FEDERAL UNIVERSITY OF AGRICULTURE
ABEOKUTA NIGERIA

80th INAUGURAL LECTURE

THE MUDDY WATERS IN WINNING THE REVOLUTIONISED CYBERSECURITY GAME

by

Professor Adesina Simon Sodiya
(Professor of Computer Science and Information Security)

Department of Computer Science,
College of Physical Sciences
Federal University of Agriculture, Abeokuta, Nigeria.

THE MUDDY WATERS IN WINNING THE REVOLUTIONISED CYBERSECURITY GAME

by

Professor Adesina Simon Sodiya *FNCS, FBCS*
Professor of Computer Science and Information Security

Department of Computer Science,
College of Physical Sciences
Federal University of Agriculture, Abeokuta, Nigeria.

FUNAAB INAUGURAL LECTURE
Series No. 80

Wednesday August 16, 2023

FUNAAB INAUGURAL LECTURE

Series No. 80

by

Professor Adesina Simon Sodiya*FNCS, FBCS*
Professor of Computer Science and Information Security

The 80th Inaugural Lecture was delivered under the Chairmanship

of

The Vice-Chancellor

Professor Babatunde Kehinde

B.Sc (Agric Biology); M.Sc (Crop Improvement),
Ph.D (Ibadan), FGSN, FAIMP, FIHSC

Published Wednesday August 16, 2023

ISBN: 798 - 978 - 781 - 093 - 8

FUNAAB INAUGURAL LECTURE SERIES

Professor Adesina Simon Sodiya *FNCS, FBCS*
B.Sc. (Ago-Iwoye), M.Sc. (Lagos), MBA (Ago-Iwoye) and Ph.D (Abeokuta)
Professor of Computer Science and Information Security

Department of Computer Science,
College of Physical Sciences
Federal University of Agriculture, Abeokuta, Nigeria.

THE MUDDY WATERS IN WINNING THE REVOLUTIONISED CYBERSECURITY GAME

Protocols

The Vice-Chancellor

Deputy Vice-Chancellor (Academic)

Deputy Vice-Chancellor (Development)

The Registrar

The Bursar,

The University Librarian,

Dean, College of Physical Sciences,

Other Deans and Directors,

Head, Department of Computer Science,

Other Heads of Departments,

Distinguished members and Professional Colleagues,

Members of my Family,

Gentlemen of the Print and Electronic Media,

Distinguished Ladies and Gentlemen

Great FUNAABITES.

1.0 PREAMBLE

Mr. Vice Chancellor, Sir, I am highly delighted and privileged to stand before you, your Management team and this distinguished audience to present my Inaugural Lecture as a Professor of Computer Science and Information Security in the Department of Computer Science, College of Physical Sciences of the great and unique Federal University of Agriculture, Abeokuta.

My journey in this university started as a Senior System Analyst in 1995, and as an academic (Assistant Lecturer), I rose through the ranks to become a Professor in 2015. This inaugural lecture is the 2nd from the Department of Computer Science, and the 3rd from the defunct Mathematical Sciences Department. The first titled "*Total Quality: A Mathematical Panacea for National Productivity Improvement*" was delivered by Prof. Adewale Roland Tunde Solarin in 1999. The first from the Department of Computer Science was delivered by Prof. A. T. Akinwale. This lecture is also the sixth Inaugural Lecture from the College of Physical Sciences (COLPHYS), coming after those of Prof. Joseph A. Olowofela, Department of Physics, and Prof. (Mrs.) Catherine O. Eromosele, Prof. Akinola K. Akinlabi and Prof. Enoch O. Dare of the Department of Chemistry.

This Inaugural Lecture offers a remarkable opportunity for me as a Professor to inform colleagues in the University, and the general public about the trend, progress and stellar achievements in my core area of research career (Cybersecurity). It is indeed a great previlege to present the 80th Inaugural Lecture titled- ***The Muddy Waters in Winning the Revolutionalised Cybersecurity Game***. The topic was chosen to enable me introduce, discuss my scholarly achievements, and analyse some implications in my chosen field of Cybersecurity. I will also be presenting my general

contributions to learning, research and service to the university and the wider community. I humbly crave your indulgence to join me as we explore the digital space and cyber-world.

2.0 INTRODUCTION

Computer Science is the systematic study of feasibility, expressions, theories, models, processes and methods that underlie the acquisition, representation, processing, storage, communication of, and access to information. Computer Science is the study of principles, applications and technologies of computing.

Information Technology (IT) is concerned with all technologies used in the capturing, manipulating, processing, storage, managing and communicating information. IT is an offshoot of Computer Science.

2.1 Computing / Information Technology IT

Some distinguishing characteristics of Computer Science/ Information Technology are that it:

a. combines theory and practical approaches
b. requires thinking both in abstract and concrete terms
c. requires precision, creativity, careful reasoning and critical thinking
d. is an enabler and provides support for other disciplines
e. is felt and used by almost everybody
f. is a revolutionary tool

Some core areas of Computing are:

a. *Software Engineering*: The branch of computer science that deals with the design, development, testing, and maintenance of software applications.
b. *Artificial Intelligence and Robotics*: Deals with the simulation or approximation of human intelligence in machines. Robotics is the engineering and operation of machines that can

autonomously or semi-autonomously perform physical tasks on behalf of a human. Robotics and Artificial Intelligence are interwoven.

c. *Computer Engineering*: The discipline that embodies the science and technology of design, construction, implementation, and maintenance of software and hardware components of modern computing systems and computer-controlled equipment.

d. *Data Science*: This is the field of study that combines domain expertise, programming skills, knowledge of mathematics and statistics to extract meaningful insights from data.

e. *Information and Communication Technologies (ICT*): This is the study of tools, techniques and resources used to transmit, store, create, share or exchange information.

f. Information Security/Cybersecurity: Information security is the general act and practice of the prevention and detection of unauthorized or malicious activities in digital infrastructure. Cybersecurity is the practice of protecting an organization's server, electronic system, database system from malicious attacks. The concern of cybersecurity experts is to address challenges posed as we move from one platform to another. The four IT platforms based on development in the digital ecosystem are described as follows:

1st Platform: The 1st IT platform was basically about the "Early Computers". There was no networking in this era. It is basically about the centralization of data and processing capability. The 1st platform influenced industrial revolutions based on machines powered by water, steam, and mass production using assembly lines. The concept of information started at this platform with the protection of individual and centralized systems

2nd Platform: The 2nd platform influenced the industrial revolutions based on automations using electronics and computers. Networking was the major improvement in this platform, with the advent of Internet. This led to biggest flux of networks linked together to share data and billions of networks were connected. This then enhanced improved collaboration, productivity and high performance computing. The advent of network and the associated security issues made information security to be popular on this platform

3rd Platform: The third generation deals with the advent of mobile devices, distributed platforms, social media, cloud computing and big data. It was about creating global communities and quintillion scalable. The 3rd platform influenced the industrial revolutions based on introduction of connected devices to automate processes further. With the popularity of the Internet, the world clearly became a global village and attention shifted from information security to cybersecurity

4th Platform: Artificial intelligence and ambient computing are the major features on this IT platform. The use of sensors Internet of Things (IoT), machine Intelligence and robotics for effective implementation of e-governance, digital economy and smart cities. The 4th platform influenced the industrial revolutions based on introduction of big data analytics, robotics, virtual reality and artificial intelligence technologies to automate process further. It is about creating smart processes, systems and environment. The emergence of new technologies has created more cybersecurity concerns that are currently being addressed by researchers and professionals.

Digital revolution has now taken us to the fourth IT platform as indicated in Figure 1

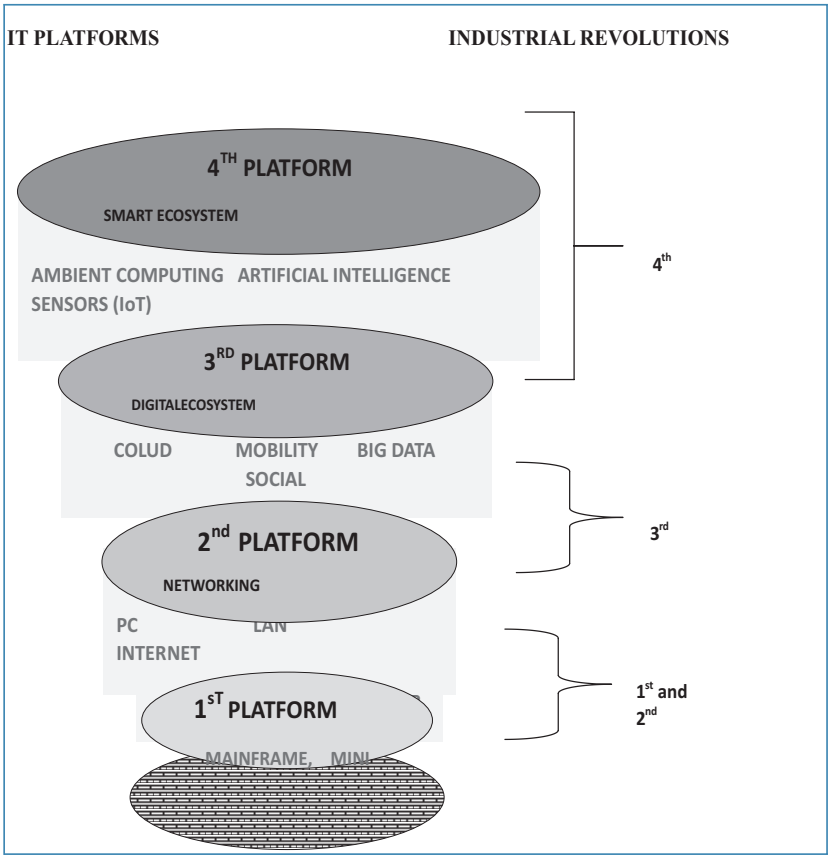

Figure 1:Information Technology Platforms

2.2 Information Security / Cybersecurity

2.2.1 *Information Security concepts*

Information Security simply means protecting computers and network from unauthorised access. It also means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or

destruction.

Other terms that are considered subsets of information security are:

- Cybersecurity which is concerned about protecting resources available from unauthorized access. It involves the collective processes and mechanisms by which sensitive and valuable information and services on internet-based systems are protected from tampering or collapse by unauthorized activities, untrustworthy individuals and unplanned events.
- Computer System Security which means the collective processes and mechanisms by which sensitive and valuable information and services on computer-based systems are protected from unauthorized access
- Data Security which is way of protecting database and storage from destructive forces and unwanted actions of unauthorized users.
- Network security which means protecting network resources from unauthorised access.
- Cloud Security, also known as cloud computing security, which is a collection of security measures designed to protect cloud-based infrastructure, applications, data and services from unauthorised and malicious activities.

2.2.2 *Cybersecurity goals*

According to Sodiya and Onashoga (2015), the value of computer and network resources can be compromised in three major ways, commonly referred to as the CIAs of cybersecurity:

- ***Confidentiality***: prevention of unauthorized disclosure of information;

- ***Integrity***: prevention of unauthorized modification of information; and
- ***Availability***: prevention of unauthorized withholding of information

Others include:

- **Authenticity**: **t**his is to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.
- **Non-repudiation**: in law, it implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

2.2.3 *Types of Cyberattack*

Cyberattacks are deliberate and malicious attempts to compromise digital assets. Common examples of cyberattacks are:

a. Insider threats:

An insider attack involves someone from the inside (within the organisation), such as disgruntled employees, attacking the organisational networks **.**Insider attacks are always intentional and malicious. Malicious insiders intentionally eavesdrop, steal, or damage information **,** use information in a fraudulent manner **,**or deny access to other authorized users.

b. Malware:

Malware are malicious codes that can cause distortion on digital systems and eventually cripple the system. They

can hijack a user's browser, redirect his search attempts, bring nasty pop-up ads, track what websites he visits, and prevent him from performing certain functions. Examples are worm, viruses, trojan horse, spyware, adware, dialers, hijackers and ransomware.

c. Socially -engineered attacks:

Most traditional social engineering attacks use psychological manipulation to trick users into making security mistakes or giving away sensitive information. Examples are phishing, pharming, masquerading and cloning. For example, we should know that ibank.gtbank.com/ibank3/main.aspx is different from ibank.gtbank.com/!bank3/main.aspx

d. Authentication attacks:

An attacker tries to crack the passwords stored in a network account database or a password-protected file. Examples include dictionary, a brute-force, shoulder surfing, keylogging and hybrid attacks

e .Distributed Denial of Service attacks:

Distributed Denial of Service (DDoS) attacks are web-based attacks intended to make critical resources unavailable to legitimate users. Indicators could include inability to access the website, system abruptly reboots or stops responding several times , and abnormally slow network performance

f. Ransomware attacks:

These are malicious software designed by criminals to prevent users from getting access to their digital resources

until ransom is paid. Usually, the resources of the organisation are encrypted until a ransom is paid.

2.2.4 *Motives of Cyberattack*

Some of the motives for cyberattacks include:

a. *Vendetta/Revenge*: Retaliating against a specific target/individual/company by using hacking techniques to cause harm, disrupt operations, or damage their reputation.

b. *Pleasure*: Engaging in malicious activities for amusement, fun, pleasure often resulting in inconvenience, embarrassment, or disruption for the targeted individuals or organizations.

c. *Hackers' Ethics*: This is concerned with hackers' characters, including curiosity, pursuit of knowledge and freedom of information. It also involves challenging established systems, as a means of exploration, testing limits, or exposing vulnerabilities.

d. *Terrorism*: The use of malicious digital tactics by the attackers to instill fear, terror, cause widespread disruption of information, damage critical system infrastructure, or disseminate extremist ideologies with the intent to further political, social, or ideological goals.

e. *Political and Military Espionage*: This involves the targeted infiltration and compromise of government digital entities, information, digital organizations, or individuals' digital systems to gain sensitive information, acquire intelligence, or gain strategic advantages for political or military purposes.

f. *Business or Economic (Competition) Espionage*: This involves the theft or compromise of business information, trade secrets, or business strategies to gain a competitive advantage, undermine rival companies, or benefit financially.

2.2.5 *Cybersecurity Lifecycle*

Cyberattacks have become more rapid recently and also very frequent in today's digital world. The cybersecurity lifecycle provides a structured framework for defending against evolving cyber threats. It is crucial to remain vigilant, adapt to new threats, and foster a culture of security awareness to safeguard digital assets.

To effectively defend against these cyber threats, a systematic lifecycle is presented in Figure 2. The key stages of the lifecycle are as follows:

a. Assess: The first stage of the cybersecurity lifecycle is assessment. This involves proper identifications and comprehensively understanding the assets, computer systems, risks and personnel who are within the organization's digital infrastructure. Assessment activities include conducting risk assessments, vulnerability scans, and penetration testing to identify potential weak points.
b. Plan Protection: Once the assessment phase is completed, the next step is to develop a cybersecurity plan. This plan outlines the strategies, policies and procedures the organization must take to protect the data and assets. It includes measures such as:
    i. Conducting employee awareness training.
    ii. Defining access controls
    iii. Implementing encryption mechanisms
    iv. Conducting employee awareness training.
c. Observe and Detect: This stage involves continuous monitoring and detection to identify and respond to potential threats promptly. Real-time monitoring enables the identification of anomalous activities, suspicious behavior as knowing potential security breach of data or cyberattacks are inevitable. Prompt detection enhances the organization's ability to respond effectively and minimize the impact of an

incident.

d. Respond: When a security incident occurs and have been discovered by the organization, the ability to respond swiftly and effectively is critical. The response stage involves executing the incident response plan, which outlines the steps to contain and mitigate the effects of a security breach. It includes actions such as
   i. Isolating affected systems,
   ii. Notifying relevant stakeholders
   iii. Improve earning so as to avoid future breaches of similar types

e. Recover: This stage focuses on the prompt and effective recovery of systems and data, as well as the restoration of normal operations within an organization. It provides an opportunity for organizations to learn from the incident and improve their cybersecurity posture.

Figure 2: The Cybersecurity Lifecycle

3.0 MY RESEARCH FOCUS

My research focus has been on developing techniques, methods and systems for preventing and detecting cyberattacks. Some of the areas I have conducted impactful research are described as follows.

3.1 Secure Software Engineering

Secure software engineering is a methodology for creating software that incorporates security into every phase of the software development life cycle (SDLC). Majority of software vulnerabilities come from defects that are unintentionally introduced into the software during design and development. Some defects come from lack of focus on security issues during software development. Therefore, to significantly reduce software vulnerabilities, security must also be deeply integrated into the full software development life cycle (SDLC).

Sodiya et al. (2006) addressed the challenges and problems associated with producing secure software products, and therefore proposed the Secure Software Development Model (SSDM) as a solution. SSDM major stages include Requirements Phase, Design Phase, Implementation Phase, Security Specification Phase, Review Phase and Penetration Testing Phase. The study also introduced the "Laws of Software Security”," which provided guiding principles for software developers to produce secure software products. These laws emphasized the importance of continuous security knowledge, error prevention, timely error correction, secure development process, clear security specifications, and the overall protection of the security engineering process. A case study of an accounting system referred to as Standard Accounting (SA) was used to implement the SSDM principles. The case study demonstrated the effectiveness of SSDM in improving software security by comparing the security breaches recorded in the old accounting package with the implementation of SA.

Another notable study by Fadahunsi et al (2019) developed UMLsec-based proctored examination model. The study identified the challenges associated with assessment in educational system. With the proliferation of virtual learning and distance education, secure and quality virtual assessment is crucial. In this work, a UML_sec based proctored based virtual assessment system was developed. To validate the model, several proctored examinations were conducted using the UMLsec-based assessment approach and data were collected on students' performances.

The results obtained in Sodiya et al. (2006) demonstrated that the model provides practical and accurate insights into the relationship between personality traits and software security. This improved assessment approach offers a valuable tool for both individuals and organizations to identify individuals with the appropriate personality traits for developing secure software. The empirical results obtained on the work done in Fadahunsi et al. (2019) demonstrated that the UMLsec-based proctored examination model effectively provided an enhanced assessment of students.

3.2 Authentication Systems

Authentication systems and access control mechanisms play a pivotal role in securing digital systems and protecting sensitive information from unauthorized access. These systems verify the identity of users and grant appropriate permissions based on their credentials. Authentication is the process of verifying the identity of a user, process, or device, often as aprerequisite to allowing access to resources in a system.

The identity of a certain user or process is challenged by the system and proper steps must be taken to prove the claimed identity.

Authentication involves two stages:

a. *Identification*: users supply valid identities

b. *Verification*: the supplied identities are confirmed

However, despite continuous advancements in security measures, instances of compromise and attacks on authentication systems are still prevalent in the digital realm, posing significant risks to individuals and organizations. Real-life instances of authentication system and access control compromises are widespread and have had severe consequences. This incident not only resulted in financial losses for the company but also compromised the privacy and trust of their customers. In another case, a large e-commerce platform suffered from a credential stuffing attack in which attackers exploited weak passwords and gained unauthorized access to user accounts. This led to unauthorized transactions, compromised personal information, and subsequent financial losses for both the affected users and the platform itself. Statistics further highlight the significance of authentication system breaches. Generally, authentication attacks accounted for more than 80% of all reported data breaches in the one past year which resulted in the loss of several billions of Naira in Nigeria.

In response to the critical need for robust protection against the myriad of attacks on password authentication systems, Sodiya et al (2014) introduced a Secured Keystroke Authenticated Password Against Keylogger (SKAPAK) algorithm. As presented in Algorithm 1, SKAPAK is a novel approach designed to mitigate keylogging attacks. It works by dynamically generating decoy keystrokes alongside the actual keystrokes, making it difficult for keyloggers to decipher the legitimate input. By introducing noise and obfuscation, SKAPAK aims to confuse and deceive keyloggers, thereby enhancing the security of password entry and thwarting potential unauthorized access to sensitive information.

ALGORITHM 1: THE SKAPAK ALGORITHM

INPUTS: Fooled Authentication Data {Userstring, FooledString I FooledToken)
OUTPUTS: Normal Authenti cation Data (Userstring, PasswordString I PasswordToken)

```
Algorithm SKAPM Algorithm
        Iteratively Listen for a User Request
                If Type of User Request is Authentication Then
                        Understand User Rule -Based Principle used to form FooledToken
                        Capture User FooledT oken from the Fooled Authentication Request
                        Filter PasswordToken from the FooledToken by applying the Learned Rules
                        Prepare the New Authentication Request Data
                        Forward Normal Authentication Request Data to the Authentication Domain
                End If
        Continue Iteration
End Algorithm
```

The SKAPAK algorithm is implemented within Fool the Keylogger Model (FKM), a novel method for user authentication, employing three distinct domains: User Domain, Fooled Domain, and Authentication Domain. Within the User Domain, a counterfeit-password is created by combining genuine password characters with random alphanumeric or noise characters. This counterfeit-password is used as non-normal authentication data during the login process.

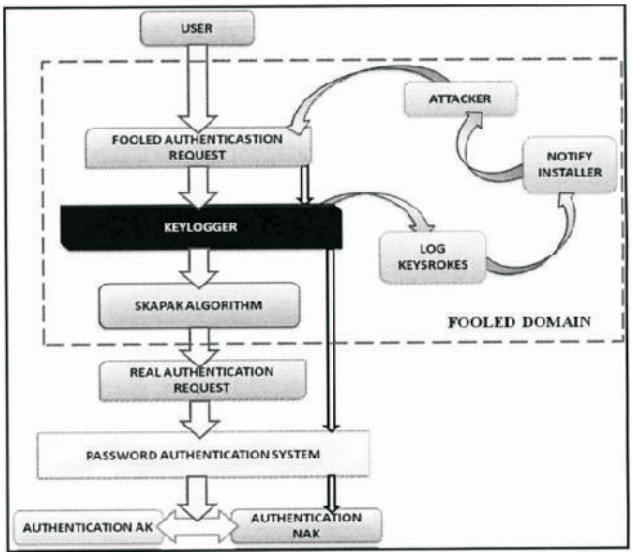

Figure 3: Description of the Fooled Domain Mechanism

The Fooled Domain, depicted in Figure 3, facilitates the implementation of the intelligent SKAPAK algorithm. This algorithm effectively extracts the password token from the counterfeit-password, making it undetectable to keyloggers. Subsequently, a valid authentication request is generated using the normal authentication data. The Authentication Domain is responsible for verifying and acknowledging the user's credentials, ensuring the reliability of the authentication procedure.

Confidence Measure (CM) was used to measure the degree of Confidence of the user in the FKM. It measures the accuracy or the extent in percentage to which the PasswordString was concealed from the visibility of the Keylogger.

$$CM = \frac{E(?)}{?} \text{ x } 100 \qquad (1)$$

where *x* is a positive integer that denotes the relationship that exits between the FooledString and KeyloggerString.

In Sodiya et al. (2011), an enhanced version of the semi-global alignment algorithm, called the Cross-semiglobal algorithm, was proposed. This approach enhanced the reliability, accuracy and efficiency of previous masquerade detection systems. The algorithm took into account, the behavioral patterns and activities of users and compared them to a threshold sequence generated from normal users' behaviours. By carefully analyzing the sequence of users' behaviours and comparing them with a threshold sequence, the algorithm determines the degree of similarity and detects any discrepancies that may indicate masquerading. The key innovation lies in constructing the scoring function based on legitimate users' sequences of commands, instead of relying on fixed gap scores used in previous pairwise algorithms. The evaluation was conducted by way of experimentation using systematically generated ASCII-coded sequence audit data from Windows and UNIX operating systems, and simulating both non-intrusive and intrusive scenarios.

Additionally, a One Time Server Specific Password (OTSSP) authentication was developed, along with two others, in Onashoga et al. (2012) to enhance the robustness of authentication systems. This scheme addressed the vulnerabilities associated with traditional password-based authentication methods by introducing a secure and dynamic password generation mechanism. In the OTSSP scheme, each user is assigned a unique server-specific password that is generated by combining multiple factors which are user's static password, a time-based value, and a server-specific secret. This password is only valid for a single authentication session and becomes obsolete thereafter. The dynamic nature of the password significantly reduced the risk of password reuse, interception, or brute-force attacks.

The OTSSP scheme includes the registration and login phases as presented below:

$$h(ID_h||S) \oplus ID_h, h(P||ID||S) \oplus ID_h \quad (2)$$

a) Registration Phase

User → Server: $TV = h(ID \,||\, S) \oplus IDh$

$$PV = h(P \,||\, ID \,||\, S) \oplus IDh$$

b) Login Phase:

i. User → Server: $E_s(ID_h, h_2(ID_h \,||\, S))$
ii. User ← Server: N
iii. User → Server: P_R|
iv. User ← Server: Success/Fail

$$P_R = h^2(Pi \,||\, ID \,||\, S) \oplus IDh \oplus h^2(IDh \,||\, S) \,||\, h^2(h(P \,||\, ID \,||\, S) \oplus N) \quad (3)$$

where;

TV represents a value generated by the user and sent to the server.

PV stands for another value generated by the user and sent to the server.

h () represents a cryptographic hash function.

ID is the user identifier.
S is a secret value.
ID_h is a hashed identifier.
P is a plaintext value.
⊕ represents the bitwise exclusive OR operation.
$E_s()$ represents the encryption function.
$h_2()$ represents another cryptographic hash function.
P_i represents some additional information related to the user.

The server verifies P_R against the *TV* and *PV* stored in the registration phase. It derives *h* (*ID h* ||S) and *h* (P_i||*ID*||*S*) by respectively XORing the *TV* and *PV* stored in the registration phase with the ID_h derived in step (ii) of the login phase. The server then computes h_2 *(Pi||ID||S)* ⊕ Id_h ⊕ h_2 *(ID_h || S)||h_2 (h(P||ID||S)⊕N)* and checks if it matches with P_R received from the user before granting a successful authentication. The scheme leverages cryptographic techniques, including symmetric encryption and hashing algorithms, to ensure the confidentiality and integrity of the password generation process. Additionally, the use of a server-specific secret adds an extra layer of protection against offline attacks, as the password cannot be deciphered without the knowledge of the server-specific secret.

In an effort to bolster password security, an approach aimed at enhancing the security of stored passwords in mobile devices was developed in Agholor et al. (2016). The work identified the limitations of existing Password Managers and proposed an approach to address these issues. The approach combined Transformed-Based Algorithm and the Modified Levenshtein Distance to generate faux passwords. The goal is to make it difficult for attackers to identify the real password through offline attacks. By proposing a Decentralized File Format Password Manager architecture (DFF-PM), credential information across

different files were distributed, which further enhances security. The architecture included Credentials module, Manager module, Security module and Storage module, which were used for encryption and decryption. With DFF-PM, the credentials were stored in random in a decentralized file format, which is debilitating to the advances of attackers.

The formal representation of the DFF-PM is described as follows:

$S = \{H(S_1, S_2, \ldots., S_b\};$

$U = \{U_1, U_2, \ldots, Ub\};$

$F = \{U_b, H(S_b)\};$

$$F1 = \{RAND\ (H(S\{1, b\}, S\{2, b\}\ \}\ \}\ , \qquad (4)$$

where;

S is the set of passwords,
U is the set of usernames
H is the hash function,
S [a,b] are real and faux passwords.
F is the set of username and password hash pairs stored in a single file format.

F1 is the set of randomly generated values obtained by hashing combinations of real and faux passwords, stored in different files in a decentralized file format.

The study described in Agholor et al. (2016) involved empirical survey, which employed the systematic evaluation of the types of password manager end-users prefer the most. The study categorized password managers into three types such as Desktop, Online, and Mobile. The objective, which was to identify the most preferred, most convenient, and most trusted type of password manager among end-users, was fulfilled by the development of a questionnaire and also pre-tested to ensure its reliability. The reliability correlation coefficient of 0.91 demonstrated the

questionnaire's effectiveness. The questionnaire was then administered to gather data from 4,850 participants. The results obtained in Sodiya et al (2014) revealed remarkable outcomes. The outcome of the User Confidence Measure in FKM Model proved that the user FooledString is always the string captured by the Keylogger and it is the KeyloggerString of the attacker, giving the user almost 100% confidence or assurance that his PasswordString is well secured against the threats of keylogging attacks. The data analysis revealed a staggering concealment rate of over 99.5% for passwords from keyloggers. Additionally, the model demonstrated a high usability and acceptability rate, surpassing 95%. Most notably, the proposed scheme successfully eliminated shoulder surfing threats, which involve unauthorized observation of a user's login session. These findings validate the effectiveness of the FKM in providing robust protection against keylogging attacks. Fool the Keylogger Model (FKM) is an effective architecture deployable as a countermeasure scheme aimed to dissuade attackers and prevent unauthorized access. This study not only contributes to the field of cybersecurity but also addressed a crucial aspect of authentication system security. By introducing innovative techniques and algorithms, it enhances the resilience of authentication systems and safeguards sensitive data from unauthorized access.

The new technique in Sodiya et al. (2011) was evaluated based on their hit rate and false positive rate. The result indicated hit rate of 82.1% and a lower false positive rate of 5.4% in Cross-semiglobal, as against a hit rate of 75.8% and a false positive rate of 7.7% in the previous Semi-global algorithm. These results indicate the effectiveness of the techniques in accurately identifying desired targets (hit rate), while minimizing the occurrence of false positives.

By implementing the OTSSP scheme in Onashoga et al. (2012), authentication systems experienced several positive implications.

Firstly, the scheme strengthens the overall security of the system by minimizing the impact of password-related attacks, such as password guessing and theft. Since the server-specific password is valid for a single session only, even if an attacker manages to obtain the password, it becomes useless for subsequent authentication attempts. Secondly, the dynamic password generation mechanism enhances the system's resistance to replay attacks. As each authentication session requires a unique password, the scheme prevents the reuse of captured passwords, thus mitigating the risk of unauthorized access.

The results obtained in Agholor et al. (2016) showed that out of 100 stored passwords, only one successful login by an attacker was recorded, indicating a breakthrough rate of 1%. In contrast, the existing Password Manager had a breakthrough rate of 28%. Based on these findings, it can be concluded that the Password Manager performed better than existing solutions in protecting stored passwords. The research also highlighted the feasibility and real-world applicability of the new system. The work also encourages people to use password managers in the effective management of multiple passwords.

3.3 Intrusion Detection

A set of attempts to compromise a computer or computer network resources' security is known as intrusion. Systems that detect internal and external attacks on digital systems and undertake some measures to eliminate them are known as intrusion detection systems (IDSs). They are simply systems that detect computer intrusions. They work like burglar alarms that work underground and monitor the system for intrusive behaviours. Intrusion detection system (IDS) works in addition to authentication systems and other security mechanism as an ad hoc security solution to protect flawed computer systems. It goes off if someone tampers with or manages to get past other security mechanisms such as authentication mechanisms and firewalls.

There are two types of intrusion detection methods:

Anomaly detection: This deals with detection of certain deviations from normal users' behaviours.

Misuse detection: Patterns (sometimes called signatures) of all known attacks must be described in some abstract form and given to IDS. These patterns are used later to identify an intrusion.

Intrusion detection is needed as another wall to protect computer systems. The elements central to intrusion detection are: resources to be protected in a target system, i.e. user accounts, file systems, system kernels, etc.; models that characterize the "normal" or "legitimate" behaviour of these resources; techniques that compare the actual system activities with the established models, and identify those that are "abnormal" or "intrusive". Over the years, researchers and designers have used many techniques to design intrusion detection systems. But, there have been one or more problems with present intrusion detection systems. Some major ones include:

High number of false positives: False alarms are high and attack recognition is not perfect. Lowering thresholds to reduce false alarms raises the number of attacks that get through undetected as false negatives. Improving the ability of an IDS to detect attacks accurately is the primary problem facing IDS manufactures today.

High number of false negatives: We know that some intrusions still go undetected in some systems. That means that the present-day IDSs still cannot detect all computer intrusions. Also, improving the ability of an IDS to detect attacks is the primary problem facing researchers.

Lack of efficiency: IDSs are often required to evaluate events in real time. This requirement is difficult to meet when faced with a very large number of events as is typical in today's networks. Consequently, host-based IDSs often slow down a system and network-based IDSs drop network packets that they do not have time to process.

IDS security: Few papers discuss IDS resilience, i.e. the ability of the IDS to resist attacks against itself.

In Sodiya et al. (2004), a combined strategy for intrusion detection (CSIDS) was proposed to solve some of the identified challenges. The approach involved the design and implementation of an intrusion detection system that consists of two subsystems: data mining and expert system strategies. In CIDS, data mining was in profiling users' normal patterns, while an expert system was used in detection and reporting. The model for our design is represented in Figure 4.

We use a network system log file as our data source. The log file serves as the input to our own data mining algorithm for effective user profile construction. The profile construction was based on rules defined in the profile template. The users' profiling was in two categories. in two categories. One is the normal users' profiling (represented by P1; P2; .. .; Pn) while the second was the sequential pattern profiling (represented by SP1; SP2; .. .; SPn). The monitor was introduced to reduce the false alarm rate in intrusion detection (represented by M1; M2; .. .; Mn). The normal profiles, sequential profiles and the monitors served as the input to the detection system (expert system). Then, the response unit, which is also handled by the expert system, responds in real time if an event is anomalous or intrusive.

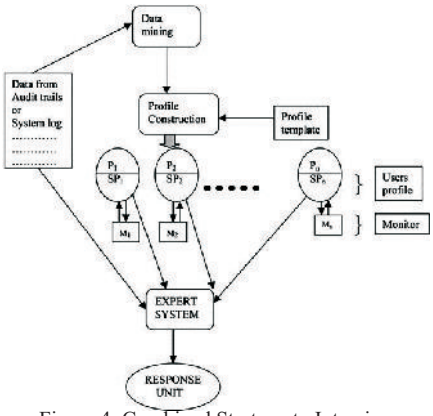

Figure 4: Combined Strategy to Intrusion

The algorithm for the detection system is divided into phases.

(a) The initial check phase: In this phase, a check is made to confirm if the current record in the system is available in the DN database. If the record is found in the DN database it moves forward for sequence check. If the record is not found the system raises an alarm immediately.

(b) Sequence check phase: After if has been confirmed that the record exists in the DN database, the system moves forward to check for the sequential pattern relevance of that activity or event. The sequential check model is represented as follows:

Let us represent the pattern where the current record (Rc) in the system log exists by Sp (S_1,S_2,S_3,.. ..S_m) and the last event of a user be represented by UL. m represents the number of patterns that exist for a user and p represents the sequence number. Rc passes sequential check phase if there exist:

$$U_L = S^p \text{ for } n = 1; \quad (5)$$

and

$$U_L = S^{p-1} \text{ for } n = 1; \quad (6)$$

where n represents the position of Rc in the sequence.

If it follows a sequence in the database, it would return back to the system and would consider that activity as being normal. If it does not, the system raises an alarm.

(c) Alarm investigation phase: Our design makes use of passive reporting. The system would just make an intrusion report to the SSO and would not automatically stop the event.

A method that effectively combined techniques was described in Sodiya et al. (2004). The improvement on this work was presented in Sodiya et al. (2005) for better performance. In Sodiya et al. (2005) data mining technique was used in creating two types of profiles (normal and sequential pattern profiles) and an expert system was used in the area of detection and reporting. The only major amendment is on the normal patterns profiling. Instead of

just transforming the cleaned database into a normal profile directly, the Apriori data mining algorithm was modified for the normal profiling.

The CSIDS principles are presented belo

(a) Apriori principle:

- Collect a single item count. Find large items;
- Find candidate pairs, count them large pairs of items count them large pairs of items;
- Find candidate triplets, count them ¼ large triplets of items, and so on;
- Guiding principle: every subset of a frequent item set has to be frequent; and
- Use the principle for pruning many candidates.

(b) CSIDS principle:

- Collect all possible transactions for user 1 and find the supports (the candidate table for user 1 is generated as against single item candidate generation in Apriori);
- Generate the candidate table for the next user (as against candidate pair count/generation in Apriori);
- Generate candidate tables for users on the network (as against item level candidate generation in Apriori); and
- Keep these candidate tables as normal profile database.

The Dc is transformed into a normal profile database consisting of tables of all possible activities of the user on the system during the profiling period. This is represented by $P_1 \ldots P_n$ in CSIDS. The Dn represents the normal profiling database. Apart from these changes in the normal profiling, all other aspect of the profiling system remain the same.

Sodiya et al. (2005) addressed the privacy concerns in IDS

usingpseudonymization technique. The privacy issue has been a serious problem in anomaly detection because users's behaviours are monitored and analysed before intrusions are detected. The design made use of a dynamic key generation algorithm that generates a key randomly when an intrusion is detected. The keys are only released when an intrusion occurs and immediately swapped to protect harmful access to the mapping database. Another crucial part of our design was that the system does not provide any information about how the keys are generated. The length and nature of the password that generates the keys are not easily deduced because of the techniques used.

The algorithm used for the work is a private key block cipher algorithm. This algorithm was composed of a key generator that was used in the crypts file function. It was a library from which any application can access its functions. The key generator was not based on a "static" mathematical function but on the password itself. That means the way a key is generated is a function of the password used. A new feature introduced is that the algorithm is dynamic. This means you can change the way the algorithm operates just by changing its parameters. The key generation's round could also be specified to increase the number of operations of the algorithm.

The key lengths that are generated are powers of two (e.g. 128, 256, 512, 1,024 bits, etc). To generate a key, there were two different methods: randomly or pseudo-randomly. For the random method, 16 random characters were generated and stored in the memory. For the pseudo-random method, the user is asked to type some characters that are then stored in the memory. The maximum number of characters that can be entered is 16, which corresponds to a key length of 128 bits.

Sodiya (2006) presented a Multi-level and Secured Agent-based Intrusion Detection System (MASIDS) to address some of the problems with centralized systems. The centralized IDS

architecture is usually faced with the problems of limited detection efficiency, high number of false positive alarms, limited ability to analyse and detect distributed attacks, and low protection of IDS.

The components of MSAIDS architecture provides a methodology where intrusion detection was do neat two levels viz: the Lower Level Detection LLD and Upper Level Detection ULD. The main focus of the LLD is to have some agents to first detect intrusions independently and subsequently report back to the ULD for further investigation and confirmation of intrusions. At the LLD level, there are two categories of agents: the data agents and processing agents. There are four data agents and they move around the nodes in the network to collect associated information from application messages, authentication events, system calls, TCP connections and others. There are two processing agents working at this level and they are known as Node Agents. The first node agent Node-1-agentwasresponsiblefortheconstructionofthe first level database. The agent collects the data from the data agents to build a database with the information collected. This agent was also in charge of data cleansing, classification and for matting. The second agent Node-2-agent was responsible for data mining and first level intrusion detection. Data mining algorithm was applied on the information in the data warehouse to extract suspicious activities and communicates the possibility of intrusions to the interface agent through the Alarm Agent (AA). The upper level (ULD) was known as confirmation level and it was involved in separate intrusion detection process. There are low-level agents that are responsible for separate data collection from different sources. It is essential not to rely on the data gathered by node-1-agent in the LLD. These low level agents gather data from the data agents and inform the Controller and Protector (CP)about the nature of data gathered. The CP acts as the facilitator agent. The CP passes the data to the data mining agent for storage and mining activities. The

data mining agent then applies data min-ing algorithm on the database so as to extract patterns or associations of intrusive events. If there is any intrusion suspected, it is reported by the Interface Agent IA to the Site Security Officer (SSO). The data base at the ULD provides another view of the knowledge and activity of the monitored distributed network. The interesting thing about this architecture is that if there is no signal or alarm from LLD, the ULD does not check intrusions. The low level agents just constantly gather data and these data are used to update the ULD data base. A full intrusions check is not initiated if there is no trigger from the LLD. This enables few agents to be active at the same time and ease the problem of protocol and language definitions associated with the communication between agents.

Between 98 and 100% detection efficiency, 0 to 2% false alarm rate and privacy preservation of 99 to 100% were achieved in most of the work. This shows my significant contributions in the field of intrusion detection. Our work also formed part of the foundational research in the field of intrusion detection.

3.4 Phishing Detection

Phishing attacks are criminal attempts that fraudulently deceived both experienced and naive online users through fake websites into divulging their sensitive personal credentials. Phishing is one of the severest cyber-attacks that open doors for other attacks such as ransom ware where critical online assets can come under serious threats. Huge financial losses and brand damages often occasioned any successful phishing attacks with no regards to any digital boundaries. For instance, Stats and Trends' 2017 security reports indicated that nearly about $5 billion were lost between October 2013 and December 2016 affecting more than 24,000 victims worldwide in a W-2 type of phishing attack. The W-2 phishing emails have been reported to be the most dangerous phishing email scams in recent times as its goal is to file fraudulent tax returns and

claim refunds. To mitigate the adverse effects of phishing, various countermeasures have been provided by security communities and research institutions. Despite the availability of myriads anti-phishing systems, phishing continues unabated due to inadequate detection of a zero-day attack, superfluous computational overhead, use of phishing kits (i.e. exploit kit which simplify creation of fraudulent websites) and high false rates. Although Machine Learning approaches have achieved promising accuracy rate, the choice and the performance of the feature vector limit their effective detection. Hence, the situation has led to an arms race between the phishers and the security solutions thereby necessitating a constant review of existing solutions in the face of newer attack.

To respond to this clarion call as a researcher and academic institution, an enhanced machine learning-based predictive model was proposed in Orunsolu et al. (2022)**.** The predictive model consists of Feature Selection Module which was used for the construction of an effective feature vector. These features were extracted from the URL, webpage properties and webpage behaviour using the incremental component-based system to present the resultant feature vector to the predictive model. The proposed system uses Support Vector Machine and Naïve Bayes.

Let *w* be a request that needs classification i.e.

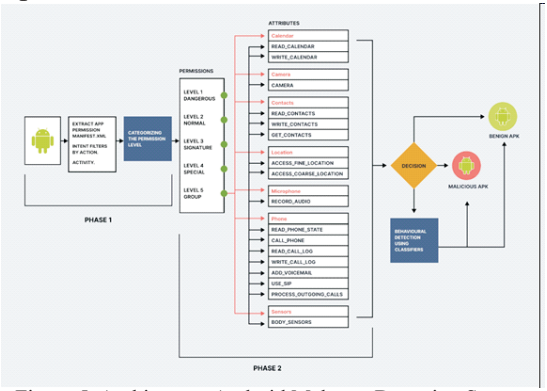

Figure 5: Architecture Android Malware Detection System

In the first phase, a time-based filter was employed to prioritise the execution of Android applications based on permissions and intents. One way of achieving this is to explicitly define the resources that can invoke the permission and map the resources to the permission level. Suppose an application A consisting of P permissions and I intents. Let P_i be the i-th permission sample and T_kP_i is the percentage of k-th permission in S. In addition, let I_i be the i-th intent in a given intent sample and T_kI_i is the percentage of k-th intents in an application. The priority scheduling is computed using equation 10

$$T_kP_i = \frac{\sum_{i=1}^{m} p_i}{\sum_{i=1}^{n} s_i} \quad (17)$$

$$T_kI_i = \frac{\sum_{i=1}^{m} I_i}{\sum_{i=1}^{n} L_i} \quad (18)$$

Let $F = \min (T_kP_l, T_kI_l)$. If F is greater than the threshold defined by the user then the application is placed in lower priority otherwise, it is placed in High priority. Any application that is placed in lower priority will be subjected to behavioural detection.

The second phase consists of behavioural checks. Once an app is assigned to a low priority, a further check is carried out to ascertain the true state of the App. The feature sets generated from phase II, which consist of 3-tuple (Permission, Intent, Activity) together with labels (malware and benign) were used to build the support vector machine classifier.

Similarly, Sodiya et al. (2021) developed a new malware paradigm for generative adversarial network (GAN) with a fully-connected neural network (FCN) architecture. The model generates malware images from random noise distribution and learns to distinguish them from real malware images. The generated malware exhibits similar characteristics to real malware but with modified features. In a related research effort, Falana et al. (2022) developed an ensemble technique called Mal-Detect, which utilizes a combination of Deep Convolutional Neural

Network (DCNN) and Deep Generative Adversarial Neural Network (DGANN) to analyze, detect, and categorize malware as shown in Figure 6.

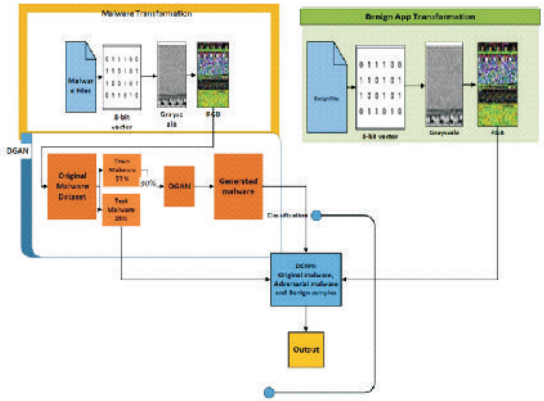

Figure 6: Deep Generative Adversarial Network Framework

The proposed Mal-Detect approach involved converting both malware and benign file binaries into RGB binary images. A deep generative adversarial neural network was employed to enhance the dataset to generate new malware images from original malware samples. The generated malware images, and the original malware and benign file images undergo pre-processing and training using Deep Convolutional Neural Networks to extract important features.

In Sodiya et al. (2014), the approach was evaluated using an experiment consisting of 20,750 malicious program and 15,000 clean programs. The result indicated a performance metric of True positive of 93.9%, False alarm of 0.08 and detection accuracy of 92.9%. This result showed the potential of ANFSMD as an efficient and effective approach for detecting various categories of malware, including zero-day and polymorphic variants (Sodiya et al., 2014). Falana et al. (2021) performed series of experiments on different machine learning classifiers. The result showed that PEDAM had the best accuracy of 95.24% when compared with Naïve Baye, KNN, and Random forest with an accuracy of 82.3%,

71.4% and 76.5% respectively. In Sodiya et al. (2021) an experiment was conducted using the MalImg dataset, which consists of image-based malware samples. Due to technical constraints, 52.83% of the dataset was used to generate new malware data, resulting in a significant increase of 224.98% and amounting to 98.66% of the original dataset. Evaluation metrics such as Mean Squared Error (MSE), Structural Similarity Index (SSIM), and a customized enhancer (ABV) were employed to assess the generated images. The scores obtained from these metrics ranged from 0 to 1, with lower MSE scores and higher SSIM and ABV scores indicating better results. The best scores obtained were 0.02 for MSE, 0.91 for SSIM, and 1.00 for ABV, while the worst scores were 0.07, 0.02, and 0.68, respectively. Additionally, a diffing tool (KDiff3) was used to examine the uniqueness of the generated images. These evaluation metrics and analyses highlight the efficacy of the proposed method in malware prediction and data augmentation. Similrly, Falana et al. (2022)tested the effectiveness of Mal-Detect against three benchmark datasets: MaleVis, Mallmg, and Virushare. The evaluation results demonstrated the superiority of Mal-Detect over other state-of-the-art techniques across all tested malware datasets. These results highlighted our significant contributions to the development of efficient malware detection system.

3.5 Distributed Denial of Service (DDoS) Detection

Distributed Denial of Service (DDoS) attacks pose major threats to IT-based systems. DDoS attacks are malicious attempts to prevent legitimate users from accessing online services or resources. DDoS attacks are launched to exhaust critical resources of the victim causing a partial or total unavailability of services to genuine users (Tinubu *et al.,* 2023). The availability of networks, servers, applications and websites is greatly impaired by DDoS attacks. They are often targeted at IT services, financial services, cloud services, e-commerce platforms, media/entertainment content amongst others. According to forecasts, DDoS attacks are

anticipated to rise from 7.9 million in 2018 to 15.4 million in 2023. Attackers are adapting their strategies to counteract mitigation techniques. These statistics, as well as the mutation in attack strategies demonstrates the frequency and sophistication of DDoS attacks, and necessitates the development of efficient and effective detection and mitigation systems.

In Tinubu et al. (2022a), the design and implementation of an intelligent model for the detection of application-layer Distributed Denial of Service (DDoS) attacks and the prevention of service degradations during Flash Events (FE) were presented. The cloud-based model consisted of two key components; the DDoS attack detection system and the FE management system. The DDoS attack detection system comprised of the Firewall, Proxy and DDoS Classifier. The DDoS classifier uses a Multi-Layer Perceptron (MLP), which is a class of Artificial Neural Network (ANN) composed of multiple layers of neurons with the information moving unidirectionally from the input layer through the hidden layers to the output layer. The MLP classifier detects DDoS attacks on application servers which are hosted within the Software-Defined Networking (SDN) in the cloud. All requests from legitimate client devices and the compromised devices on a botnet are sent through the cloud edge network which releases control of the packets to the SDN. The Flash Event (FE) management system consists of an asynchronous processing of requests to prevent performance degradations of the application servers. All legitimate requests sent through the cloud edge network to the application servers are analyzed and processing decisions are made based on some constraints. These constraints determine if the requests are to be synchronously or asynchronously processed. Then, requests that can cause a FE are queued and processed on a First-In, First-out (FIFO) basis.

In addition, Tinubu et al. (2022b) developed a machine learning model named 'DT-Model' for the classification of Distributed

Denial of Service (DDoS) attacks and Flash Events (FE) using a Decision Tree C4.5 algorithm. In each stage, the features with the highest information gain ratio are chosen and saved at the associated node. This method wass repeated for subsets of the sample dataset D that was split into several classes till a leaf node was touched, at which point all samples are members of the same class. The classification rules were the pathways from one node to the next. The DT-Model determines the class label by comparing the values of the sample data to the different classification criteria. The procedure comes to an end after the model is constructed. Similarly, in Tinubu et al. (2023), a behavioral model for characterizing flows in flooding DDoS attacks was presented. A network traffic-based analysis was carried out for the identification of anomaly behaviors of attack flows. From the behavioural characteristics observed of the attack flows, three (3) unique features namely the Flow rate, Arrival rate and Inter-arrival time of packets were identified for the detection of DDoS attacks.

In Tinubu et al. (2022a), a demo application was set up wherein HTTP flood attack was launched and a Flash Event was simulated. The experimental results clearly showed that the MLP classifier with an accuracy of 99.99% and a detection time of 18.604seconds outperformed other machine learning classifiers. Also, the evaluation of the FE management system showed a great reduction in service degradation.. In Tinubu et al. (2022b), the DT-Model classified incoming traffic into either attack flows or FE flows with an accuracy of 99.7%. A comparative analysis was carried out using four machine learning algorithms and the performance evaluation clearly showed that the Decision Tree classifier outperformed other classifiers namely the Support Vector Machine (SVM), K-Nearest Neighbor (K-NN) and Naıve Bayes which achieved a classification accuracy of 97.9%, 94.6% and 83.1% respectively. The results reflect the capability of the designed model in averting service unavailability on the web and

digital applications.

4.0 CYBERSECURITY GAME

4.1 Game Theoretic Approaches for Attack Prevention and Detection

Despite several considerable efforts from the research community on cybersecurity, the cyberspace remains far from being completely secured. Traditional solutions as Firewalls, Intrusion Detection Systems (IDS), honeypots, antivirus, among others have been widely employed for attack prevention and detection. However, these defense approaches lack quantitative analysis and decision frameworks, and are struggling to keep up with the growing sophistication of attacks. Most of these approaches do not consider the attacker's dynamic behaviors and strategies. Analytical frameworks and decision support systems that are efficient and effective in tackling real-world cybersecurity issues are therefore required to overcome the inadequacies of traditional solutions.

Game theory is the science of strategy for decision-making. Game theory is the optimal decision-making of independent and competing entities in a strategic setting. It is a mathematical framework capable of depicting conflicting situations where several strategic decision makers, called players, attempt to maximize their utilities. Decision-making frameworks rooted in Game theory effectively analyzes the strategic interactions between attackers and defenders. In recent years, game theory has become a mainstream methodology for cyber defense decision-making. Game theory offers a quantitative assessment of a system's security and the prediction of security outcomes. Security decisions can be analyzed methodically, rather than depending only on heuristics, as obtainable in most conventional defense solutions.

Game-theoretical approaches overcome conventional solutions for cybersecurity as described below. These rationales make game-theoretic approaches of great interest in attack-defense scenarios:

(i) Proven Mathematics: Majority of conventional solutions implemented in preventive devices (e.g., firewall) or in reactive devices (e.g., anti-virus programs) depend only on heuristics. However, game-theoretic methods can analyze security decisions methodically with proven mathematics.

(ii) Reliable Defense: Based on the analytical outcome from the game, robust and reliable defense mechanisms against attackers can be designed for prevention and detection systems.

(iii)Distributed Solutions: The use of appropriate game models ensures that defense mechanisms are distributed compared to conventional mechanisms where decision-making is centralized.

4.2 Players and Approaches

The basic elements in any Game are the Players, Actions, Strategies and Payoffs.

a. *Player:* is a decision-making entity in a game. A player (a person, machine or group of persons) within a game has several objectives and makes strategic decisions to implement them.

b. Action: an action implies a move in the given game.

c. Strategy: a plan of actions in all possible situations of the game.

d. Payoff: *t*he returns of strategies taken within a game, either positive or negative.

Game theory is built on the assumption that all the players are rational and for whatever game, there exists a strategy that will make a player emerge as the winner of the game. The goal of each player is to always choose the best strategy which maximizes his

payoff considering the strategies of the opponents.
In a Cybersecurity Game, the players are the Attackers and Defenders.
Case Study: Distributed Denial of Service (DDoS) attack Scenarios

a. Attackers
The rational attacker strives to find the optimal strategy for flooding the network with malicious flows, to cause total/partial unavailability of services. A Poisson distribution is considered as a generating function at each malicious node

$$F_{TOTAL} = \sum_{i=1}^{n} X_i + \sum_{j=1}^{m} X_j \text{ bps} \qquad (19)$$

Usually, attackers have different intents of launching attacks. To categorize attacker's intent, the following cases are considered.
Case 1: Vulnerability test
Case 2: Performance Degradation
Case 3: Partial shutdown of target system
Case 4: Complete shutdown of target system
These intents are achieved through Strategies. The mapping from cases of attacker's intent to attack strategies is one-to-many.
b. Defenders
The defender is concerned with protecting the network resources of the target system as much as possible, primarily to increase resource availability to legitimate users. The defender is assumed to have a clear knowledge of the bandwidth of the network and focuses on finding an optimal strategy to counter attacks.

4.3 Modelling Cybersecurity as Game
A cybersecurity game can be modelled as a *two-player* game, wherein the attackers and defenders are two teams who strive to maximize their payoffs. An attack-defense game is best modeled as a *non-zero-sum* game, where the player with the highest payoff wins the game. *Non-cooperative games* are valid for attack-

defense systems as the players are in a competition and are not bound to cooperate with each other. An *incomplete-information* game depicts a real-life attack-defense scenario as no player may have the full knowledge of all other player's strategy sets and payoffs.
Sophisticated attacks are usually intentional with well-defined objectives. The players achieve their individual objectives through strategies. Strategies in attack-defense games are interdependent as the defender's decision of strategy depends on the attacker's choice of strategy, and vice versa. The strategy sets of the players consist of finite number of attack and defense strategies. A pair of strategies from the attack and defense strategy sets constitutes a *'play'*. Thus, any attack-defense game is a set of plays.

Modeling the attack-defense game involves the consideration of the *utility functions* which determines the *payoffs* gained by the attackers and the defenders in a given play. The attack-defense game is repeated for a possible number of plays should reach a stable state in which all players are satisfied with their payoffs and have no incentives to deviate. This is the optimal attack/defense strategy of the game and can be obtained from the Nash Equilibrium.

Considering the intensifying sophistication of cyber-attacks, it is important to analyze the dynamic interactions between intelligent attackers and defenders. Any attack-defense game should be modeled as a *Dynamic game*, which allows the rational players to adjust their attack/defense strategies towards obtaining higher payoffs over the opponents. This reflects the dynamic behaviors of players in realistic attack-defense systems. The randomized choices of the players form a mixed strategy game.
The dynamic interactions between players of the game can be modeled by a stochastic process for the maximization of utilities. The game moves from one state to another according to the

player's choices of strategy. The players receive their payoffs based on the actions chosen in each state of the game. The resulting model is a ***Stochastic game.***

To counter attack strategies, the defender's decision of strategies is powered by an *inference engine* which determines the appropriate defense strategy from its strategy set for each play of the game. It is pertinent for the defender system to consist of a knowledge base for storing game plays and their outcomes.

A conceptual model of a Cybersecurity Game is presented in Figure 7.

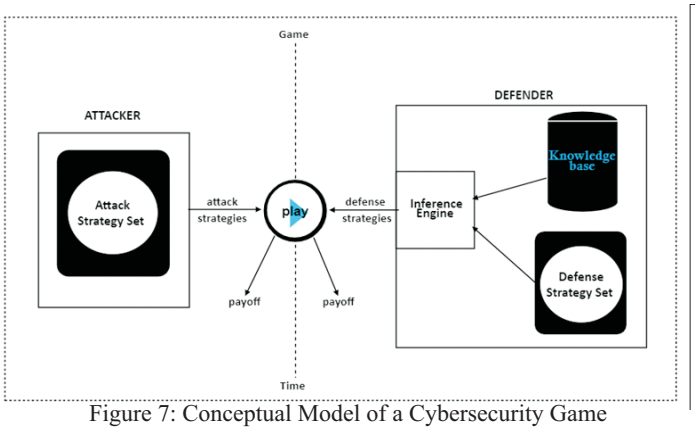

Figure 7: Conceptual Model of a Cybersecurity Game

In the case study, Distributed Denial of Service (DDoS) attack scenarios are analysed, and a game-theoretical approach is developed to enforce secure, resilient and dependable networked systems. In the developed system, a dynamic attack-defense game is modelled for a scalable defense mechanism.

4.3.1 *Game Formalization*

The interactions between the Botmaster and the Defender(s) in a Distributed Denial of Service (DDoS) attack scenario is modeled as a Game G_m.

The Game G_m is formulated as a:

- Two-player game: The attackers *(A)* and defenders *(D)* are considered as two players *P*.
- Dynamic game: This allows the players to alter attack/defense strategies (S_A, S_D) towards increasing their payoffs, thus reflecting the dynamic nature of players in an attack-defense system
- Non-zero-sum game: The player with the highest payoff wins the game.
- Non-cooperative game: The players are not bound to cooperate with each other as strategies are chosen independently by rational players to maximize their own payoffs.
- Finitely repeated game of incomplete information: The game is repeated *r* times, with the outcomes of all preceding moves observed before the next move. Also, the attacker has incomplete information or knowledge about the defender's strategies and payoffs, and vice versa.

Two strategy sets exist for the players, $S = (S_A, S_D)$. The Attack Strategy Set (ASS) is a finite set $S_A = \{S_{A1}, S_{A2}, ..., S_{AY}\}$ which includes finite number of attack strategies where $s_i \in S_A$ is an attack launched. The Defense Strategy Set (DSS) is a finite set $S_D = \{S_{D1}, S_{D2}, ..., S_{DZ}\}$ consisting of all possible defense strategies $S_j \in S_D$.

The game *Gm* is a set of plays. A play Φ is a pair of strategies (S_i, S_j) from the respective strategy sets. Two utility functions $\{U_A, U_D\}$ determine the payoffs gained by the two players in a given play. The utility function of a player is $U: S_A X S_D$ ---- R where R is a real valued function. Each player will either get a positive or negative payoff.

The game model should reach a stable state q_0 in which all players are satisfied with their payoffs and have no incentives to deviate. This is the optimal attack/defense strategy of the game and can be

obtained from the Nash Equilibrium.
Hence, Game *Gm* is defined as:

$G_m = \{(A, D), (\Phi: s_i x s_j), (U_A, U_D)\}$ (20)

The following sequence occurs between the attacker and the defender at a time *t*.

a. Players (A, D) selects strategies (S_i, S_j) from their respective strategy sets $\{S_A, S_D\}$.
b. For each play (s_i, s_j), the players evaluate their rewards and costs, to determine their payoffs $\{U_A, U_D\}$.
c. The game transits to a next play Φ until a stable state q_0 is reached.

4.3.2 *Game-Inspired Defense Architecture*

The main components of the Game-Inspired Defense Architecture are the Attacking System, Defending System and the Back-End, as represented in Figure 8.

In the attacking system, the botmaster uses Command-and-Control (C&C) servers to control bots to send malicious requests through varying attack strategies. These attack strategies are received by the Defending System. The defending system is powered by a Game Inference Engine. The Decision-making Model in the Game Inference Engine produces appropriate defense strategies to block malicious traffic while forwarding legitimate traffic to the server. Also, the defending system updates its knowledge base at the back end to enhance its learning capability and increase detection accuracy further.

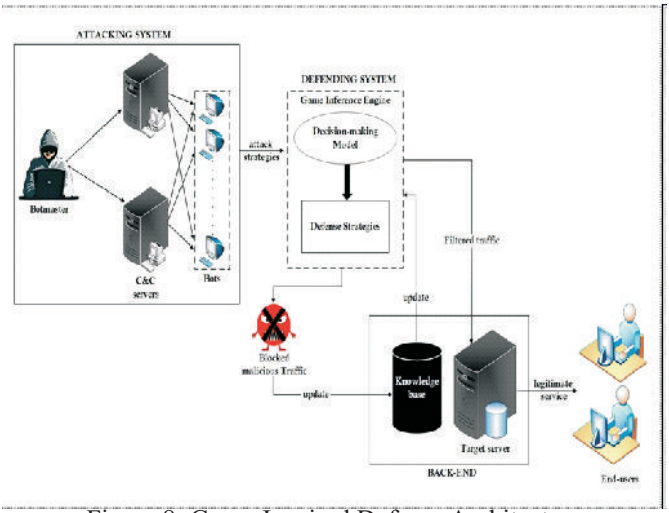

Figure 8: Game-Inspired Defense Architecture

4.3.3 *Game Inference Engine*

The Game Inference Engine (GIE) is the core of the Game-Inspired Defense Architecture, determining an appropriate defense strategy to counter each attack strategy. The Decision-Making Model in GIE is structured by a Markov Decision Process.

A Markov Decision Process (MDP) is a formalism extending Markov chains with actions and rewards. A Markov Decision Process is a discrete-time stochastic control process which models decision making for the maximization of utility. The stochastic process models the system behaviours, with a main advantage of capturing the system's dynamic behaviours.

The resulting game is a *Stochastic* game wherein the possible states is predicted based on the Markov transition model.

4.4 Cybersecurity Real players

a. Cyber or Digital Underworld (Cybercriminals): These are individuals or teams of people who use technologies and tools to commit malicious activities on digital systems or networks. Examples are hackers, crackers, social engineers,

cyberstalkers, 'yahoo-yahoo' and cyberspies
b. Cybersecurity Solution Providers (Organisations / Experts / Researchers: They constantly analyse the security of digital infrastructure and evolve strategies for safeguarding data and other resources. They develop hardware and software tools for mitigating attacks. They are responsible for threat analysis, risk assessment, cybercrime investigations and digital forensics
c. Wailers: Those who feel direct and indirect impact of cyberattacks such as governments, organisations, individuals and customers

4.5 The Muddy Waters in Winning the Cybersecurity Game

In a literal sense, *Muddy waters* simply describes water that is turbid or murky due to the presence of suspended particles or sediment. However, in a figurative or metaphorical sense, "*Muddy waters*" may be used to describe a situation, issue, or topic that is unclear, confusing, or lacking transparency. When someone "muddies the water," they may use tactics such as spreading misinformation, masquerading, deceit, presenting conflicting arguments, diverting attention to unrelated matters, or introducing unnecessary complexities. The term *Muddy waters* was coined to describe some specific activities of cybercriminals. The name was likely chosen for its metaphorical implications, evoking the image of murky or unclear waters, which could symbolize the elusive and covert activities of cybercriminals.

In the ever-evolving landscape of cybersecurity, new threats continue to emerge, challenging the defenses of organizations and governments worldwide. Security concerns grow day by day, with unpredictable rise of cyberattacks. Cybercriminals also used both existing and customized protocols to get their targets. Attackers' strategies are constantly unclear, oblivious and not definitive. It is indeed muddy waters!

4.6 Winning the Revolutionarised Cybersecurity Game

Attacks on Information Technology infrastructure will continue to grow and there will be increasing stories from the winners and vanquished. The cybersecurity experts have continued to witness tremendous revolution because attack landscape is ever changing and attackers will continue to adopt new sophisticated tactics and approaches. Consequently, winning the cybersecurity game requires adopting coordinated, dynamic, novel, multi-level, multiform, multi-approach, multi-tactics and multi-tiered strategies. Every of the players must be smart and highly skillful enough to be able to win the 'rofo-rofo' game. A cybercriminal can present himself/herself online as a legitimate friend, assistant, philanthropist, guidance, help-seeker, expert, owner of business or property, and so on.

The two sacred winners of cybersecurity game are presented as follows:

a. Cybersecurity Solution Providers / Experts are winning because they continue to evolve solutions that have curtailed mirage of small and large scale attacks

b. Digital Underworld (Cybercriminals) are still winning because organisations, governments and individuals still continue to experience different forms and landscape of attacks

But, the bigger winners are the cybercriminals!

5.0 CONCLUSION

Individuals, organisations and government will continue to experience different forms and magnitudes of cyberattacks. Cybersecurity Social engineering (phishing, pharming and spamming), insider, spoofing, identity theft, authentication, DDoS and ransomware attack incidences will continue to happen all over the world. It is now critical, more than ever, for everyone to pay

attention to cybersecurity issues. Addressing cybersecurity challenges is critical for rapid digital transformation and sustainable national development. Proactive strategies must be put in place by various organisations, including educational institutions. Machine learning and artificial intelligence are two technologies that could be used to develop proactive cybersecurity solutions. Using these modern technologies help to mitigate risks and reduce hazards.

Cybersecurity markets are expanding fast. As a nation, we need to develop our potentials to build indigenous capacity and have large share of the market. Cybersecurity professionals and experts are still limited in Nigeria to handle growing challenges. It is indeed a great development that NUC has approved B.Sc. Cybersecurity in Nigeria to develop necessary skills, knowledge and expertise in the field of Cybersecurity.

Muddy waters represent the unstable and multiform techniques used by cybercriminals in targeting their objects. Understanding the attackers' tactics, motivations and the potential impacts is essential for organizations to bolster their defenses and safeguard sensitive information. By staying informed, implementing best practices and fostering collaboration, we can work towards a more secure digital landscape.

A major concern is whether the attackers will be winners forever. It is certain that systems and network will continue to be penetrated and attacked. Security experts and researchers are fighting hard, but new proactive and robust approaches need to be employed. How prepared are we as individuals, organisations and government? We all need to all wake up and “shine our eyes”.. Cybersecurity must be seen as the business of everybody.

6.0 RECOMMENDATIONS

6.1 Individuals

i. Practice Password Safety: Always use strong and unique passwords for all online accounts. Passwords get old and become susceptible to thefts and attacks too. So, reset your passwords regularly to keep them fresh and unhackable.

ii. Enable Automatic Software Updates: Mitigating the danger of cybersecurity hacks by enabling automatic updates on your devices is a fool-proof way to beat out hackers.

iii. Review privacy settings: Regularly review and adjust the privacy settings on your social media accounts. Limit the visibility of your posts, personal information, and contact details to trusted connections. Be cautious about what you share publicly.

iv. Be mindful of friend requests and connections: Only accept friend requests or connection requests from people you know and trust. Be wary of requests from unknown individuals, as they may be attempting to gain access to your personal information or engage in malicious activities.

v. Enable two-factor authentication (2FA): Activate two-factor authentication on your social media accounts whenever possible. This adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone, in addition to your password.

vi. Be cautious of suspicious messages and links**:** Be wary of messages, comments, or direct messages containing suspicious links or requests for personal information. Avoid clicking on unknown links or downloading attachments from untrusted sources.

vii. Think before you share: Before posting or sharing content on social media, consider the potential impact and who can see it. Be cautious about sharing personal details, such as your

location, schedule, or financial information, as this information can be exploited by cyber criminals.

viii. Regularly review connected apps and permissions: Periodically review the third-party apps or services connected to your social media accounts. Remove any apps that you no longer use or trust. Check and adjust the permissions granted to these apps, limiting access to only necessary information.

ix. Get basic education about cybersecurity and privacy: Familiarize yourself with cybersecurity and data privacy fundamentals

x. Be cautious of public Wi-Fi: Avoid accessing your social media accounts through public Wi-Fi networks, as they may not be secure. If you need to use public Wi-Fi, consider using a virtual private network (VPN) to encrypt your connection and protect your data.

xi. Report suspicious or abusive behavior: If you encounter suspicious or abusive behavior on social media, report it to the platform's support team. This helps maintain a safer online environment for yourself and others.

6.2 Governments / Corporate Organisations

For proactive cybersecurity management, corporate organisations and government should:

i. Create security training and awareness programme within the organization

ii. Make sure that all connections to the network are known, documented and monitored

iii. Have an efficient access control system

iv. Implement trusted and efficient intrusion prevention and detection systems

v. Have an effective programme for backup and recovery

vi. Use security applications from reliable vendors

vii. Ensure periodic evaluation of all security apparatus

viii. Regularly apply security patches and software updates.

ix. Apply the least-privileged principle across the network, especially to critical systems and services.

x. Secure domain controllers (DC) using best practices.

xi. Enable multifactor authentication (MFA) to prevent lateral movement.

xii. Every organization must develop policies and plans for cybersecurity management.

xiii. Conduct regular risk and vulnerability assessments on Information Technology platforms.

xiv. Develop a multi-lingual attack reporting platform.

xv. Set up Computer Emergency Response Team (CERT) for swift response to attack incidences.

xvi. Intelligence of the hackers must be harnessed by government for the development of our nation

6.3 The University Community

Apart the stated recommendations, the university should support the creation of College of Computing to develop adequate manpower and expertise needed in the field of cybersecurity.

7.0 ACKNOWLEDGEMENTS

I give glory and adoration to the Almighty God for His love over my life. The Lord is my light! He has been so kind to me! He has been my source of inspiration from birth till now. I will ever remain grateful to you Lord.

I thank my caring parents, Late Mr. Samson A. Sodiya (died December 28, 2015) and Mrs. Christiana Idowu Sodiya, for their determination, restlessness and doggedness in making me to be successful in life. They taught me the ways of God, hard work, diligence, respect, honesty, and inculcate in me the values of education. My parents actually borrowed, sold their resources and made sacrifices for me to have sound education. Adieu Daddy! May you continue to rest in the blossom of the Almighty God. My mummy, (fondly called Mama Sina), you are the best mother in the whole world. I appreciate you always ma. I also thank all my siblings: Kayode Sodiya, Doyin Sodiya. Gbemi Sodiya, Kemi Aina and Seyi Sodiya. I must specially recognized my uncle (who I also call my second daddy), Chief Jonathan O. Soremi, for his immense support, unconditional love, encouragement and support in my journey in life. I appreciate all my cousins for providing opportunities to lean on each other in our development in life. Some of them are Dapo Soremi.Yemi Soremi, Tunji Soremi, Tunde Atobatele, Olumide Soremi, Demola Soremi, Akinwunmi Soremi, Bukola Aiyelabola, Akintunde Soremi and Yinka Olujinmi.

My secondary school classmates (the eminent set of BBHS) deserve special mention for their total cooperation and support during and after school periods. Some of them are Bar. Dare Oloyede, Dr.Femi Soetan, Dr.Tunde Sobande, Dr. Aydele Sogebi, Bar. Dotun Onafowope, Dr. Jide Dasaolu, Engr. Bola Sowunmi, Dr. 'Segun Adeleye, Dotun Olaifa and Engr. Onafowora. Also, I appreciate my colleagues at undergraduate and postgraduate levels. They created a true friendship environment for me to thrive. Some of them are Fola Solu, Gbenga Oduwaye, Tunde Abosede, Ope Adesanya, Dr. Lanre Ayannuga, Demola Quadri, Mrs. Tundun Adekunte, Dr. Tunji Oreyingbo,, Segun Oyebolu, Demola Quadri, and Seyi Ogunlaru. I cannot hold my joy when I remember the sweet memories and affectionate times we shared together during our school days.

I cannot forget my childhood friends and staunched folks who have made significant impact in my development. Mr. Segun Adeleye, Anuoluwapo Dosunmu, Mr. Sina Sanusi, Mr. Afolabi Adekanmbi, Pharm. Kehinde Ajayi, Prof. Biodun Badmus, Jide Sofunde. I thank you so much for your kindness, sincerity, and generosity.

On my journey through life's path to this height, I acknowledge the contributions of some lecturers at various points of my academic training, notably; Prof. H. O. D. Longe who taught me at both undergraduate and postgraduate levels, and later became my supervisor at Ph.D level. It was a wonderful priviledge to be under his tutelage as I developed my academic career. I cannot also forget Late Prof. S. B. Jayesinmi, Late Prof. B. A. Sofoluwe, Prof. Charles O. Uwadia, Mr. Niyi Ajao, and Prof. J. A. Ayeni, who supervised my M.Sc. dissertation in University of Lagos I thank you so much for your sacrifices and selflessness in ensuring that I made progress in life.

My sincere thank goes to Prof A. R. T. Solarin, who facilitated the commencement of Ph.D programmes in the defunct Department of Mathematical Sciences. I thank you for your leadership acumen and disposition when we were together.
Mr. Vice Chancellor Sir, kindly permit me to express my indebtedness and appreciation to many people in this great University who had assisted in their respective capacities in providing enabling environment for my growth and development. First among them is of course the substantive Vice Chancellor, Prof. Olusola Babatunde Kehinde, for giving me the opportunity to present this 80th Inaugural Lecture. I sincerely appreciate your friendliness, tenacity, leadership skills and commitment to the development of this unique Federal University of Agriculture, Abeokuta. I would like to express my deep gratitude to you Sir for your invaluable support at all times.

I would like to appreciate the following former Vice-Chancellors of the Federal University of Agriculture, Abeokuta for creating the needed opportunities for me to work in this university. The 2nd Vice-Chancellor, Prof Julius Okojie, approved my temporary appointment as Assistant Lecturer in 2001 in the defunct Mathematical Sciences Department, The 3' Vice Chancellor, late Prof. Isreal Adu, confirmed my appointed in 2002. The 4th Vice-Chancellor, Prof Olaiya Oluwafemi Balogun, who gave me accelerated appointment as a Senior Lectuer, and the 5" Vice-Chancellor, Prof. Bamidele Oyewole, who appointed me as Acting Head, Computer Science and also processed my promotion to Professorship position, and the 6th Vice-Chancellor, Prof. F. K. Salako, for his encouragement and support to become the President of Nigeria Computer Society (NCS). I also worked closely with the 1st and 2nd Acting Vice-chancellors, Prof. Ishola Adamson and Prof Olalade Enikuomehin and wish to express my special appreciation for their contributions to my development.

I would like to thank the present Deputy Vice Chancellor (Academic), Prof. C. O. N. Ikeobi, Prof. K Adebayo, Deputy Vice Chancellor (Development), the Registrar, Dr. Adebola Adekola, the Bursar, Mr Chukwunwike Ezekpeazu and the Librarian. Dr. Kehinde A. Owolabi. My thanks go to former Principal Officers, notably, Prof (Mrs) Morenike Dipeolu, Prof Lateef Sanni, Prof O. J. Ariyo, Prof C. F. I. Onwuka, Prof S.T. O. Lagoke, Prof T. A. Arowolo, Prof M. A. Waheed, Prof C. O.Adeofun and Prof I. C. Eromosele.

My profound thanks go to my Dean, Prof. A. T. Akinwale for his encouragement and support since I joined the university. He really encouraged me to present this special inaugural lecture. I am particularly grateful to my Head of Department, Prof. (Mrs.) O. T. Arogungade for her esteemed support, contributions and

coordination of activities toward this Inaugural Lecture. My regards go to my colleagues with whom I have worked harmoniously with over the years and have inspired me to provide the needed leadership. Let me specially mention Prof O. Folorunso, Prof. O. A. Ojesanmi, Prof (Mrs) S, A, Onashoga, Prof. (Mrs) O. I. Arogundade, Prof. (Mrs) O. R. Vincent, Dr. F. T. Ibharalu, Dr. A. Abayomi-Alli, Dr. D. O. Aborisade, Dr. (Mrs) E. O. Ojo, Dr. (Mrs.) Alabi, Dr. (Mrs.) C. O. Tinubu, Dr. Olorunjube Falana, Mrs A. O.Adejimi, Mr. C. O. Ugwunna and Mrs. Morenikeji Kareem.

My heart is full of gratitude to the other Heads of Department in the College of Physical Sciences, Prof. (Mrs) Modupe Idowu, Prof. B. I. Olajuwon, Prof. (Mrs) I. C.Okeyode and Dr O. M. Olayiwola. They are providing platforms for enhancing good relationship and needed academic leadership in the college. I would like to appreciate former Deans of the College of Physical Sciences, Prof. Oluyemisi Eromosele and Prof Amidu Mustapha for their leadership roles and continuous efforts in lifting the college up. I thank also the present and past Deputy Deans, Prof. V. Makinde and Prof A. K. Akinlabi for their loyalty and support to run the College.

I am most grateful to the fellow professors in the College for their assistance and genuine love at all times, notably; Prof J. A. Oguntuase, Prof. O. J. Adeniran, Prof A. A. A. Agboola, Prof M. O. Omeike, Prof O. D. Akinyemi, Prof G. A. Adebayo (Dean, PGS), Prof (Mrs.) I. C. Okeyode, Prof L. A. Arogundade, Prof E. A. Dare and Prof. Adewuyi. Prof. S. O. N. Agwuegbo, Prof. T. A. Afolabi, Prof. A. I. Adeogun, Prof. S. A.Amolegbe, Prof. S. S. Sojinu, and Prof. I. A. Osinuga. I must also appreciate some of the upcoming professors in the college; Dr. (Mrs) T. F. Akinhanmi, Dr F. O. Oladoyinbo, Dr. A. T. Aremu, Mr F.Akinwunmi, Dr. S. A.Akinleye, Dr. E. O. Adeleke, Dr E. Ilojide, Dr. M. T. Raji, Dr O. J. Ogunsola, Dr A. A .Adeyanju, Dr. D. O. Adams, Mr A. A. Yusuff

and Mr F. M. Nkwuda. Others are Dr. (Mrs) O. Alatise, Dr F. G. Akinboro, Dr. J. O.Akinlami, Dr G. O. Layade, Dr A. A. Alabi, Dr O. T. Olurin, Dr S.A. Ganiyu, Dr O. P. Adebambo, Dr. A. I. Egunjobi, Mr. K. D.Ajayi, Dr. (Mrs) F. S. Apantaku, Dr. G. A. Dawodu, Dr. (Mrs.) A. A. Akintunde, Dr. (Mrs.) O. A. Wale-Orojo, Dr. A. T. Soyinka, Mr. A. Ajayi and Mrs B. S. Adetona.

I also appreciate the Dean of our Sister College, Prof. (Mrs.) Kehinde and the former Deans, the defunct College of Natural Sciences, Late Prof E. O Asiribo, Prof T. O. S. Popoola and Prof A. D. Agboola. I would like to appreciate present Deans and former Deans of the various Colleges in this great University for the love to me and the College of Physical Sciences notably, Prof O. A. Akinloye, Prof. M. O. Atayese, Prof O.S. Sowande, Prof I. I. Omoniyi, Prof E. O. Fakoya, Prof S. O. Ismail, Prof. O. U. Dairo, Prof M. A. Idow, Prof W. A. O. Afolabi, Prof (Mrs) B. B. Phillip, Prof A. O. Dipeolu, Prof C. O. Ikeobi, Prof J. G. Bodunde, Prof J. K. Adewunmi and Prof A. K.Akinloye. I appreciate all my research collaborators; Prof I. A.Adejumobi, Dr O. A. Akinola, and Prof Afolabi. Generally, I want to specially thank all the academic and non-teaching staff of the University for their Attendance.

My endless gratitude goes my professional colleagues in Nigeria Computer Society (NCS) and Computer Professionals (Registration Council of Nigeria) – CPN. Notable ones are members of the last National Executive Council (NCS): Mr. Kole Jagun FNCS – President/Chairman of Council, CPN, Dr. Muhammad Sirajo Aliyu, FNCS – Deputy President, Prof. Adesola Aderounmu, FNCS – Immediate Past President, Prof. Oludele Awodele, FNCS – Chairman, Credentials Committee, Dr. Charles C. Onyekwu, FNCS – Chairman, Ethics and Disciplinary Committee, Mrs. Shulammite A. Ilebiyi, FNCS – Chairman Audit Committee, Mrs. Margaret John David, FNCS – Chairman, Publicity, Events and Trades Services Committee, Dr. Olusoji B. Okunoye, FNCS – Chairman, Innovation, Research and

Development Committee, Dr. Moyin Florence Babalola – Chairman, Education and Manpower Development Committee, Ayodeji Rex Abitogun, FNCS – Chairman Conferences Committee, Mr. Bayo Mohammed Onimode – Ex-Officio, North Central Zone, Mr. Bassey Okwong Esang, FNCS – South South Zone, Prof. Adebukola Onashoga, FNCS – Ex-Officio, South West Zone, Dr. Stanley Adiele Okolie, FNCS – Ex-Officio, South East Zone, Mr. Abubakar Musa Mohammed, FNCS – Ex-Officio, North East Zone, Dr. Usman Abdullahi Ali, FNCS – Ex-Officio, North West Zone, Mr. Chinenye Mba-Uzoukwu, FNCS – President, Institue of Software Practitioners of Nigeria (ISPON), Mrs. Bamidele O. Bayo-Osibo, FNCS – President, Nigerian Women in Information Technology (NIWIIT), Dr. Segun O. Olorunyomi, FNCS – President, Nigerian InfoTech Professionals in the Civil & Public Service (NITPCS), Adedayo P. S. Arogundade, FNCS – President, InfoTech Systems and Security Professionals (ITSSP), Prof. Yusuf Benson Baha – President, Academia in Information Technology Profession (AITP) and Adesegun Adekunle, FNCS – Executive Secretary. My special thanks to the past presidents and elders of our society, namely Prof. (Bishop) 'Bayo Akinde Mr. Tunde Ezichi, Prof. C. O. Uwadia, Sir. Demola Aladekomo, Prof. O. D. Adewunmi, Prof. G. A. Aderounmu, Dr. Abimbola Salako, Dr. Odeyemi, Prof. (Mrs.) Adenike Osofisan, Chief (Dr.) Leo Stan, and Mr. Ibrahim Tizhe (Provost, College of Fellows). Some of members that have played key roles in my academic and professional career are Alhaji Mohammed Bello, Registrar CPN, Mr. Bimbo Abioye, MD/CEO FinTrack, Mr. Kazeem Tewogbade MD Bluechips Technologies. I must thank all fellows and members of NCS who are attending this event.

I must recognize and appreciate some wonderful and exciting people that I met during my professional engagements, namely, Mr. Kashifu Inuwa, DG NITDA, Engr. Aliyu Aziz, DG NIMC,

Prof. Muhammad Abubakar, DG Galaxy, Arch. **Sonny Echono,** Executive Secretary, Tetfund, and Dr. Illyasu B. Gaashinbaki, President, Chartered Institute of Forensic and Certified Fraud Investigators of Nigeria. They have become dependable partners and true friends.

I want to specially thank all my students at both undergraduate and postgraduate levels in Nigeria and abroad. Through them, I have been able to manifest my potentials. Specifically, I wish to mention those completed their Ph.D programmes under my supervision namely, Dr. 'Ronke Ikuomola, Associate Professor at Ondo State University of Science and Technology; Dr. D. A. Aborisade, a Senior Lecturer, Dr. C. O. Tinubu, Dr. Olorunjube Falana, Lecturer II in my department; Dr. Abiodun Orunsolu, Principal Lecturer at Moshood Abiola Polytechnic Abeokuta, Dr. Sunday Agholor; Chief Lecturer and Dr. 'Dayo Elugbadegbo a Principal Lecturer both at Federal College of Education, Osiele, I specially recognize and appreciate all my current and previous masters students too.

Special gratitude to all my academic and professional colleagues that have joined all over the world. I appreciate all my friends and colleagues in Confederation of Africa Computing and Information Technology Societies (CACITS): Churchils from Kenya, Moira from South Africa, Joyce from Zimbabwe, Kwaku from Ghana, Christophe from Rwanda and Wisdom from Ghana. You are all wonderful and committed to IT development in Africa.

To all my Pastors, Pastor Kolawole Ajibowo (PICP) and Pastor 'Kunle Ajisafe (APICP), and other church members, I am grateful for all your prayers and love. The list of those to be acknowledged is indeed inexhaustible. I do profusely apologise to all those who deserve to be so acknowledged at this gathering. God knows all of you and I owe you a lot of gratitude.

I cannot end this lecture without appreciating the members of Publication Committee, especially Prof. (Mrs.) H. A. Bodunde and Prof. (Mrs.) Bosede Sotiloye. Their contributions have really enriched this lecture. To all those present here today including all around the world watching through webinar (zoom), I remain eternally indebted and hereby inform that comments and criticism remain most welcomed (sodiyaas@funaab.edu.ng) which will engender further research.

Mr Vice Chancellor Sir, I am exceptionally grateful to my nuclear family. They have shown staunch and utter supports throughout my academic career. They have always provided abundant care, meaningful guidance and nurturing home. My children: Ibukunoluwa, Ayomipo, Ireoluwa and Anuoluwa Sodiya, are special blessings in my life. I deeply appreciate my delectable, alluring, dependable, sedulous, amiable and diligent wife, Prof. (Mrs.) Comfort Ibironke Sodiya. She has provided conducive atmosphere that allowed me to reach this level of academic achievement. She has tolerated my inadequacies and excesses. Your presence in my life has indeed enabled progress in my life. Thank you for being there as a pillar of support and encouragement. My prayer is that God will continually shield you, the children and I, and bless us with good health and sound mind.
I thank you all for your kind attention.
God bless (amen).

8.0 REFERENCES

Abiodun, O. A., **Sodiya, A. S.**, Kareem, S. O., Oladimeji, G. B. (2021). Performance Assessment of some Phishing predictive models based on Minimal Feature corpus. *The Journal of Digital Forensics, Security and Law: JDFSL* 16, 1-19

Aborisade, D. A., Reich, C., **Sodiya, A. S.** and Akinwale, A. T. (2016). "Call Response Rate as Baseline for Detecting DRDoS

Attack in Cloud Database Service", 5th Conference on Software Technology and Processes (STeP 2016) held on 3th May, 2016 at Hochschule Furtwangeng University, Germany. Pp 49 – 60. www.degruyter.com, http://www.step2016.de

Aborisade, D. O., **Sodiya, A. S.** and Ikuomola, A. J. (2013). "A Survivability Architecture for Object-Oriented Software Systems", *Journal of Information Assurance and Security*, Vol. 8, No. 4, pp 167-176, published by Machine Intelligence Research Labs., USA.

Adebesin, A. A., **Sodiya, A. S.**, Orunsolu, A. A., Lawal, O. A., & Kareem, S. O. (2021). A Proposed Distributed Anti-Phishing Framework for mitigating Cyber-attacks in Smart Environments.

Adigun M. F., Orunsolu A. A., **Sodiya A. S.** and Onashoga, S. A. (2018). An Efficient Framework for a Secured Internet of Things Architecture, Proceedings of the 1st International Conference of Education and Development, Organised by Academia in Information Technology, Abuja, between 25 – 27 April, 2018.

Agholor, S., **Sodiya, A. S.** and Aborisade, D. A. (2016). A comparative analysis of cybersecurity laws of selected countries, Proceedings of the 2nd International Conference on Intelligent Computing and Emerging Technologies, held between 20 – 22 November, 2016 at Babcock University, Ilisan, Ogun State.

Agholor, S., **Sodiya, A. S.**, Akinwale, A. T. and Adeniran, O. J. (2016). A secured Mobile-Based Password Manager, Published in the proceedings of 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC), held between 21 – 23 April, 2016 in Beirut, Lebanon.

Agholor, S., **Sodiya, A. S.**, Akinwale, A. T., Adeniran, O. J. and Aborisade, D. O. (2016). A Preferential Analysis of Existing Password Managers from End-Users' View Point, *International Journal of Cyber-Security and Digital Forensics* (IJCSDF) Vol. 5,

No. 4, pp 187-196, published by the Society of Digital Information and Wireless Communications (SDIWC), USA.

Agholor, S., **Sodiya, A. S.**, and Aborisade, D. O. (2018). A Mathematical Model for Resolving Minimum Password Length Controversy, *International Journal of Cyber-Security and Digital Forensics* (IJCSDF) Vol. 7, No. 1, pp 1 - 9, published by the Society of Digital Information and Wireless Communications (SDIWC), USA.

Akinwale, A. T., Shonubi, A. J., Adekoya, A. F., **Sodiya, A. S.** and Mewomo, O. T. (2013). "Ontology of Input Validation Attack on Web Application", *Business Informatics*, 4(30), pp 11-23, published by Wroclaw University of Economics, Poland. Available online at http://www.wydawnictwo.ue.wroc.pl/o_wydawnictwie/63,informatyka_ekonomiczna_business_informatics.html

Fadahunsi, I., Arogundade, O. 'Tale, ***Sodiya, A. S.****, & Olajuwon, B. (2019).“Towards a UMLsec-Based Proctored Examination Model”, International Journal of Systems and Software Security and Protection, Vol. 10, No. 2, pp 44–67. doi:10.4018/ijsssp.2019070103*

Falana, O. J., **Sodiya, A. S.**, Onashoga, S. A. and Folorunso, O. (2022). Mal-Detect: An Intelligent visualization approach for malware detection, by Elsevier *Journal of King Saud University – Computer and Information Sciences*, accepted for publication.

Falana, O. J., **Sodiya, A. S.**, Onashoga, S. A. and Oyewole, T. (2020). “PEDAM: Priority execution-based approach for detecting android malware”, published in Springer Lecture Notes in Network and Systems. 254.

Oluwumi E.O., Tinubu, C.O., Falana, O. J., **Sodiya, A. S.**, and Odeniyi, O.Y. (2022).Modelling Cybersecurity Knowledge and Attitudes of Online Users. In Proceedings of the International

Conference of Nigeria Computer Society (NCS), **A.S. Sodiya** and O.B. Okunoye (Eds.), 33: 194-201, ISSN: 2141-9663, Published by the Nigeria Computer Society (NCS).

Oluwumi, E. O., **Sodiya, A. S.**, Onashoga, S. A., Chima, A. O., & Emmanuel, J. A. (2019).An Enhanced Pattern-based Detection for Computer Virus. *International Journal of Information Security, Privacy and Digital Forensics,* Vol. 3(1), pp. 45 – 51.

Onashoga, A., **Sodiya, A.**, and Osinuga, I. (2019). Privacy Preserving Location-Based Client-Server Service Using Standard Cryptosystem. *Journal of computing and information technology*, 27(4), 47-63.

Onashoga, S. A., **Sodiya, A. S.**, and Afolorunso, A. (2012). "A One-time Sever-specific Password Authentication Scheme", *Journal of Computing and Information Technology*, Vol. 20, No. 2, pp 85-93, ISSN: 1330-1136, published by University of Zagreb, Croatia. Available online at www.cit.srce.hr.

Oni, O. O., **Sodiya, A. S**., Vincent, O. R. Okeyinka, I. K. and Afolorunso, A. (2020). "A three-tiered notification system for critical information infrastructure protection using control flow integrity", *Journal of Computer Science and Its Applications*, December 2020.

Orunsolu, A. A, **Sodiya, A. S.**, Akinwale, A. T., and Olajuwon, B. (2017). A Users' Awareness Study and Influences of Social-Demography Perception of Anti-Phishing Security Tips, *Acta Informatica Pragensia*, published by University of Economics, Prague, Czech Republic, Vol. 7, No. 2, pp138-151.

Orunsolu, A. A. and **Sodiya, A. S.**(2017). An Anti-Phishing Kit Scheme for Secure Web Transactions, Proceedings of the 3rd International Conference on Information Systems and Privacy, Portugal held between 19 – 21 February 2017.

Orunsolu, A. A. **Sodiya, A. S.**, Kareem, S. O. (2020). Link calculator–an efficient link-based phishing detection tool. *Acta Informatica Malaysia*, 4(2), 37-44.

Orunsolu, A. A., **Sodiya, A. S.**, and Folorunso, O. (2019). A predictive model for phishing detection, *Journal of King Saud University – Computer and Information Sciences*, published by Elsevier. Available at 10.1016/j.jksuci.2019.12.005.

Orunsolu, A. A., **Sodiya, A. S.**, and Oyekan, D. F. (2012). "Destructible Password Functionality Authentication Protocol", *African Journal of Computing and ICTs*, Vol. 5, No. 2, ISSN: 2006-1781, published by IEEE Nigeria Computer Chapter. Available online at http://www.ajocict.net.

Orunsolu, A. A., **Sodiya, A. S.**, Folorunso, O. O., Agboola, A. A. A. (2016).A Distributed Password Authenticated Key Exchange Protocol Using A Hybrid Approach. Annals. *Computer Science Series* 14 (2)

Orunsolu, A., Afolabi, O., **Sodiya, A. S.**, and Akinwale, A. T. (2017). An Anti-Phishing Scheme for Secured Web Transaction, *International Journal of Electronics and Information Engineering*, published by National Chung Hsing University, Taiwan, Vol. 6, No. 2.

Sodiya, A. S., Longe, H. O. D. (2004a)."An Improved Two-Tiered Strategy To Intrusion Detection", *International Journal of Information Management and Computer Security*, Vol. 13, No. 3, pp 235-243, ISSN: 0968-5227, published by Emerald, UK. Available online at www.emeraldinsight.com/imcs.htm

Sodiya, A. S., Longe, H. O. D., and Akinwale, A. T. (2004b). "A New Two-tiered Strategy To Intrusion Detection", *International Journal of Information Management and Computer Security*, Vol.

12, No 1, pp 27-43, ISSN: 0968-5227, published by Emerald, UK. Available online at www.emeraldinsight.com/imcs.html

Sodiya, A. S., and Longe, H. O. D. (2004c). "Intrusion Detection Systems: The problems, Prospects and the Way Forward", *Journal of Applied Computer Science*, Vol. 12, No. 1, pp 83-95, ISSN: 1507-0360, published by Technical University of Lodz, Poland. Available online at http:/www.ics.p.lodz.pl/jacs.html

Sodiya, A. S., H. O. D. Longe (2004d). A new combined strategy to intrusion detection. *Journal of Applied Computer Science* 12 (1), 97-116

Sodiya, A. S., Longe, H. O. D., and Akinwale, A. T. (2005a). "Maintaining Privacy in Anomaly-based Intrusion Detection System", *International Journal of Information Management and Computer Security*, Vol. 13, No. 1, pp 72-80, ISSN: 0968-5227, published by Emerald, UK. Available online at www.emeraldinsight.com/imcs.htm

Sodiya, A. S., Longe, H. O. D., and Ibrahim, S. A. (2005b). "Data Mining Based Intelligent Equipment Maintenance In Telecommunication Network", *Journal of Applied Computer Science*, Vol. 13, No. 1, pp 29-38, ISSN: 1507-0360, published by Technical University of Lodz, Poland. Available online at http:/www.ics.p.lodz.pl/jacs.html

Sodiya, A. S. (2006a). "Multi-level and Secured Agent-Based Intrusion Detection System", *Journal of Computing and Information Technology*, Vol. 14, No. 3, pp 217-223, ISSN: 1330-1136, published by University of Zagreb, Croatia. Available online at www.cit.srce.hr

Sodiya, A. S., Ibrahim, S. A., and Ajayi O. B. (2006b). "Towards Building Secure Software Products", *Journal of Issues in Informing Science and Information Technology*, ISSN: 1547-

7684, Vol. 3, 2006, pp 635-646, ISSN: 1547-7684, published by Informing Science Institute, USA. Available online at http://IIST.org

Sodiya, A. S. (2007a). "A Natural Language Architecture", *Journal of Computing and Information Technology*, Vol. 15, No. 1, pp 25-32, ISSN: 1330-1136, published by University of Zagreb, Croatia. Available online at www.cit.srce.hr

Sodiya, A. S., Ikuomola, A. J. and Adeniran, O. J. (2007b). "An Expert System-based Site Security Officer", *Journal of Computing and Information Technology*, Vol. 15, No. 3, 2007, pp 227-235, ISSN: 1330-1136, published by University of Zagreb, Croatia. Available online at www.cit.srce.hr

Sodiya, A. S., Longe, H. O. D., Onashoga, S. A., Awodele, O. and Omotosho, L. O. (2007c)."An Improved Assessment of Personality Traits In Software Engineering", *Interdisciplinary Journal of Information, Knowledge and Management*, Vol. 2, pp 163-177, IISN: 1555-1229, published by Informing Science Institute, USA. Available online at http://IJIKM.org

Sodiya, A. S., Onashoga, S. A., and Oladunjoye, B. A. (2007d). "Threat Modeling Using Fuzzy Logic Paradigm", *Journal of Issues in Informing Science and Information Technology*, USA, Vol. 4, 2007, pp 53-61, published by Informing Science Institute, USA. Available online at http://IIST.org

Sodiya, A. S., Onashoga, S. A., Rosanwo, O. D. and Lawal, B. H. (2008a). "Managing ICT Infrastructure in Higher Educational Institutions", Proceeding of 3rd International Conference on Science and National Development, O. E. Asiribo and J. A. Oguntuase (Eds), pp 60-67, ISBN: 978-2783-85-4, published by College of Natural Sciences, University of Agriculture, Abeokuta, Nigeria.

Sodiya, A. S., Akinwale A. T. and Onashoga, S. A. (2008b)."A

Framework for Mixed Cropping Decision Support System", Proceedings of the 22nd National Conference of Nigeria Computer Society (NCS), Y. O. Folajinmi and I. K. Oyeyinka (Eds) Vol. 19, pp 181-186, published by NCS.

Sodiya, A. S., Longe, H. O. D., and Fasan, O. M. (2008c). "Software Security Risk Analysis Using Fuzzy Expert System", *INFOCOMP: Journal of Computer Science*, Vol. 7, No. 3, pp 70-77, ISSN: 1807-4545, published by Universidade Federal de Lavras, Brazil. Available online at www.dcc.ufla.br/infocomp

Sodiya, A. S., and Onashoga, S. A. (2009a). "Components-based Access Control Architecture", *Journal of Issues in Informing Science and Information Technology*, USA, Vol. 6, 2009, pp 53-61, ISSN: 1547-7684, published by Informing Science Institute. Available online at http://IIST.org

Sodiya, A. S., Onashoga, S. A. and Adepoju, B. T. (2009b). "Evaluating the Impact of Intrusions on Computer System", *Journal of Computer Science and Its Applications*, Vol. 16, No. 1, June, 2009, ISSN: 2006-5523, published by Nigeria Computer Society, Nigeria.

Sodiya, A. S., Akinwale, A. T., Okeleye, S. A. and Emmanuel, J. A. (2010). "A Decision Support System for Intercropping", *International Journal of Decision Support System Technology*, Vol. 2, No. 3, 2010, pp. 51-66., ISSN: 1941-6296, published by Information Resources Management Association, USA. Available online at www.igi-global.com/ijdsst

Sodiya, A. S., Onashoga, S. A., and Adelani, D. I. (2011a). "A Secured E-voting Architecture", Proceedings of the 8th International Conference on Information Technology: New Generations, Las Vegas, USA, S. Latifi (Ed), pp 342-347, published by international Institute of Electrical and Electronics Engineering (IEEE).

Sodiya, A. S., Folorunso, O. and Ogunderu, O. P. (2011b). "An Improved Semi-Global Algorithm for Masquerade Detection", *International Journal of Network Security*, Vol. 13, No. 1, 2011, pp. 31-40, ISSN: 1816-353X, published by National Chung Hsing University, Taiwan. Available online at http://ijns.femto.com.tw/

Sodiya, A. S., Folorunso, O., Komolafe, P. A. and Ogunderu, O. P. (2011c)."Preventing Authentication Systems from Keylogging Attacks", *International Journal of Privacy and Security*, Vol. 7, No. 2, pp 3-27, ISSN: 1553-6548, published by Information Resource Management Association, USA. http://jips.cob.tamucc.edu/issues.htm

Sodiya, A. S., Onashoga, S. A., Afolorunso A. A. and Ogunderu, O. P. (2011d)."A Countermeasure Algorithm For Password Guessing Attack", *International Journal of Information and Computer Security*, Vol. 4, No. 4, ISSN: 1744-1765, published by Inderscience, Switzerland. http://www.inderscience.com/browse/index.php?journalID=151

Sodiya, A. S. and Orunsolu, A. A. (2013). "An Adaptive Hierarchical Access Control Architecture Using Compliance Variance", *Anale. Seria Informatica*, Vol. 11, No. 2, pp 109-115, published by "Tibiscus" University, Romania.

Sodiya, A. S., Falana, O. J., Onashoga, S. A. and Badmus, B. S. (2014). "Adaptive Neuro-Fuzzy System for Malware Detection", *Journal of Computer Science and Its Applications*, Vol. 21, No. 2, pp 20-31, published by Nigeria Computer Society, Nigeria.

Sodiya, A. S., Onashoga, S. A., Solarin-soda, T. and Falana, O. J. (2015a). "A Hybrid Approach to Masquerade Detection", *Journal of Computer Science and Its Applications*, published by Nigeria Computer Society, Vol. 25, No. 1.

Sodiya, A. S. and Adegbuyi, B. (2015b). A Framework for Protecting Users' Privacy in the Cloud, *International Journal of Information Security and Privacy*, USA. Vol. 4, No. 10, pp 1 – 11. DOI: 10.4018/IJISP.2016100102.

Sodiya, A. S. and Adesegun, O. (2017). A Metamorphic Malware Detection System, *International Journal of Information Security, Privacy and Digital Forensic*, published by Nigeria Computer Society, Vol. 1, No. 1.

Sodiya, A. S., Mustapha A. M, Adegboyega, A. A. and Odeniyi, O. Y. (2019). A Framework for Participatory E-government System, Proceedings of the 2nd International Conference of Education and Development, Organised by Academia in Information Technology, Abuja, between 24 – 26 April, 2019.

Sodiya, A. S., Oluwumi, E. O., Onashoga, S. A., and Akinola, O. A. (2021). A Data Augmentation-based System for Future Malware Prediction. *International Journal of Information Security Privacy and Digital Forensics*. Vol. 5, No. 2, Dec. 2021

Tinubu, C. O., Aborisade, D. O, **Sodiya, A. S**., and Ganiyu, M. A. (2009).“Towards detecting credit card frauds using Hidden Markov Model”, *Jo*urnal of Computer Science and Its Applications, Vol. 26, No. 2, 2009, ISSN: 2006-5523, published by Nigeria Computer Society.

Tinubu, C.O., **Sodiya A.S.**, Aborisade, D.O. and Afaraetu, R. (2019). PHISHLIGENT: An Intelligent Anti-Phishing Classifier. In Proceedings of the 3rd International Conference on Applied Information Technology, A.T Akinwale, O. Folorunso, E. Godspower and S.A Onashoga (Eds.) 202-210, ISBN: 978-978-950-229-5, Published by Nigeria Computer Society (NCS) and Department of Computer Science, Federal University of

Agriculture, Abeokuta.
Tinubu, O. C., O. J. Falana, **Sodiya, A. S.** (2021).Modelling Attendees' Participation in Virtual Events. *Journal of Computer Science and Its Application* 28(2), 70-74.

Tinubu, C.O., **Sodiya, A. S.**, Ojesanmi, O.A., Adeleke, E.O. and Adebowale, A.O. (2022). DT-Model: A Classification Model for Distributed Denial of Service Attacks and Flash Events. *International Journal of Information Technology*, 14(6); 3077-3087. Springer. https://doi.org/10.1007/s41870-022-00946-5

Tinubu, O. C., **Sodiya, A. S.**, Ojesanmi, O. A., Adeleke, E. O., & Timehin, A. A. (2022). An Intelligent Model for DDoS Attack Detection and Flash Event Management. *International Journal of Distributed Artificial Intelligence (IJDAI)*, *14*(1), 1-15.

Tinubu, C. O., Falana, O. J. Oluwumi, E. O., **Sodiya, A. S.**, Rufai, S. A. (2023).PHISHGEM: a mobile game-based learning for phishing awareness. *Journal of Cyber Security Technology*, 1-20.

Tinubu, C. O., **Sodiya, A. S.**, Ojesanmi, O J. (2023).A behavioral model for characterizing flooding distributed denial of service attacks. *International Journal of Information Technology* 15 (2), 955-964

Vincent. O. R., Babalola, Y. E., **Sodiya, A. S.** and Adeniran, O. J. (2021). A Cognitive Rail Track Breakage Detection System Using Artificial Neural Network, *Applied Computer Systems*, Vol.26, No..2, 2021, pp.80-86. Published by Riga Technical University, Poland. https://doi.org/10.2478/acss-2021-0010

University Senate Building

ISBN: 798-978-781-093-8