International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 02, February-2015

Hybridized Network and Data Security System: A Web–Based Approach

Silas, Abasiama Ita
Department of Computer Science,
University of Port Harcourt, Choba,
Rivers State, Nigeria

Enoch, O. Nwachukwu
Department of Computer Science,
University of Port Harcourt, Choba,
Rivers State, Nigeria

Abstract: This paper presents a hybridized security system for web-based application which minimizes the possibility of hacking in WLAN. We examine network security through symmetric encryption and fake packeting techniques. Our system is based on packet hiding techniques. The key idea is to hide the packets of data in the browser. This can be achieved through a mechanism known as cryptography and fake packet, so that even if the hackers can break into the network and get the packets, they will not be able to understand the packet contents. From the results obtained, it can be seen that cryptography when combined with fake packets using proxy servers can greatly enhanced security in web applications. The methodology used was Object-Oriented Analysis and Design Methodology (OOADM). A program in Java was developed that handles the proxy-servers where the encryption, decryption and fake packets processes are applied.

Keywords— Ciphers, Cryptography, Fake packets, Proxy servers, Secret key

I. INTRODUCTION

Network, data security and information exchange have become more important to personal computer users, organizations, banking, health, military and environmental monitoring. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms [5]. The world is becoming more interconnected due to Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of utmost importance because of intellectual property that can be easily acquired through the internet. There can be breach in intellectual property [5].

Information security is one of the most important issues to be considered when describing computer networks. In addition, the success of sending and receiving sensitive data using wireless networks depends on the existence of a secure communication (the Virtual Private Network, VPN) [6].

When considering network security, it must be emphasized that the whole network is secured. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message. When developing a secure network, the following need to be considered [3];

- Access – authorized users are provided the means to communicate to and from a particular network.
- Confidentiality – Information in the network remains private
- Authentication – Ensure the users of the network are who they say they are.
- Integrity – Ensure the message has not been modified in transit.
- Non-repudiation – Ensure the user does not refute that he used the network.

This work addresses the problem of client to client based security (i.e communication oriented security), and presents an improved hybridized security system for web-based application (client based security) that will minimized hacking in wireless local area network (WLAN).

The rest of this paper is structured as follows. Section II provides a critical analysis Cryptography while Section III discusses the related work, and a detailed description of our proposed system with the Design architecture is exposed in section IV. Experimental setup with the proposed system and the result is discussed in Section V with Section VI concluding the paper by summarizing our contributions and stating the recommendation.

II. CRYPTOGRAPHY

Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable [9].

According to [8], Cryptography is the practice and study of techniques for secure communication in the presence of adversaries'. Typically, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security.

A. Types of Cryptography

There are several types of Cryptography, some of these includes;

Asymmetric or Public Key Cryptography: In the two-key system, (also known as the public key system) one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message [7].

It involves two pairs of keys: one for encryption and another for decryption. Key used for encryption is a public key and distributed. On the other hand key used for decryption is private key, [7]

Symmetric or Private Key Cryptography: In symmetric key cryptography (also known as private-key cryptography), a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key. However, the key may be compromised during transit. If you know the party you are exchanging messages with, you can give them the key in advance. However, if you need to send an encrypted message to someone, you have never met; you will need to figure [2] out a way to exchange keys in a secure way. One method is to send it via another secure channel.

Hash Function: The Hash Funtion uses a mathematical transformation to irreversibly "encrypt" information. This algorithm does not use keys for encryption and decryption of data. It rather uses a fixed-length hash value which computed based on a plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. These algorithms [4] are typically used to provide a digital fingerprint of a file's content, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords to provide some measure of the integrity of a file.

B. Application Areas of Cryptography Source: [7]

Cryptographic algorithms are widely being used to solve problems belonging to data confidentiality, data integrity, data secrecy and authentication and various other domains. It uses various cryptographic algorithms as mentioned above as per requirement of the action. The areas of applicability of cryptography and its variants have been explained. The amount of distinction among all the variants of cryptography is less because the entity in all the algorithms is information that needs to be secured. Some of the application areas of cryptography include;

Secure Message Transmission Using Proxy-Signcryption: The proxy signature schemes allow proxy signers to sign messages on behalf of an original signer, a company or an organization. It is based on the discrete logarithm problem. The signcryption is a public-key primitive that simultaneously performs the functions of both digital signature and encryption. Integration of proxy signature and signcryption public key paradigms provides secure transmission .It is efficient in terms of computation and communication costs. It is used for low power computers in which a given device may transmit and receive messages from an arbitrarily large number of other computers.

Transferring Files on Network: Files that are to be exchanged between users need to be protected against malicious users and attackers. Symmetric Key cryptographic uses only single key for both encryption and decryption. In this technology symmetric key is then encrypted with public key which is associated with sender of file to obtain encrypted file and this encrypted file is then send to receiver. To decrypt the file, encrypted file system component driver uses private key which is associated with receiver to decrypt the symmetric key used to encrypt file. The encrypted file system component driver is then uses symmetric key to decrypt the file.

Certificates and Authentication: A certificate is an electronic document which identifies an individual, a server, a company, or some other entity and to associate that identity with a public key. Certificate authorities (CAs) issued certificate which binds a particular public key to the name of the entity that the certificate identifies (the name of an employee or a server). In addition to it, a certificate includes a serial number, name of certificate authority who issued it. And also it includes digital signatures of the issuing CA. Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate. This technique uses SSL protocol. In this protocol server present its server identity to client. Process of authentication at server side includes public key encryption and digital signatures. Once it

has been confirmed that it is server. After sever authentication, Client also present its identity to server. And once it's also conformed both indulge in communication using symmetric-key encryption technique.

Digital Signature and Authentication: Authentication based on public key cryptography has an advantage over many other authentication schemes because no secret information has to be shared by the entities involved in the exchange. Authentication basically means something that is real or genuine. It is done in order to know the actual identity of a person. Authentication in private and public computer network including the internet is basically performed through the use of login passwords. By the password, it is assumed that the user is genuine, trustworthy or real. A digital signature or we can also say digital certificate is an electronic signature that can be used to authenticate the identity of the sender of a message that has been sent is unchanged. A digital signature can be used with any kind of message like message send through electronic mail, whether it is encrypted or not so that the receiver can be sure of the sender's identity. A digital certificate contains the digital signature of the certificate- issuing authority so that anyone can verify that the certificate is real.

III. RELATED WORKS

In [2], they proposed a new algorithm which contains two levels of Exclusive OR (XOR) operation using symmetric key cryptography (i.e using the same key for both encryption and decryption). MATLAB was used for the implementation. The algorithm is very procedural and time wasting because at each point decryption, the decimal value of the cipher text must be converted to binary format selecting one text after the other. This algorithm is useful in transmission of messages and data between one user and another, but not very efficient when dealing with large volume of data/ information.

Vineet Mishra et al. [9] in their work on Combating Packet Sniffing, used Public-key (asymmetric) cryptography and fake packet to secure data/ packets from sniffers/ hackers. The plain text is encrypted on the sender's side with the use of sender's private key. This is encrypted again, using the receiver's public key. The final cipher text can be decrypted only by the authorized receiver, who alone has the matching private key. The idea behind using fake packets is to bamboozle the sniffer. These fake packets were also destined to the same destination. Since the sniffer shall collect all the packets destined to a particular IP address, it shall end up storing these fake packets too. This approach used public key cryptography which has a disadvantage of speed, also the number of fake packets was not specified, which could be excessive, thereby reducing the processing and communication speed

Another related work, [8] used compression along with encryption using RSA algorithm. This system is basically used for mobile communication. This system provides a solution to the SMS security problem. The approach that is used in this system is to secure the SMS message using Hybrid Compression Encryption (HCE) system. This system compresses the SMS to reduce its length, then encrypts it using RSA algorithm. But this system is using RSA. RSA is a Public Key Encryption method. A disadvantage of using public-key cryptography for encryption is on speed, it is relatively slow when comparing with symmetric cryptography.

Futhermore, [1] combined Steganography and cryptography to provide efficient method of hiding data from unauthorized user. In their work an audio medium was used for the steganography and the LSB (Least significant Bit) algorithm was employed to encode the message inside the audio file. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the right-most position. This method is suitable for internet users for more secured communication, but this system has a limitation with length, its efficiency drops as the length of data increases.

IV. PROPOSED SYSTEM

The aim of the proposed system is to design a Hybridized Network and Data security System for web-based application that will hide packets in WLAN browsers. The proposed system integrates the cryptographic and fake packet system into two proxy servers, so that all communication in the network must pass through these proxy servers before reaching its client or user.

In the proposed system, Cryptography and fake packets is combined to give two tier securities to data. The content of the packets is encrypted using Data encrypted standard (DES) encryption algorithm, the DES key is generated using random key spec generator which is supported by Java. A specified number of fake packets were introduced into the original packets to bamboozle the hackers. Thereafter, these packets are broken into chunks to increase the security of data, so that even if the packets can be seen, you will not understand the packets content. Two proxy servers that work with the proposed system were configured as a background application to sit on the gateway of the corporate network, so that all client requests must pass through these proxies to their various destinations.

A. Design of Propsed System

The detailed design of the proposed system reveals the details of each component. The specific components that make up the system design are; Wireless Local Area Connection (WLAN), Proxy server A, Proxy server B, and a Public network. These components are further discussed in details and the Architectural and Detailed diagram is given in fig. 1 and fig. 2 respectively.

WLAN Components: This component consists of various clients or users in a particular geographical area or branches. It is in this component that any web-application request can be made. These users must be connected to a network, which can be a wireless access point, a modem or hotspot (phone hotspot). In our system, we used a phone hotspot to connect all our clients.

Proxy Server A Component: A proxy server is an intermediary machine, between a client and the actual server, which is used to filter or cache request made by the client. It is when another machine makes requests from your computer to a server computer. This application protects the client by sending out web request on behalf of the client to the server, so that the server is unable to learn the origin of the request and cannot trace the client's IP address (internet protocol) or location. ProxySys A in our proposed system is a normal web proxy server, which listens on port 8010, and all clients (web-based application) are configured to send request to this port. So whenever a request is being made by a client, this proxy receives the request, fetches the content, adds additional 8 fake bytes of packets, encrypts these Packets, scatters it, then forwards it to proxy server B and stores a copy for future use. So next time when another client requests for the same webpage the proxy server just replies to the request with the content in its cache thus improving the overall request-reply speed.

Proxy Server B Component: Proxy server B, on receiving these encrypted packets, used the same key spec to decrypt, filter, remove the fake packets and send it back to proxy server A to display the content to the client that made the request.

These two proxies (A&B) can be used interchangeably depending on the set-up configuration in the system.

Public Network (Web Server): This is where proxy A fetches it content before encrypting. It is actually where the client request would have come directly to without the proxy server. Hacker can possibly stay here to sniff packets in the network.

B. Algorithm of the Proposed System

The algorithm of the proposed system is given as;

Step 1: Change the configuration proxy settings in your system to manual proxy configuration.

Step 2: Check your network connections and ensure your system is connected to the WLAN.

Step 3: Start up the proxy servers at both ends

Step 4: A user makes a web application request

- This request is sent to proxy server A
- Proxy A, receives the packets of data, adds eight (8) bytes of fake packet to the original packet, encrypts the packets using a specific random DES key spec generator and forwards the encrypted packets to proxy B.
- Proxy B decrypts the packets using the same key, filter out the fake packet, arrange the random nature of the packet and send the plain text back to proxy A.
- Proxy A, now displays the requested web application page(s) to the user or client.

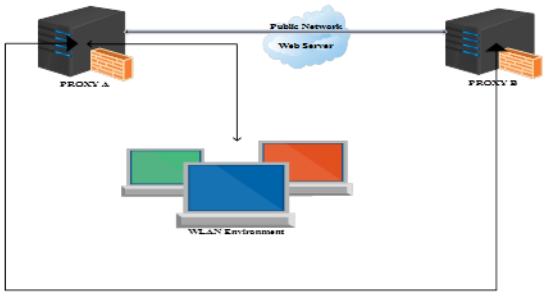

Fig 1: Architectural Design of the Proposed System

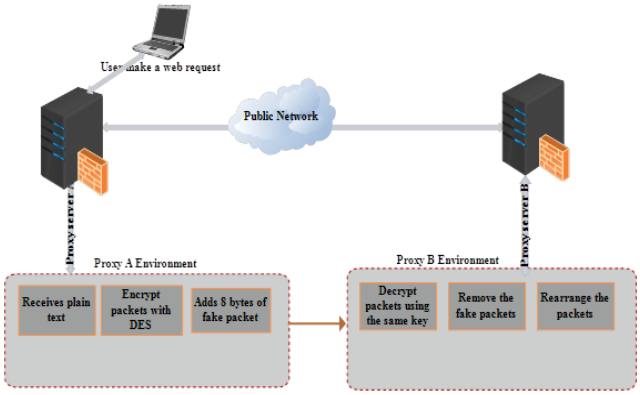

Fig 2: Detailed Design of the Proposed System

V. EXPERIMENTAL SETUP AND RESULT

The proposed system was implemented using NetBeans 8.0.1 version of Java programming language. The whole program was implemented in five major classes viz, the encpdecp module, fake-packet module, requestHandler module, proxysysA module and proxysysB module. The proxysysA and B was configured to listen on port 8010 and 8011 respectively, these two modules control the whole system, encpdecp and fake-packet are embedded into these two proxy servers, and the request-Handler class handles all communication between these classes through the socket server. For all clients in the network, their proxy system configuration must be set to manual proxy configuration setting as shown in Fig. 3, thereafter, the two proxy servers must be started (running) before a client can then make a web request, as shown in Fig. 4 (i.e when one of the proxy server is not running).

When a request is made on the web browser, the system forwards it to ProxySys A for encryption and fake packetting, then sends the encrypted packets to proxySysB for decryption, thereafter, the page(s) will be displayed to the client that made the request. All these processes occur in less than 10 seconds because the security is embedded into these two proxy servers.

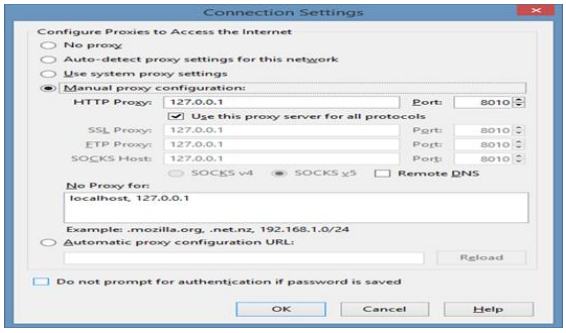

Fig. 3: The proposed system when the manual proxy configuration is set correctly

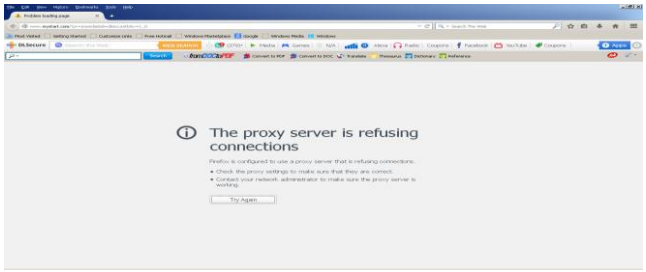

Fig. 4: The Proposed System when one of the Proxy Server is not started

VI. RESULT DISCUSSION

We opened a web page (www.uniport.edu.ng) with our hybridizes security system when the packets are encrypted, the output of the packets content are not readable as shown in fig. 5, and we opened the same web page when our packets are not encrypted, the output of the packets content can be seen clearly as shown in fig.6 which can be used by hackers to lunch attacks on our network.

The output of the implemented hybridized web application security is discussed here. The proxysysA was designed to receive web request from the end-user's, encrypt the packets, send it to proxysys B to decrypt and forwards it to proxysysA to display the requested page(s) to the client. These proxy servers (A and B) where configured to listen on port 8010 and 8011. From the output in fig. 6, it can be seen that when packets are not encrypted, you can clearly read the content which can be manipulated by hackers or sniffers, thereby putting the network in an unsecured mode, but when using our hybridized system, it can be seen as shown in fig 5 that the packets content are unreadable.

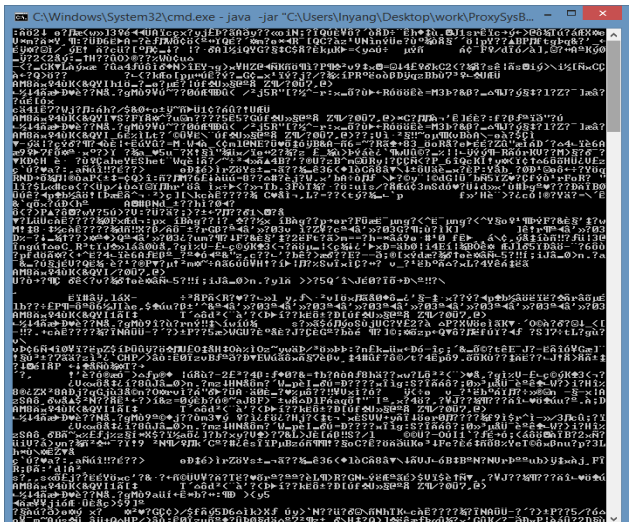

Fig. 5: Screen shot from command prompt when using our hybridized security system

In Fig.5, the output when the web page (www.uniport.edu.ng) was opened using our hybridized security system. From the output, it can be seen that the packets content are unreadable which cannot be manipulated by hackers. This is due to the fact that our security system has layers of security such as; Proxy Servers, Packet cryptography and fake packets.

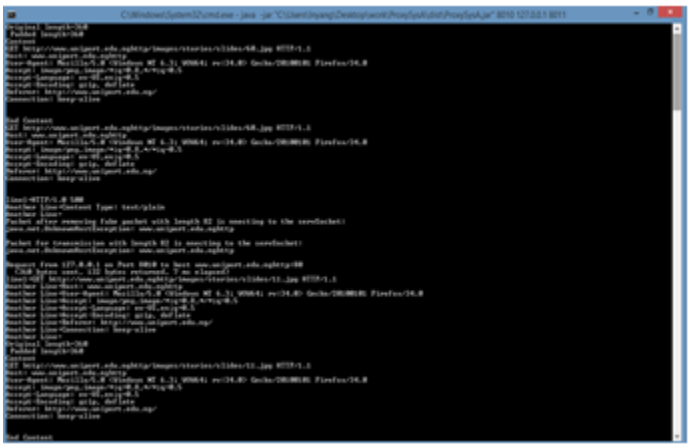

Fig. 6: Screen shot from command prompt when the packets are not encrypted

In Fig.6, the output when the web page (www.uniport.edu.ng) was opened without using our hybridized security system. From the output, it can be seen that the packets are readable which can be manipulated by hackers, thereby exposing the network to threats.

A. *Key Features Of Proposed System*

- Speed: The proposed system uses symmetric key cryptography (private key) which performs faster than asymmetric cryptography
- Proxy servers: The proposed system uses two proxies to configure its security, these proxies act as a firewall on the network, so that the sniffer cannot have the ip address of any user or client, thereby minimizing hacking/packet sniffing n this system.
- Fake packets: The use of a specified number of fake packets reduces the bandwidth which in turn increases the speed of communication.
- Random Key: The use of random key spec generator makes it harder for hackers, since this key set can be easily changed by the programmer without affecting the entire system.
- Client oriented Security

VII. CONCLUSION AND RECOMMENDATION

One of the main reasons why most network security systems fail is because of a single point or layer of security. We have to increase the level of security by applying other methods of security system such as our hybridized security system, which is a combination of two (cryptography and fake packets) known methods of securing web application against hackers.

We hereby recommend this hybridized security system to co-operate organization like Industries, government agencies, Institutions, Banks etc, who need their information to be much more secured.

A. *Contributions to Knowledge*

This research has succeeded in developing an improved client oriented security system which integrates cryptography and fake packets into two proxy servers and these proxy servers runs on the background of the browser not just between two clients as in the existing systems. Also, the system uses DES cryptography random secret key spec generator which cannot be predicted or determined by hackers.

REFERENCES

[1] Abikoye Oluwakemi C., Adewole Kayode S., Oladipupo Ayotunde J., Efficient Data Hiding System using Cryptography and Steganography. International Journal of Applied Information Systems (IJAIS) – ISSN: 2249- 0868 Foundation of Computer Science FCS, New York, USA Volume 4, No.1, 2012.

[2] Ajit Singh and Rimple Gilhotra, Data security using private key encryption system based on arithmetic coding, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, 2011.

[3] Dowd, P.W., McHenry, J.T., *Network security: it's time to take it seriously, Computer*, vol.31, no.9, pp.24-28, 1998.

[4] Nentawe Y. Goshew, Data Encryption and Decryption Using RSA Algorithm in a Network Environment, International Journal of Computer Science and Network Security, vol.14, no.5, pp.82-86, 2014.

[5] Priyank Sanghavi, Kreena Mehta & Shikha Soni., *Network Security International Journal of Scientific and Research Publications,*Volume 3, Issue 8, ISSN 2250-3153, 2013.

[6] Ramaraj, E., and Karthikeyan, S., A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking. Journal of Computer Science 2(9), 2006.

[7] Shivangi Goyal, *A Survey on the Applications of Cryptography, International Journal of Science and Technology* Volume 1 No. 3, March 2012. University School of Information Technology, Guru Gobind Singh Indraprastha University 16-C, Dwarka, Delhig.

[8] Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed & Ahmed M Mahfouz. Hybrid Compression Encryption Technique for Securing SMS, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue(6), 2009.

[9] Vineet Mishra, Snigdha S., Parthan, Sayalee Pote and Naman Avasthi, Combating Packet Sniffing, International Journal of Information and Computation Technology. ISSN 0974-2239, Vol. 3, no. 10, pp. 1101-1106, 2013.

AUTHORS BRIEF

Silas Abasiama Ita holds a B.Sc (Hons) in Computer Science/Mathematics at the University of Port-Harcourt, Rivers State, Nigeria, in 2009. She recently concluded her Master of Science degree in Computer Science at University of Port Harcourt, Nigeria. Her research interest includes: Network/Data security, Modeling, Distributed Database/Distributed Processing, Software Engineering and Artificial Intelligence. She is an Associate member of CISCO, member of IEEE and IEEE-Computer Society.

Enoch O. Nwachukwu is a Professor of Computer Science and former Head of Department of Computer Science, Faculty of Physical Science and Information Technology, University of Port Harcourt, Nigeria. He has a first degree in Electronics/Electrical Engineering, University of Ife, Nigeria, and received His M.Sc and PhD in Computer Science from the University of Manchester UK. His research interests focus on Artificial Intelligence application, Expert Systems, Software Engineering and network Security. He is a Fellow of Nigeria Computer Society and a Member of Nigeria Society of Engineers.