# UNIVERSITY OF ILORIN

**THE TWO HUNDRED AND THIRTY-NINTH (239TH)**
**INAUGURAL LECTURE**

# "DECONSTRUCTING THE CRAWLING MINDSETS: COMBATTING SECURITY CHALLENGES OF NET-CENTRIC COMPUTING"

***By***


**PROFESSOR RASHEED GBENGA JIMOH**
**ND (Offa); B.Sc. (Ilorin); M.Sc. (Ibadan); Ph.D. (Sintok);**
**FICENT, SMIEEE, MCPN, MAITP, MITSSP, MISOC, MNITPCS**

**DEPARTMENT OF COMPUTER SCIENCE,**
**FACULTY OF COMMUNICATION AND INFORMATION SCIENCES,**
**UNIVERSITY OF ILORIN, ILORIN, NIGERIA.**


***THURSDAY, 17TH AUGUST, 2023***

**This 239th 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**

**17th August, 2023**

**ISBN: 978-978-8556-30-5**

**Published by:**

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

**Printed by**
**Unilorin Press, Ilorin, Nigeria.**

**PROFESSOR RASHEED GBENGA JIMOH**
**ND (Offa); B.Sc. (Ilorin); M.Sc. (Ibadan); Ph.D. (Sintok);**
**FICENT, SMIEEE, MCPN, MAITP, MITSSP, MISOC, MNITPCS**

**DEPARTMENT OF COMPUTER SCIENCE,**
**FACULTY OF COMMUNICATION AND**
**INFORMATION SCIENCES,**
**UNIVERSITY OF ILORIN, ILORIN, NIGERIA.**

***Blanck***

***Courtesies***

The Vice-Chancellor,
Deputy Vice-Chancellor (Academic),
Deputy Vice-Chancellor (Management Services),
The Registrar,
The 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,
Great students of the Better-By-Far University,
Distinguished students of the Faculty of Communication and Information Sciences,
Greatest Computer Science students,
Gentlemen of the Print and Electronic Media,
Distinguished Guests,
Ladies and Gentlemen.

**Preamble**

In the name of Almighty Allah, the most Gracious, the most Merciful, the Originator, the Terminator, the Alpha and Omega, the Omnipotent and the Omnipresence whose only endorsement made today's lecture a reality. All praises and adorations to you alone! *Alhamdulillah Rabili Alamin.* Mr. Vice-Chancellor Sir, the person humbly standing before this distinguished audience today to present the 239$^{th}$ inaugural lecture of the University of Ilorin in its series, titled "**Deconstructing the Crawling Mindsets: Combatting Security Challenges of the Net-centric Computing**", the 3$^{rd}$ from the Faculty of Communication and Information Sciences and the very 1$^{st}$ from the Department of Computer Science was raised by

Parents who could neither read nor write in any language but were destined to produce the First Professor of Computer Science and the First inaugural lecturer from the Department of Computer Science, University of Ilorin. It is on this note that I seek your permission to start this lecture by praying for my late father, Alhaji Olawale Aweda JIMOH who departed this world 23 years ago. His passion for getting his children educated came from the unjust treatment he received during his periods of active participation in grassroot politics by the so-called political elites of his time despite his undeniable impacts. In short, today's event is a manifestation of his answered prayers. May *Allah* forgive him all his sins and grant him *Aljanat Firdous*, Amina.

Mr. Vice-Chancellor Sir, my coming to the University of Ilorin was so divine in nature. As the Best-graduating student at the Federal Polytechnic, Offa in 1998, I was confident of securing admission into the Computer Science programme of the Federal University of Technology, Akure, only to be delayed by one day in getting my academic transcript to Akure which prevented me from gaining admission into the University as planned., I was very sad about it but as a Muslim, I took it as the wish of Allah and quickly proceeded to obtain a change of institution form to the University of Ilorin. That was the first time I visited Ilorin in my life but to the glory of God, I eventually secured the admission. Even during my undergraduate days, I never thought of working with University of Ilorin because B.Sc. Computer Science was hot cake then and we all looked up to multinational companies for greener pastures.

To the will of Allah, I graduated with a Second Class (Upper Division) and got employed in the same company where I did my mandatory one year National Youth Service immediately at the then Data Processing Maintenance and Services (DPMS), an IBM Business partner located at Onikan, Lagos with a monthly salary close to =N=100,000 as at then. The company used to be a stop over to cross to any desired multi-national companies because most multinational companies in Nigeria such as Shell, Chevron, Exonmobi, CFAO etc were all DPMS's clients. As DPMS staff, we were all saddled with visitations, consultations on deployment, repair, supports and maintenance of IBM Servers and Operating Systems of those notable multi-national companies running on IBM

servers with OS400 as their operating system. I made it a necessity to acquire the relevant IBM certifications to enable me cross over to a multi-national company of my choice. Rather than moving to an IT company as planned, I got a call from a good friend of mine that the Department of Computer Science had been created from the then Mathematics Department which formerly housed the B.Sc. Computer Science Programme and that the University was interested in recruiting those who graduated with a Second Class (Upper Division) from the Department. It was a tough decision for me because I had started enjoying the goodies of IT profession with a driver assigned to me any time I was going to client's location for support services. That call and the information provided became a turning point in my life. I then went ahead to forward my Curriculum Vitae despite the huge sloppy disparity in salary and conditions of service of a System Development Manager to a University Graduate Assistant. My consolation was the opportunity to be closer to my life partner who got admitted to the University as well in addition to aiding my ambition to pursue postgraduate studies. To the glory of Almighty Allah, I was offered the job. It then became a tough decision to pick up the lecturing opportunity over my IT career as family members were skeptical of my choice. I was determined to take up the job so that I can use the platform to actualise my dream for Ph.D. *Alhamdulillahi*, today, the rest is history and this gathering is a testimony to divine direction in taking that tough decision. The University of Ilorin became a natural and nurtural training ground for me far beyond certificate acquisition.

Mr. Vice-Chancellor Sir, my interest in the field of computing started far back from my primary school days at Baptist Day Primary School, Ikirun where my then class Teacher, Mrs. Babatunde introduced the class to the Abacus counting machine. She alluded to the historical development of the counting machine purposely to make numeric computation easier. That triggered my inquisitiveness to see all other computational devices mentioned in that class. My eagerness to see that magic machine called a computer kept increasing until I was admitted into the Federal Polytechnic Offa to study Computer Studies where I made the computer laboratory my second home. It is worthy of note that my first significant savings were used to procure a 486 desktop

computer system which was a great accomplishment during my undergraduate days at the University of Ilorin. During my undergraduate days, I was visiting the then NUNET at the then administrative building of the University to send one message or another via email before I was able to procure my personal desktop in my 400 Level. During these periods, I was always conscious of the vulnerability of my conversations over the electronic medium and such feelings among others triggered my research interest in the area of information and cyber security. Today, I thank *Allah* for making it a fruitful inquisitiveness.

**Introduction**

Mr. Vice-Chancellor Sir, the alarming rate of cybecrimes nowadays through all forms of attacks can never be overemphasised. People are defrauded of their hard earned resources through undue access and privileges illegally gained by hackers. It is more rampant in this part of the world being adopters of ICTs with little or no awareness about the adaptive culture/ethics for secured cyber operations. According to the report by the Economic and Financial Crime Commission, just in year 2022 alone, Two Thousand Eight Hundred and Forty Seven (2,847) Nigerians were convicted of various cybercrimes which was the highest in the history of the Commission (EFCC, 2022). This alarming trend in cybercrimes has developed in many Nigerians, a kind of technophobia and digital exclusiveness as a means to avoid being victims who eventually are called the people of "crawling mindests" as being operationally used in this lecture.

Mr. Vice-Chancellor Sir, the menace of cybercrimes is quite enough to justify the decisions by people of crawling mindsets However, the advantages of digital transformation calls for the need to deconstruct those crawling mindsets by preferring ethics, strategies and techniques for securing day-to-day operations in the emerging cyber space.

We are in the information age. Consequently, information is viewed as a valuable asset whose protection should be of great concern. Information is a very valuable resource and must be protected against harmful attack from the inside as well as outside the organisation. Hence, information security can be conceptualised as the protection of important data against unauthorised users. It

was revealed that hackers leverage on undue access to privilege information which could be mined to discover some other privileges purposely to gain unauthorised access to information resources. Guard (2023) revealed that majority of banking related attacks and frauds were largely caused by careless disclosure of sensitive information to unauthorised persons/imposters. The fraudsters employ different approaches to get needed information. Thus, information should be seen as valuable assets whose undue disclosure can cause grave damage. The open nature of the Internet makes it vital for digital businesses to pay serious attention to the security of their networks. As companies move more of their business functions to the public network, they need to take precautions to ensure that the data cannot be compromised and that data is not accessible to anyone who is not authorised to access the functions. The integration of Information and Communication Technologies (ICTs) into our day-to-day operation has practically changed the space with which we all operate from physical to cyberspace. Indeed, our perception of assets should equally change from traditional/physical assets to digital assets. Securing the new form of asset therefore requires a new perspective. The situation gets compounded by the need to share information and resources across computer networks and even network of networks (the Internet). The efforts to attain secured interaction and operations in cyberspace are endless engagements with no return on investment and very sacrosanct in the emerging digital era (**Jimoh**, Abikoye & Balogun, 2017). At the same time, there is need to rise up to the challenges because jettisoning migration to a digital era is not an option except settling for crawling when the world is moving at a very fast pace. Mr. Vice-Chancellor Sir, the crawling mindsets need to be deconstructed through various cyber security mitigating techniques which informed my major research contributions.

**Historical Evolution of Security**

Mr. Vice-Chancellor Sir, the word "security" is as old as the history of man. The security risk/danger to life and property triggered the evolution of various security mechanisms depending on the value of assets, the significance of threats and associated vulnerabilities. The notion of security has changed rapidly over the ages as a result of the development in science and technology.

Security in the Stone Age was developed immediately as humans began to possess things of value (assets) and the need to protect such assets. Then, early primitive security system was set up using rocks, branches, trees and so on to build caves around territories until later when wolves were domesticated to serve as home guards. This transient to the Security of Ancient Egypt with the invention of the first ever lock discovered during the reigns of Khorsabad in the city of Nineveh, the capital of ancient Assyria. This was the genesis of the use of doors and locks which was advanced in so many ways to provide enhanced security. Then, to the era of Security in Ancient Rome in which the Romans later adopted and improved the Egyptian locks by replacing wooden locks with metal which paved ways for better keys. The Romans came up with an early form of padlocks made of bronze to secure their huge assets against intruders. This was followed by the security of the middle Ages, with a number of evolving security measures such as the crossbow, arrow, moat and bridge to block intruders. These were used along with high walls. The Industrial Age and Victorian Era was a time of much progress, discovery and innovation in various fields including security. The Victorians developed more sophisticated locks. This was followed by early alarm systems using magnetic contact on windows and doors with the invention of electricity in the 1800s. The current security age is the 21st Century Digital Security due to the transition from physical assets to digital assets. It can be seen from the historical development of security that, the security approach is a function of the asset's value, nature, environment, technology and culture (Fen, 2023).

**Islamic Provisions and Supports for Ethics and Principles of Information Security**

Mr. Vice-Chancellor Sir, it would interest this august audience to know that, the principles and practices of information and cybersecurity have long been recognised and implemented in the early Islamic civilisation (Sonny, 2010). Thus, the complete guidance provided by Islam can be attested to by the provisions and supports made by the teachings and practices of the Prophet Muhammad (S.A.W) with regards to information security particularly when such provisions predated the current digital era.

According to Yousif (2004), the Companions of the Prophet (S.A.W) employed the most meticulous data collection, verification and validation techniques available to them at that time when compiling the Qur'an in ensuring the authenticity of the compilation. This further attested to the importance attached to information by the Prophet (S.A.W). He was reported to always say "*…that good Muslims are those whose action and speech never harm other people*" (Kitman, 1997), this is a very fundamental ethical standard in information and cybersecurity. This is a further attestation to the fact that Islam has indeed provided standards and principles even for disciplines yet to be discovered.

The significance of information as a valuable asset was equally acknowledged in Islam evidenced by the following hadith: "*Islam does not prohibit Muslims to outsource knowledge and information from anywhere in the world, including from non-believers or from their land because knowledge is considered a missing virtue, which is worth of acquiring wherever a Muslim finds it (narrated by al-Turmidhi, Ibn Majah, al-Baihaqi, al-Tabrani, and Ibn Abi Shaiban*)"

Mr. Vice-Chancellor Sir, all the major metrics used in information and cybersecurity were clearly provided for in the teachings and practice of Islam. These metrics include Confidentiality **(*Sitr*)**: Protecting the privacy and confidentiality of individuals' information is emphasised in Islam. Islamic principles encourage safeguarding personal data and preventing unauthorised access or disclosure;

- **Integrity (‘*Adl*):** Ensuring the accuracy and reliability of information is vital. Islam promotes honesty and truthfulness in all aspects of life, including information management. Protecting data integrity and preventing unauthorized modifications are key considerations;
- **Availability (*Musharaka*):** Ensuring that information and digital systems are accessible when needed and this cannot be overemphasised in Islam. This principle promotes the

availability of information to support decision-making, productivity, and efficient functioning of society; and

- **Ethical Use (*Adab*):** Islamic teachings emphasise the ethical use of information and technology. This includes avoiding malicious activities, such as hacking, spreading misinformation, or engaging in cybercrime. Ethical guidelines are derived from Islamic values, promoting responsible and accountable behavior in the digital era. Globally, the information security management involves the listed metrics in assessing the security level of any net-centric computing. This further justifies the unassuming provisions made by Islam to guide our ways and manners as human, *Allahu Akbar*.

**Information Security**

Information Security (InfoSec) is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) perceived information security as an engagement that revolves around Confidentiality, Integrity, and Availability (CIA) (Calder & Watkins, 2005). These three metrics form the basis of evaluating how secured a net-centric environment is perceived.

In conceptualising Information Security; Asset, Vulnerability, Threat, and Risk must be properly understood. An asset is anything of value to organisations, governments or individuals. By knowing which assets you are trying to protect, as well as their value, location, and exposure; asset owners can be more accurate in determining the time, effort, and financial requirements in securing those assets. A vulnerability is a weakness in a system or its design that could be exploited by a threat. Vulnerabilities are sometimes found in the protocols themselves, especially in the case of some security weaknesses in Transfer Control Protocol/Internet Protocol (TCP/IP). Often, the vulnerabilities can also be found in the operating systems as well as

applications. A threat is any potential danger to assets. A threat is realised when someone or something identifies a specific vulnerability and exploits it. If the vulnerability exists theoretically but is never exploited, then the threat is considered latent. The entity that takes advantage of the vulnerability is known as the threat agent or threat vector. A risk is the likelihood that a particular threat using a specific attack will exploit a particular vulnerability of a system that results in an undesirable consequence (Sheng et al., 2007; Shen, 2014).

Mr. Vice-Chancellor Sir, I must say that nature has mandated us to live in the emerging net-centric computing era. As the range of computer networks expands, the security challenges are also increasing. A typical illustration of this scenario can be deduced from the alarming malware growth rate between 2009 and 2018 as shown in Figure 1. **Malware** is malicious software introduced by attackers for the purpose of gaining unauthorised access and privileges.

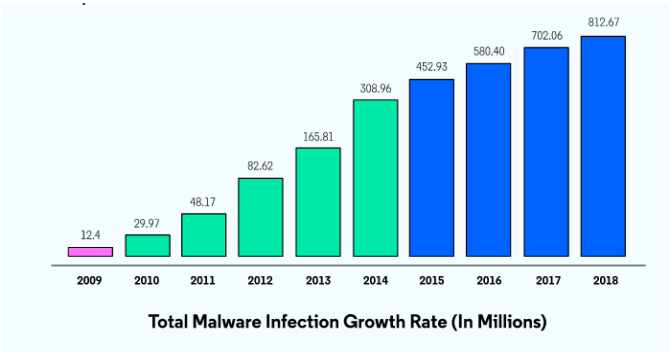


**Figure 1:** Malware growth rate between 2009 and 2018 (Abhishek & Sunil, 2020)

Security attacks are majorly achieved through intrusion into a network i.e., an unauthorised person (attacker) gaining access to a network through some forms of manipulations as described in Figure 2 below thereby acquiring undue privileges for various unethical malicious reasons. Obviously, these attacks do not happen

without existing vulnerabilities in the net-centric operational environments, which are then exploited by the attackers.

**Figure 2:** Network Intrusion Scenario

Mr. Vice-Chancellor Sir, the most common cyber attacks include Malware-based , Phishing , Man-in-the-middle, Denial of Service, SQL injection , DNS tunneling, Zero-day exploits, Password , Drive-by download , Cross-site scripting (XSS) , Rootkits, DNS spoofing, Internet of Things (IoT) , Session hijacking, URL manipulation, Cryptojacking, Inside threats as shown in Figure 3.


**Figure 3:** Types of Cyber Attacks (Wallarm.com, 2023)

**Cybersecurity and its Evolution**

Cybersecurity is the practice of protecting systems, networks, and programs from cyber attacks. The attacks are usually targeted at accessing, changing, or destroying sensitive information, financial fraud; or interrupting normal business processes (Carigen et al., 2014; Cybersecurity, 2018; Gordon et al., 2020; Gupal et al.,

2020; Khaleefah & Al-Mashinadi, 2023). Eeffective implementation of cybersecurity measures is challenging today, because of expanded network range coupled with emerging innovative attack techniques. Cybersecurity is one of the leading niches of Information Technology (IT). It refers to the tools, frameworks, techniques, and practices implemented to ensure the security of computing, information and other systems and users is guaranteed. Typical examples of cyber attacks are identity theft, fraud, extortion, malware, phishing, spamming, spoofing, spyware, trojans and viruses, stolen hardware, such as laptops or mobile devices, denial-of-service and distributed denial-of-service attacks, breach of access, password sniffing, system infiltration, website defacement, private and public web browser exploits, instant messaging abuse, intellectual property theft or unauthorised access.

The history of information and cybersecurity dates as far back as the 1970s. Prior to this time, only passwords were used to access and secure computers (Knowledgehut.com, 2023). The initiator was the Advanced Research Projects Agency Network (ARPANET) which constructed a connectivity network prior to the invention of the Internet. “I'm the creeper; catch me if you can!” was printed using a program developed by Bob Thomas, an ARPANET developer, by means of Personal Computers (PC) connected to the network. For the first time, this program switched from one machine to another by itself. This was the first computer worm recorded in the history of cybersecurity. Thus, the emergence of network connectivity for sharing information and resources was the origin of cybersecurity. Later, Ray Tomlinson, an ARPANET researcher developed the first networked mail messaging system. Subsequently, Tomlinson created a program called Reaper that used every tool at its disposal to find and eliminate the creeper worm having understood the pains associated with the innovations (Davis, 2021).

The birth of digital commercial activities in the 1980s triggered increased high-profile attacks and the terms "Trojan Horse" and "computer virus" both made their debut in 1983. Throughout the Cold War, the threat of cyber espionage increased. The official release of the first commercial antivirus programs in 1987 marked the actual launch of cybersecurity (Davis, 2021).

Thus, the Internet saw growth and development of mammoth proportions in the 1990s as the World goes online, ushering in the decade of e-revolutions. Concerns regarding polymorphic viruses started, the DiskKiller malware was introduced by PC, and cybercriminals invented new ways to bypass antivirus. Therefore, Secure Sockets Layer (SSL) was developed in 1995 to secure internet transactions, web browsing, and online data. Again, Netscape later developed the protocol for SSL and followed by HyperText Transfer Protocol Secure (HTTPS), which is widely used today. Relatedly, threats diversify and multiply in the year 2000s as a result of internet growth. The year 2000s marked the beginning of unethical practices in cyberspace such as; card hacking, yahoo assaults, and much more. Today, we are with many sorts of sophisticated attack techniques (Davis, 2021; Shen, 2014). Thus, the larger the network coverage, the higher the security risks. It is worth noting that these security challenges are not enough reason to choose crawling at the expense of jet pace of the digital era.

**Net-Centric Computing**

Net-centric computing refers to the design, development, and use of computing systems and applications that are built on top of network infrastructure, particularly the Internet. This approach emphasises the use of distributed computing resources and services that are accessible through standard network protocols and interfaces (Kelvin & Vladimir, 2009). Net-centric computing enables the creation of complex systems that can be scaled and adapted to changing needs without requiring significant changes to the underlying hardware or software. It also enables the development of applications that can be accessed from anywhere in the world, providing users with greater flexibility and mobility. Examples of net-centric computing include cloud computing, web-based applications, and social networking sites. In all cases, the focus is on leveraging network resources to provide powerful, flexible, and scalable computing solutions. Figure 4 below depicts the basic components of net-centric computing with all the components interconnected through the internet, enabling data and services to be accessed and shared across different devices and locations.

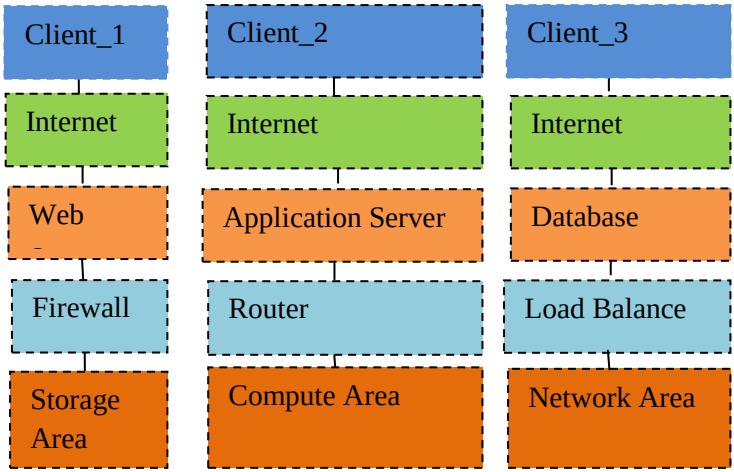


**Figure 4:** Net-centric Computing Environment (Petrova, 2003)

A simple explanation of Figure 4 above will be instructional:

- **Internet:** the network infrastructure that connects all the components together.
- **Web Server:** a server that hosts web-based applications and services accessible through the Internet.
- **Cloud Server:** a server that provides cloud-based computing resources, such as processing power and storage, accessible through the Internet.
- **Database**: a server that hosts databases and provides access to data through the Internet.
- **Web Client:** a client device, such as a desktop computer or laptop, that accesses web-based applications and services through a web browser.
- **Mobile Client:** a client device, such as a smartphone or tablet, that accesses web-based applications and services through a mobile app.

Mr. Vice-Chancellor Sir, the gains are actually more than the pains and the more reasons we need to put in place all mechanisms towards increasing the latency of all potential cybersecurity threats. It moves from mere user-device communication to device-device, device-anything communications

leveraging on the Internet of Things (IoTs) technology. Figure 5 presents a typical IoTs environment. Such an environment places no restriction on sharing of information and resources; this is the main gain here. The actual pain is the cybersecurity challenges which are quite surmountable through consciousness and upholding the ethics, standards and practice of information security management.

**Figure 5:** Internet of Things (IoTs) Environment (Kawam,oto, 2022)

**The Crawling Mindsets**

Mr. Vice-Chancellor Sir, you will agree with me that many people have settled for going traditional ways in their operation in an attempt to avoid the prevailing cyber attacks of the digital era. As a result of this fear, many settle for onsite banking transactions rather than exploring the electronic banking opportunities. They settle for physical meeting at the expense of the virtual meeting platforms, their commercial activities are limited to physical shops, they denied themselves of the virtual learning opportunities and also the job opportunities of the gig economy. In the course of this lecture, I categorised these set of individual to be of crawling mindsets. The implication is that they are denied all opportunities that come with the digital revolution and thereby limit their paces of accomplishments. The price is that they can never attain competitive advantage simply because they chose to operate in the non-compliant pace.

Deconstructing these mindsets, therefore, comes with a lot of efforts in raising their consciousness on the required ethical, cultural and technical solutions to the cybersecurity challenges of

the digital era. Mr. Vice-Chancellor Sir, it is not all about technical preparedness, it involves a radical cultural shift on the perception of information from a mere data to seeing information as valuable assets whose protection becomes sacrosanct. It is such culture that will inform us as individuals to be able to consciously determine the way information is treated depending on its value, nature, environment and sensitivity. It would surprise you sir that many people use their birthday, month and year as their passwords for all authentications forgetting that the details are available on all social media. This will make password hacking easier. This vulnerable attitude was due to lack of consciousness of the current perspective of information and the era we all live at the moment. Efforts to deconstruct the crawling mindsets should, therefore, be a continuous business of the Government and other stakeholders in the information and cybersecurity profession to allow everyone to be on the same page with regards to the security requirements and expectations towards achieving secured operations on the cyber space since crawling in the fast paced digital era is not only retrogressive to the individuals concerned but also to national productivity.

**Disparity between Developing and Developed Digital Nations on Perception of Information**

There exists, a clear disparity in terms of sustainable framework and policies capable of driving the digital economy and this accounted for some of the pains we suffered in this part of the world in navigating the digital era. Mr. Vice-Chancellor Sir, permit me to present a practical experience during my visit to the United Kingdom in 2014. I went to the Imperial College, London to confirm the postgraduate admission status of a younger colleague with copies of her application forms and credentials with me believing that the possession of all those documents was enough justification that I had the candidate's consent. On approaching the Admission Officer, I was told to contact the candidate to send them official email detailing her permission to make such enquiry on her behalf with my details and passport number clearly stated then I should come back the following day for the information. I followed the instruction and on the following day, I was briefed on the status

of her admission. The point here is that the correct perception of information being the cardinal component of the digital era had been long incorporated into their national framework and policies which made their survival in digital era much more seamless. Mr. Vice-Chancellor Sir, only God knows how many people do have access to our internal memos in transits because the Messenger is not aware of the danger. I must say that Nigerian Government equally has a pivotal role to play here. Quite a number of researchers have attested to the need for developing national cybersecurity maturity models and frameworks and awareness to provide necessary guidelines towards achieving secured cyber operations (Li et al., 2019; Shen, 2014; Srinivas et al., 2019; Markopoulou et al., 2019; Petersen et al., 2020; Rabii et al, 2020; Kweon et al., 2021; Kioskili et al., 2023 & Villar et al., 2023).

**My Research Contributions in the Area of Information and Cybersecurity**

Mr. Vice-Chancellor Sir, considering the gains associated with the NCC era, all hands must be on deck to combat the security challenges so as to achieve a secured operations/activities in this vastly connected environment since jettisoning the innovation will amount to crawling when the world is moving at a very fast pace. My research contributions towards combating security challenges of NCC cut across biometric security, security risk assessment, security of card and cardless financial transactions, security in Grid environment, intrusion, spambot/botnet, phishing and DoS detection and cryptography.

**Biometric security**

**Jimoh** and Noshuhada (2009) revealed the promising nature of biometrict authentication technology based of its uniqueness. Biometrics is a method of using a specific human trait (behavioural or psychological) or a combination of traits in identifying a computer user due to the uniqueness of biological traits such as fingerprint, facial recognition, voice recognition, iris scan, finger vein, hand geometry, retina and signature. It has been globally revealed that the human iris is the most unique trait for identification in terms of recognition accuracy despite its implementation challenges. Table 1 presents the performance of

various biometric traits using five basic metrics (recognition accuracy, cost, size of template, stability and security level).

***Table 1:*** *Comparison Table for all Biometrics (Arun & Anil, 2003)*

| S/N | Biometrics | Accuracy | Size of Template | Stability | Security Level |
|---|---|---|---|---|---|
| 1 | Fingerprint | Medium | Small | Low | Low |
| 2 | Facial Recognition | Low | Large | Low | Low |
| 3 | Voice Recognition | Low | Small | Low | Low |
| 4 | Iris scan | High | Small | High | Medium |
| 5 | Finger Vein | High | Medium | High | High |
| 6 | Hand Geometry | High | Small | Medium | Medium |
| 7 | Retina | High | Small | Low | Medium |
| 8 | Signature | Medium | Medium | Low | Low |

Human traits covered in the course of my research include the iris, fingerprint and facial recognition being the most subscribed biometrics.

**Iris scan**

Mr. Vice-Chancellor Sir, iris and retina are two distinct features of human eye used for recognition purposes as shown in Figure 6. However, my research engagement was limited to iris.

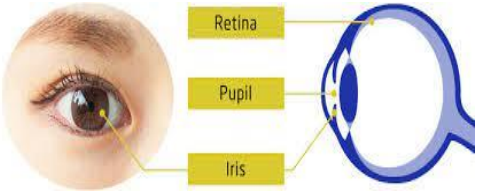


**Figure 6:** Iris Biometics (Arun & Anil, 2003)

The Iris is the coloured, donut-shaped portion of the eye behind the cornea and surrounds the pupil. A person's Iris pattern is unique (even for identical twins) and remains unchanged throughout

human life cycle. Also, covered by the cornea, the Iris is well protected from damage, making it a suitable body part for biometric authentication (Arun & Anil, 2003; **Jimoh** & Norshuhada, 2010a; **Jimoh** & Norshuhada, 2010b). In the course of my research, **Jimoh** and Norshuahada (2009) conducted an experiment to determine the uniqueness of Iris across different races. It was found that, there was no clear distinction between iris across the white and black races and that iris authentication is the most appropriate biometric authentication method for public authentication due to its unique nature of capturing. However, the cost of implementation accounted for its restricted adoption in most parts of the world.

There exist arguments within the literature for what could have caused the delay in the adoption of iris authentication technology, despite its proven excellent performance in terms of recognition accuracy. Subsequently, **Jimoh** and Norshuhada (2010b) investigated the acceptability of iris-based authentication in public domains using the Unified Theory of Acceptance and Use of Technology (UTAUT), where the perception of 351 sampled potential users was quantitatively collected to determine its future successful implementation based on six dimensions of Behavioural Intention (BI) of the UTAUT model (Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Condition, Attitude and Anxiety). The findings revealed that all the dimensions, except anxiety, were major determinants in accepting the use of iris technology for public authentications. Thus, based on the psychological constraints associated with authentication in public domains, Iris appears to be the most acceptable human trait for public authentication. However, its delayed in its full adoption can be traced to the high cost of implementing iris authentication compared with the most patronised fingerprint authentication system.

**Fingerprint**

Mr. Vice-Chancellor Sir, the strength of the fingerprint among all biometric traits is the seamless and relatively low cost of implementation and that accounts for its wide acceptability and adoption. I made quite a number of research contributions in this area particularly in enhancing the quality of fingerprint features towards a better recognition accuracy. Adewole, **Jimoh,** Abikoye, and Ajiboye (2015) proposed stepwise biometric procedures for

managing student's attendance in higher institutions of learning with a detailed review of various algorithms as the basis for enhanced image acquisition, preprocessing and minutiae extraction technique (Adewole, **Jimoh** & Abikoye, 2014) with the aim of selecting the optimum algorithm for the implementation. The procedures involved enrolment, fingerprint matching and attendance management. The results showed that the developed system is capable of reducing students' impersonation during lectures and examinations in higher institutions of learning. Awotunde, **Jimoh** and Matiluko (2012) equally developed a multi-modal ATM authentication approach leveraging on fingerprint and short message code in a cashless society.

**Security Risk Assessment**

Mr. Vice-Chancellor Sir, knowledge of the magnitude of security risk associated with net-centric operations will afford, individuals, organisations and IT Managers the opportunity to pay serious attention in putting up security mitigation efforts. I and my co-researcher have contributed immensely in this area both to the security risk assessment of the software development process and that of the Bring Your Own Device (BYOD). The emergence of BYOD strategy has brought considerable benefits to enterprises. However, secure access control to vital enterprise resources is one of the challenges confronting BYOD adoption. Efforts in filling this research gap led to the development of an Extended Security Risk Analysis Model (ExtSRAM) that combined the concepts to evolve a risk-based and context-aware model to mitigate access control challenges in BYOD. The developed model comprised three blocks, including static risk analysis, user contextual profiling, and risk computation. The developed ExtSRAM utilised the Bayesian network to model user contextual profile and static enterprise risks. Again, the model was formulated on six assumptions for it to be realistic for the BYOD strategy. Theoretical validation of ExtSRAM justified its soundness and completeness in estimating security risks for dynamic access control with accuracies of 91.5%, 97.1% and 80% for three distinct email usage scenarios (Ganiyu & **Jimoh**, 2018a; 2018b &2021). This shows that the model can accurately

measure associated security risks of the device to be able to make an informed deployment decision.

Mr. Vice-Chancellor Sir, now focusing on the security of software development as a process, believing that the quality of the end product (software applications) largely depends on the process. Security Risk Assessment (SRA) of Software Development Life Cycle (SDLC) as a single combined process does not provide an extensive SRA at each phase of SDLC process leading to the development of unsecured software prone to attacks. Therefore, this informed the development of an SRA model for each phase of SDLC in a joint research effort. We implemented the Adaptive Neuro-Fuzzy Inference System (ANFIS) SRA model for each phase of SDLC using the risk factors identified and validated for each phase. The simulation results showed for each of SDLC that the best simulation was achieved using 80/20 for the requirement, integration and operation phases, while 70/30 for the design and implementation phases with an accuracy of 98.2%. Also, the evaluation of the SRA model based on 20% and 30% test datasets for each phase showed that the model with low error rates performed better with an accuracy of 87.9%. Thus, the SRA model for assessing security risk at each phase of SDLC provided a more secured software development process than SRA as a single combined process of SDLC (Olusanya & **Jimoh**, 2018 & **Jimoh** et al., 2022).

Another way of attacking any software is through the database using SQL injections. Researchers have proposed many approaches to mitigate SQL injection attacks. However, many of these techniques only detect very few attack types among the seven most popular attack types. In filling this gap, Olalere, Raji, Idris and **Jimoh** (2018) developed a Naive Bayes-based pattern recognition model for detecting and categorising SQL injection attacks. The developed model was trained and evaluated with 16,050 instances of datasets from both vulnerable and non-vulnerable web pages. The findings showed detection and categorisation accuracy of 98% and 99% respectively reflecting a better performance compared to base models. Thus, the model was considered suitable for measuring the vulnerability of any software application to SQL injection attacks.

**Security of Card and Cardless Financial Transactions**

The alarming financial frauds arising from digital banking initiatives have triggered the interest of researchers in information security to proffer possible ways of mitigating such risks associated with electronic banking systems. **Jimoh** and Babatunde (2014) developed a prototype of an enhanced Automated Teller Machine (ATM) authentication using Short Message Service (SMS) verification. The developed prototype was tested by Ten (10) respondents who were users of ATM cards and the data collected was statistically analysed. The findings showed a promising mitigating impact of ATM transaction-related frauds.

Mr. Vice-Chancellor Sir, one of the achievements of ubiquitous computing is the contactless payment systems which eliminated all payment barriers to e-commerce. This does not mean that it is free of cyber attacks. In ensuring enhanced security of contactless transactions on the POS terminal, Yusuf & **Jimoh** (2018) modelled a system with a strong two-factor authentication mechanism using both PIN and Fingerprint. In maintaining the privacy of the biometric templates, algorithms were developed for secured storage and matching of fingerprint templates on contactless smart cards using Public-Key Infrastructure (PKI), cryptographic primitives and Match on Card (MoC) technique, which provided privacy, confidentiality, integrity, mutual authentication and non-repudiation of the fingerprint template. The use of PIN and Fingerprint Authentication System (FAS) provided a strong two-factor authentication mechanism in the proposed system with False Acceptance Rate (FAR) of 0.13% and a False Rejection Rate (FRR) of 0.44%, which are within acceptable standards for the security performance of biometric systems (Yusuf & **Jimoh**, 2018 &Yusuf, 2020).

**Security in Grid Environment**

One of the advantages of the Grid environment is the optimization of resources by reducing the cost of procuring several computing units. However, there are security challenges associated with the implementation of such an innovative and cost-saving computing environment. As part of my research contributions, some of the issues arising in the Grid environment which include security, quality of service, load balancing etc. were addressed by developing

an enhanced scheduling algorithm in a grid environment to ensure the survival of processing jobs in the presence of processor crashes and thereby satisfying availability (A) which is one of the three fundamental metrics used in information and cybersecurity. A modified ant-colony algorithm with checkpoints was adopted in the design. It was revealed that critical jobs spent more time check-points than non-critical jobs. Also, the overall interval checkpoint made in all computing resources history was improved with 89% computation saving 91% of jobs from re-computing (Faki & **Jimoh**, 2015 &2017).

Similarly, Abdulraheem, Tomori, **Jimoh** and Salimonu (2016) equally developed an authentication and authorisation control in a computational Grid environment by using fingerprint minutiae features and attribute-based access control. The model was developed by hybridising fingerprint biometrics and Attribute Based Access Control (ABAC) for authenticating and authorizing computational grid users based on attributes of the users for computational grid resources. It was revealed to be a reliable authentication solution in a grid environment.

**Intrusion, Spaming, Phishing and Denial of Service Detection**

Mr. Vice-Chancellor Sir, intrusion, spaming, phishing, and denial of service are serious security issues in Net-centric computing environments where a non-authenticated user (intruder) across a computer network gains undue access to the network for any of the nefarious reasons and this area has attracted a lot of research attentions (Sheng et al., 2007; Borky et al., 2019; Carlton, Levy & Ramim, 2019; Shuhal et al., 2022; Katagiri, 2023; Masi et al., 2023 & Mijivil et al., 2023).

The Net-centric computing environment resulted in complexities in detecting possible intrusions across the network due to expanded network coverage, in filling these research gaps, I jointly developed an enhanced Deep Neural Network (DNN) enabled by Cuckoo Search Algorithm (CSA) for intrusion detection in Wide Area Network (WAN) (**Jimoh** et al.,2022). Similarly, Balogun and **Jimoh** (2015) developed a hybridised anomaly intrusion detection system using Decision Tree (DT) and K-Nearest Neighbour (KNN) where node information was determined according to the rules generated by the DT. The node information

(as an additional attribute) along with the original set of attributes was then passed through the KNN to obtain the final output with the goal of determining whether the node information provided by the DT is capable of improving the performance of the KNN. A performance evaluation was carried out using a 10-fold cross-validation technique on the individual base classifiers (decision tree and KNN) and the developed hybrid classifier (DT-KNN) using the KDD Cup 1999 dataset on WEKA tool found to demonstrate better accuracy and efficiency compared with the individual base classifiers (decision tree and KNN). Similarly, a hybrid intrusion detection framework for optimum usage of multi-agents (mobile) for the detection of intrusion across network nodes was developed using two comparators (Mustapha & **Jimoh**, 2016; Mustapha, **Jimoh**, Nwaiwu & Alimi, 2008) where graph theory was used for mobile agent assignments to various nodes within a network system towards optimising the mobility of mobile agents across the network nodes and thereby improving the intrusion detection rate as well as its accuracy. The framework proved to be of better efficiency with respect to time of detection, storage space and reduction of network congestion.

In the same spirit and in a joint research efforts, with the aim of enhancing the intrusion detection process through effective feature selection and classification, we developed an enhanced feature selection and classification towards accurate detections of attack(s) in network traffic. We employed an optimised Principal Component Analysis (PCA) using Particle Swarm Optimisation (PSO) to optimally select relevant features from the principal space of PCA in order to determine relevant features for the classifier. The results obtained were passed into the misuse detector using C4.5, the first-level classifier, to classify the network traffic into normal and attack. The "assumed" normal traffic was further passed to the anomaly detector, the second-level classifier using a Support Vector Machine (SVM) for the detection of a new attack that the misuse detector has not previously detected. Experiments replicated on intrusion NSL-KDD and KDD CUP99 datasets at **75%** training and **25%** testing for the raw dataset, reduced PCA and optimized PCA_PSO. The results showed that enhancing the feature selection phase and classification method reduces the false alarm and

improves the system's ability to detect zero-day attacks (Folorunsho & **Jimoh**, 2017& Folorunsho, Adebola & **Jimoh**, 2022).

Mr. Vice-Chancellor Sir, the emergence of the Internet of Many Things (IoMT) also called for increased network range and thereby further expanding the magnitude of security threats due to the limitless sharing of information and computing resources. The gains always come with associated security pains and combatting the security challenges becomes necessary, I and my co-researchers developed a new approach to intrusion detection in IoMT systems using deep learning techniques with a specific interest in healthcare systems being the IoMT system's most patronised domain. The model is capable of detecting intruders during data transfer, allowing for efficient and accurate analysis of healthcare data at the network's edge. The performance of the model was tested using a real-time NF-ToN-IoT dataset for IoT applications comprising telemetry, operating systems, and network data. The performance evaluation compared with existing intrusion detection models with the same dataset showed a better detection accuracy of 89.0% (Awotunde, Abiodun, Adeniyi, Folorunso, & **Jimoh**, 2022).

Many attackers engage in unethical mission to deny individuals or organisations access to certain computing-related services just to claim they have control over them. This is referred to as a Denial of Service (DoS) attack and this audience could recall that this University also experienced such ugly incidence at a time with very serious implications on University's core processes. In an attempt to contribute to the research efforts in mitigating this form of attack, I with my co-researchers developed a Network Traffic Analysis System named F-NTAS for detecting Denial of Service (DoS) attacks based on Random Early Detection (RED) algorithm (Nudunagu, Fadayomi, Ganiyu & **Jimoh**, 2019). The system can automatically sniff a network, capture live packets, dumps packet traffic to file, visualise network traffic and monitor packet traffic characteristics. Practically, F-NTAS was used in real-time to capture and analyse internet traffic for probable DoS attacks. Interestingly, results obtained from the system demonstration revealed that network traffic is a randomised sinusoid sequence and the characteristics of the traffic could distinguish normal traffic from a malicious one to detect imminent DoS attack.

Mr. Vice-Chancellor Sir, due to the importance placed on network intrusion in the emerging ubiquitous computing environment, I with one of my postgraduate students explored the process of using the human body to fight Pathogens and how that process can be borrowed to improve the security of Net-centric information and resources (Salau-Ibrahim & **Jimoh &** 2017; 2020). Two algorithms in the domain of computer immunology well suited for anomaly detection (Negative Selection and Dendritic Cell algorithm) were employed. The findings revealed that the accuracy obtained for the hybridised algorithm outperformed the two algorithms when used separately. The hybridised algorithm, Negative selection algorithm and Dendritic cell algorithm achieved detection accuracies of 97.93%, 71.70% and 96.77% respectively. The implication of this is that with high detection accuracy, many computer threats are going to be latent.

Similarly, I jointly carried out a study that focused on botnet behavioural analyses through application of machine learning algorithms for botnet malware detection. Leveraging on the limitation of signature-based botnet detection approaches with high false positive rates and lack of real-life datasets and high-class imbalance problem as well as heterogeneous data types in the dataset. We dveloped an innovative pre-processing techniques and feature handling to achieve improved botnet identification models from the real-life, high-class imbalance dataset. After extensive feature pre-processing and feature engineering, two different ensemble machine learning models were built for botnet identification. The first model was based on the bagging technique while the second one was based on boosting approach. The models were evaluated using accuracy, precision, recall, f1-score, and false positive rate as metrics. The findings revealed better performance for both RF-based and Adaboost-based Botnet detection models (RF-based: Accuracy 99.68, Precision 99.33, Recall 99.56, F-Measure 99.24, FPR 0.03), (Adaboost-based: Accuracy 99.76, Precision 99.67, Recall 99.75, F Measure 99.46 and FPR 0.02) (Oyelakin & **Jimoh**, 2019,2020a, 2020b & 2021).

Similarly, Balogun, Mojeed., Adewole, Akintola, Salihu, Bajeh and **Jimoh** (2021) developed an Optimised Decision Forest (ODF) for website phishing detection using a Genetic Algorithm

(GA) for the selecting optimal diverse individual trees in a forest to generate an efficient sub-forest. Specifically, accurate and diverse trees from a decision forest were passed into GA as an initial population to generate a more robust forest with high efficacy. The performance of the developed ODF was evaluated using three phishing datasets from the UCI repository. Findings from the experimental results revealed that ODF performed better than selected baseline classifiers. Particularly, ODF recorded a high detection accuracy (98.37%), AUC (0.999), f-measure (0.98), and MCC (0.967) values with a low false-positive rate (0.016). In addition, ODF outperformed some existing ML-based phishing attack models. Additional effort towards enhanced website phishing attack detection was the development of a Functional Tree (FT) based meta-learning model for detecting phishing websites though an empirical analysis of FT and its variants (Balogun et al, 2021). The developed FT-based meta-learners were found to be effective in detecting legitimate and website phishing with an accuracy of 98.51% and a false positive rate of 0.015. The approach was, therefore, considered promising approach in improving the detection of websites' phishing attacks.

Taking the research further, Balogun, Adewole, Bajeh and **Jimoh** (2021) developed a Cascade Generalisation based Functional Tree (CG-FT) for website phishing detection considering variants of FTs, a hybridisation of multivariate decision trees and discriminant function using constructive induction. Logistic regression was employed for splitting tree nodes and leaf prediction, unlike the conventional decision tree that simply split nodes based on the data. Three datasets with varied instance distributions, both balanced and imbalanced, were used in the empirical investigation of the performance of the developed CG-FT. The results showed that FT has improved performances over some selected baseline classifiers. Relative to FT, the CG-FT techniques showed improvement in the detection of phishing attacks with Area under the Curve (AUC) and True Positive rate (TP-rate) ranging from 98–99.6% and 92–97% respectively in the datasets. The use of FT and its hybridisation with cascade generalisation (CG-FT) showed an improved performance in mitigating website phishing attacks.

Similarly, in joint research efforts, we developed a hybridised rule-based URL phishing detection model based on combination of machine learning-based and rule-based approaches to detect phishing URLs. The machine learning-based approach involves feature extraction, selection, and classification using the Random Forest algorithm. The rule-based approach involves the extraction of features such as domain name, IP address, and SSL certificate information to create rules for identifying phishing URLs. The performance of the model was evaluated using accuracy, precision, recall, and F1 score. The results showed that the hybrid model outperformed other existing phishing detection models in terms of accuracy and F1 score with accuracy of 0.9453 and 0.9908 respectively. It was then concluded that a combination of machine learning and rule-based approaches can improve the accuracy of phishing URL detection. Therefore, the rules generated from the hybridised algorithm are capable of identifying phishing links in real-time with a reduction in false alarms (Adewole, Akintola, Salihu, Faruk & **Jimoh**, 2019).

In addition, Adegbola, Folorunsho, Salau-Ibrahim and **Jimoh** (2022) developed a hybridised approach for the classification of web traffic using source-content classification leveraging on behavioural features and semantic analysis of the content requested within a session as a means of web robot detection using a web access log. The two features were pre-processed to reflect user browsing sessions and further divided into 60% for training and 40% for testing. We then introduced additional three coherent features (session text coherence, session word relatedness and session topic coherence) for measuring every aspect of the content of the web page. A replication was then performed on five randomly split datasets for behavioural, semantic and combined features. The study revealed 7568 unique sessions with 6993 humans, 558 spambots and 17 non-spambots; session text coherence (STC), session word relatedness (SWR) and session topic coherence (ST) were functionally expressed as STC = sw/(n*m), SWR = k/(n*m), and ST = c/(n*m) respectively, where **n** represents the number of relevant topics, **m** is the number of top words in each topic, **sw** represents the sum of weights, **c** is the count of unique topics and **k** denotes the count of the unique word. The hybridised

features performed effectively with an accuracy of 93.67% compared to the individual features. This provided a more accurate model for spambot detections.

Mr. Vice-Chancellor Sir, when we talk of spam attacks, social media are not excluded just like any other web applications, in providing necessary contributions to the security of posts in social media, **Jimoh**, Oyelakin, Olatinwo, Obiwusi, Muhammed-Thani and Ogundele (2022) conducted an experimental evaluation of two ensemble learning models for Twitter spam classification involving publicly available dataset on Twitter spam studies in four different groups with different Twitter spam evidence. Exploratory analysis of the datasets was carried out, one at a time. Thereafter, a label encoding technique was used to handle the categorical features. Two tree-based ensemble learning algorithms namely: Random Forest and Extra Trees algorithms were selected for the development of the hybridised Twitter spam detection models. Each set of the dataset files was used for the training and testing of the model. The performances of the Twitter spam detection models recorded better performances in terms of accuracy, precision, recall and f1-score.

Similarly, Adewole, **Jimoh,** Akintola and Abikoye (2018) developed a framework incorporating 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 in the Twitter environment. The risk assessment function was formulated to compute the risk score from the outputs of two stream-based classifiers. The streaming K-means algorithm was carried out at the clustering stage to detect spam campaigns. Experimental results demonstrated enhanced accuracy and scalability of the developed ensemble framework.

Mr. Vice-Chancellor Sir, phishing/spaming attacks also occur in Short Messages Services (SMS) where fraudulent text messages are sent to deceive users into disclosing sensitive information. In addressing this security challenge, **Jimoh**, Adewole, Aderemi and Balogun (2020) investigated the use of Unigram and Bigram features for short messages spam detection. The study was conducted using a dataset of SMS messages with various machine

learning algorithms that were trained and tested with different combinations of unigram and bigram features. The results showed that the use of both unigram and bigram features improved the performance of the classifiers compared to using only unigrams or bigrams. We later evaluated the impact of feature selection techniques and found that the use of chi-squared feature selection improved the performance of the classifiers. It was then concluded that the combination of both unigram and bigram features significantly improve the accuracy of short message spam detection. Akande, Gbenle, Abikoye, **Jimoh**, Akande, Balogun and Fatokun (2022) developed a new mobile application called SMSPROTECT that automatically detects smishing attacks and alerts mobile users of potential security threats. The model used carefully selected rules to analyse the retrieved message and asserts possible unusual phishing patterns. The result of the analysis was then forwarded to the mobile application through the developed Application Program Interface (API). The final decision to retain or discard the spam depends on the user's notification.

**Cryptography (Encryption and Decryption)**

Mr. Vice-Chancellor Sir, another means of securing information across a network is by making the original messages (plain) in transition meaningless to attackers by converting the original message to an encrypted (cypher) text through encryption by the sender to be decrypted back to plain text by the receiver. In contributing to the security of computing operations in the Internet of Things (IoTs) environment, through a collaborative research efforts with my co-researchers, we developed lightweight cryptography based on the Tiny Encryption Algorithm (TEA) for an IoT-driven setup to enhance speed benefit from a software perspective rather than hardware implementation. The proposed algorithm was used to reduce the time for encryption in the IoT platforms and to preserve the trade-off between security and efficiency. In terms of memory use, execution time, and precision, our algorithm proved to be more efficient in IoTs environment (Abdulraheem, Awotunde, **Jimoh** & Oladipo, 2021 & Awotunde, **Jimoh**, Folohunsho, Adeniyi, Abiodun & Banjo, 2021).

Significant research efforts were equally made in the area of encrypting multimedia (video) messages across the internet. In a

joint research efforts with a postgraduate student of mine, a video encryption algorism using Residue Number System (RNS) was developed to secure video transmission across a computer network (Babatunde, **Jimoh** & Gbolagade, 2016 & Babatunde, Babatunde, **Jimoh**, Abikoye & Isiaka, 2017). Another significant contribution in the area of multimedia security was the development of a Deep Fake detection and classification model using five-layered Convolutional Neural Networks (CNNs). Once the model recovered the face region of the video frames, features were extracted from these faces using the CNN improved with ReLU. The DeepFake-detection-influenced video, with CNN enabled with ReLU were employed to ensure the model correctness while retaining an appropriate weight. The performance evaluation of the developed model from experimental results under real network diffusion conditions showed prediction rate of 98% for DeepFake films and 95% for Face2Face movies. The recommended model outperformed other CNN-based systems like Meso4, MesoInception4, Xception, EfficientNet-B0, and VGG16 with an accuracy rate of 86% (Awotunde, **Jimoh,** Imoize, Abdulrazaq, Li & Lee, 2022).

As part of my contributions in ensuring efficient encryption/decryption of sensitive messages across computer networks, a modified blowfish cryptographic system was developed using a 128-bit block size, a 128-bit key and a new F-function formula was derived (Gbolagade & **Jimoh**, 2017). The modification was also done on the original structure by using the # function to replace XOR thereby enhancing the security. The algorithm's performance was evaluated based on time, and avalanche. Upon testing, the modified blowfish scheme demonstrated better efficiency with regards to key generation, encryption, and decryption at an average of 26.99ms, 1651.83ms, and 2765.04ms respectively compared to blowfish with 21.65ms, 1297.76ms and 2176.59ms due to block size difference. Applying a 128-bit block size enhances the security strength by reducing the chances of having duplicate blocks that may reveal the information. The modified Blowfish is faster compared to Twofish with an encryption and decryption average time of 2418.08ms and 4002.70ms. The added derivation improved the avalanche of the modified blowfish. Blowfish achieved 95.14% while modified

Blowfish attained 99%. The proposed algorithm can be used to secure large files to reduce the processing clock cycles.

In cryptography, the efficiency of the key generation approach is central to the efficiency of the entire cryptography process. **Jimoh**, Olatunde, Suleiman and Muhammed (2017) equally conducted performance analysis of public key cryptosystem using multiple data, and the findings provided the basis for selecting appropriate method depending on the nature of data. In the same spirit of optimising the cryptographic process, Omolehin, Abikoye and **Jimoh** (2008) developed a data encryption and decryption algorithm using a 4-row Rail Fence Cipher. The algorithm was designed to demonstrate the possibility of developing cryptographic systems using a 4-row rail cipher thereby increasing the security through increased efforts in key generation and management towards achieving higher reliability, confidentiality and integrity of the process which was actually achieved. Taking the research further, Omolehin, Abikoye and **Jimoh** (2009) developed an algorithm that can encrypt and decrypt data using a Modified Rail fence Cipher. The modification included 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. This ensured that the key is kept confidential at all times.

Naturally, some communication channels are meant to be insecure and for one reason or another we are bound to operate in some of these channels. In ensuring secured communications on such channels, **Jimoh**, AbdulRaheem, Salimonu and Mejabi (2017) developed an elliptic curve cryptosystem model for securing communication across the unsecured channel.

Mr. Vice-Chancellor Sir, just recently, through collaborative research efforts with my co-researchers, we evaluated two well-known cryptographies (RSA and ElGamal) using mixed data such as binary, text, and image files. CPU internal clock was used to obtain the time complexity used by both algorithms during encryption and decryption. The algorithms used CPU internal memory to obtain memory usage during the encryption and decryption of mixed data. Evaluation criteria such as encryption time, decryption time, and throughput were used to compare the

algorithms. The results revealed that RSA was a time-efficient and resourceful model, while the ElGamal algorithm was a memory-efficient and resourceful algorithn (Adeniyi, Imoize, Awotunde, Lee, Falola, **Jimoh** & Ajagbe, 2023). The findings will avail future researchers in cryptograpgy domain the opportunity of an informed choice of either of the algorithms based on their priorities.

**Postgraduate Supervision**

Asides numerous undergraduate projects supervised, I have been able to successfully supervise forty (40) master's and fifteen (15) Ph.D. theses with 80% in the area of information and cybersecurity with a good number of them occupying leadership positions in various organisations. I am currently supervising six (6) Ph.D. and Masters theses.

**Ongoing Research**

In a bid to reposition the University as the cybersecurity hub in Nigeria and Sub-Shara Africa, I am currently coordinating a team of experts to develop a grassroot-based security intelligence and escalation system in an effort to combat the national insecurity. The research is at incubation stage with Ilorin South Local Government as the initial scope. Figure 7 shows a picture of members of the research team and all traditional rulers in Ilorin South Local Government during an interaction.

**Figure 7:** Interactions with traditional Rulers in Ilorin South Local Government

**Award of Research Grants**

Mr. Vice-Chancellor Sir, I have either as lead researcher or collaborator attracted the following research grants:

1. Akorede, M.F., Olawuyi, N. Y., Femi, E., Ayeni, A.A., **Jimoh, R.G.** (2018) - Real- Time Demand Response Algorithm for Minimising Industrial Consumers Electricity Billing, 2015 – 2017, Institutional Based Research Fund (IBRF), TETFUND, (**=N=1, 200,000:00**); Completed.
2. **Jimoh, R.G.**, Abisoye, O.A. & Uthman, M.M.B (2016 - 2019). Hybridized Malaria Prediction Model for Farmers in Minna Niger State, Nigeria, 2016 – 2018 Institutional Based Research Fund (IBRF), TETFUND, (=N=1, 000,000:00); Completed.
3. Olasehinde-Williams, F. A. O, Yahaya, L. A, **Jimoh, R. G.**, Olajide, S. B., Uyanne, E. O., Sanya, E. O. & Owolabi, H. O. (2016 - 2019): Development of Brin-Friendly Learning Approach, Institutional Based Research Fund (IBRF), TETFUND. (=N=1, 600,000:00); Completed.
4. Raji, B. A, Adeoye, M. K., **Jimoh**, **R. G**., K. Eifediyi & O. Ayinde (2022). Development Of Soil Health Dataset For Upscaling Specialty Fertiliser/Soil Management In Kwara And Niger States For Enhanced Staple Crops Production, National Research Fund (NRF), TETFUND, (=N=41,000,000:00); On-going.

**Contributions to Teaching and Professional Development**

Over the years, I have taught several courses at both undergraduate and postgraduate levels in the Department of Computer Science and I have equally serviced other Departments such as Library and Information Science, Telecommunication Science, Business Administration, Educational Management, Educational Technology and Nursing Science in many ICT-related courses. I muted the idea of the Professional Masters Programme in Information Technology (M.IT) housed by Ilorin Business School to allow our professional colleagues in the industries have the opportunity of advancing their educational career seamlessly. I played a major role in the development of the curriculum for the programme. My alignment with the reality of the emerging teaching paradigm driven by ICTs to motivate self-learning potentials of the 21st century learners as a way to achieving desired transformation in learners through life-long learning inspired my teaching philosophy.

Mr. Vice-Chancellor Sir, I have equally contributed immensely to the growth and development of computing profession in Nigeria. Infact, I served as Chairman of the Kwara State Chapter of the Nigeria Computer Society (NCS) between 2013 and 2018. My sacrifices and contributions during the period earned me the highly celebrated NCS presidential award in 2019. I equally served the education and manpower development committee of the Computer Professionals Registration Council of Nigeria (CPN) for four years as a member of the Council where I was actively involved in the review of the curriculum for the CPN professional examinations and certifications. As a member of National Executive Council (NEC) of NCS, I equally served in several committees and same goes for many interest groups of NCS such as Nigeria Information Technology Professionals in Public and Civil Service (NITPPCS), Academia in Information Technology Profession (AITP) and Information Technology and Systems Security Professional (ITSSP) as a member of NEC till date.

**My Contributions to the Growth and Development of the University**

Mr. Vice-Chancellor Sir, as an Alumnus of the University coupled with my passion to see a better University of Ilorin at all times, I have had the privilege to serve and contribute to my alma mater in many ways. With the kind support of my then Dean, Prof. L. O. Aina, I took it upon myself to seek the intervention and support of NITDA on ICT which gave birth to Computer Laboratory we now enjoy and making the computer science as practical-based discipline more enjoyable to learners and instructors. To the glory of God, it was a fruitful venture with NITDA's intervention of 25 million naira worth of desktop computers and ICT equipment in 2018 which assisted in setting up a dedicated Computer laboratory for practical courses. In similar vein, having realised the need to acquire required expertise in computer security, I approached International Business Machines (IBM) for their free educational service to train, examine and certify staff and students of the University in the area of security this we have long achieved to the glory of God and benefits of mankind since 2015.

As Acting Head of the Department of Computer Science between 2013 and 2015, I was able to secure professional accreditation for the programme for the first time in the history of the Department. I equally facilitated professional membership of not less than eighty percent of the staff through professional executive development programme here at University of Ilorin. As the Acting and Substantive Dean of the Faculty between 2017 and 2021, I was able to position the Faculty as the flagship of the University particularly in the area of ICT development. I organised the maiden Faculty's International Conference on ICTs for National Development and its Sustainability. All these ventures increased the visibility of the University nationally and internationally. In advancing my community service, I was equally privileged to serve our Union, the Academic Staff Union of Universities (ASUU) at the branch level for two consecutive terms as the Branch Treasurer between 2015 and 2019 and it was one of the very challenging moments though an experience gathering opportunity. I thank God for the wisdom to jealously deliver the mandates without betraying the trusts. My appointment as the Pioneer Deputy Director of Ilorin Business School also gave me the opportunity to contribute to the development of the school despite all odds.

I have equally served in many University committees too numerous to mention with significant contributions. The most recent among them, Chairman, University of Ilorin Digitalisation Committee deserves mentioning. Mr. Vice-Chancellor Sir, you will agree with me that my endeavours at the University of Ilorin since recruitment to date have not been limited to academic work alone, I have given, and by God's grace will continue to give, my best to the Better-By-Far University. Over the years, I had the privilege to serve several Institutions and Organisations within and outside Nigeria in different capacities as External Assessor/Examiner/ Technical Adviser. Just recently, I was appointed the Director Computer Services and Information Technology (COMIST), the ICT unit of the University.

**Conclusion**

We must come to understand the reality that integration of ICTs within a Net-centric computing environment for seamless operations is not contestable except we settle for crawling at a jet

age with serious implications of not catching up with our competitors and the rest of the world. Thus, crawling in the digital era when the rest of the world is moving at a very fast pace can never be an acceptable option. However, the limitless sharing of information and information resources due to the expanded network accounted for the rapidly increasing security threats.

Thus, the option left with us is to wake up to the calls and find a way of eliminating or reducing the cybersecurity challenges associated with operations in the emerging Net-centric computing environment through adoption of information security management ethics and standards coupled with implementation of suitable cybersecuty techniques capable of achieving reliable authentication, security risk mitigation, secured sharing of information and information resources, intrusion-free operations and integrity-proven cyber activities.

**Recommendations**

I wish to recommend as follows that:

1. Iris biometric authentication being the most accurate biometric authentication approach in public domains, should be encouraged through reasonable investment by Government to support the use of the biometric technology in public places;
2. the use of fingerprint authentication should be encouraged in all educational processes within the university system to prevent cases of impersonation and campus insecurity. Students biometrics can be easily collected from the JAMB's Central Admission Processing System (CAPS);
3. detailed assessment of security risk associated with software applications and ICT devices should be a precondition to adoption and integration of computer systems towards mitigating likely security attacks;
4. sophisticated authentication methods should be encouraged to guarantee security of both card and cardless financial transactions so as to prevent all associated financial frauds;
5. adequate research attentions should be given to security of operations in Grid-based computing environment towards sustainable quality of service in the Grid environment;

6. Government should fund commercially viable research outputs on intrusion, spam, phishing and denial of service detection and prevention to guarantee safe and secure net-centric activities;
7. Government should double its efforts and provide funds for aggressive awareness on the need for cultural adaptation to the emerging digital era with specific attention geared towards the use of the three basic languages in Nigeria;
8. NITDA's developed data protection and privacy regulations should be well communicated to all Nigerians in three basic Nigerian languages towards achieving desired inclusiveness in rasing consciousness of all citizens on general information security ethics and practice;
9. the culture of investments in the area of cybersecurity should be improved and subsequently adequate budgetary allocations be made by public and private organisations;
10. Organisations at all levels should identify and subsequently categorize their digital assets based on their values and security risk to determine the level of cybersecurity investment;
11. expected prominence should be given to information security management in the ICT policies of organisations at all levels towards achieving secured operations in the digital era;
12. a dedicated cybersecurity unit should be institutionalised in all organisations (private and public) to drive the expected cybersecurity initiatives;
13. Organisations should hire experts in the core areas of information and cybersecurity with adequate training and retraining given the dynamism of the discipline;
14. cybersecurity specialised programme should as a matter of urgency commence in all higher institutions of learning for effective capacity building and cybersecurity R&Ds;

**Acknowledgements**

Unto the Almighty Allah, without whom all favours are nugatory. Allah says in Quran 2:152, "*therefore, remember Me, I will remember you and be thankful to Me, and do not be ungrateful to Me"It is on this note,* my ultimate appreciation and gratitude goes

to Almighty *Allah* Who only by His mercies made possible my creation, survival, growth, career advancement and academic/ professional breakthrough despite all odds. All glories and adorations belong to Him alone. I say *Al-hamdulillahi Rabbil Alamin*. Mr. Vice-Chancellor Sir, please permit me to publicly akcnowledge some of the people who have played pivotal roles in my life:

To my late father and first mentor, Late Alhaji Olawale Aweda Jimoh who taught me to be resilient, selfless and hardworking. Though you are no more to witness the dividends of your proactive mentorship, your memories and legacies lingers on. May Almighty Allah enlarge your grave and grant you the best of *al-jannat. Aamin*. To my wonderful, caring and supportive mother, Alhaja Nimotallahi Ibiwumi Alake Jimoh, I am indeed thankful to you for not only bringing me into this world but also remained supportive and prayerful in seeing me projecting the name of your darling husband through my enviable career accomplishments. If I have the course to come to this world again with the choice of choosing a mother, no other person is qualified to take your place. I love you, Mum. May Allah grant you long life in sound health. *Aamin*.

To my Ph.D. Supervisor: Prof. Dr. Norshuhada Shiratuddin, your care and hospitality made me to feel homely even while away from my loved ones. Is it the granted opportunities to benefit from your numerous research grants as a Research Assistant which was a big soft landing for me as a self-sponsored foreign student without any form of scholarship. Allah really used you for me and there is nothing I can do to pay you back other than continuous prayers and demonstrating such uncommon mentorship traits to all my postgraduate supervisees believing that part of the rewards shall be yours. I pray that Allah will ease all your affairs, grant you long life in sound health to enjoy the dividends of your hardwork and kindness. I am sincerely thankful, Ma.

Permit me to especially appreciate the late Dr. Ahmed Qusamat of blessed memory, a one-time National Chairman of National Republic Conventions whose companion will always continue to linger in my memory. Late Dr. Qusamat was my indirect mentor because I got the inspiration not to relent on my

educational pursuits until attainment of Doctorate degree from him because he was one the most celebrated politicians in my home town and I concluded that it was the Ph.D. that gave him that nitch. You actually inspired me to be a Ph.D. holder. I pray that Allah forgives him of all his sins and accepts him to *Al-Janat Firdous*.

To Professor Shuaib Oba Abdulraheem, a former Vice-Chancellor of this great University and former Chairman Federal Character Commission, the TALBA of Ilorin and our mother Alhaja Taibat AbdulRaheem whom I started working with even as a student of this University. Sir, you have touched my life in so many ways even unknown to you. May Allah grant you long life and sound health. *Aamin.*

To my grand Principal and Mentor, Professor Is-haq Olanrewaju Oloyede, a former Vice-Chancellor of this great University and the current Registrar and Chief Executive, Joint Admissions and Matriculation Board (JAMB), your positive roles on my journey of life are sincerely appreciated, sir. I have enjoyed both the direct and indirect mentorship opportunities from you which were instrumental to my ability to cope even in difficult and challenging situations. I am sure today; you feel fulfilled for facilitating my recruitment into the University. I say *Jazakallahu Khairan*. May Allah continue to bless you and all yours and keep taking you to greater places. I thank our mother Dr. Mrs. Raheemat Oloyede for being a mother always.

To Professor AbdulGaniy Ambali who under his tenure I got promoted to the rank of Associate Professor and he equally found me worthy to be appointed as the pioneer Deputy Director, Ilorin Business School, Ag, Head of Computer Science Department and subsequently the Ag. Dean of the Faculty of Communication and Information Sciences, those opportunities provided the needed platforms for acquiring the required experiences about university administration. May Allah continue to bless you, grant you long life in sound health and lastly to Professor S.A. Abdulkareem whose tenure was a strength gathering moment for me. I say thank you, sir.

To my Principal and current Vice-Chancellor, Professor Wahab Olasupo Egbewole, SAN, appreciating you here is just a formality because you have always been my pillar of supports even before your appointment as the Vice-Chancellor. Sir, you were

among the very few Elders I could see during the turbulent periods as the Dean of the Faculty of Communication and Information Sciences as if it was a crime to aspire in life. Your encouragements kept me going amidst unwarranted moves to pull the entire Faculty down over parochial personal sentiments at the expense of the larger interest of the University. The struggle made me stronger and more pious because I was convinced that the truth shall always prevail and I thanked *Allah* for proving me right. Asides the usual supports and encouragements, you have always given me what I considered rare opportunities to showcase my talents as a seasoned university scholar and administrator right from your days as the Director of General Studies, you gave me the opportunity to drive your idea of Digital Skill Acquisition in the University through the newly approved GNS 312. It was an indication that you are a visionary leader, an innovation initiated by you as far back as 2016 which was just recently introduced by NUC in the new CCMAS. We are truly Better-By-Far. Sir, I pray for a successful tenure, may your vision 1:10:500 be realised in no distant time. May this appointment be the beginning of many good things in your life and above all, may you live long in sound health. *Jazakallahu Khairan.*

To my Professional and Academic Elders in the computing profession, Professors Akinde, Adagunodo, Aderounmu, Sadiku, Osofisan, Uwadia, Chiemeke, Ejiofor, Omidiora, Olabiyisi, Obiniyi, Sodiya, Awodele, Oluwade, Adewale, Owolabi, Ahmed and others too numerous to mention, I say a big thank you for providing the required leadership at different stages of my career advancement. Permit me to single out my wonderful Mentors, Professors Adesola Aderounmu and Musa Isiyaku Ahmed, the Vice-Chancellor, Federal University of Agriculture, Zuru who have contributed immensely to my professional, leadership and academic career advancement.

To my senior and fellow Professor in the Faculty of Communication and Information Sciences, the late Professor Ajibero of blessed memory, wishing you eternal rest, Professors Sadiku, Aina, Isa, Mejabi, Idowu, Azeez, Tella, Oladele and Abikoye, I thank you for all your supports always. Permit me to single out Professor Lanrie Olatokunbo Aina, a former Dean of CIS and former National Librarian for the roles he played towards my smooth career advancement. May you live long in sound health.

To the members of the Computer Science family, University of Ilorin, Professors Oladele, Abikoye, Drs. Ameen, Oladele (Mrs.), Babatunde, Mabayoje, Bajeh, Adewole, Akintola, Hamzat-Usman, AbdulRaheem, Balogun, Salihu, Oladipo, Awotunde, Balogun (Mrs.), Asaju-Gbolagade, Ajiboye, Mr. Balogun, Sadiku, Gambari, Mrs. Olaoye, Adeoye and Adedeji, you have always been wonderful members of one big computing family here at University of Ilorin. I sincerely thank you all. To all members of the CIS family, I thank you immensely for not only electing me as your substantive Dean (2019 -2021) but also supported me in so many ways towards a successful tenure against all odds. I equally thank all my teachers in the Department of Mathematics. All my teachers from the Federal Polytechnic Offa, and all staff of COMIST, I thank you sincerely.

To the leadership of Compatriots, Professors Quadri, Omotoso, Fawole, Okesina, Obaleye, Adeleke, Eke, Wahab-Johnson and all members of Compatriots, I thank you for your support always. I wish to appreciate the leadership and entire members of the University of Ilorin Alumni worldwide with a specific mention of our branch Chairman, Professor B. L. Adeleke whose supports are so numerous to mention here. I commit you to *Allah* for His rewards both here and in the hereafter.

To my Father/Mother-in-law, Sheikh Ismail Abiodun Ashola, Raji, the founder and proprietor of Mahdul-Al-Rahmat Arabic and Islamic Institute, Ishagatedo, Lagos, I really count myself lucky to have you as a replacement for my late father. Thank you for adequately filling that gaps (morally, spiritually and financially) when most needed and Alhaja Ganiyat Raji, your complimentary motherly care and love can never be overemphasized. I count myself lucky to choose my life partner from your wonderful family. May Allah grant both of you a long life in sound health.

To my siblings, Mr. Lawal Gafar, Mr. Ismail Akinsola, Mr. Asimiyu Akinsola, Iya Adeola, Alhaja Olaoti Folashade and Latifat. Thanks for your supports at all times, may Allah continue to sustain you all. To my extended family, my Uncles Alhaji AbdulAzeez Adejumo, Alhaji AbdulAzeez Akinsola, Mr. And Mrs. Famiwaye and many others, stepmothers and Aunties who are too numerous

to mention here. I say *Jazakumullahu Khairah* to you all. Your different supportive roles at various points are greatly appreciated.

Special thanks to all the royal Fathers in attendance with specific mention of the Aragbiji of Iragbiji Land, His Royal Majesty, Oba AbdulRasheed Olabomi, Odundun II, your supports at all times are mostly appreciated sir. *Ki ade pe lori, Ki bata pe lese, ki iru kere pe lowo*, may Iragbiji continue to witness many more good things during your reign. *Aamin*. I equally appreciate my senior colleague in the profession, His Royal Majesty, Oba Professor Adekunle Okunoye, the Eburu of Iba and a Professor of Information Systems at Xavier University Ohio, USA, Sir, I thank you for being supportive always. *Epe fun wa* sir.

Special appreciation to all my spiritual fathers here present and those who are unavoidably absent with specific mention of *Sheikh* AbdulAzeez Arisekola Abojo, Baba n Quran, *Sheikh* Sulaiman Tiamiy Elemo, Late *Sheikh* Sheu Ahmad, the former Chief Imam of Ira, may Allah accept him to Aljanat Fridous, Prof. Abdulsalam AbdulGaniy Oladosu, the former Chief Imam of the University of Ilorin, Prof. Nasir Abdulsalam, the current Chief Imam of the University of Ilorin, *Sheikh* Lukman Isalekoto and lastly my *Sheikh*, my friend and brother, *Sheikh* Mohammad Thoir Abdulsalam Oniwiridi. I say *Jazakumullahu Khairan*.

To all the staff of the University of Ilorin who have rendered one support or another which time may not permit to list here. I say a very big thank you. *Jazakumllahu Khairan*. To my friends within and outside the University: Chief Adedokun Sunday, Alhajis Wole Badmus, Otunba Ayotunde Babatunde, Alhajis Akeem Adejumo, Abdulwasiu Adejumo, AbdulRahman Salaudeen, Shakir Abiodun Oyelami, AbdulGaniy Jemil, Lukman Omotosho, Dr. Wasiu Raji, Barrister Shehu Bashir, Professors Olumide Longe, Abiodun Salman, Juliana Ndunagu, Mohammed Saka Jimoh, Mikhail Olaniyi, Alhassan John Kolo, Toyin Enikuomehin, Olalere Maruf, Kazeem Gbolagade, Caleb Akanbi, Fransisca Oladipo (VC, TAU), Abduljeleel Shittu, Mukaila Aremu (Provost, Kwara COED), Akeem Oyerinde, Masters. Tunde Jimoh, Bode Oyeleke, Adedoyin Taiwo, Dauda Oyewo, Olanrewaju Maruf (MM), Ahmed Jelil Abiodun (GOC), Amubieya Samuel, Engr.Rasak Ahmed, Isiaka Oyewo, Abolade Kazeem, Ayantola Jimoh, and many others who

are too numerous to mention. I thank you all. Permit me to single out a friend and brother from another mother, Dr. Morenikeji Alex AKANMU for standing with me at all times. May Allah spare my life to celebrate you as well. *Aamin*. Majority of personalities mentioned here were partners in the Student Union struggle and we all shared life bonds. The leadership training as a long-serving member and majority leader in the then legislative arm of the Students Union Government as a student, likewise, the k2k group of the Wole Badmus (Wolly Bee) led NANS regime provided a firsthand leadership experience which became much useful in my subsequent leadership positions as a staff of the University. I thank you all. I wish to publicly acknowledge our elder brother and admirer, Alhaji Abdulbaqi Jimoh, your love, supports and encouragements can never be taken for granted. To the leadership and members of the Alumni Associations of *Mahd-Al-Robby* Arabic and Islamic Institute, Abojo, Ikirun; Onanolapo Memorial High School Ikirun, Federal Polytechnic Offa, University of Ilorin Ilorin, University of Ibadan and Universiti Utara Malaysia, I thank you all. I appreciate all members of Ikirun Progressive Union (NIPU) under the leadership of our national President Alhaji Dr. Mustapha for your love always. My special appreciation to the Asiwaju of Ikirun Land, Retired Deputy Inspector General of Police, 'Dewale Ghazali Lawal. My High Chief Onifade Maruf, the ELEMO of Ikirun land.

To my academic sons and daughters: Doctors A. S. Faki, Senior Lecturer & Head of Department of cybersecurity and Information Technology, Bingham University, Karu; S. O. Ganiyu, Lecturer at the Department of Computer Science, Kampala International university, Kampala, Uganda; O. A. Abisoye, Senior Lecturer & Head of Department of Computer Science, Federal University of Technology, Minna, Niger State; A.N. Babatunde, Senior Lecturer, Department of Computer Science, Kwara State University, Malete; I. O. Mustapha, Lecturer and Director of Diploma Studies, Al-Hikmah University Ilorin; Olayinka O. Olusanya, Postgraduate Coordinator, Department of Computer Science, Tai Solarin University of Education, Ijagun, Ogun State; M. O. Lawrence, Lecturer, Department of Computer Science, Baze University, Abuja; J. B. Awotunde, Lecturer I, Department of

Computer Science, University of Ilorin; O. Folorunsho, Post-Doctoral Research Fellow, Unit for Data Science and Computing, North West University, South Africa/Senior Lecturer, Department of Computer Science, Federal University, Oye-Ekiti, Yusuf Abduljelil Olayinka, Assistant Manager, Information Technology Department and Team Lead, e-Naira Project, Central Bank of Nigeria, Abuja; P. O. Adebayo, Lecturer in Department of Computer Science. Federal Polytechnic, Nasarawa, Nasarawa State, T. T Salau-Ibrahim, Former Sub Dean Student Affairs Unit, Al-Hikmah University Ilorin, I. A. Adegbola, Ag. Head of Department, Department of Computer Science, Oyo State College of Education, Oyo; A. M. Oyelakin, Postgraduate Coordinator, Department of Computer Science and Sub-Dean, Postgraduate School, Al-Hikmah University, Ilorin, Ni and Morufat D. Gbolagade, Department of Computer Science, Al-Hikmah, University Ilorin. You are all signatures to my academic accomplishments. See you all at the top, *Insha Allah*.

I specially thank the former Chairman of Library and Publications Committee, Prof. Y. A. Quadri for his editorial assistance. E pe fun wa sir. I also pay special tribute to the present Chairman of Library and Publications Committee, Prof. A. A. Adeoye for making scholarship easy through his editorial versatility. *Jazakumulahu Khairan.*

To the members of my nuclear family, because you occupied a special place in my heart as a result of your special roles and unprecedented understanding of my constraints in the course of my career advancement. The first on this list is no other one but my best friend, confidant, partner, sweetheart, heartthrob and mother of my wonderful children, Dr. (Mrs.) Taibat Bolanle Ayinke Jimoh (Nee Raji). Thanking you here is just official; your appreciation is a life-long engagement for your unconditional love and supports and above all for giving me wonderful children. I love you and will always do. Thank you my better half. My children: Abdulmui'z Opemipo Jimoh, Muheebdeen Abiodun Jimoh, Abdulmujeeb Abisodun Jimoh and Mujeebah Tiwatope Ajoke Jimoh. I love you all and I pray that you shall all be greater than me. *Alhamdulillahi Robili Alamina.*

## References


Abdulraheem, M., Awotunde, J. B., **Jimoh, R. G**., & Oladipo, I. D. (2021). An efficient lightweight cryptographic algorithm for iot security.mIn Information and Communication *Technology and Applications: Third International Conference, ICTA 2020, Minna, Nigeria, November 24–27, 2020, Revised Selected Papers*, 444 - 456.

Abdulraheem, M., Tomori, R.A., **Jimoh, R.G.** & Salimonu, I.R. (2016). Authentication and authorization control in computational grid environment using fingerprint minutiae features and attribute based access control, *Anale. Seria Informatica*, 14(1), 67 – 77.

Abhishek, K. & Sunil, K. N. (2020). cybersecurity against DDoS, Malware, spoofing attacks using machine learning with genetic algorithm, International *Journal of Advanced Science and Technology*, 29(5), 5388 - 5400.

Adegbola, I.A., Folorunsho, O., Salau-Ibrahim, T.T., **Jimoh, R.G.** (2022). Hybridized spambot detection using source-content classification, *Journal of Theoretical and Applied Information Technology*, 100(10),3242–324.

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); 245-263.

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., Akintola, A. G., Salihu, S. A., Faruk, N., & **Jimoh, R. G.** (2019). Hybrid rule-based model for phishing URLs detection. In Emerging Technologies in Computing: *Second International Conference, iCETiC 2019*, London, UK, August 19–20. Proceedings 2 (pp. 119-135).

Adeniyi, E. A., Imoize, A. L., Awotunde, J. B., Lee, C., **Jimoh, R. G.** & Ajagbe, S. A. (2023). Performance analysis of two famous cryptographic algorithms of mixed data, *Journal of Computer Science, 19 (6): 694.706.*

Akande, O.N., Gbenle, O., Abikoye, O.C., **Jimoh, R. G.**, Akande, H. B Balogun, A.O., Fatokun, A. (2022).SMSPROTECT: An automatic smishing detection mobile application, ICT Express, 2022, 9(2), 178 - 186.

Awotunde, J. B., **Jimoh, R. G**., Imoize, A. L., Abdulrazaq, A. T., Li, C. T., & Lee, C. C. (2022). An enhanced deep learning-based deepfake video detection and classification system. Electronics, 12(1), 87.

Awotunde, J. B., **Jimoh, R. G.** & Matiluko, O. E. (2015). Secured automated teller machine (ATM) using fingerprint authentication and short-code message in a cashless society, *Proceedings of the 12th International Conference on Information Technology for Inclusive Development*, 99 - 110, Nigeria Computer Society, 11th – 13th July, 2015.

Awotunde, J. B., Abiodun, K. M., Adeniyi, E. A., Folorunso, S. O., & **Jimoh, R. G.** (2022). A deep learning-based intrusion detection technique for a secured IoMT system. In Informatics and Intelligent Applications: First International Conference, ICIIA 2021, Ota, Nigeria, November 25–27, 2021, Revised Selected Papers (pp. 50-62).

Awotunde, J. B., **Jimoh, R. G.,** Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M. & Banjo, O.O (2021). Privacy and security concerns in IoT-based healthcare systems, The Fusion of Internet of Things, *Artificial Intelligence and Cloud Computing in Health Care*, 105 – 134.

Arun, R. & Anil, J. (2003). Information fusion in biometrics, *Pattern Recognition Letter*, 24(13), 2115 - 2125.

Aura.com (2023). 17 types of cyber attacks commonly used by hackers,hhttps://www.google.com/search?q=Examples+of+cyber+attacks&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiOl-H9zvXAhVhmVwKHQ1DDIoQ_AUoAnoECAEQBA&biw=1366&bih=657&dpr=1

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

Babatunde, A.N., **Jimoh, R.G.** & Gbolagade, K.A. (2016). An algorithm for a residue number system based video encryption system. *Anale. Seria Informatica*, 14(2), 137 – 145.

Balogun, A. O, Kayode S. Adewole Muiz O. Raheem Oluwatobi N. Akande Fatima E. Usman-Hamza Modinat A. Mabayoje Abimbola G. Akintola Ayisat W. Asaju-Gbolagade Muhammed K. Jimoh, **Jimoh, R. G.** & Victor E. Adeyemi (2021). Improving the phishing website detection using empirical analysis of Function Tree and its variants, *Helliyon*, 7(7), e07437.

Balogun, A.O., Mojeed, H.A., Adewole, K.S., Akintola, A.G., Salihu, S.A., Bajeh, A.O., **Jimoh, R.G.** (2021) Optimized decision forest for website phishing detection. In: Silhavy R., Silhavy P., Prokopova Z. (eds) Data Science and Intelligent Systems. CoMeSySo 2021. *Lecture Notes in Networks and Systems, 231*.

Balogun, A. O., Adewole, K. S., Bajeh, A. O., & **Jimoh, R. G.** (2021). Cascade generalization based functional tree for website phishing detection. In Advances in cybersecurity: *Third International Conference, ACeS 2021, Penang, Malaysia*, August 24–25, 2021, Revised Selected Papers 3 (pp. 288-306).

Balogun, A. O. & **Jimoh, R. G.** (20015). Anormally Intrusion detection using an hybrid of detection tree and k-nearest neighbour, *Journal of Advances in Scientific Research and Applications (JASRA)*, 2(1), 67 – 74.

Borky, J. M., Bradley, T. H., Borky, J. M., & Bradley, T. H. (2019). Protecting information with cybersecurity. Effective Model-Based Systems Engineering, 345-404.

Calder, A. & Watkins, S. (2005). IT governance: A manager's guide to data security and BS 77991ISO 17799, ("d edn.). London: Kogan.

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills. Information & Computer Security, 27(1), 101-121.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).

Cybersecurity (2018). Framework for improving critical infrastructure cybersecurity. URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP, 4162018.

Davis, V. (2021). The history of cybersecurity. Accessed via https://cybermagazine.com/cyber-security/history-cybersecurity on 17th November 2022.

EFCC (2022). Report of the convicted cybercriminals in nigeria,

https://www.premiumtimesng.com/news/top-news/562065-over-2800-persons-convicted-of-cybercrime-in-2022-efcc.html?tztc=1

Faki, A. S. & **Jimoh, R. G.** (2017). Improving job survivability with priority scheduling model in grid environment, *International Journal of Information Security, Privacy and Digital Forensic (IJISPDF)*, 1(1), 42 – 47.

Faki, A. A., & **Jimoh, R.G.** (2015). Reducing checkpoint overhead in grid environment, *International Journal of Computing and ICT Research*, 11(1), 72 – 83.

Fen, S. (2023). A Brief history of security. What is the one key security lesson history can teach us? Assessed via https://www.vodafone.com/business/news-and-insights/blog/gigabit-thinking/a-brief-history-of-security on 2nd June 2023.

Folorunsho, O., & **Jimoh, R. G.** (2017). A Framework for implementing hybrid Intrusion Prevention Model Based on Soft-computing Techniques. In Proceedings of 11th *International Conference on ICT Application, AICTTRA* 2017, Department of Computer Science and Engineering.

Folorunsho, O. Adegbola, I. A. & **Jimoh, R. G.** (2022). An enhanced feature selection and classification model for

network intrusion detection system using data mining techniques. Indian *Journal of Computer Science and Engineering*, 13(1), pp 145-156.

Ganiyu, S. O. & **Jimoh, R. G.** (2021). Extended risk-based context-aware model for dynamic access control in bring your own device strategy, *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics, Theories and Applications*.

Ganiyu, S. O. & **Jimoh, R. G.** (2018a). Characterising risk factors and countermeasures for risk evaluation of bring your own devices, *International Journal of Information Security Science*, 7(1), 49- 59.

Ganiyu, S. O. & **Jimoh, R. G.** (2018b). Comparative analysis of risk evaluation models for risk-aware access control in bring your own device Environment, *International Journal of Information Security Research*, 8(2), 810 - 820.

Gbolagade, M. D., **Jimoh, R. G.** &Mejabi, O. V. (2017). Design of hybridized wireless sensor network using k-means clustering and genetic algorithm. *Circulation in Computer Science* l2(5), 1-6.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, 6(1), tyaa005.

Gupta, B. B., Perez, G. M., Agrawal, D. P., & Gupta, D. (2020). Handbook of computer networks and cybersecurity. Springer, 10, 978-3.

Hogan Guard (2023). Nigeria security intelligence Report. Isheri, Lagos: Hogan Institute.

**Jimoh, R. G.**, Oyelakin, A. M., Olatinwo, I. S., Obiwusi, K. Y., Muhammad-Thani, S., Ogundele, T. S.& Ayepeku, O. F. (2022). Experimental evaluation of ensemble learning-based models for twitter spam classification. *5th Information Technology for Education and Development (ITED),* 1-8 IEEE Xplore.

**Jimoh, R. G.**, Imoize, A. L., Awotunde, J. B., Ojo, S., Akanbi, M. B., Bamigbaye, J. A., & Faruk, N. (2022). An enhanced deep neural network enabled with cuckoo search algorithm for

intrusion detection in wide area networks. *5th Information Technology for Education and Development (ITED)*, 1-5. IEEE Xplore.

**Jimoh, R. G.**, Olusanya, O. O., Awotunde, J. B., Imoize, A. L., & Lee, C. C. (2022). Identification of risk factors using anfis-based security risk assessment model for SDLC phases. *Future Internet*, 14(11), 305.

**Jimoh, R. G.**, Adewole, K. S., Aderemi, T. E. & Balogun, A. O. (2020). Investigative study of unigram and bigram features for short message spam detection, I*nternational Conference on Emerging Applications and Technologies for Industry 4.0 (EATI' 2020)* Lecture Notes in Networks and Systems Book Serins, Published by Springer in Intelligent Technologies and Robotics.

**Jimoh, R.G.,** Abdulraheem, M., Salimonu, I.R. & Mejabi, O.V. (2017). Elliptic Curve Cryptosystem in Securing Communication across Unsecure Channel, *Circulation in Computer Science*, 2(6), 7-12.

**Jimoh, R. G.**, Abikoye, O.C. & Balogun, A. O. (2017). Computer security and privacy. In W. O. Egbewole & R. G. Jimoh (eds). Digital Skill Acquisition (GNS 3112), General Studies Division, University of Ilorin, Ilorin, Nigeria, 111- 132, ISBN: 978-36284-0-6

**Jimoh, R.G.**, Olatunde, Y.O., Suleiman, O.M. & Muhammed, B.J. (2017). Performance analysis of public key cryptosystem using multiple data, *Proceedings of Information Security Conference*, 35 – 40, Information Technology Systems and Security Professionals (ITSSP), Shodiya A, S. (eds).

**Jimoh, R. G.** & A. N. Babatunde (2014). Enhanced automated teller machine using short message service authentication verification, *International Journal of Computer and Information Engineering*, 8(1), 14 – 17.

**Jimoh, R. G.** & Norshuhada, S. (2010a). The Acceptability of iris-based authentication for public domain: an instrumental design, Proceedings of International Knowledge Management

Conference (KMICe, 2010), Indexed by Thomson Reuters, 624 - 628.

**Jimoh, R. G.** & Norshuhada, S. (2010b). Modelling the factors that influence behavioural intention to use iris authentication approach for public authentication among Nigerian users of public terminals, African *Journal for The Psychological Study of Social Issues (AJPSSI)*, 13(1), 21- 39.

**Jimoh, R.G.** & Norshuhada, S. (2009). Evaluating current authentication methods: prediction of a more suitable authentication approach for public interaction, Proceedings of *International Conference on Computing and Informatics (ICOCI09)*, 251 – 257, Published by Universiti Utara Malaysia (UUM), Indexed by IEEE. Available Online at http://www.icoci.cms.net.my

Kawamoto, D. (2022). IoT devices connecting the world. Accessed via https://builtin.com/internet-things/iot-devices on 12th July 2023.

Katagiri, N. (2023). Hackers of critical infrastructure: expectations and limits of the principle of target distinction. International Review of Law, Computers & Technology, 1-20.

Kelvin, J. & Vladimir, N. D. (2009). Exploring network-centric information architectures for unmanned systems, *Control and Data Dissemination*, 1-16, accessed online on 2nd May, 2023.

Khaleefah, A. D., & Al-Mashhadi, H. M. (2023). Methodologies, requirements and challenges of cybersecurity frameworks: A Review. Int. J. Wirel. Microw. Technol, 13, 1-13.

Kitman, S. A. (1997) The protection and disclosure of secrecy in the perspective of Islamic Fiqh. Amman:Dar al-Nafiiis.

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. Applied Sciences, 13(6), 3410.

Konowledgehut.com (2023). The History of Cybersecurity: A Detailed Guid, Available Online at *https://www. knowledgehut.com/blog/security/history-of-cyber-security* Accessed on 8th May, 2023.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: an empirical evidence. Information Systems Frontiers, 23, 361-373.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. Information & Computer Security.

Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, 35(6), 105336.

Masi, M., Sellitto, G. P., Aranha, H., & Pavleska, T. (2023). Securing critical infrastructures with a cybersecurity digital twin. *Software and Systems Modeling*, 1-19.

Mijwil, M., Aljanabi, M., & Ali, A. H. (2023). ChatGPT: exploring the role of cybersecurity in the protection of medical information. *Mesopotamian journal of cybersecurity*, 2023, 18-21.

Mustapha I. O & **Jimoh R. G.** (2016). "Modeling an enhanced intrusion detection system using mobile agent: a methodological framework". *Association for Computing Machinery (ACM)*, 1755, 227-233

Mustapha I. O and **Jimoh R. G.**, J. C. Nwaiwu and M. O. Alimi. (2018). An optimized intrusion detection model". *International Journal of Informati Security, Privacy and Digital Forensics*. Nigeria Computer Society. Vol. 2, No 1, pg 84-95.

Olalere, M., Raji, A. E., Idris, I. & **Jimoh R. G.** (2018). A Naive Bayes based pattern recognition model for detection and categorization of structured query language injection attack, *International Journal of Cyber-Security and Digital Forensics*, 7(2), 189 – 199.

Olusanya, O.O & **Jimoh R.G.** (2018). Determining risk factors in the formulation of anfis model of security risk assessment of SDLC phases. *Proceedings of 1st International Conference on ICT for National Development and It's Substainability (ICT4NDS)*, Faculty of Communication and Information Sciences, University of Ilorin, Nigeria. April 17th – 19th, 2018.Pp 162

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

Ndunagu, J., Fadayomi, B., Ganiyu, S. O. & **Jimoh, R. G.** (2019). Development of F-NTAS: a network traffic analysis system for detecting denial of service attacks, *International Journal of Information Processing and Communication*, Published by Faculty of Communication and Information Sciences, University of Ilorin, 7(1), 401 - 409.

Omolehin, J.O., Abikoye, O.C. & **Jimoh, R.G.** (2009). Development of data encryption and decryption algorithm using Modified Rail Fence Cipher, *journal of association for the Advancement of Modelling and Simulation Techniques in Enterprise*, 14(2), 69 – 78.

Oyelakin A.M**.** & **Jimoh R.G**. (2021), A survey of feature extraction and feature selection techniques used in machine learning-based botnet detection schemes, *VAWKUM Transactions on Computer Sciences*, 9 (2021),1-7.

Oyelakin A.M**.** & **Jimoh R.G**. (2020a). The paradigm shift of centralised botnets to decentralised DGA-botnets in the underground cyber economy: an overview, *Journal of Computer Science and Control Systems, Faculty of Engineering and Computer Science, Oredia University, Romania* 13(1), 48-51.

Oyelakin A.M. & **Jimoh R.G.** (2020b). Towards building an improved botnet detection model in highly imbalance botnet dataset-A Methodological Framework, *Middle East Journal of Applied Science & Technology*, 3(1) 34-40.

Oyelakin A.M. **& Jimoh R.G**. (2019**).** A review on the identification techniques for detection-evasive botnet malware, *in the Proceedings of Nigeria Computer Society (NCS), July 2019 International Conference*

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). Workforce framework for cybersecurity (NICE framework).

Petrova, K. (2003). Net-centric computing: A postgraduate course., Accessed via https://www.academia.edu/1086849/NET_CENTRIC_COMPUTING_A_POSTGRADUATE_COURSE on 5th January, 2023.

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cybersecurity maturity models: a systematic literature review. Information & Computer Security, 28(4), 627-644.

Salau-Ibrahim T.T & **Jimoh R.G.** (2020). "Negative selection algorithm based intrusion detection model". *Proceedings of the 20th IEEE Mediterranean Electro-technical Conference (MELECON 2020).* Edited by Pietro Romano & Luigi Costanzo Pp. 202-206. Universita degil Studi di Palermo. 15th – 18th June 2020.

Salau-Ibrahim T.T & **Jimoh R.G.** (2017). "Designing an intrusion detection system with artificial immune system algorithms". *Proceedings of the 11 th International Multi-Conference on ICT Applications.* Edited by: Professor E.R. Adagunodo, Professor G.A. Aderounmu, Dr. E.A. Olajubu, Dr. B.I. Akhigbe & Dr. I.P. Gambo. Pp. 1-10. Obafemi Awolowo University, Ile-Ife. 1st – 4th November 2017.

Schlatt, V., Guggenberger, T., Schmid, J., & Urbach, N. (2023). Attacking the trust machine: developing an information systems research agenda for block chain cybersecurity. International journal of information management, 68, 102470.

Sheng, S., Chan, W. L., Li, K. K., Xianzhong, D., & Xiangjun, Z. (2007). Context information-based cybersecurity defense of protection system. IEEE Transactions on Power Delivery, 22(3), 1477-1481.

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. Scitech Lawyer, 10(4), 16.

Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). banking information resource cybersecurity system modeling. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(2), 80.

Sonny, Z. (2010). Information security in the islamic perspectives: the principle and practice, Proceedings of the 3rd I*nternational Conference on Information and Communication Technology for the Moslem World (ICT4M)*, IEEE Xplore, Received from https://ieeeexplore.org/document/5971936

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cybersecurity: Framework, standards and recommendations. Future generation computer systems, 92, 178-188.

Wallam.com(2023). Cyber Attacks, Accessed via https://www. wallarm.com/what/what-is-a-cyber-attack on 3rd June 2023.

Yusuf, O, A. & **Jimoh, R. G.** (2018). Authentication Mechanism in Public Payment System: Challenges and Solutions, R. A. Lawal, Eds, 1st *International Conference on ICT for National Development & Its Sustainability*, University of Ilorin.

Yusuf, O. A. (2020). Modeling an enhanced authentication mechanism for contactless card payment transactions on point of sales terminal, *Unpublished Ph.D. Thesis*, Department of Computer Science, University of Ilorin.

Yousif, A. F. (2004). Islam & science. Kuala Lumpur: IIUM

Villar Miguelez, C., Monzon Baeza, V., Parada, R., & Monzo, C. (2023). Guidelines for renewal and securitization of a critical infrastructure based on IoT networks. Smart Cities, 6(2), 728-743.