with utmost excitement with you, my beloved mother. Though you are no longer with me to witness this achievement, your love and guidance remains deeply rooted in my heart. I wish you are here to see me shine, to share the pride and joy that you and daddy's unwavering support nurtured. Your absence weighs heavily on me, but I take solace in knowing that your spirit lives on through me. This lecture is not just a professional accomplishment, it's a testament of you and daddy's constant faith in me. I dedicate this moment to you and daddy's memory, honouring the sacrifices you and daddy made and the dreams envisioned for me.

Vice-Chancellor, sir, permit to ask the audience to stand in five minutes in remembrance of my parents and mentee.

I am grateful to all the teachers who taught me at the primary, secondary, and university levels. My special thanks go to Dr. (Mrs.) Fola Olowoleni (the former Registrar of the University of Ilorin), Mrs. B.O. Ishola, and Dr. (Mrs.) Josephine Iyabo Oyebanji, whom God used to facilitate my employment at the University of Ilorin. My Ph.D. supervisors; Prof. J.S. Sadiku, Prof. J.O. Omolehin, and Prof. J.A. Gbadeyan, and my M.Sc. supervisor, Prof. B.A. Oluwade. Thank you for all your mentoring and guidance.

I acknowledge the past VCs and other principal officers for the roles played in my career growth and development. To Prof. I. O. O. Amali, who under his tenure I was offered an appointment as a Graduate Assistant. To the immediate past VC, Prof. S. A. Abdulkareem, who under his tenure I got promoted as a Reader and appointed as the Deputy Director (Research), Centre for Research, Development and In-house Training (CREDIT). He also appointed me as the Ag. Head of the Department of Computer Science, making me the first female to occupy the headship of my Department. For your belief in handwork, dedication, and commitment, I say thank you, sir. To the current VC, Prof. W.O. Egbewole, who announced my professorship, thank you for being a great leader of excellence.

To all my academic and professional advisers, Professors G. A. Aderounmu, J. S. Sadiku, J. A. Gbadeyan, E. R. Adagunodo, Francisca Oladipo, Adenike O. Osofisan, Stella C. Chiemeke, K. Rauf, A. S. Idowu, and J. O. Omolehin, thank you all for playing a vital role in guiding my academic journey. Please permit me to single out Prof. J.O. Omolehin whose guidance has been instrumental in shaping my academic career; I am forever grateful. To all the professors in the Faculty of Communication and Information Sciences: Professors L. O. Aina, J.S. Sadiku, A. Issa, Omenogo V. Mejabi, Adetoun O. Idowu, A. Tella, A. L. Azeez, R.

O. Oladele, Tinuke O. Oladele, A. O. Ameen, and Saudat S. Abdulbaqi, and all other members of the Faculty's teaching and non-teaching staff, your supports are highly appreciated. I want to appreciate Professors L. O. Aina, A. Issa, and Omenogo V. Mejabi for the various opportunities they gave me to grow administratively by way of assigning administrative tasks which have given me the requisite administrative acumen as a staff and professor in the Faculty and University. I especially thank the present Dean, Prof. A. L. Azeez, for supporting and always believing in me, you also set up Inaugural Lecture planning committee for the success of this outing.I appreciate all the members of the committee ably led by Dr. Fatimah E. Usman-Hamza, for their efforts in making today a success.

My special thanks go to the Library and Publication Committee under the leadership of Prof. A. A. Adeoye for the meticulous editing and feedback on my paper. Your input has greatly improved its quality. I equally thank those that read and edited the drafts of the lecture, Prof. R. G. Jimoh, Dr. Amos Bajeh, Dr. Shakirat A. Salihu, and Dr. Samiat O. Abubakre.

To the members of staff of the Department of Computer Science, the one-big family; you are all more than colleagues to me. You are my brothers, sisters, friends, sons, and daughters. My special appreciation goes to Professors R. O. Oladele (HOD), A. O. Ameen, Tinuke O. Oladele, Drs. A. O. Babatunde, D. R. Aremu, A. R. Ajiboye, A. Muyideen, Ghaniyyat B. Balogun, P. O. Adebayo, I. D. Oladipo, Ikeola S. Olatiwon, Mr. A. Jamiu, Mrs. Taibat Adebakin, Mrs. Mary O. Olaoye, Mrs. Latifat B. Adeoye, Mrs. Sadiat O. Hussien, Mr. A. A. Gambari and Mrs. Rashidat O. Adedeji. To my academic sons and daughters, Drs. Amos Bajeh, Abimbola G. Akintola, Shakirat A. Salihu, Fatimah E. Usman-Hamza, K. S. Adewole, Joseph Awotunde, Peter Sadiku, Gbenga Balogun, Ayisat W. Asaju-Gbolagade, and Mr. H. A. Mojeed, thank you for the immeasurable love. Prof. R. G. Jimoh and Dr. M. A. Mabayoje, thank you for all you do. To all the past and present Departmental Secretaries, Mrs. F. Olanrewaju, Mrs. Folake Bamidele, Mrs. F. O. Akano, and Mrs. Christianah F. Boluwade, you were all like mothers to me. Also, to all the past and present clerical and administrative staff, Mrs. Mary E. Obans, Mrs. Taibat A. Abdullahi, and Mrs. Oluwakemi Ademola thank you for the support and care.

I also extend my gratitude to all the academic staff of Department of Computer Science, Department of Physical Science of Al-hikmah University, Ilorin.

I appreciate Prof. K. W. Wahab who was my director at CREDIT; Prof. Kehinde Okoro, who was the Deputy Director (Training) while I was the Deputy Director (Research); Prof. Y.O. Imam (Research Manager, Humanities Cluster); Mrs. Roseline Yusuf; Mr. Adegboyega; Mrs. Nafisat Ariyo and others, thank you for making my tenure worthwhile.

To all my research collaborators, especially the AI4FS team, Prof. M.A. Albinu (the VC, Summit University), Prof. Bamidele Adebisi (Manchester Metropolitan University), Dr. Taliha Folorusho, Dr. Shakirat Folorusho, and others, working alongside with you have been an enriching and rewarding experience. To all my friends within and outside the university, Drs. Rafiat A. Oyekunle, O. Oloyede, Lambe Mustapha, Yinka Adedoyin, M. A. Akamu, Prof. Kunle Olawepo (family friend), Prof. L. F. Oladimeji, Remi Kolawole, Bimbo Abolaji (twinny), Adeyosola Olawepo-Ajiboye, Oyikansola Adekeye, Bimpe Peterson-Babalola, Prof. Yidiat O. Aderinto, Mrs. Adeboye (Wumi Ventures), Mrs. Desola Fatoba, Dcns. Moyinoluwa Owolabi, Mrs. Mustapha, Dr. Akin Babatunde, Engr. Adewumi, Dcns. Deborah Moses, Elder Yejide Raji, Elder Yemisi Aina, Elder Omolara Omiyinka, Elder Rachael Ishola, Mrs. Oluremi Adaran, you are all appreciated.

I will like to extend my heartfelt appreciation to Nigeria Computer Society and Nigerian Women in Information Technology (NIWIIT), Kwara State chapters for their unwavering support.

I render my greetings and admiration to all my academic sons and daughters, Drs. Taye Oladele Aro, Benjamin Aruwa Gyunka, Noah Oluwatobi Akande, Hakeem Akande, Roseline Oluwaseun Ogundokun, Shakirat Aderonke Salihu, Fatimah Taofeek-Ibrahim, Morufat Gbolagade, Esau Taiwo Oladipupo, Peter Sadiku, Mrs. Ganiyat Afolabi-Yusuf and Evelyn Temitayo, whose scholarly journeys I have had the privilege to guide and study. You were all part of the success story today and you are the future of our field. To all my M.Sc. supervisees (too numerous to mention), thank you all for being an integral part of this journey. I love you all. God bless.

To all the royal fathers present, the Eledidi of Edidi, Oba J. K. Aboyeji, and the Oniwo of Iwo, Oba Architect Olutade. Thank you, and God bless you. To all the pastorate, board of elders, and members of the 1st ECWA Church under the distinguished leadership of Rev. (Dr.) B. M. Owojaiye, thank you for your prayers, mentorships and support all these years.

To my one and only pastor, father, mentor, and boss, Pastor J. T. Aboyeji the Presiding Pastor of The Potters Porch International Churches (TPPIC)thank you, sir, for imparting on me the grace of Hope, Possibility and Assurance, and also the mentality of speedy accomplishment. You taught me not to be slothful in business, to be fervent in spirit, and to diligently serve the Lord. You have always been there for me through thick and thin. Also, to my spiritual mother, Pastor (Mrs.) Oluseyi Aboyeji (the Senior Pastor of TPPIC) you are the epitome of humility, your disposition has taught me what a virtuous woman should be. To all my fellow pastors in the vineyard, Pastor Tayo Owolabi (the State pastor), Pastor Victor Ige (the Director General, Nigeria Geological Survey Agency), Pastor Raji Michael, Pastors Adebowale Adeniji, Babajide Kayode, Fidelis Ehihi, and Austin Iwueze and their wives. I am honoured to serve alongside with you in sharing the love and message of our Lord and saviour Jesus Christ. To all the ministers, elders, deacons, deaconesses, workers, Virtuous women, Mighty men and entire members of TPPIC: you are great. I also appreciate Pastor John Ishola.

To my paternal and maternal family members, the Adeoyes, Idowus, Aransiolas, Adebayos, Iranloyes, and Bolarins. Please, permit me to single out the following people: Dr. Yinka Adebayo, Mr. Adebayo Idowu, Dr. (Mrs.) Iyabo Adunbarin, Mrs. Ronke Kunle-Olawepo, Mr. Adeyemi Adebayo, Mrs. Victoria Folake Adedoyin, and Mrs. Christiana Biola Ajiboye, you are all well appreciated.

To my father and mother-in-laws, Late Prince J. O. Abikoye and Mrs. M. T. Abikoye, thank you, sir and ma. Your encouragement over the years has been instrumental to attaining this significant milestone, and I am grateful for everything you have done. My husband's siblings and their spouses, Pastor and Mrs. Akinola and Olanike Ajiboye, Mrs. Olubunmi Lawal, Mr. and Mrs. Rotimi and Funke Abikoye, Pastor and Mrs. Kayode and Shola Lawal, and Dr. and Mrs. Tayo and Shade Abikoye. Thank you all for all you do. My special appreciation goes to Mr. and Mrs. A.O. Oyeniyi and their children (Bimbo Ajulo, Derin, Muyiwa Oyeniyi, and Gboyega Oyeniyi). To the No. 13 FAS Close Squad, Damilola Ajiboye, Kolawole Ajiboye, Akinwumi Ajiboye, Olumide Lawal, Bukola, Ibidun, Shade Olaitan and her husband, and also GRA, Flower Garden residents, Nike Ogunremi, Bukola Lawrence, Fatimah Abdullahi, Ife Oladebo, Amina Mohammed, Wale Ogunremi, and Fumilayo Aboyeji, I am deeply grateful for the unwavering support.

To my siblings, Mr. Oluwaseye George Adeoye (Saudi Arabia; he is representing my father here today), Mr. Oluwagbenga Godwin Adeoye, Mrs. Oluwayemisi Susan Babarinde, and Mrs. Oluwatobi Joan Ben-Babatunde, including their spouses Bukola Adeoye, Bimbo Adeoye, Dr. Damilola Babarinde, and Dayo Babatunde, your belief in me from the early days of my academic pursuit to this day has been a constant source of strength. I cherish the memories and moments we have shared and the encouragement you have provided, and I am thankful for the unity and love that define our family.

To my children and cheerleaders, Oluwashina-Ayomi Nathanael, Oluwasemilore Glory, and Oluwasemilogo Kristabel (Morenikeji mi), I am filled with immense gratitude towards you all for your understanding, support, and love which have been my pillar of strength throughout this journey. I am aware of and deeply grateful for the sacrifices that you have made to accommodate my career aspirations. Being your mother is the greatest joy ever. I love you all.

Finally, to my crown and forever mine, the man behind the scene; Prince Oluwole Olasoji Abikoye; your love, care, support, and understanding have allowed me to pursue my dream with confidence. Thank you for being my greatest supporter. You are my jewel of inestimable value. May we live long together in sound mind, good health, and prosperity to eat the fruits of our labour. I love you beyond measure.

To everyone that has contributed to my achievements and success in one way or the other that time will not permit me to mention their names, I say God bless you all.

Mr. Vice Chancellor, permit me to end this inaugural lecture with this song by Neon Adejo.

References

Abikoye, O. C., & Oluwade, D. (2008). Computational analysis of GSM security algorithm, *African Journal of Computing & ICT (IEEE Nigeria Computer Chapter),* (1) 3, 27-33.

Abikoye, O. C., & Bajeh A. O. (2009). Development of a model for the implementation of GSM security algorithm, *Journal of Mathematical Association of Nigeria, ABACUS*, (36)2, 89-99.

Abikoye, O. C., Mabayoje, M. A., & Ajibade, R. (2011). Offline signature recognition & verification using Neural Network, *International Journal of Computer Applications*, (35) 2, 44-51.

Abikoye, O. C., Omolehin, J. O., & Sadiku, J. S. (2012). Some refinement on iris localisation lgorithm, *International Journal of Engineering and Technology Explore*, (2) 11, 1835-1841.

Abikoye, O. C., Adewole, K. S., & Oladipupo, A. J. (2012). Efficient data hiding system using cryptography and steganography, *International Journal of Applied Information Systems (IJAIS),* (4) 11, 6-11.

Abikoye, O. C., Sadiku, J. S., Adewole, K. S., & Jimoh, R. G. (2014). Iris feature extraction for personal identification using Fast Wavelet Transform (FWT)*, International Journal of Applied Information Systems (IJAIS),* (6)9, 1-6.

Abikoye, O. C., Adewole, K. S., & Salahdeen, N. K. (2014). Fuzzy logic approach to determine security level of biometrics, *African Journal of Computing & ICT,* (7) 4, 69-84.

Abikoye O. C., Akintola, A. G**.**, & Ibrahim, S. (2014). Design and implementation of Yoruba language cryptosystem, *Ilorin Journal of Science*, **(**1) 1, 50 – 60.

Abikoye, O. C., & Nwokolo, N. P. (2015). Object Oriented Paradigm for implementing Elgamal Algorithm,*International Journal of Information Processing and Communication (IJIPC).* (3) 1&2, 76-89.

Abikoye, O. C. & Ademarati, O. A. (2016). Information security model using two fish encryption and decryption algorithm, *International Journal of Information Processing and Communication (IJIPC).* (4) 1 & 2, 129-144.

Abikoye, O. C, Chukwu, M., & Babatunde, A. N. (2016). An improved palm vein based recognition system, *International Journal of Computing and ICT Research.* (11) 1, 9 – 18.

Abikoye, O. C., Balogun, A.O., Olarewaju, A. K., & Bajeh, A. O. (2016). Improved performance of intrusion detection system using feature reduction and J48 decision tree classification, *Ilorin Journal of Computer Science and Information Technology,* (1) 1, 71-88.

Abikoye, O. C., Aro, T. O., Obisesan, R. O., & Babatunde, A. N. (2017). Hybridized intrusion detection system using genetic and tabu search algorithm, *Anale. Seria Informatică (Annals. Computer Science Series).* 15 (1), 139-150.

Abikoye O. C., & Sanni, B. T. (2017). Keystroke dynamics authentication for a web-based sales and stock solution, *International Journal of Computing and ICT Research,* (11) 1, 84 -113.

Abikoye, O. C., Garba, Q. A., & Akande, O. N. (2017). Implementation of textual information encryption using 128, 192 and 256 bits Advanced Encryption Standard algorithm, *Anale.Seria Informatică (Annals. Computer Science Series),* (15) 2, 153-159.

Abikoye, O. C., & Gyunka, B. A. (2018) .The threat of split-personality android malware on developing economy, *Computing and Information Systems Journal*. (22), 1, 1-11.

Abikoye, **O. C.,** Aro, T. O., Ogundokun O. & Akande, H. B. (2018). Comparative analysis of selected feature extraction techniques for iris recognition system, *FUW Trends in Science & Technology Journal*, 3 (2A), 541 – 545.

Abikoye, O. C., Shoyemi, I. F., & Aro, T. O. (2019). Comparative analysis of illumination normalizations on principal component analysis based feature extraction for face recognition. *FUOYE Journal of Engineering and Technology*, 4 (1), 67-69.

Abikoye, O. C., Afolabi, G. K., & Aro, T. O. (2019). Biometric based point- of- sale authentication system. *International Journal of Software Engineering and Computer Systems (IJSECS),* 5 (1), 36-51.

Abikoye, O. C., Akande, N.O., Garuba, A.V., & Ogundokun, R.O. (2019). A secured one time password authentication technique using (3, 3) visual cryptography scheme, *Journal of Physics: Conference Series.* (1299) 1, 012059.

Abikoye O. C., Dokoro, A.H., Abdullahi, A., Akande, N. O., & Asani, E. O. (2019). Modified advanced encryption standard algorithm for information security, *Symmetry,* (11) 12, 1484.

Abikoye O. C., Gyunka, B. A., & Akande, O. N. (2020a). Android malware detection through machine learning techniques: A Review, *International Journal of Online and Biomedical Engineering (iJOE)*, (16) 2, 14-30.

Abikoye, O. C., Gyunka B. A., & Akande, N. O. (2020b). Optimizing android malware detection via ensemble learning, *International Journal of Interactive Mobile Technologies (iJIM),* (14) 9, 61-78.

Abikoye O. C., Taofeek-Ibrahim, F. A. & Aro, T. O. (2020). Optimized one dimensional-ternary pattern (1D-TP) for SMS spam feature extraction, *International Journal of Research and Innovation in Applied Science (IJRIAS)*, (5) 9, 24-31.

Abikoye O. C., Abubakar A., Dokoro A. H., Akande O. N. & Kayode, A. A. (2020). A novel technique to prevent SQL injection and cross-site scripting attacks using Knuth-Morris-Pratt string match algorithm, *European Association for Signal Processing (EURASIP) Journal on Information Security*, (14) 2020.

Abikoye, O. C., Ojo, U. A., Awotunde, J. B., & Ogundokun, R. O. (2020). A safe and secured iris template using steganography and cryptography. *Multimedia Tools and* Applications**,** 79 (31-32), 23483-23506.

Abikoye, O. C., & Ogundokun, R. O. (2021).Efficiency of LSB steganography on medical information. *International Journal of Electrical and Computer Engineering (IJECE)*. (11) 5, 4157 - 4164.

Abikoye, O. C., Ogundokun, R. O., Misra, S., & Agrawal, A. (2022). Analytical study on LSB-based image steganography approach. In*: Computational Intelligence in Machine Learning. Lecture Notes in Electrical Engineering*,Kumar A., Zurada J.M., Gunjan V.K., Balasubramanian R. (eds)., 834, 451-457.

Abikoye, O. C., Oladipupo, E. T., Imoize, A. L., Awotunde J. B., Lee Cheng-Chi & Li Chun-Ta (2023). Securing critical user information over the internet of medical things platforms using a hybrid cryptography scheme, *Future Internet*, 15 (99).

Adewole, K. S., Jimoh, R. G., & **Abikoye, O. C**. (2014). A review of algorithms for fingerprint image acquisition, preprocessing and minutiae extraction algorithm, *Ilorin Journal of Science*, (1) 2, 50-68.

Adewole, K. S., Jimoh, R. G., **Abikoye, O. C., &** Ajiboye, A.R. (2015). Stepwise biometric procedures for managing student attendance in higher institutions of learning, *The Journal of Computer Science and Its Applications*, (22) 1, 77-86.

Adewole, K. S., Jimoh, R. G., Akintola, A. G., & **Abikoye, O. C**. (2018). Spam detection and risk assessment framework based on ensemble learning in data stream environment, *International Journal of Information Processing and Communication (IJIPC)*, (6) 1, 1 – 16.

Adewole, K. S., Raheem, M. O., **Abikoye, O. C**., Ajiboye, A. R., Oladele, T. O., Jimoh, M. K., & Aremu, D. R. (2021). Malicious uniform resource locator detection using wolf optimization algorithm and random forest classifier. In:

Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics: Theories and Applications, Chiroma H., Shafi'i M. A., Philippe Fournier-Viger, Garcia N. M. (eds.), 177-196.

Akande, N. O., **Abikoye, O. C**., Adebiyi, M. O., Kayode, A. A., Adegun, A. A., & Ogundokun, R. O. (2019). Electronic medical information encryption using modified blowfish algorithm. In: *Computational Science and Its Applications – ICCSA 2019. Lecture Notes inComputer Science*, Misra, S. *et al*. (eds.), 11623.

Akande, N. O., **Abikoye, O. C.,** Adeyemo, I. A., Ogundokun, R. O., & Aro, T. O. (2018). Comprehensive evaluation of appearance-based techniques for palmprint features extraction using probabilistic neural network, cosine measures and euclidean distance classifiers, *The University of Pitesti Scientific Bulletin, Series: Electronics and Computers Science*, (18) 1, 5- 14.

Akande, N. O., **Abikoye, O. C**., Ayegba, P., Gbadamosi, B., & Adegun, A. A.(2019). Segmented retinal blood vessels of healthy and diabetic retinopathy individual, *Journal of Engineering and Applied Sciences*, (12) 16, 5794-5799.

Akande, N. O., **Abikoye, O. C.**, & Kayode, A. A. (2019). Automatic segmentation of retinal blood vessels of diabetic retinopathy patients using dempster-shafer edge based detector, *Asian Journal of Scientific Research*. (12) 3, 376-383.

Akande O. N., **Abikoye O. C.**, Kayode A. A., & Lamarim Y. (2020). IMPLEMENTATION of a Framework for Healthy and Diabetic Retinopathy Retinal Image Recognition, *Scientifica*, 2020, 1-14.

Akande, N. O., **Abikoye, O. C.**, Gbadamosi ,B., Ayoola, J., Ayegba, P., Adegun, A. A., Ogundokun, R. O. & Asani, E. O. (2020). Vascular networks segmented from retinal images of hypertensive retinopathy and glaucoma patients. *Journal of Engineering and Applied Sciences*. (15) 8, 1932-1936.

Akande, O. N., **Abikoye, O. C**., Kayode, A. A., Aro O. T., & Ogundokun, O. R. (2020). A dynamic round triple data encryption standard cryptographic technique for data security. In: *Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science*, Gervasi O. et al. (eds.), 12254.

Akande O., Ojimba N., Oghenekaro, A., **Abikoye, O. C.**, Ogundokun, R., & Akindele, A. (2022). AFHIRIS: African Human Iris Dataset (Version 1) [version 1; peer review: awaiting peer review].*F1000Research 2022,* (11) 1549.

Akande, O. N., Oluwadara, G., **Abikoye, O. C.**, Jimoh, R. G., Akande, H. B., Balogun, A. O., & Anuoluwapo, F. (2023). SMSPROTECT: An automatic smishing detection mobile application, *ICT Express*, (9) 2, 168-176.

Aro T. O., Oluwade, B., **Abikoye, O. C.,** & Bajeh, A. O. (2017). A 2-dimensional gabor-filters for face recognition system: A Survey, *Anale. Seria Informatică (Annals. Computer Science Series).* 15 (1), 104-112.

Aro, T. O., **Abikoye, O. C**., & Bajeh, A .O. (2018). Optimizedgabor features for facial recognition system, *The University of Pitesti Scientific Bulletin, Series: Electronics and Computers Science,* 5-26.

Aro, T. O., **Abikoye, O. C**., Oladipo, I. D., & Awotunde, B. J. (2019). Enhanced gabor features based facial recognition using ant colony optimization algorithm, *Journal of Sustainable Technology (JoST),*10 (1), 32-42**.**

Babatunde, A. N., **Abikoye, O. C.,** Babatunde, R. S., & Kawu, R. O. (2016). Handwritten character recognition using brainnet library, *Anale. Seria Informatică, Annals. Computer Science Series,* (14) 2, 129-136.

Babatunde, A. N.,Jimoh, R. G., **Abikoye, O. C., &** Isiaka, B. (2017). Survey of video encryption algorithms, *Covenant Journal of Informatics & Communication Technology,* (5) 1, 65-80.

Daugman, J., Dowing, C., Akande, O. N., & **Abikoye, O. C.** (2024). Ethnicity and biometric uniqueness: iris pattern individuality in a West African database, *IEEE Transactions on Biometrics, Behavior, and identity Science***,** (6) 1, 79-86.

GBC-DELL Survey. (2015). The human factor at the core of federal cybersecurity. *Government Business Council.*

Gyunka, B. A., & **Abikoye**, **O. C.** (2017). Analysis of human factors in cyber security: A Case study of anonymous attack on hbgary, Computing *and Information Systems Journal*, (21) 2, 10-18.

Gyunka, B.A., **Abikoye, O. C., &** Adekunle, A. S. (2021). Anomaly malware detection: A comparative analysis of six classifiers. In: *Information and Communication Technology and Applications. ICTA 2020. Communications in Computer and Information Science,* Misra S., Muhammad-Bello B. (eds) (1350), 145-157.

Hendrick A. M., Gibson M. V., and Kulshreshtha A. (2015). Diabetic retinopathy, primary care, *Clinics in Office Practice*, (42) 3, 451–464.

Kumar P., Rana S. B. (2016). Development of modified AES algorithm for data security. *Optik*, 127 (4), 2341–2345.

Liang, H. (2020). Research on data confidentiality and security of computer network password. *Journal of Physics: Conference Series*, *1648* (2), 022078.

Mitnick, K. D., Simon, & L., W. (2011). The art of deception: controlling the human element of security. Indiana: *John Wiley & Sons.*

Ogundokun, R. O., **Abikoye, O. C.,** Misra, S., & Awotunde, J. B. (2020). Modified Least significant bit technique for securing medical images. *In: Information Systems EMCIS 2020. Lecture Notes in Business Information Processing*, Themistocleous M., Papadaki M., Kamal M. M. (eds), 402.

Ogundokun, R. O., **Abikoye, O. C.**, Adegun , A. A., & Awotunde, J. B. (2020). Speech recognition system: Overview of the state-of-the-arts. *International Journal of Engineering Research and Technology,* (13) 3, 384-392.

Ogundokun R. O., & **Abikoye, O. C.** (2021). A safe and secured medical textual information using an improved LSB image steganography. *International Journal of Digital Multimedia Broadcasting*, 2021.

Ogundokun, R. O., Awotunde, J. B., Misra, S., **Abikoye, O. C**., & Folarin, O. (2021). Application of machine learning for ransomware detection in IoT devices. In: Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities. Studies in Computational Intelligence, Misra S., Kumar Tyagi A. (eds). 972, 393-420.

Ogundokun, R. O., **Abikoye, C. O.**, Sahu, A. K., Akinrotimi, A. O., Babatunde, A. N., Sadiku, P. O., & Olabode, O. J. (2024). Enhancing security and ownership protection of neural networks using watermarking techniques: A systematic literature review using PRISMA. *In: Multimedia Watermarking*, Kumar Sahu, A. (eds). 1-28.

Oladipupo, E. T., & **Abikoye, O. C. (**2022a**).** Modified playfair cryptosystem for improved data security**,** *Computer Science and Information Technologies***,** 3(1), 51-64.

Oladipupo, E. T., & **Abikoye, O. C.** (2022b). Improved authenticated elliptic curve cryptography scheme for resource starve applications, *Computer Science and Information Technologies*, 3 (3), 169-185.

Oladipupo, E. T., **Abikoye**, **O. C.**, Awotunde, J. B., Imoize, A. L., Chang Ting-Yi, Lee Cheng-Chi & Do Dinh-Thuan (2023). An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks, *IEEE Access,* 11, 1306-1323.

Oladipupo, E. T., **Abikoye, O. C**., & Awotunde, J. B. (2024). A lightweight image cryptosystem for cloud-assisted internet of things, *Applied Sciences*, 14 (7), 2808.

Omelina, L., Goga, J., Pavlovicova, J., Oravec, M., & Jansen, B. (2021). A survey of iris datasets, *Image and Vision Computing*, 108, art. no. 104109.

Omolehin, J. O., **Abikoye O. C.,** & Jimoh, R. G. (2008). Development of data encryption and decryption algorithm using 4 – row Rail Fence Cipher, *Journal of the Nigerian Association of Mathematical Physics*, 13, 411-416.

Omolehin, J. O., **Abikoye O. C.**, & Bajeh, A. O. (2009). Time complexity of 4 – row rail fence cipher encryption algorithm, *International Journal of Mathematical Science,* (1)1, 8-14.

Omolehin, J. O., **Abikoye O. C.,** & Jimoh, R. G. (2009). Development of data encryption and decryption algorithm using modified rail fence cipher, *Association for the Advancement of Modelling & Simulation Techniques in Enterprises (AMSE),* (14) 2, 69-78.

Rafli, M., Nusantara, N. C. A., Putri, E. R., Sari, I. P., Zamzami, N., & Muharroman, A. I. (2024). Information security behaviour and compliance with ISO 27001 in IT Companies, *Journal of Digital Business and Innovation Management,* 3 (1), 62-76.

Salihu, S. A., Quadri, S. O., & **Abikoye, O. C.** (2020). Performance evaluation of selected machine learning techniques for malware detection in android devices, *Ilorin Journal of Computer Science and Information Technology, (IJCIT)*, 3 (1), 52-61.

Prabhu, S. & Shah V. (2015). Authentication using session based passwords, *Procedia Computer Science*, 45, 460-464.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security, *Journal of Information System Security (JISSec),* 10 (3), 21-45.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review, *International Journal of Information Management*, *36* (2), 215–225.

Taofeek-Ibrahim, F. A., **Abikoye O. C.,** & Toye N. T. (2020). SMS spam detection system using effective one-dimensional ternary pattern (1D-TP), *International Journal of Computing and Technology (IJCAT)*. (7)6, 94-102.

Van Oorschot, P. C. (2021). Computer security and the internet, *Tools and Jewels from Malware to Bitcoin*. Springer International Publishing. https://doi.org/10.1007/978-3-030-83411-1