International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 10, Issue 4, pp: (1-16), Month: October - December 2022, Available at: www.researchpublish.com

IMPROVING THE SECURITY OF A DATA COMMUNICATION SYSTEM USING ENCRYPTED TECHNOLOGY

Eze Cletus Elijah[1], Alor M.O[2]

[1,2]Department of Electrical Electronic Engineering Faculty of Engineering

[1,2]Enugu State University of Science & Technology, Enugu State, Nigeria

DOI: https://doi.org/10.5281/zenodo.7277023

Published Date: 03-November-2022

Abstract: **This work presents improving security of data communication system using advanced management of encryption software scheme. The work characterized a case study network designed with data encryption technique and then improved the network using an advanced data encryption technique. The encryption technique was developed using optimized blow fish algorithm which has the ability to segment keys and input packet matrix before simultaneous encryption. This process improves security, processing speed and time. The technique was implemented on Mathlab Simulink platform and tested. The result showed that the data encryption time of the new algorithm was 79.8ms against 113.05ms of the characterized system. The decryption key was improved from 8bit to 32bit in the new algorithm making the decryption process more complex for hackers, but improved data security in the system.**

Keywords: **Encryption, Data communication, Fish algorithm, Decryption, Packet matrix.**

I. INTRODUCTION

Recently, Information and Communication Technology (ICT) has grown sporadically, no surprise considering the huge benefits it presents such as the limitless ability to send, receive, store and retrieve information in real time using the necessary hardware and software components. Today, this technology has been on the rise, due to the various effects that it has on enterprises, providing scalable infrastructures and global economic benefits, thus enabling exchange of various forms of data over networks (Afaf et al., 2016).

According to Gurjeevan et al. (2016), this wireless network has provided a platform for various forms of communications, enabling business transactions, human resource management network, international public relations, mobile communication, internet services to mention a few. Due to this effect, various organizations, both top and small scale have adopted this process for communication, transmission, received and management of classified information via data network. However most of these networks lacks adequate security features and have become a target for hackers, hence there is need for adequate data network security (Tingyuan et al., 2019).

In recent times, it was observed that computers and other devices connected to unsecured 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. There is 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 very essential part of information and telecommunication organization of all forms (Dhanraj et al., 2015).

The trend (DNS) is gaining momentum due to the sporadic application of wireless local area network based on the IEEE 802.11 wireless standard for communication. In order words this medium turn out to be a domain for the transfer of various classified information, containing details like government secrets, personal password, patient health information, company information among other valuable and classified data which are not supposed to be made public due to certain reasons (Afaf et al., 2016). The DNS have been integrated to the conventional network transport layers using various data encryption standard algorithms (DES). This encryption algorithm has been a popular secret key encryption technique and is employed in many commercial and financial applications today. Once a network is secured, the users and the devices connected can work without experiencing data breaches (Diaa et al., 2018).

To implement network security, network specialists will utilize highly complicated strategies with the assistance of hardware and software. However the conventional standard encryption technique has been manipulated over time by hackers to gain unauthorized access to network. This was achieved due to the fundamental loop holes identified in standard encryption system which mainly is the bit key. The 56 bit key is exponentially short and can easily be cracked by hacker. Also these traditional encryption techniques do not take care of authentication problems of terminal and server. It has poor security, heavy computational of encryption and decryption and low efficiency. To address these challenges, there is need for an advanced management of encryption software scheme which will help optimize the computational problems identified and ensure effective and efficient security of data communication system.

II. LITERATURE REVEIW

This literature started with the theoretical framework, where the overview of Data Communication, Components of data communication system and data communication criteria was discussed. Then, the study take a look at some of the risks and vulnerabilities that computer network users are faced with and how they affect users alongside the fundamentals of data communication security considering Data confidentiality, availability, accessibility, authentication, integrity etc. Some of the approaches and security measures that have always been followed to keep this risk at minimal level or even eradicated was also reviewed. The literature also overviewed Cryptography and Data Encryption, types of cryptography which study symmetric key and asymmetric key encryption. The encryption process was also discussed before we went further to look at some of the encryption algorithms. The common encryption algorithms that had most of our interest are the AES, DES, 3DES and the blowfish algorithms. Then we went on to discuss some of the areas where data encryption can be applied to solve network security problems. Review of relevant literatures with the work done, setbacks, limitations, and contribution to knowledge were studies and from which research gap will be established.

III. DESIGN METHODOLOGY

This section explains the materials and methods employed for the development of the proposed system.

3.1 Materials

User Equipment: This are the user equipment designed based on the ITU-T standard consisting of a transmitter, receiver and other cross layer control equipment for analogue or digital communication purposes.

Simulink model: Simulink is MATLAB-Based graphical programming environment for modeling, simulation and analyzing multi domain dynamic systems. Its primary interface is a graphical block diagramming tool and a customizable set of block libraries.

Transmitter: This a set of equipment used to generate and transmit electromagnetic waves carrying radio signals from one node to another within a network as shown in the simulink model below.

Receiver: This is a device that received radio waves transmitted via a transmitter device and encodes them in an interpretable message format as shown using the simulink model below.

Router: This is a device that employed in internet connection over multiple access points using a network switch. This is employed in both public and private domains where a single network provider is required to connect multiple digital devices over a single network. These routers are designed with built in wireless access point capabilities.

Switch: Network device that filters, forwards, and floods pieces of a message (packets) based on the destination address of each frame.

3.2 Methods

This work characterizes the Grace Point wireless data network. The aim of the characterization is to study and evaluate the data network performance and the security structure in place. This is with view of identifying the weakness in the data network security and improving the performance using the proposed system.

3.2.1 Method of Characterization

The characterization was done using the network structure in figure 3.6. The network contains various user equipment for end to end communication of packet data via the cloud. Before the communication process begins an instrument monitoring computer installed with DirectX 11 version software was connected to one end of the network, with the aim of monitoring the routed secured encrypted network performance.

To begin, the user equipment send packet to the other end of the network via a routing device designed using standard wireless encryption protocol (WEP) which generated encryption key and encrypts the network to prevent unauthorized access from intruder. This key is made public to the receiver router to decrypt the data received. This technique is applied to guarantee end to end encryption process and privacy during communication within the wireless network.

3.2.2 Data Collection

A real time characterization method was used which collected live data during the communication process. 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 below;

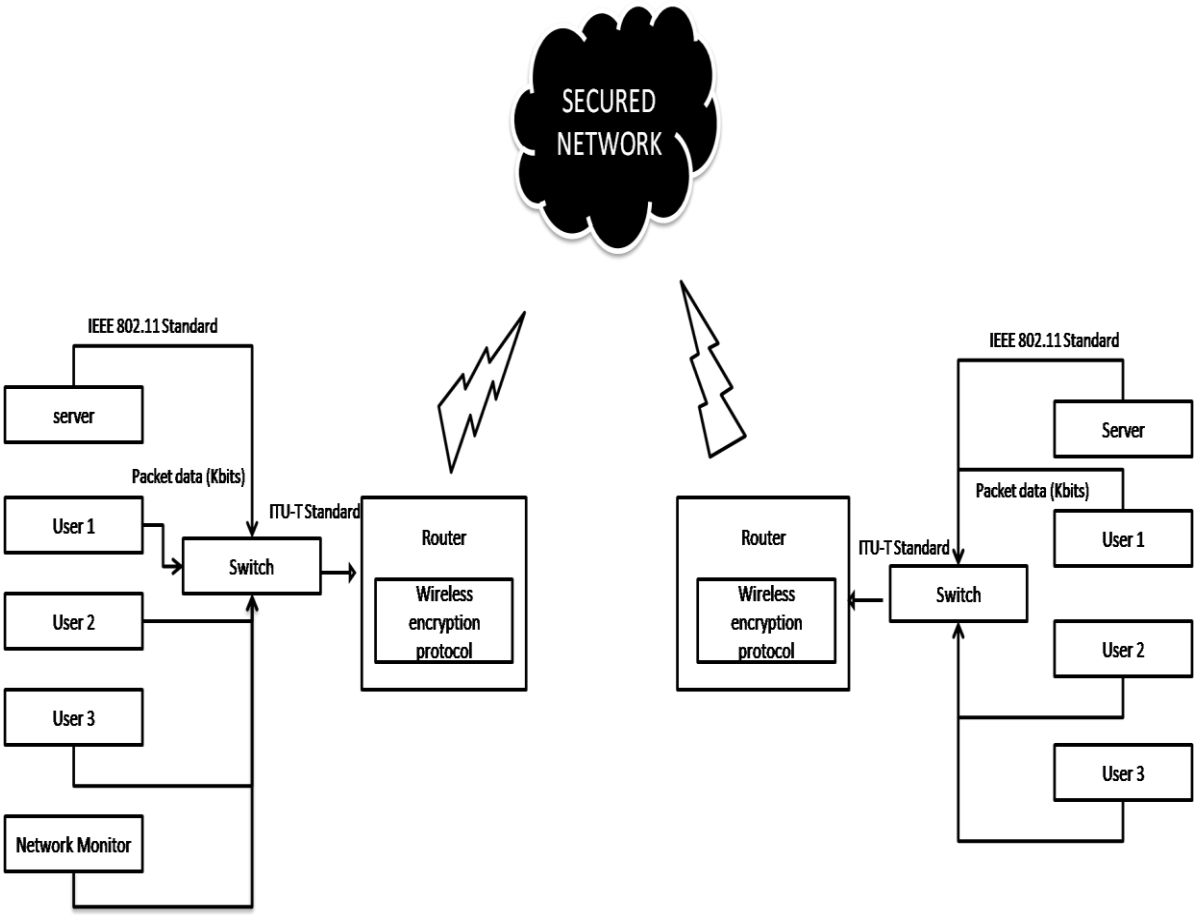

Figure 1: Grace Point Wireless Network

From the network above in figure 1, 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 characterized data are presented below considering the packet sent encrypted files, decrypted files, speed and time of encryption respectively.

Table 1: Characterized data

Packet sent (Kbits)	Date speed (ms)
1ooo	68
12oo	68
13oo	70
14oo	90
15oo	98
16oo	102
17oo	105
18oo	105
19oo	109
2ooo	115
21ooo	125
22oo	127
23oo	129
24oo	129
25oo	130
26oo	132
27oo	135
28oo	136
29oo	140
3ooo	148

These data was collected from monitoring device connected to the network and then presented as shown above. The results shows how 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 below;

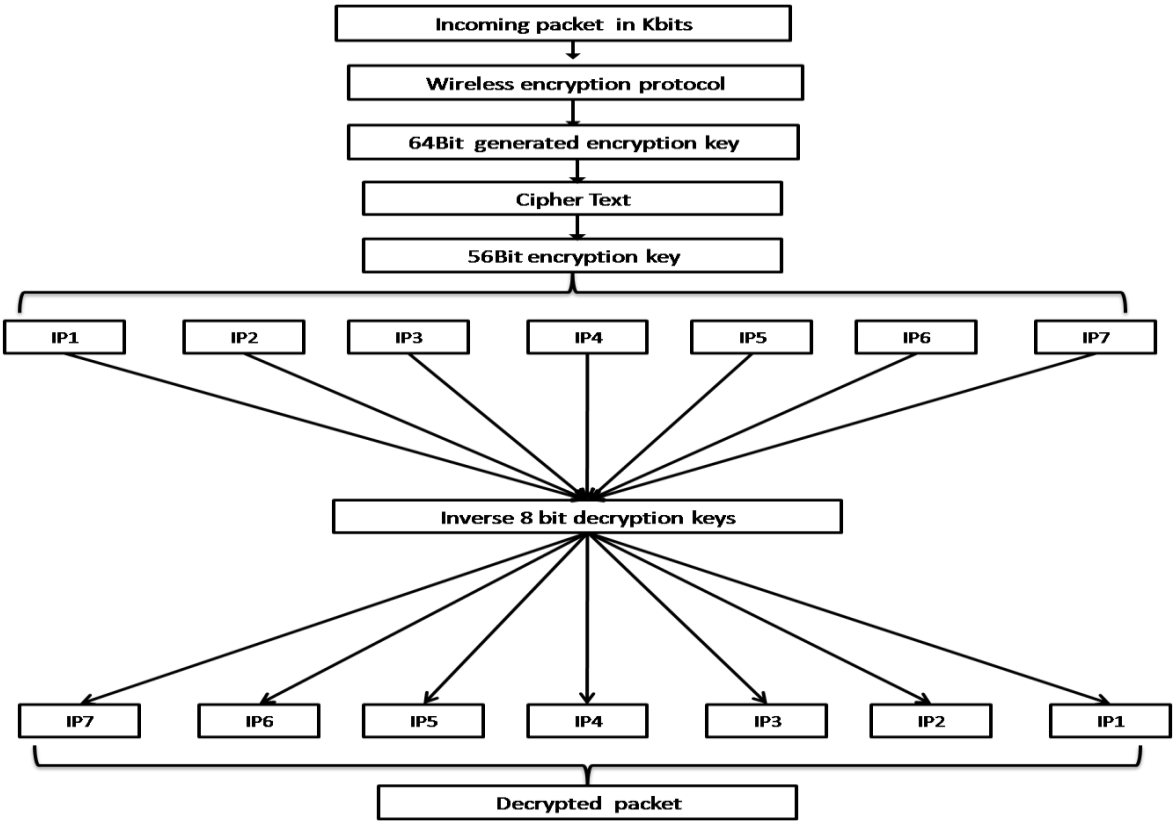

Figure 2: The conventional Wireless Encryption Protocol scheme

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. The result of the time taken from the analysis of the data collected in table 3.1 is presented in figure 3.3;

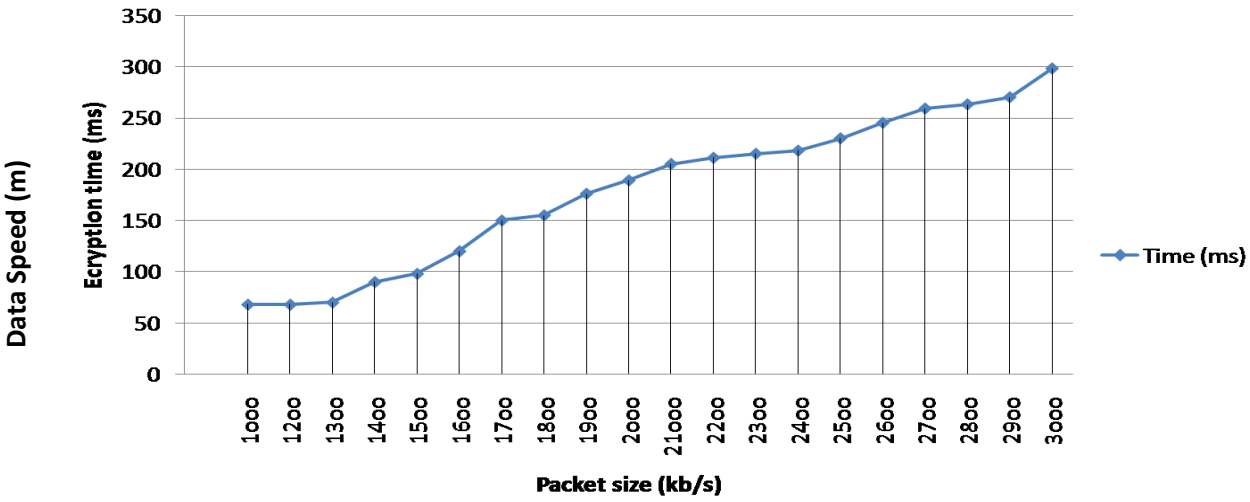

Figure 3: Encryption Time Graph

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.

3.2.3 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 speed

3.2.4 The Proposed Data Encryption Scheme

This will be done using advance data encryption (ADES) technique which is designed with improved blow fish algorithm.

3.2.5 Design of the Improved Blow Fish Algorithm

The proposed advanced encryption technique is developed 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. The improved blow fish algorithm is presented as shown below in figure 4 and is used to furnish the performance of the advance standard encryption technique.

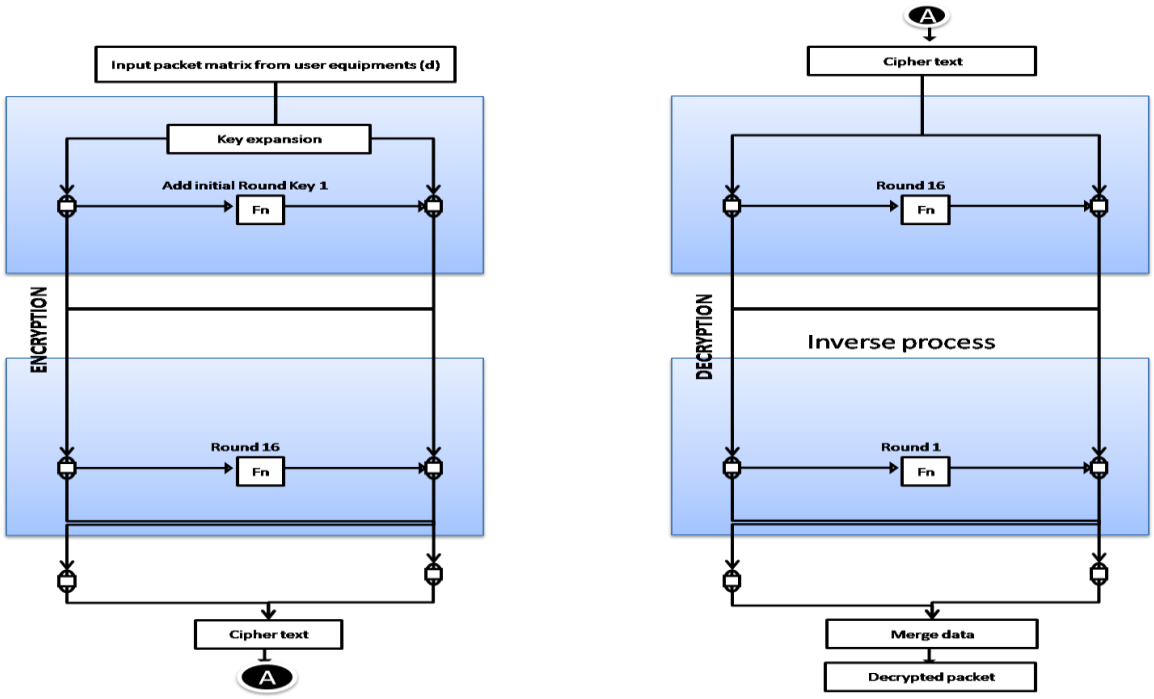

Figure 4: Improved Blow Fish Algorithm

From the figure 4, 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;

$$R_{u,t= \alpha W log2(1+SNR_{u,t})} \quad 3.2$$

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 below as

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

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.

Throughput Model

The research considers voice over internet as the service packet and the amount of user (u) data been able to be transmitted and successfully delivered to the end user is presented using the relationship between the size of the packet transmitted, the time of service request and time of packet transmission as below;

$$\text{Throughput} = \frac{VS_u}{T_{tx,u} - T_{r,u}} \quad 3.4$$

Where VS_u is the amount of packet to be transmitted by user u, $T_{r,u}$ is the time for service request and $T_{tx,u}$ is the transmission time for each packet.

3.2.6 The Improved encryption software

This section will develop the adaptive data encryption software using the improved blow fish algorithm developed in figure 3.3. The encryption software is designed using the flow chart below;

In the flow chart presented the improved blow fish algorithm already generated 16bit random key for the encryption of incoming packet. When user transit data from various user equipment through equation (3.1), the data are segmented into 32bit each and then encrypt 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

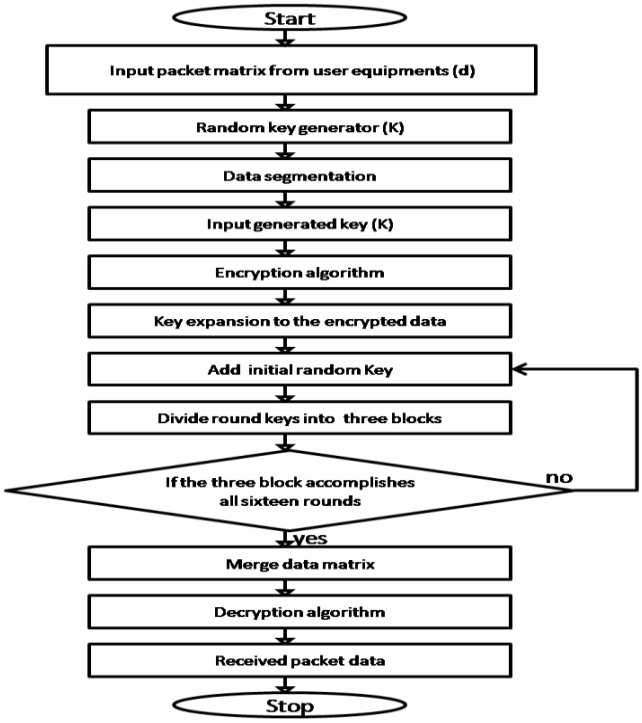

Figure 5: Improved Advanced Data Encryption Flow Chart

In the figure 5, the packet data from the user equipments 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.

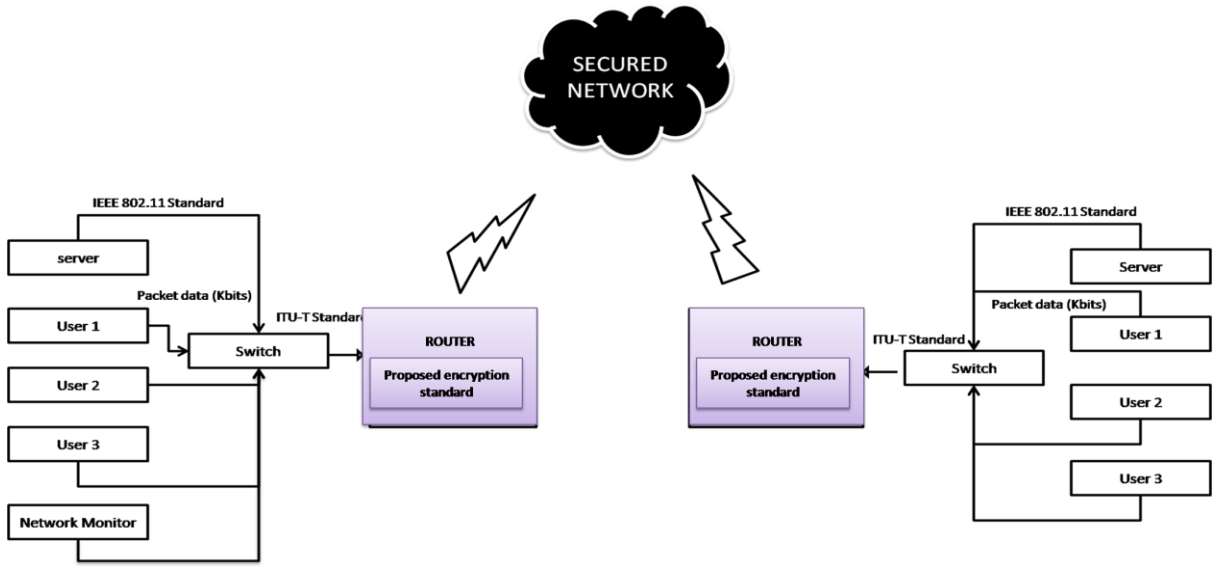

Figure 6: The Proposed System Block Diagram

From the block diagram above, the proposed system will be developed to improve the security performance of the characterized wireless network using an advanced software encryption scheme. The proposed system will improve the performance of the advanced data encryption scheme using blow fish algorithm to optimize security performance, speed and total time taken for the data processing of the characterized.

3.3 Simulation Work

Implementation of the Software

The software is implemented using Mathlab programming language, using signal processing toolbox, communication toolbox, optimization toolbox 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
```

3.3.1 Program modules

The program modules is explained using the data flow diagram, below which shows how packet data generated are encrypted before transmission and then decrypted before demodulation.

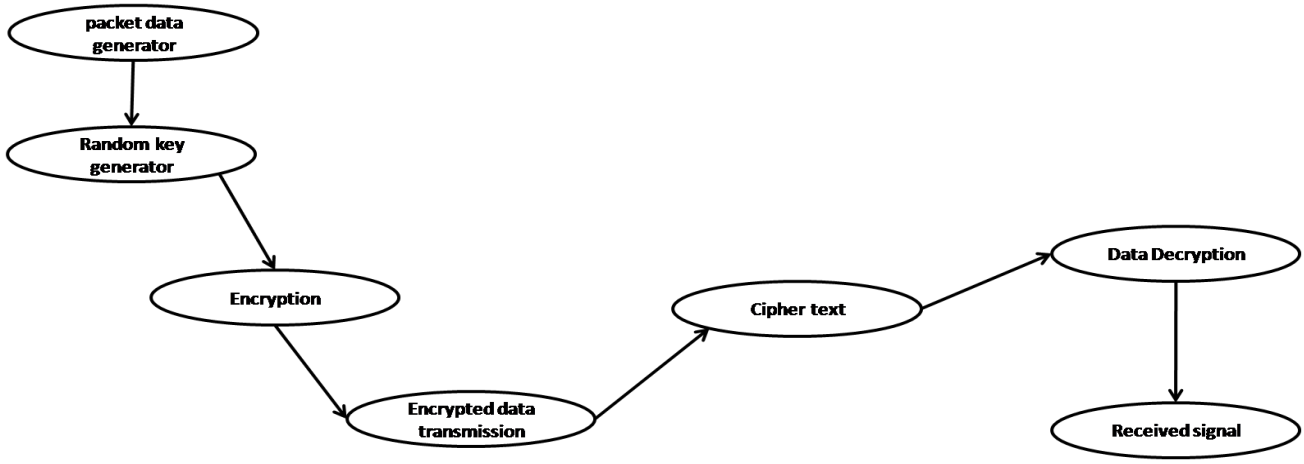

Figure 7: data flow diagram for the software encryption process

The figure 7 presents the data flow diagram of the data communication process. This 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.

3.3.2 Hardware and software specifications

The following specifications are defined to define both the software and hardware standards necessary to serve as platform for the entire application.

Software Specification:

Language: MATHTLAB

Operating System: Mac, Linux, Windows NT/95/98/2000

RAM: 256MB-8GB

Hard ware Specification:

Processor: Core, Intel P-III based system

Processor Speed: 250 MHz to 833MHz

RAM: 64MB to 256MB

Hard Disk: 2GB to 30GB

IV. RESULTS AND DISCUSSION

This chapter will discuss the results of the Mathlab scripted presented in the previous chapter as the implementation source code. The script was debugged in badges and the respective results is presented and discussed below;

4.1 Results

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

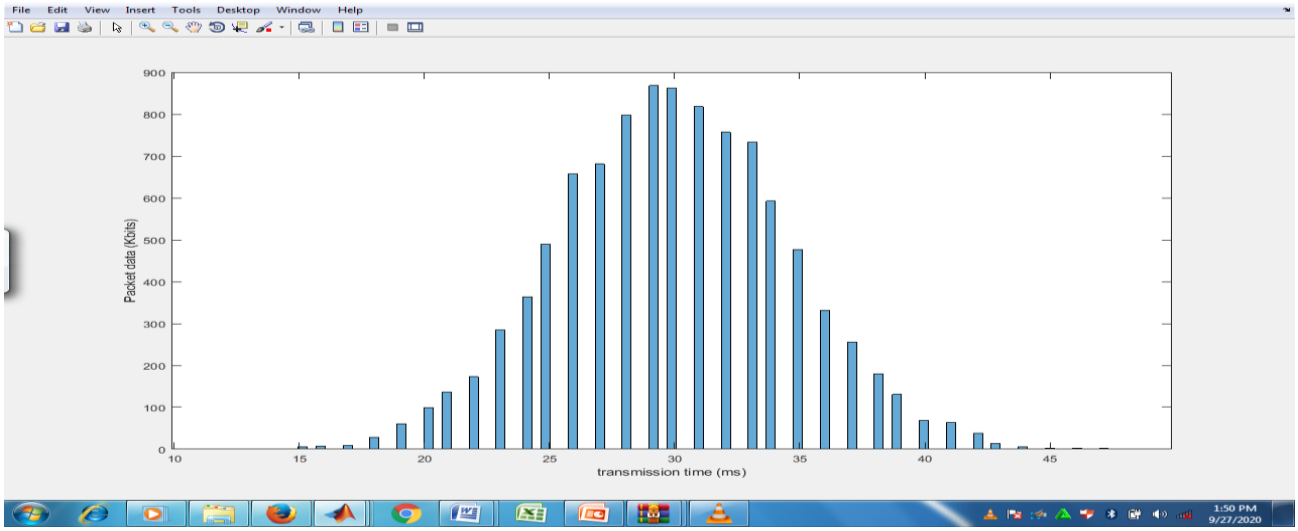

Figure 8: Packet Data Speed Profile

The result in the figure 8 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 7 for encryption before the throughput model in equation 3.3 is used to transmit.

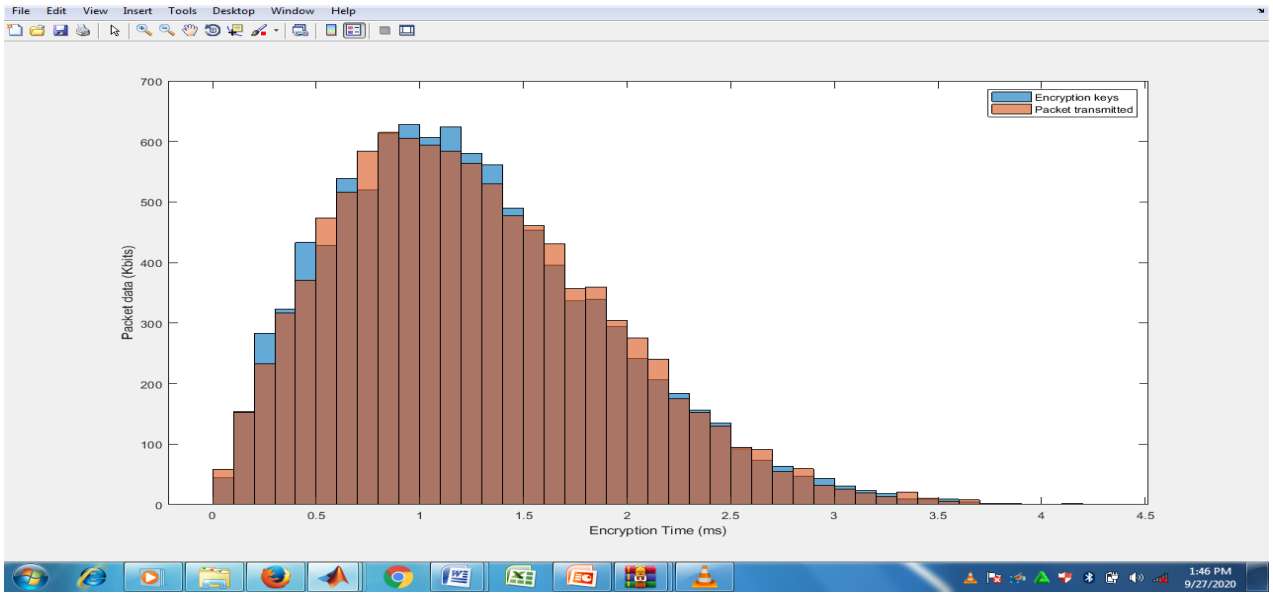

Figure 9: The encrypted signal

From the figure 9, 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.

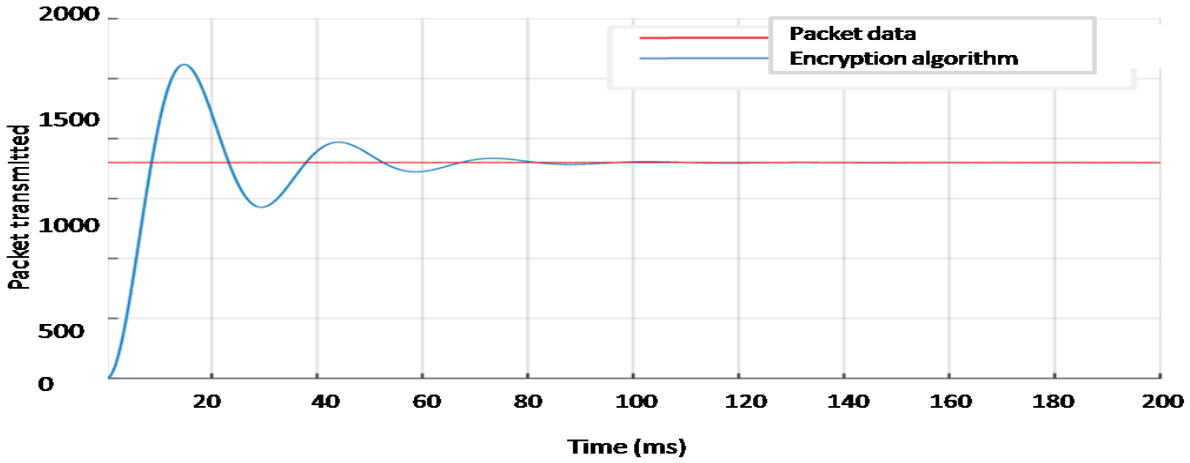

Figure 10: the encryption time

The result in figure 10 presented 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 Network

Packet sent (Kbits)	Data Speed (ms)
1ooo	68
12oo	68
13oo	70
14oo	70
15oo	71
16oo	72
17oo	75
18oo	75
19oo	76
2ooo	77
21ooo	78
22oo	78
23oo	79
24oo	84
25oo	89
26oo	90
27oo	92
28oo	93
29oo	95
3ooo	96
Average	79.8

The result in table 2 presented the performance of the improved algorithm deployed on the characterized network. The result was analyzed with excel software and the result are presented in the graph below;

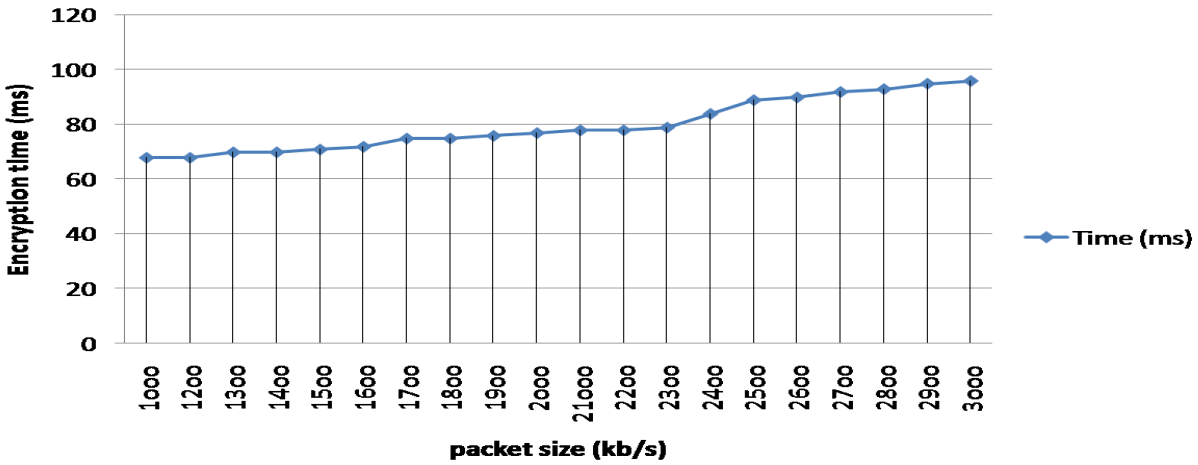

Figure 11: Performance of the improved encryption algorithm

From the result in figure 11, 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 presented below;

Table 3: Comparative analysis

Packet sent (Kbits)	Time (ms) with improved algorithm	Characterized Time (ms)
1ooo	68	68
12oo	68	68
13oo	70	70
14oo	70	90
15oo	71	98
16oo	72	102
17oo	75	105
18oo	75	105
19oo	76	109
2ooo	77	115
21ooo	78	125
22oo	78	127
23oo	79	129
24oo	84	129
25oo	89	130
26oo	90	132
27oo	92	135
28oo	93	136
29oo	95	140
3ooo	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 below;

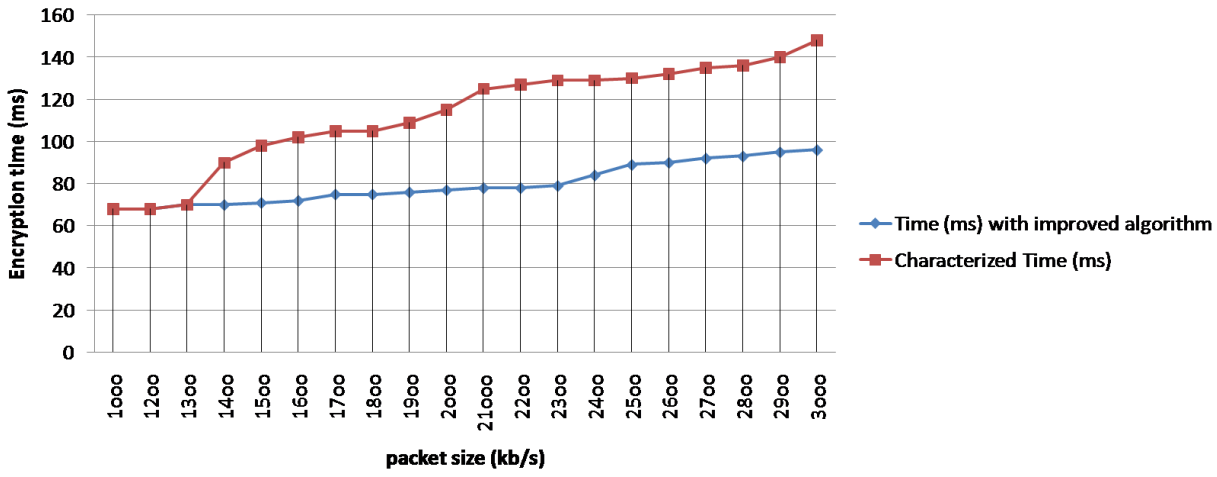

Figure 12: comparative result

The result here showed that comparative performance of the new and characterized encryption algorithm. The result showed that the characterized encryption time increases as the packet transmitted increases, while the improved encryption algorithm was fairly constant despite the increase in the packet size. The percentage increase is 29.4%.

V. CONCLUSION

5.1 Discussion

Over time, various companies have been attacked by intruders due to the vulnerabilities in the security scheme applied over their communication network structure. In the conventional system characterized, the data encryption standard technique commonly used, have lots of limitations like short encryption keys, low computational speed and time, among other challenges. This research has proposed, designed and implemented an improved security scheme for data network using advanced data encryption technique to provide a secured data transport layer for reliable communication and quality of service

5.2 Conclusion

This work presents improving security of data communication system using advanced management of encryption software scheme. From the literature reviewed, it has been revealed that the previous applications of data encryption technology applied in different data communication systems possess some level of limitations which we have identified and will channel our effort to closing it up. From the performance analysis of the different encryption algorithms reviewed earlier, it was observed that the characterized was able to encrypt data at 113.05ms, while the new algorithm was 79.8ms. The percentage improvement achieved is 24.5% improved encryption time. The decryption key was improved from 8bit to 32 bit in the new algorithm making the decryption process more complex for hackers.

REFERENCES

[1] AamerNadeem, YounusJaved, (2015). A Performance Comparison ofData Encryption Algorithms. 0-7803-9421-6/05/$20.00 ©2005 IEEE.

[2] Afaf M. Ali Al- Neaimi, Rehab F. Hassan(2016) " New Approach for Modified Blowfish Algorithm Using 4 – States Keys" , The 5th International Conference On Information Technology.

[3] Ako Muhammad Abdullah, MiranHikmat Mohammed and RozaHikmat Hama Aziz, (2015). New Security Techniques for Encrypting IP Address and Data Transfer over Wide Area Network through Three Levels. International Journal of Computer Science and Software Engineering (IJCSSE), Volume 4, Issue 3, March 2015. ISSN (Online): 2409-4285

[4] Ashima Jain (2013). Network Security, The Biggest Challenge in Communication. Advance in Electronic and Electric Engineering. ISSN 2231-1297, Volume 3, Number 7 (2013), pp. 797-804. http://www.ripublication.com/aeee.htm

[5] Ashraf Odeh, ShadiR.Masadeh, Ahmad Azzazi, (2015). A PERFORMANCE EVALUATION OF COMMON ENCRYPTION TECHNIQUES WITH SECURE WATERMARK SYSTEM (SWS). International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015. DOI : 10.5121/ijnsa.2015.7303.

[6] Bello, O and Adebari, F. A. (2012) "Data communication and Networking", Tony Terry Prints, Lagos, Nigeria.

[7] Brian Krebs, (2018). The Washington Post,"Forty Percent of Web Users Surf with Unsafe Browsers".

[8] CSI/FBI, (2017) Computer Crime and Security Survey, 9-14-2007. Content Posted by New Media Institute (NMI) Editor. Available at: http://en.wikipedia.org/wiki/Encryption.

[9] DacfeyDzung, Martin Naedele, Thomas P. Von Hoff, And Mario Crevatin, (2013). Security for Industrial Communication Systems. TheauthorsarewithABBCorporateResearch,BadenCH-5405,Switzerland. Digital Object Identifier 10.1109/JPROC.2005.849714 0018-9219/$20.00 © 2013 IEEE.

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

[11] Daipeng (2018). Application of Data Encryption Technology in Computer Network Communication Security [J]. Communication World, 2018 (02): 12-13.

[12] DarshanaPatil,Chawan P. M. (2017). A Secure Data Communication System Using Enhanced Cryptography and Steganography. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Website: www.ijircce.com Vol. 5, Issue 6, June 2017. ISSN(Online): 2320-9801 ISSN (Print): 2320-9798

[13] Dhanraj, C.Nandini, and Mohd Tajuddin (2015) "An Enhanced Approch for Secret Key Algorithm based on Data Encryption Standard", International Journal of Research And Review in Computer Science, August 2015

[14] Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhound " Performance Evaluation of Symmetric Encryption Algorithm ", IJCSNS, 2018

[15] Dong Yongwei, (2016). Application Analysis of Data Encryption Technology in Computer Network Communication Security [J]. Network Security Technology And Application, 2016 (04): 39-40.

[16] 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 (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December 2014. ISSN: 2319-8753. DOI:10.15680/IJIRSET.2014.0312008 Copyright to IJIRSET. www.ijirset.com

[17] Ferguson, J. Kelsey, S. Lucks, B. Schneier, M.Stay, D. Wagner, and D. Whiting(2010), Improved crypt-analysis of Rijndael,Seventh Fast Software Encryption Workshop, pp. 19, Springer-Verlag.

[18] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha " Performance Evaluation of Symmetric Cryptography Algorithms, IJECT, 2016.

[19] Hang Zhongshi, (2016). Application of Data Encryption Technology in Computer Network Communication Security [J].Prospect of Science and Technology, 2016,26(22): 8+55.

[20] Information Technology Laboratory, (2014). "Guideline for the analysis of LAN Security",http://www. itl.nist.gov/fipspubs/fip191.htm

[21] Jiang Jinming, (2017). On Application Mode of Data Encryption Technology in Computer Network Communication Security [J]. Scientific and Technological Innovation and Application, 2017 (01): 120

[22] KadekSuarWibawa, NyomanPiarsa, (2018). Secure Data Monitoring System with Encrypt Data Transmission over Radio Communication Based on Microcontroller. International Journal of Computer Applications (0975 – 8887) Volume 179 – No.21, February 2018.

[23] Kamaljit I. Lakhtaria, (2014). Protecting Computer Network with Encryption Technique: A Study. MCA Department, Atmiya Institute of Technology & Science, Yogidham, Rajkot, Gujarat, INDIA.

[24] Kiramatullah, Bibi Ayisha, Farrukh Irfan, InaamIllahi, Zeeshan Tahir, (2015). Comparison of Various Encryption Algorithms for Securing Data. Pakistan Institute of Engineering and Applied Sciences (PIEAS).

[25] Mageshwari and Karthikeyan (2015). CRYPTOGRAPHY POLICY BASED DATA COMMUNICATION IN TRUSTED ENVIRONMENT. International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.64 (2015) © Research India Publications; http:www.ripublication.comijaer.htm

[26] Mahmoud Shaar, Magdy Saeb, Usama Badawi, (2014). Hybrid Hiding Encryption Algorithm (HHEA) For Data Communication Security. DOI:10.1109/MWSCAS.2003.1562321 · Source: IEEE Xplorehttps://www.researchgate.net/publication/4205334.\

[27] Meng Shen, (2018). Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT. Member, IEEE, Baoli Ma, Liehuang Zhu, Member, IEEE arXiv:1809.07914v1 [cs.CR] 21 Sep 2018

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

[29] Mohan V. Pawar, 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.

[30] Nadeem Ahmad, Kashif Habib, (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

[31] Omolara O.E., Oludare A.Iand AbdulahiS.E, (2014). Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication. Computer Engineering and Intelligent Systems. www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.5, No.5, 2014.

[32] Penchalaiah, N. and Seshadri, R. ffective (2010),"Comparison and Evaluation of DES and Rijndael Algorithm (AES)", International Journal of Computer Science and Engineering, Vol. 02, No.05.

[33] Sadeq ALHAMOUZ, (2013). Data and Communication Security. Amman Arab University for Graduate Studies Amman - 11935/Jordan Sadeq@aau.edu.jo35ISSN: 1690-4524.

[34] Sagiroglu S., and Tunckanat M., (2012). A Secure Internet Communication Tool, Turkish Journal of Telecommunications, Vol. 1, No. 1, pp. 1-10

[35] Saleh Saraireh, (2013). A SECURE DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGANOGRAPHY. International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.

[36] Schneier, Bruce (2012)."The Blowfish Encryption Algorithm". Blowfish, <http://www.schneier.com/blowfish.html>.

[37] Singhal, Nidhi and Raina, J P S (2011)."Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181.

[38] SubhiAlmohtasib, Alaa H Al-Hamami, (2018). Securing Data Communication for Data Driven Applications Using End to End Encryption. Indonesian Journal of Electrical Engineering and Computer Science Vol. 10, No. 2, May 2018, pp. 756~762 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i2.pp756-762. homepage: http://iaescore.com/journals/index.php/ijeecs

[39] Surhone L. M., Timpledon M. T., and Markesen S. F.(2010). Secure Communication,Betascript Publishing.

[40] Tingyuan Nie, Teng Zhang " A Study of DES and Blowfish Encryption Algorithm",TENCON, 2019

[41] Utku KOSE, (2014). SECURITY APPROACHES IN INTERNET COMMUNICATION. https://www.researchgate.net/publication/235763148. uploaded by UtkuKöse on 26 May 2014.

[42] Verma P, Ritu Agarwal, Dhiraj Dafouti,Shobha Tyagi " Performance Analysis Of Data Encryption Algorithms " , 2015

[43] Wei CHU, (2019). Application of Data Encryption Technology in Computer Network Security. School of Computer Engineering, Bengbu University, Bengbu, Anhui 233000, China. IOP Conf. Series: Journal of Physics: Conf. Series 1237 (2019) 022049. IOP Publishing doi:10.1088/1742-6596/1237/2/022049.

[44] Wikipedia – The Free Encyclopedia: Secure Communication, (2010). [Online] Retrieved April 13, 2010 from: http://en.wikipedia.org/wiki/Secure_communication

[45] Wikiversity, (2012). "Introduction to Computers/System Software-Wikiversity" http://en.wikiversity.org/wiki/Introduction_to_Computers/System_software.

[46] Xiangqin Li, (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

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

[48] Yekini N.,AsafeAdebari F.,Adebayo BelloOlalekan, (2015). DATA COMMUNICATION & NETWORKING. Computer Engineering Department Yaba College of Technology Lagos Nigeria.https://www.researchgate.net/publication/288180515

[49] Yeu-Pong Lai and Po-Lun Hsia, (2017). "Using the vulnerability information of computer systems to improve the network security", Journal of Computer Communications, vol. 30, Issue. 9, pp. 2032-2047.

[50] Yu Dongxu, (2018). Application of Data Encryption Technology in Computer Network CommunicationSecurity [J]. Electronic Technology and Software Engineering, (19): 216-217

[51] Zhang Gaike, (2018). Application of Data Encryption Technology in Computer Network Communication Security [J]. Computer Fan, 2018 (02): 63.