International Journal of Engineering and Environmental Sciences | *ISSN 1694-4372*
Published by AIR JOURNALS | *https://airjournal.org/ijees*
16/18 Avenue des Longaniers, Quatre Bornes, Mauritius
airjournals@gmail.com; enquiry@airjournal.org

RESEARCH ARTICLE

An Enhanced Security Scheme for Data and Communication Networks

Alor, M. O.

Electrical and Electronic Engineering Department, Enugu University of Science and Technology (ESUT), Nigeria

Accepted: June 16th, 2022 | **Published: June 30th, 2022**

Citations - APA

Alor, M. O. (2022). An Enhanced Security Scheme for Data and Communication Networks. *International Journal of Engineering and Environmental Sciences, 5(4), 7-26.*

ABSTRACT

Communication in the world has become a very vital part of living, and the world is becoming more interconnected with the advancement in the networking technology. There are equally large amounts of highly treasured personal, military, commercial, and government information being transmitted over the network infrastructure worldwide. The need to take preventive measure to keep the network and data safe from unauthorized users and other threats that are increasing every day cannot be overemphasized. Previous efforts like firewalls and other essential tools used to defend networks against security threats are failing. In this paper blowfish scheme was used to enhance the security of data in the network under study. The network was first characterized to find out the encryption speed of the network with its current protection. The blowfish security algorithm was then introduced and simulation results showed that while the encryption speed of the characterized network reduces with the increase in the size of the data block being transmitted, but with the blowfish scheme the encryption speed was faster and remained fairly constant no matter the size of the data block being transmitted. The percentage improvement achieved was 24.5% on encryption time. The decryption key was improved from 8bit to 32 bit in the new algorithm making the decryption process more complex for hackers. Hence the new scheme provides a very good protection against attacks with greater processing speed and efficiency.

Keywords: *Data Security, Encryption Algorithm, Enhanced Security Scheme, Communication Network*

Introduction

In recent times, it has been observed that computers and other devices connected to unsecured data communication networks are highly vulnerable to external threats such as malware, ransom-ware and spyware attacks. A single attack can bring down the entire computer system of an organization and compromise personal classified information. Therefore, there is clear need for precautionary measures to be adopted for adequate protection of shared data and data networks security is one of the best ways to do so. Data network security (DNS) refers to protective privacy measures that are employed for the prevention of unauthorized access to computer network, database and websites. It is a very essential part of information and telecommunication organization of all forms (Dhanraj et al., 2015).

Since the evolution of internet, various organizations have employed its service for data communication, data management and data storage. This data in question contained lots of classified information such as governments secrets, patient electronic health record, passwords, account details and whole lots of other very important data not meant for public knowledge. However due to the vulnerabilities in the various data communication systems, intruders take advantage of this fact to eavesdrop this information and bring threats to the owners. Initially encryption techniques were employed to solve this problem, however due to the short computational 56 bit key in the technique, it is very easy for it to be cracked by intruders and inflict threat to the network data.

Over time the need to therefore secure wireless communication data networks have increased steadily due to the huge amount of sensitive data being transmitted and received on timely based via the networks. According to Gurjeevan et al. (2016), these wireless networks provides platforms for various forms of communications, enabling various communication activities in business transactions, human resource management network, international public relations, mobile communication, internet services to mention a few. Hence, various organizations, both top and small scale have adopted these platforms for communication and management of classified information via data network. However most of these networks lacks adequate security features good enough to protect these facilities and have become a target for hackers, hence the need for adequate data network security (Tingyuan & Teng, 2019).

To secure this network, further encryption algorithms have been proposed and used to ensure a better protection of data being transmitted by various researchers. However, the advancement in method of attacks recently has made these security techniques inefficient and inadequate. This research has therefore proposing an intelligence encryption algorithm for the security of data in wireless networks.

Theoretical Framework

In today’s computing world, information and data security is an urgent need in the domain of information and communication technology. This is due to the various attack techniques employed by various unauthorized individuals to gain access to classified information. The provision of flexible simple and security of data is the main aim of various researchers in the field of wireless network security.

Various techniques for access control schemes with lots of differential advantages have been proposed in the past to solve the problem of network and packet sniffing. However, despite the success and efforts achieved by the existing systems, there is still need for a more robust, reliable, confidential easy to use security scheme.

According to Mageshwari and Karthikeyan (2015), the data encryption scheme seems to have the most employed security techniques, however research suggest that this form of security for data network transportation is currently experiencing various form of attack due to some of the developed technologies employed by intruders to decrypt the encrypted files. Generally, data network security threats are classified as;

a. Unstructured threat
b. Structured threat
c. External threat
d. Internal threat

(a) Unstructured Threat

This is a type of network threat developed by armature hackers or unprofessional who want to gain access to the network. They mainly used simple hacking tool like the password cracker of shell script to remotely try to gain access to the network.

(b) Structured Threat

Unlike unstructured threat, these types of hacker are more experience than the unstructured type. The sophisticated tool they employed are stronger than that used for the unstructured threat.

(c) External Threat

This type of network attack is initiated by outsiders, which are unauthorized people from the outside environment. This type of network attack is normally experienced in firms like the banks which normally suffer from this type of attack as intruders want to gain unauthorized access to their server.

(d) Internal Threat

This type of threat is directly opposite the external threat. In this type of network threat low level worker with less network privilege tries to gain access remotely to unauthorized access point.

Risks in Data Communication Networks

Some of the risks of data networks are exposed includes:

a. Threats

This can be a person or event that can cause damage to data or network (Nadeem and Kashif, 2014). It can be natural for example lightening; flooding, wind or accidental, such as accidental deletion of files.

b. Vulnerability

This can be defined as weakness in any network that can be exploited by a threat (Nadeem and Kashif, 2014). Network technologies have been applied in various sectors like banking, E-commerce, tax etc. and these network devices carry a lot of sensitive information with them, therefore it is very important to protect and secure these devices from these weaknesses such as malicious hackers and attackers to reduce the chances of data exploitation and manipulation (Yeu-Pong and Po-Lun, 2017).

c. Inappropriate Access of Resources

Unauthorized access occurs when a user tries to access a resource that is not permitted for him/her. This may occur because administrators not properly assigned the resources. It also happens when the user does not possess enough privilege to access the resources. Company which have different departments and users, some users have inappropriate access to any network resources, mostly because the users are not from the same department or may be such users who are from outside the company. For example, access to the accounts department data is inappropriate by the administrators for the users which belong to some other department. In this case administrators need to grant more access rights than a user desires.

d. Disclosure of Data

In any organization, some information which is either stored in a computer in the network or transmitted may require some level of confidentiality. Illegal access occurs when someone who is not authorized for that tries to read the data. It mostly happens because the information is not encrypted.

e. Unauthorized Modification

Unauthorized modification of data is the attack that affects data integrity. Any changes in data or software can create big problems; it can possibly corrupt databases, spreadsheets or some other important applications. Any minor unauthorized change in software can damage the whole operating system or all applications which are related to that software and perhaps need to reinstall the software with all related applications. This change can be made by unauthorized as well as authorized users. Any change in the data or in application can divert the information to some other destinations. This information can be used by any outsider or hacker who can make some changes and again send to the destination.

Some reasons that can cause the unauthorized modification are (Mohan & Anuradha, 2015).

i. Lack of protection tools.
ii. Granting write permission to the user that requires only read permission
iii. Access control mechanism that allow unnecessary write permission.
iv. Lack of encryption of data

f. Disclosure of Network Traffic

There are majorly two different kinds of data that we are referring to when we talk about data security, first type of data is that which is in the system or computers, and the second one which is being transferred from machine to machine or share among the network users. These two types of data fall under two types of security viz: computer security and network security. The tools that are designed to protect the first type of data fall in computer security category, while the protection of data during transmission called network security category. However, its not easy to distinguish a clear difference between these two types of security. As discussed earlier, users know which type of data is confidential. It is also important to maintain the confidentiality of that data during its transmission. The data which can be compromised consist of passwords, e-mail messages, user names or any other useful information that could be used in future for negative purpose. Even e-mails and passwords which are stored in encrypted format in system, they can also be captured during transmission as a plaintext (Mohan and Anuradha, 2015).

g. Spoofing of Network Traffic

During the transmission of data two things are vital that assures the integrity of data, one is that, data coming from a trusted host and second is that the data contents are not altered, manipulated or changed. Spoofing occurs when someone tries to pretend to be a trusted host. IP spoofing, Email spoofing and Web spoofing, are some types of spoofing. Messages transmitted over any network consist of some address information: sender address and receiver address. An intruder or any hacker initially finds the IP address of a trusted host after compromising the host, intruder can then modify the message (packet header) so that it appears that the message is coming from that trusted host, as shown in Figure 2.1. Same thing is in email spoofing that email looks like it came from Sam, but in reality, Sam did not send any email. Someone who was pretending to be Sam sent the email. In web spoofing attacker create a web page like bank's site or any email like Gmail web page but this web page is basically under the control of attacker so when you put your information it goes directly to the attacker. Several reasons are behind spoofing for example transmitting the network traffic in plaintext; not using any message authentication code technique etc.

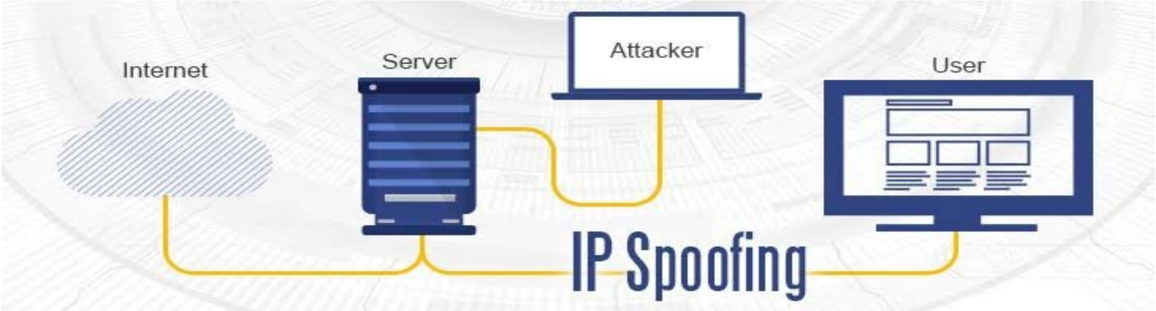

Figure: 1 IP Spoofing (medium.com, 2020).

h. Disruption of Network Function

Basic function of any network is to share the resources and information. A disruption occurs when network did not provide the needed functionality on time. Interruption in network has effects on one type of functionality or on different functionalities. Several reasons may lay behind the disruption on network. Network has no ability to detect the traffic, sometimes network goes down because of some of these useless traffic occasions, Network with single point of failure, Hardware failure, Improper maintenance of network equipment and Unauthorized access to network components. These may cause the changing in the configuration of the components which also disrupt the network function

Common Threats in Data Communication Networks

Security is a continuous process and continuous war between attacker and defender. There is no security mechanism that exists which gives the complete protection. Several types of attacks can be eliminated but others will be left to take place. Implementation of a security mechanism sometimes cost too much therefore some administrators simply tolerate the expected losses and find its most cost-effective solution.

Below we list some threats that one can face while using the computer or network system.

i. Errors and Omissions
ii. Disgruntled Employees
iii. Malicious Application Terms
iv. Physical and Infrastructure
v. Malicious Hackers
vi. Fraud and Theft

Early Adopted Security Measures

Cryptography (Data Encryption and Decryption)

As a new way of communication, computer network communication can accelerate the speed of information dissemination and expand the scope of dissemination. However, network information communication also has certain security problems, and there will be danger of information exposure and theft. Therefore, data encryption is a necessity for computer network communication. Data encryption technology in computer network communication security, in general, is to improve the security of computer network communication through the use of auxiliary technology (Xiangqin, 2020).

The need for secure communication dates back to the beginnings of human society. Ever since the first men started to gather in small groups, there was the need to transmit some kind of information from one person to another, while keeping it hidden from others. In the early days of civilized man, they would make a simple pattern change to an alphabet, or substitute other letters or numbers into the written messages, to successfully hide the private information (Ashima, 2013).

Cryptography (Data Encryption and Decryption) is the art and science which provides method of storing and transmitting data in a particular form to introduce secrecy in information security (Darshana, 2017). It is an important element of any technique which provides message transmission security. Here message is concealed in such form so that authenticated recipients can only decrypt and read the message. Authenticated and intended user can access the data as they possess the secrete key, no-one can read them without having access to the 'key’. The information input and output in the process of computer communication are accomplished through data, while data encryption is to process the original data information according to specific algorithms and rules, making it a hidden file. And a unique unlocking method must be used to read the information smoothly, which will enhance the security of information (Dong, 2016).

There are two kinds of data encryption techniques; one is link encryption (Ye, 2018). Link encryption technology is to ensure the consistency with the communication line technology, and clear the basic program design of the link, so that the information needed to be encrypted can be transmitted completely. The other is node encryption, which mainly optimizes the program according to the characteristics of the number of data needed to be transmitted in the running process, to make it possible that different encryption techniques can use the same encryption method to encrypt nodes. Node encryption can better improve the security of data in the network. But the nodes of data are vulnerable to hacker attacks, which is also the disadvantage of node encryption (Dai, 2017).

Secured communication involves encryption process at the sending end and decryption process at the receiving end of the communication system, (Miodrag, 2019). Over the years, there are many aspects to security solutions on many applications, ranging from secure commerce and payments to private communications and protecting passwords. In modern times, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. The Figure 2.2 showed types of cryptograph.

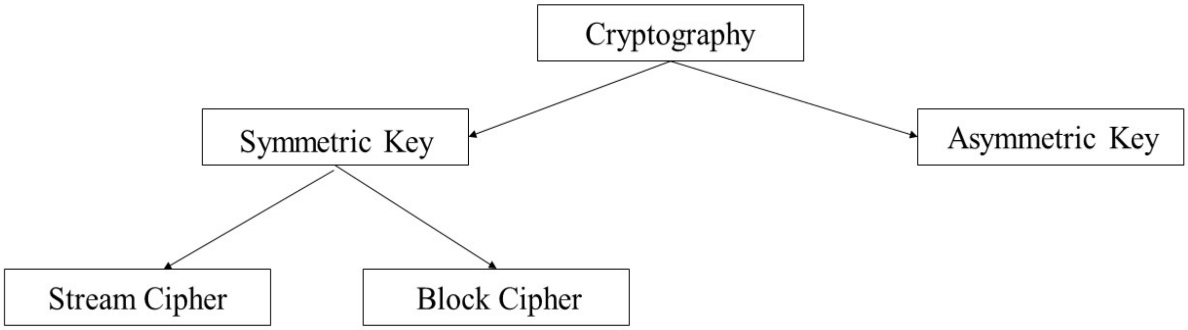

Figure 2: Types of Cryptography

Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography. Cryptography refers to encryption, the process of converting ordinary information (plaintext) into unintelligible cipher text. Cryptography is divided into two types, Symmetric Key Cryptography and Asymmetric Key Cryptography.

i. Symmetric Key

In Symmetric Key Cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message. The receiver uses the shared key and decryption algorithm to decrypt the message (Ezeofor & Ulasi, 2014), this means the person encrypting the message must send the key to the recipient before they can decrypt it.

ii. Asymmetric Key

In Asymmetric Key Cryptography each user is assigned a pair of keys, public key and private key. The public key is announced to all members while the private key is kept secret by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message. According to Ezeofor and Ulasi (2014), this allows a user to freely distribute his or her public key to people who are likely want to communicate with him or her without worry of compromise because only someone with the private key can decrypt a message.

The process of converting plain text into Cipher text is called enciphering or encryption while restoring the plain text from the Cipher text is called deciphering or decryption. Decryption is the reverse, moving from unintelligible cipher text to plaintext. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. This is a secret parameter for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks. Encryption has long been used by militaries and governments to facilitate secret communication. The process of encryption and decryption is shown in Figure 3

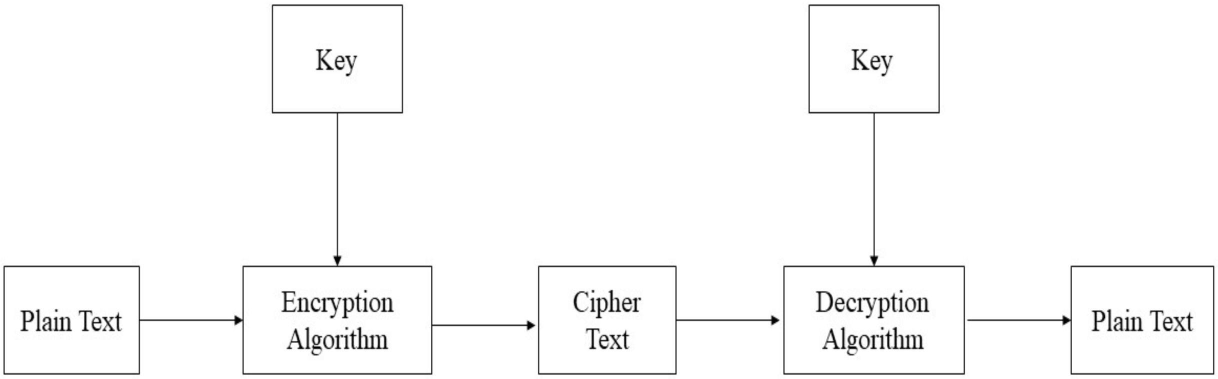

Figure 3: Encryption and Decryption Process

The challenge cryptography is that technology is advancing and evolving, and crimes are increasing as well, then data networks and its services need to be well safe to avoid leakages and losses. Though there have been several works done to strengthen the classical ciphers such as an algorithm that allowed diffusion was incorporated to the Vigenere stream cipher strengthening it considerably but there are still need for further strengthening since the benefits of cryptography is to offers individual privacy and confidentiality and, in some circumstances, also authentication and non-repudiation (e.g. legal 'signatures') and Especially important in explicitly Authorization.

Proposed Enhancement Scheme

This research proposed a Blowfish Algorithm standard for the enhancement of the data network security. This an encryption mechanism is a symmetric block cipher standard. It will be fast for encrypting data with a 32-bit processor at the clock speed of 18 cycles per byte. It uses a compact memory size of 5K of less. This standard has a simple structure, which is easy to implement and use. Therefore, the strength of the standard could be easily determined. The length of the key of the Blowfish standard is variable and can have the length of 448 bits. This gives the user higher security, but the speed issues must be considered when deploying higher values of the key length. The Block size of this Blowfish algorithm is usually 64 bits (Schneier, 2012).

Methodology and Results

Characterization Process

A real time characterization method was used which collected live data during the communication process from the study field (Gideon communications limited). Before this process begins the encryption mode of the router was turned on and packet data was transmitted, while the monitoring device was used to measure the performance. The network characterized is presented as shown in Figure 4;

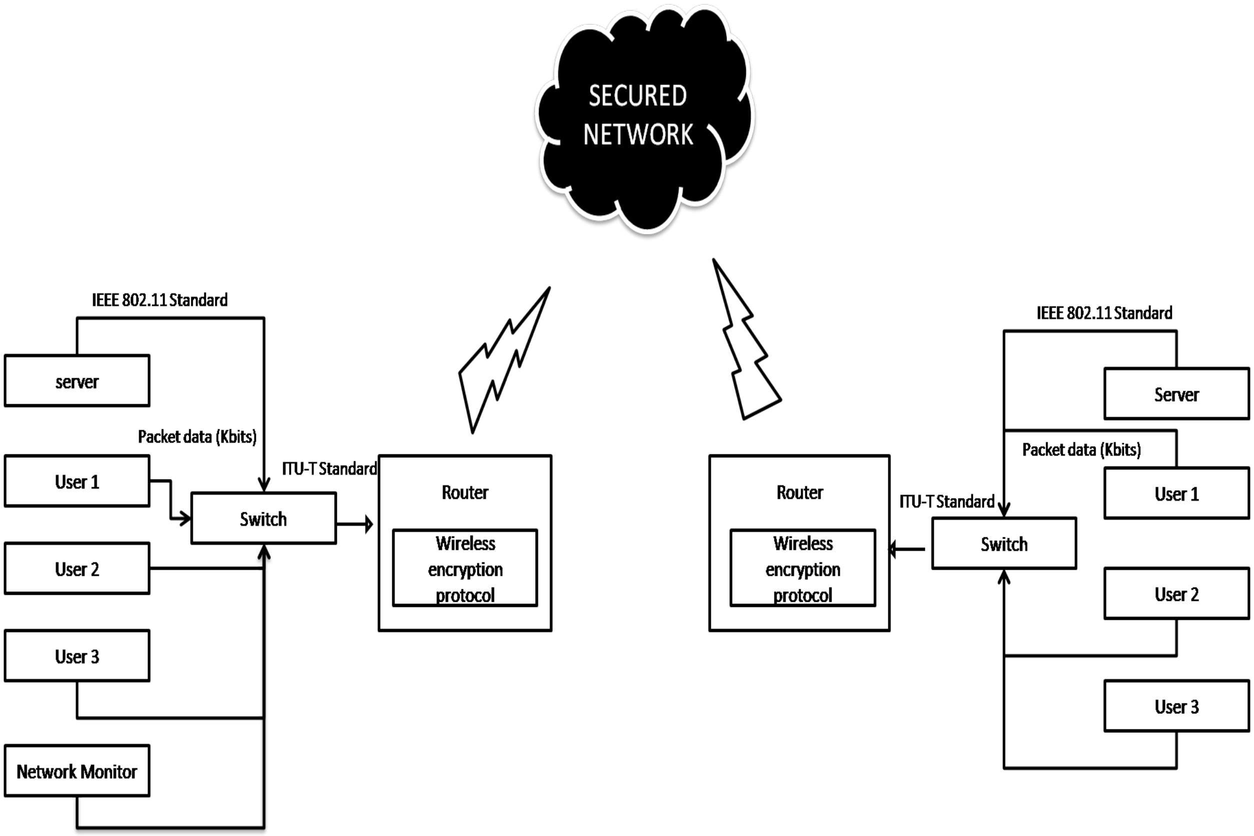

Figure 4: Gideon communications wireless network

Figure 4, is the system block diagram of Gideon communications wireless network. When the communication process begins and data are transmitted, the router automatically generates an encryption key and encrypts the transport layer before transmission to the cloud. This key was used to decrypt the message at the receiver end. The result obtained is presented in Table 1 considering the packet sent, encrypted files, decrypted files, speed and time of encryption respectively.

Table 1: Characterized data

Packet sent (Kbits)	*Data encryption speed (ms)*
1000	68
1200	68
1300	70
1400	90
1500	98
1600	102
1700	105
1800	105
1900	109
2000	115
21000	125
2200	127
2300	129
2400	129
2500	130
2600	132

2700	135
2800	136
2900	140
3000	148

The result shows that as data block sent increases data encryption speed reduces. The wireless encryption protocol (WEP) generates a 64bit encryption key for each packet sent and encrypts the packet using 56bit of the cipher keys generated. The remaining 8bit key is inverted for decryption at the receiver end. The comprehensive description of the WEP is presented in Figure 4;

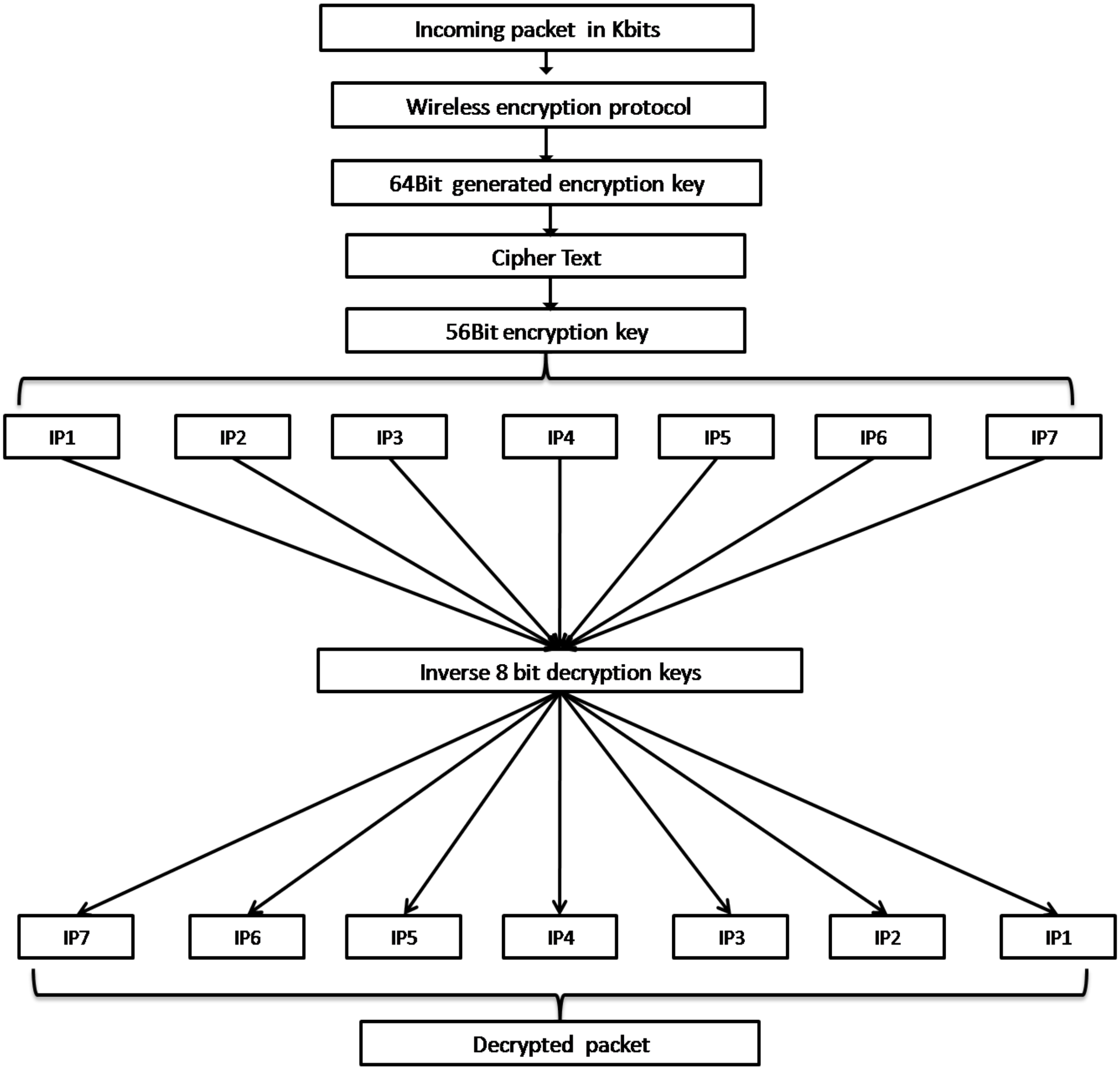

Figure 4: The Conventional Wireless Encryption Protocol Scheme

The conventional WEP scheme first generates encryption 56bit keys for the protection of packets transmitted in the network. When incoming packets are detected by the routing device, the size are divided into 8bit each and then encrypted before transmitted to the cloud. The same technique is employed at the receiving end, but using inverse 8bit encryption keys. The time taken for the encryption process was measured using the model in equation 3.1;

$$T = \frac{1}{Nb}\sum_{j=1}^{Nb}\frac{M_i}{ti}(\text{kb/s}) \qquad 3.1$$

Where T is the time of encryption, Nb is the number of incoming packets, Mi data size and ti is data rate. The model was used to compute the total time it takes the routing device to encrypt a packet and then transmit to the cloud. Analysis of the result obtained is shown in Figure 3.3

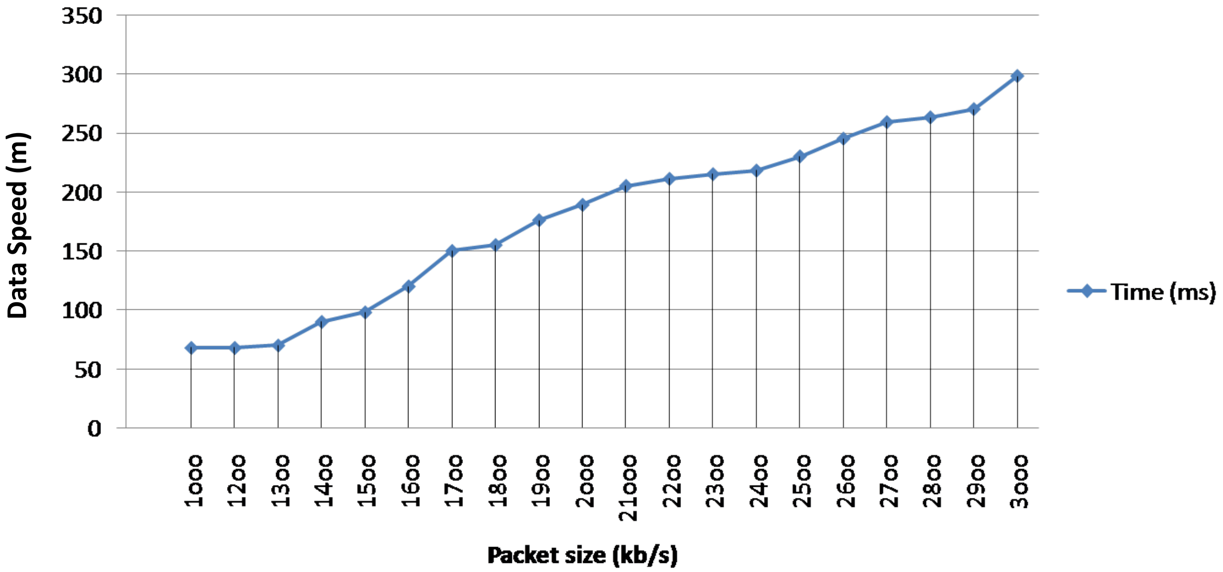

Figure 5: Encryption Time Process

From the result it was observed that the encryption time for the characterized system increases as the packet transmitted increases and the average encryption time is 113.05ms, which is too much a delay time.

Weakness of the Characterized System

i. The decryption key is too short and can be guessed easily
ii. It takes too much time to process and speed is dependent on data size
iii. The network lacks confidentiality
iv. Low efficiency and throughput velocity

Enhanced Security Scheme using Improved Blow Fish Algorithm

The proposed enhanced method was achieved using expanded blow fish algorithm (EBFA). This is a symmetric encryption algorithm which uses the same secret key (private key) for both encryption and decryption of packet data. The algorithm expands packet into fixed length blocks of 64bits each during encryption and decryption using a variable length key from 32 bits to 448 bits. This expansion process is done to improve processing speed and throughput. The functionality of key expansion makes it hard to crack by hackers. The improved blow fish algorithm is presented in Figure 3.4

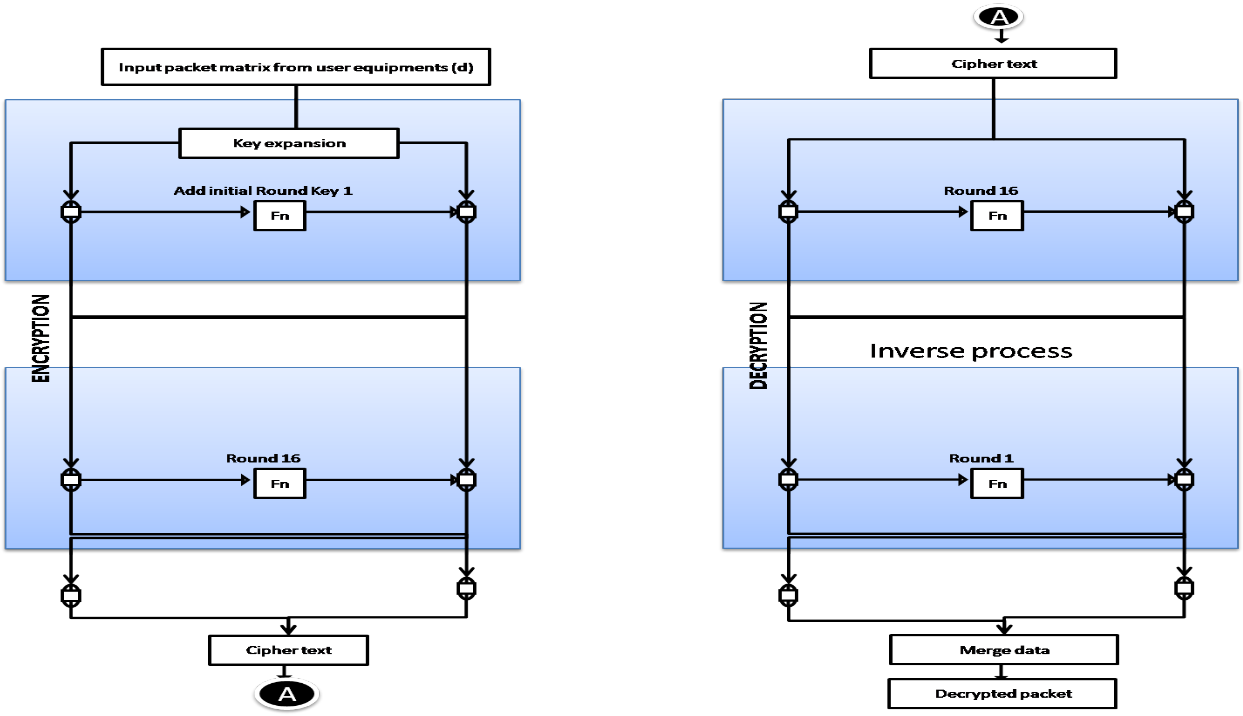

Figure 6: Enhanced method using Blow Fish Algorithm

From Figure 6, the improved blow fish algorithm expands the input packet matrix into 32bit each and then adds initial key function for 16 rounds to generate the cipher text. The key generated was used to encrypt the packet and then transmit to the cloud. The increase bit size for each packet size was done to improve the speed of encryption and then random 16 keys generated and used are made to improve the difficulty in generating the decryption key by hackers. Also, at the receiver end the same method was used to invert the random 16bit encryption key generated and then decrypt the packet.

Data Rate Model

The data rate model was developed using the relationship between the packet data, bandwidth size and time as presented below;

$R_{u,t= \alpha W\log 2(1+SNR_{u,t})}$ 3.2

Where W is the bandwidth, α is the fraction of bandwidth employed for the packet data transmission, packet data is presented at user u, SNR is signal to noise ratio and time slot of t, applying the round robin scheduling on the equation 3.2 to compute the average packet data for u is presented in equation 3.3

$R_{u,t} = \frac{1}{N_t} R_{u,t}$ 3.3

Where $R_{u,t}$ the highest data rate which can be transmitted once, Nt is the number of the network users scheduled at the time slot considered.

Development of the System Software

This section developed the adaptive data encryption software using the improved blow fish algorithm of Figure 3.3. The encryption software is designed using the flow chart of Figure 3.5

This flow chart presents the enhanced blow fish algorithm which generates an 16bit random key for the encryption of incoming packet. When user transit data from various user equipment through equation 3.1 comes, the data are segmented into 32bit each and then encrypted with the 16bit encryption key for security before throughput in equation 3.3. The receiver end also inverts the random 16 bit key generated and used to decrypt the data when received. The logical flow chart is presented below

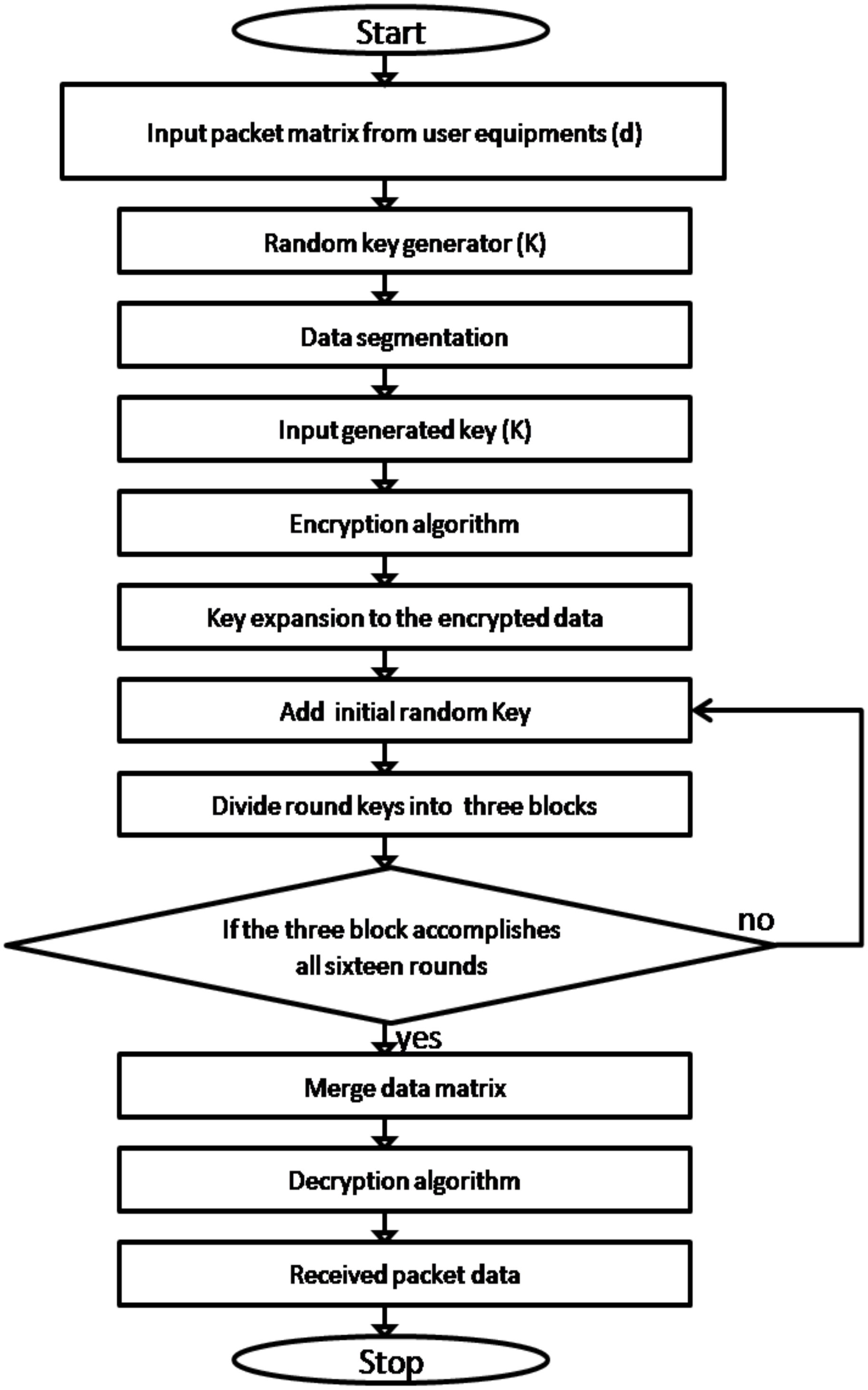

Figure 7: Enhanced data encryption flow chart

In the Figure 3.5, the packet data from the user equipment is identified by the security scheme as an input matrix and then segmented to improve operating speed. The algorithm automatically generates random keys of about 468bit and then input it to the segmented data to encrypt the file based on the encryption algorithm (improved blow fish algorithm). After the encryption process, the key is expanded to the encrypted blocks to ensure more security using add initial random key function. They keys are divided into three blocks of which each block completes the add initial random key functions of n iterations, when this is completed, the data matrix are merged and the encryption process reversed for decryption and then the packet data is received by the user.

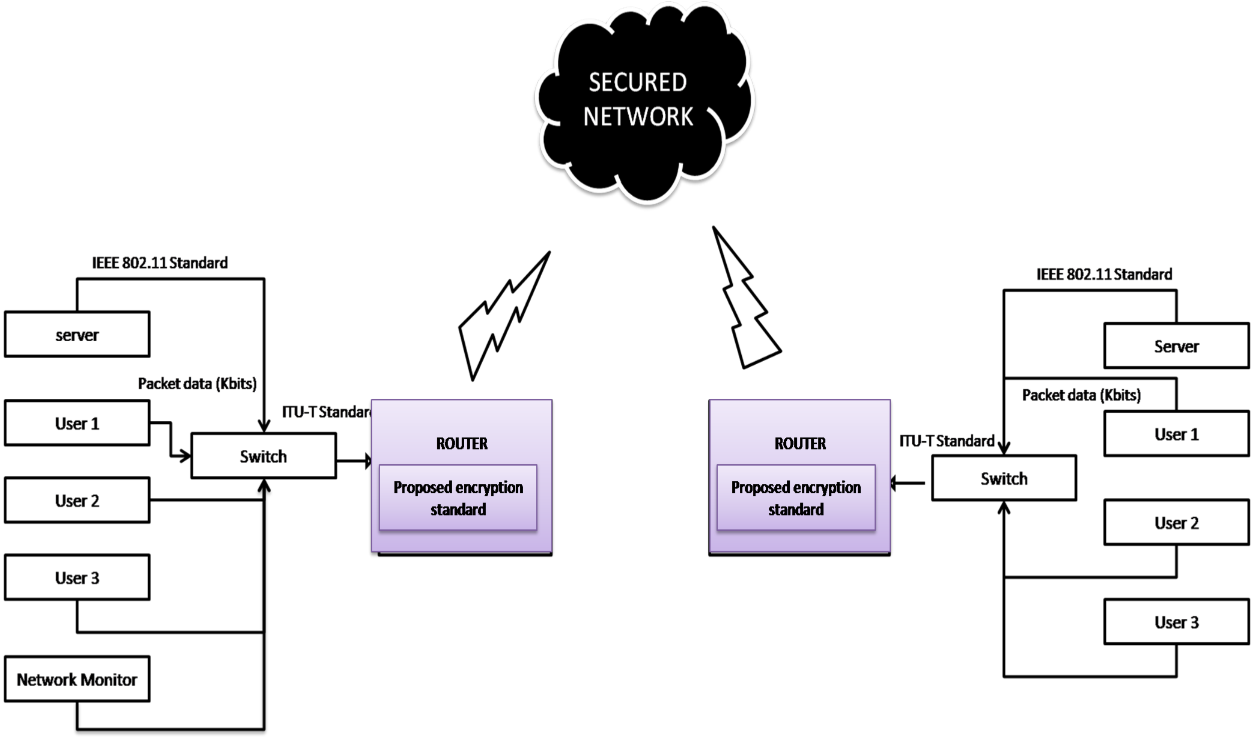

Figure 8: The enhanced system block diagram

Figure 8, is the enhanced system that will improve the security performance of the characterized wireless network using the advanced software encryption scheme using blow fish algorithm to optimize security performance, speed and total time taken for the data processing of the characterized system.

Implementation of the Software

The software for this research was implemented using Mathlab programming language, with its signal processing, communication, optimization toolboxes and the proposed algorithm developed in the previous section. The source codes are presented below;

Source Codes

```
classdef AES < handle
   %   Detailed explanation goes here
   properties (Access = private)
      secretKey
      cipher
   end
      methods
      function obj = AES(secret, algorithm)
         import java.lang.String;
```

```
        import java.util.Arrays;
        import javax.crypto.Cipher;
        key = String(secret).getBytes("UTF-8");
        sha = MessageDigest.getInstance(algorithm);
        key = sha.digest(key);
        key = Arrays.copyOf(key, 16);
        obj.secretKey = javaObject('javax.crypto.spec.SecretKeySpec',key, "AES");
        obj.cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
    function encrypted = encrypt(obj, strToEncrypt)
        import java.util.Base64;
        import java.lang.String;
        import javax.crypto.Cipher;
        obj.cipher.init(Cipher.ENCRYPT_MODE, obj.secretKey);
        encrypted =
string(Base64.getEncoder().encodeToString(obj.cipher.doFinal(String(strToEncrypt).getBytes("UTF-8"))));
     end
function encrypted = encryptStructuredData(obj, structuredData)
       encrypted = obj.encrypt(jsonencode(structuredData));
function decrypted = decryptStructuredData(obj, encryptedStructuredData)
        decrypted = jsondecode(obj.decrypt(encryptedStructuredData));
     end
function decrypted = decrypt(obj, strToDecrypt)
        %DECRYPT Summary of this method goes here
        %   Detailed explanation goes here
        import javax.crypto.Cipher;
        import java.lang.String;
        import java.util.Base64;
        obj.cipher.init(Cipher.DECRYPT_MODE, obj.secretKey);
        decrypted = string(String(obj.cipher.doFinal(Base64.getDecoder().decode(strToDecrypt))));
     end
```

Program Modules

The program modules are explained using the data flow diagram of Figure 3.7 which shows how packet data generated is encrypted to cipher text using the random keys generated and then transmitted as an encryption signal to the receiver end. The receiver section decrypts the signal and then encodes back to the normal packet desired.

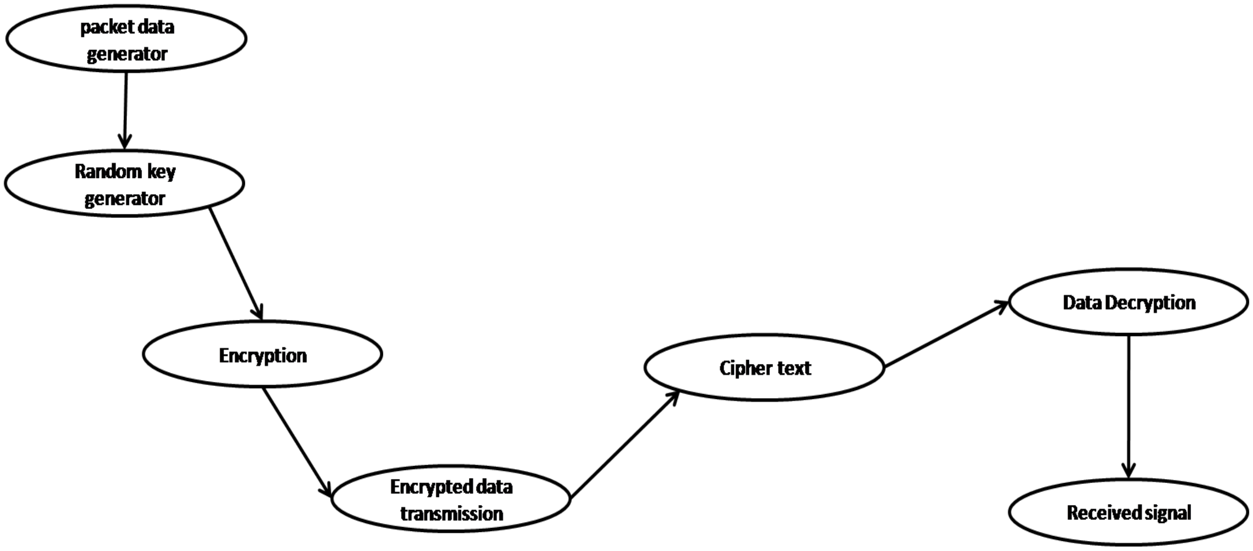

Figure 9: Data flow diagram for the software encryption process

The results presents the transmitted packet before and after encryption, then the encrypted files as they propagate through the network channel was presented, alongside the decrypted file at the destination end. The total time and for this process was validated using comparative approach after series of iterations. The packet data generated for transmission is presented in Figure 10

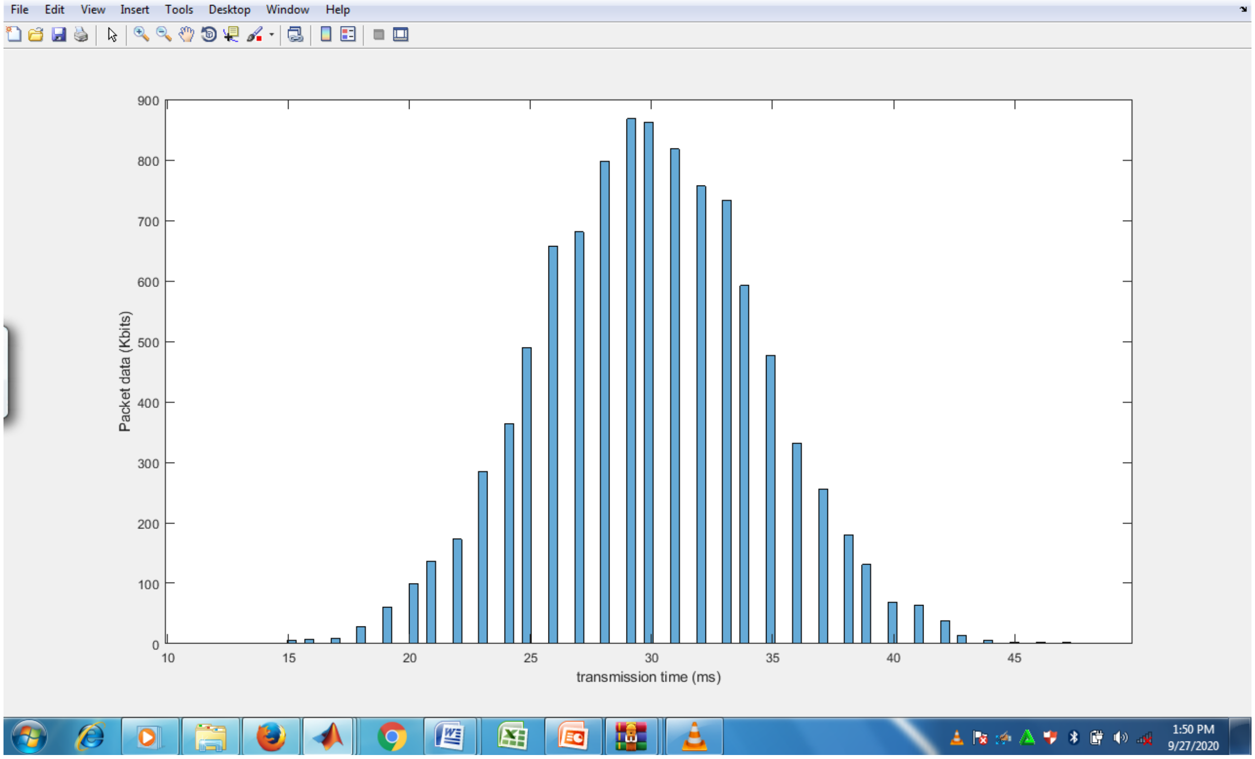

Figure 10: Packet Data Speed Profile

The result in the Figure 10 shows the packet data generated for transmission by the transmitter nodes using the data rate model in equation 3.2. These packets are constellated by the routing equipment for encryption. The constellation process collects all generated packets from the transmitter nodes and then feed forward to the algorithm in Figure 9 for encryption before the throughput model in equation 3.3 is used to transmit.

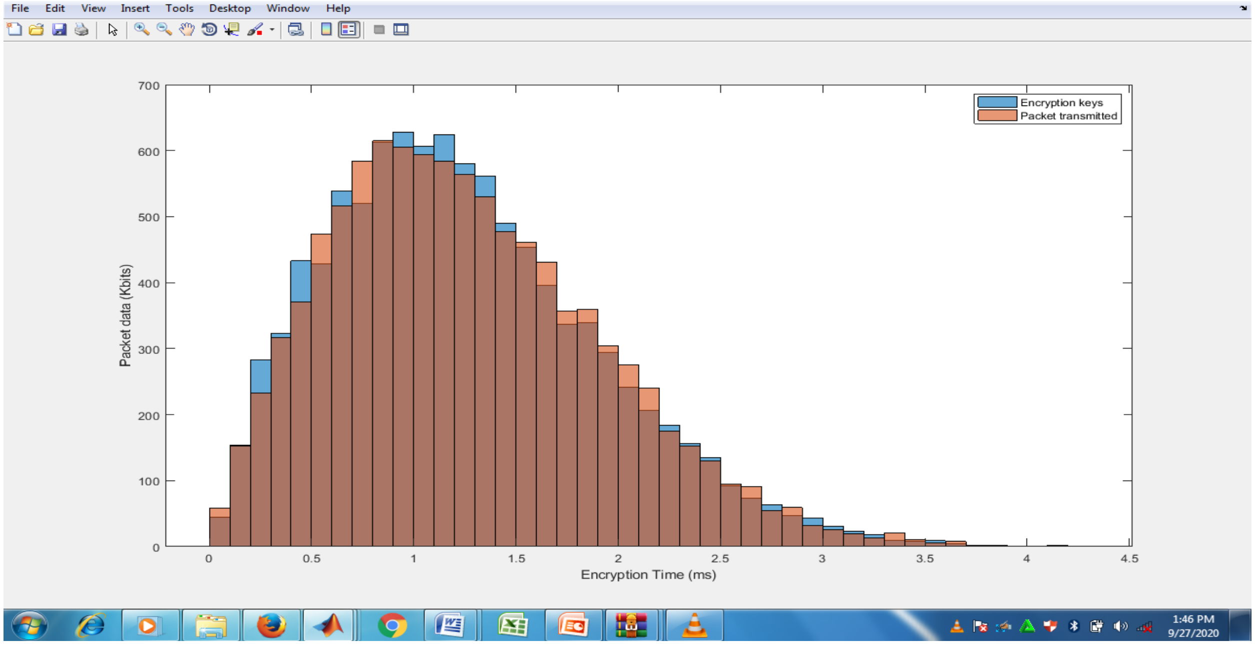

Figure 11: The Encrypted Signal

From Figure 11, the transmitted signal is encrypted by the router. This was done by the algorithm which identified the incoming packet from equation 3.2 and then encrypted the packet using the already generated 16bit encryption keys in a cipher text formation in the ratio of 32 bit each before throughput in equation 3.3 was allowed.

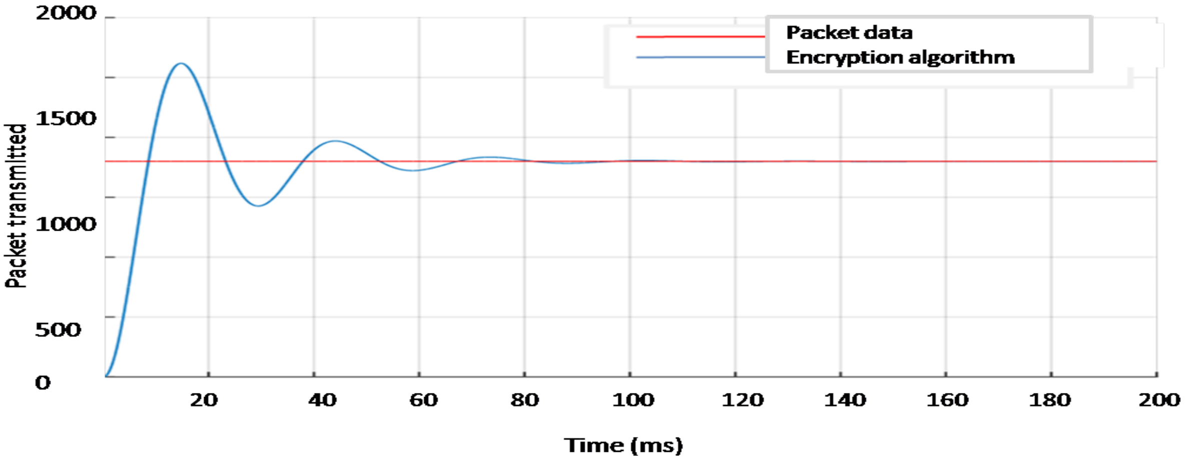

Figure 12: The encryption time against the packets transmitted

The result in Figure 12 shows the average encryption time used by the improved algorithm for the protection of the data network. The encryption time was computed using the model in equation 3.1 and the result showed that the algorithm detected the incoming packet from equation 3.2 and started the encryption process at 10ms, then completed it at 79.8ms. The implication of this result showed that the process time of encryption is very fast at it beats the specific delay time which was 150ms specified by the ITU standard as latency.

Table 2: Performance of the enhanced network

Packet sent (Kbits)	*Data encryption Speed (ms)*

1000	68
1200	68
1300	70
1400	70
1500	71
1600	72
1700	75
1800	75
1900	76
2000	77
21000	78
2200	78
2300	79
2400	84
2500	89
2600	90
2700	92
2800	93
2900	95
3000	96
Average	79.8

The result in table 3 presented the performance of the enhanced algorithm deployed on the characterized network. The result was analyzed with excel software as presented in the graph of Figure 13;

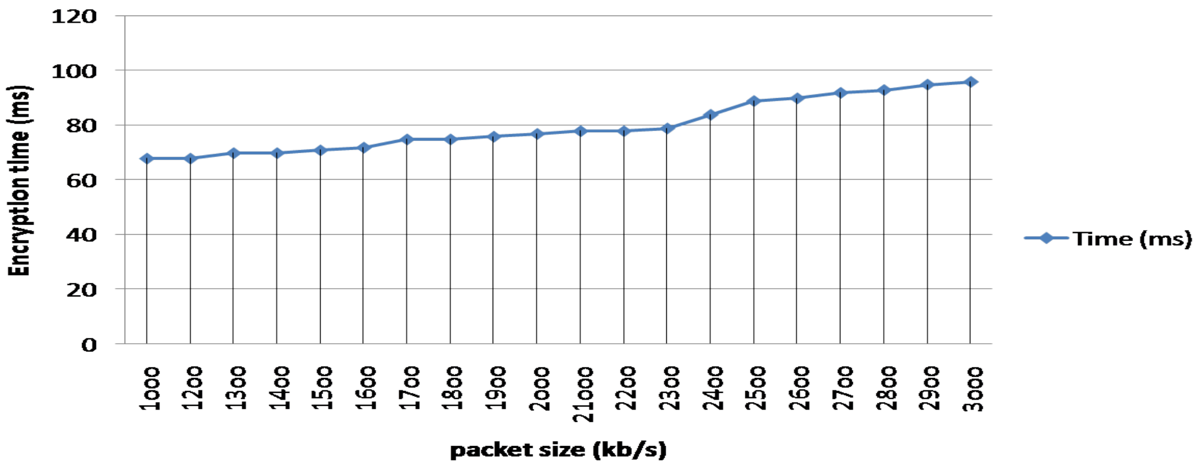

Figure 13: Performance of the improved encryption algorithm

From the result in Figure 13, it was observed that the encryption time for all packet sizes are fairly constant which is very good indicating that increase packet size do not unnecessary caused latency. The average encryption time in the result is 79.8ms. The comparative result of the characterized and the new system developed is shown in table 3;

Table 3: Comparative Analysis

Packet sent (Kbits)	*Time (ms) with improved algorithm*	*Characterized Time (ms)*
1000	68	68
1200	68	68
1300	70	70
1400	70	90
1500	71	98
1600	72	102
1700	75	105
1800	75	105
1900	76	109
2000	77	115
2100	78	125
2200	78	127
2300	79	129
2400	84	129
2500	89	130
2600	90	132
2700	92	135
2800	93	136
2900	95	140
3000	96	148
Average	79.8	113.05

The result in the table 3 presented the comparative performance of the new and characterized system. The result was analyzed using excel software and then presented in Figure 3.12;

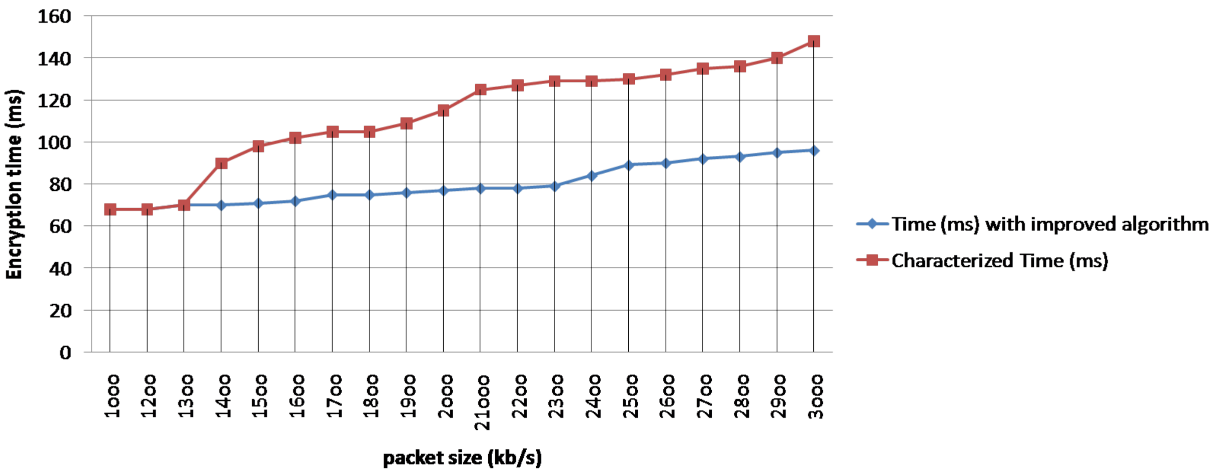

Figure 14: Comparative Result

Discussion

The results of the comparative performance of the new and characterized encryption algorithm shows that the characterized encryption speed reduces as the size of data block being transmitted increases, while that of the improved algorithm was fairly constant despite large increase in the size of the data block being transmitted. The percentage improvement achieved is 24.5% improved encryption time. The decryption key was improved from 8 bit to 32 bit in the new algorithm making the decryption process more complex for hackers.

Conclusion

This paper presents an enhanced security scheme for data and communication networks. From the related literatures reviewed, and the results of the experimental work performed using a blowfish enhancement security algorithm, blowfish security scheme has a very fast encryption speed with a 32 bit decryption key which makes it a good data network security system.

Reference

Ashima, J. (2013). Network Security, The Biggest Challenge in Communication. *Advance in Electronic and Electric Engineering*, ISSN 2231-1297, 3(7), 797-804. http://www.ripublication.com/aeee.htm

Dai, Y. (2017). Application of Data Encryption Technology in Computer Network Communication Security [J]. *Electronic Technology and Software Engineering*, 24, 208-209.

DarshanaPatil, C. P. M. (2017). A Secure Data Communication System Using Enhanced Cryptography and Steganography. *International Journal of Innovative Research in Computer and Communication Engineering,* 5(6)

Dong, Y. (2016). Application Analysis of Data Encryption Technology in Computer Network Communication Security [J]. *Network Security Technology and Application*, 04, 39-40.

Ezeofor, C. J. & Ulasi, A. G. (2014). Analysis of Network Data Encryption & Decryption Techniques in Communication Systems. *International Journal of Innovative Research in Science, Engineering and Technology, 3(12)*

Gurjeevan, S., Ashwani & Sandha, K. S. (2016). Performance Evaluation of Symmetric Cryptography Algorithms, IJECT.

Mageshwari and Karthikeyan (2015). Cryptography Policy Based Data Communication in Trusted Environment. *International Journal of Applied Engineering Research*

Miodrag, M. (2019). A Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security. *Entropy* 21, 701; doi:10.3390/e21070701. www.mdpi.com/journal/entropy.

Mohan, V., Pawar and Anuradha, J., (2015). Network Security and Types of Attacks in Network. International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015). doi: 10.1016/j.procs.2015.04.126.

Nadeem, A. & Kashif, H., (2014). Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution. School of Engineering Department of Telecommunication Blekinge Institute of Technology SE - 371 79 Karlskrona, Sweden. Thesis No: MEE10:76

Schneier, B. (2012). The Blowfish Encryption Algorithm. Blowfish, http://www.schneier.com/blowfish.html.

Tingyuan, N. & Teng Z. (2019). A Study of DES and Blowfish Encryption Algorithm, TENCON.

Xiangqin, L. (2020). Application of Data Encryption Technology in Computer Network Communication Security. *Journal of Physics: Conference Series* 1574 (2020) 012034 IOP Publishing doi:10.1088/1742-6596/1574/1/012034

Ye, J. (2018). Application of Data Encryption Technology in Computer Network Communication Security [J]. *Information Communication, (*06), 70-71.

Yeu-Pong, L. & Po-Lun Hsia, (2017). Using the vulnerability information of computer systems to improve the network security. *Journal of Computer Communications*, 30(9), 2032-2047.