DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5873

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

HYBRID SECURITY ARCHITECTURE FOR DATA COMMUNICATIONS (SADC)

Tewhasom Aregay
Head, Department of Computer Science
Adigrat University
Ethiopia

Dr. M.Anand Kumar
Professor, Department of Computer Science
Adigrat University
Ethiopia

Abstract: Communication networks and Internet had a tremendous growth in the recent past years. Today most of the government sectors, financial institutions, corporations, military and others exchange huge amount of confidential information by using the Internet Application Layer security is a growing area of concern for developers, designers, quality assurance specialist and programmers. Application security is the prevention of flaws and vulnerability that occur in the design, development, and deployment of applications that run on application layer of TCP/IP Protocol Suite. Although IPv6 both simplifies and improves IPv4, it poses several significant security challenges. First, even though IPSec support is mandatory in IPv6, its use is not. Not using IPSec exposes a network to old IP-related attacks as well as attacks related to IPv6-specific features. A working IPSec infrastructure is also difficult to deploy and manage, further reducing IPSec's use. Some problems that affect IPv4 networks such as application-layer attacks, rogue devices and packet flooding can also affect IPv6 networks. Finally, several other new, unanticipated security problems will arise as the hacking community starts actively targeting IPv6 networks. This paper proposes new security architecture for data communication.

Keywords: Communication, Encryption, Decryption, Internet, IPv4, and IPv6.

1. INTRODUCTION

Internet plays a vital role in exchange of information across the world. Today most of the government sectors, financial institutions, corporations, military and others exchange huge amount of confidential information using the Internet [1]. With the rapid growth in technology security became a crucial issue that is to be solved to protect the confidential information from the unauthorized users. The Internet today is being utilized by billions of clients for an extensive assortment of business and non business purposes. It is controlled by various elements [2]. It pointed out that Internet is mainly used as an efficient means for communication, entertainment and education. There is a need for protecting confidential data because of the rapid growth of Internet.

The Internet was however originally designed for research and educational purpose and not for commercial applications. So Internet was not planned in view of security. As the Internet develops the current security structure was not satisfactory for the present application [3]. This was mostly because of the absence of security benefits in the TCP/IP Protocol Suite. The absence of confirmation instrument of TCP/IP Protocol Suite is fundamentally because of the poor security component of bundles and communicates nature of the lower layer conventions. Moreover there are no defense mechanisms for the application layer of the network model. IPSec do not provide any security for applications in application layer. Internet Control Message Protocol attacks is still possible which a major setback of IPv6 [4].

This research aims at designing, implementing and evaluating new security architecture as an alternate to the existing TCP/IP Protocol Suite with the objective of improving the security. The rest of the paper is presented as follows. In
section II we describe the architecture of TCP/IP model followed by cryptographic algorithms in section III. We then describe the proposed architecture in section IV. In section V, we analyze the performance and finally conclude in section VI.

2. LITERATURE SURVEY

The fast development of the present Internet, which works utilizing Internet Protocol adaptation 4(IPv4) has made various issues for the organization and operation of the worldwide systems. Parcel of research works was being finished by the examination groups to enhance the existing version of internet protocol. The work [5] called attention to the issues of the present rendition of Internet convention The author [6] displayed a few key upgrades offered by the Internet Protocol variant 6 (IPv6) over current Internet Protocol adaptation 4 (IPv4). For example, IPv6 tending to and directing ideas, changes to the base IPv6 parcel size, streams, and movement classes, the neighbor disclosure and hub auto design instruments.

A few issues that influence IPv4 systems, for example, Reconnaissance, Unauthorized get to, Host introduction and related assaults, Routing assaults, DoS assault on DAD convention, Man-in-the-center assault, Multicast-based assaults and Spoofing assaults can likewise assault IPv6 systems. In addition a few other new unexpected security issues will probably develop as the hacking group begins effectively focusing on IPv6 systems. The paper [4] pointed out some of the security issues of IPv6. The work [7] proposed a security mechanism to enhance security for TCP/IP suite. The work adds three modules to TCP/IP model, for example, security arrangement, security control and information security layer. Not at all like IPsec, which

connects all security implementations to IP layer, has the proposed engineering appropriated the proposed module into their pertinent layer. The security strategy has a place with application layer, and the security control and administration situated in the vehicle layer. The information security layer is situated between the transport layer and the IP layer. It was also identified that the concept is similar to that of IPsec mechanism. So, more than 50% IPSec related attacks are still possible with this model.

The work [8] proposed a model called secure Internet access to gateway using secure socket that uses secure socket layer (SSL) to provide a secure channel between client and gateway server. A smart card was used for client authentication and encryption/decryption of the data. This works aims to deliver the maximum amount of security to the communications link of the Internet gateway for unified automation network access (IGUANA) system, while still being practical and effective in its use and implementation. The work [9] proposed a novel cryptographic algorithm that uses both IDEA and blowfish for encryption as well as SHA-1 to generate hash values. It was stated that the architecture helps to provide a secure cryptographic algorithm for next generation of security. The limitation of this approach is difficult to implement the architecture in handheld devices. Also when both IDEA and Blowfish algorithms are used at the same time, there will be overhead in terms of processing. It will not be suitable for bulk data transfer as well as for complex applications.

The author [10] presented a new security model for IPv6 networks. The new model is based on the end-to-end connectivity that is restored in IPv6, thus allowing the use of host based security systems together with the perimeter security devices. However, the use of HBS complicates the security trust management. Therefore another component of the model was introduced namely a policy based security management approach.

The work [11] proposed an algorithm for security inter-layer communication and a solution for Cross-Layer signaling between nodes of TCP/IP model. The security mechanisms in the MAC layer are added to existing security mechanisms in other layers of the TCP/IP model, and therefore it generates multiple encryption of information. The author [12] presented a hybrid encryption algorithm with the combination of both DSA and RSA It was expressed that the proposed work have improved the hardness in security by consolidating the RSA and DSA encryption calculations by including some greater security codes. The major limitation of the proposed work was that security flaws of RSA and DSA will have the same affects in this hybrid algorithm.

The paper [13] proposed another crossover cryptographic calculation .The proposed calculation was composed by the mix of DES and AES calculation. In the event that the plain-content of b bit, at that point initially bit utilizes AES to scramble and second piece utilizes DES to encode. The decoding procedure is transform of the encryption procedure. The principle restriction of this half and half calculation is that the procedure is accomplished for every last piece like that of stream ciphers. It was also identified that there will be a maximum overhead in terms of processing.

3. PROPOSED WORK

Initially the proposed architecture was implemented with three well known existing cryptography algorithms such as Blowfish, Elgamal and MD5 Hash algorithm. The work was published in the paper [14]. To begin with the plain-content Pt is scrambled utilizing Blowfish encryption. The keyk that is utilized for encryption is additionally encoded utilizing Elgamal encryption. At that point the figure content Ct alongside the figure key Ck will be sent to goal. In the meantime message process for the plain-content will be computed utilizing MD5. At that point the message process will be encoded utilizing Elgamal encryption. Presently Cm will be sent to goal alongside Ct, Ck. At the collector end first the key is unscrambled utilizing Elgamal decoding. Next with the acquired key the Cipher-content is decoded. In the meantime message process is computed utilizing SHA. At that point the message process that is received from the source end is contrasted and the process that is ascertained in the beneficiary side. The ALSP design that is proposed here utilizations both symmetric and asymmetric cryptography to give every one of the parts of system security, for example, secrecy, trustworthiness, verification, non-disavowal, accessibility and get to control. From the above architecture it was found that to obtain maximum security, the block size and key size of the algorithm should be large enough. Another aspect in terms of performance is that, it was identified that the encryption time to be reduced to get the better performance. Based on the analysis, the proposed architecture was formulated as

- A 512 bit block cipher instead of Blowfish and IDEA
- An Algorithm that take minimum time for encryption process
- Algorithm that support real time application such as voice data.

SF Block cipher is a 512 bit block cipher. This Block cipher is based on a design principle known as Substitution Permutation Network (SP Network). It takes a block of the plain-text and the key as inputs, and applies several alternating rounds or layers of substitution boxes (S-boxes) and permutation boxes (P-boxes) to produce the cipher-text block. The block size of the algorithm is 512 bit and the key size is also 512 bit. The implementation of the algorithm can be found in the paper [15]. The following figure shows the working process of the architecture.

Finally the architecture was implemented with three algorithms namely SF Block cipher which is 512 bit, Elgamal algorithm and SHA-2 hash function. The analysis shows that the proposed model was more secure than that of the previous model and the performance was good when compared to other existing algorithms. The following figure shows the working process of the architecture.

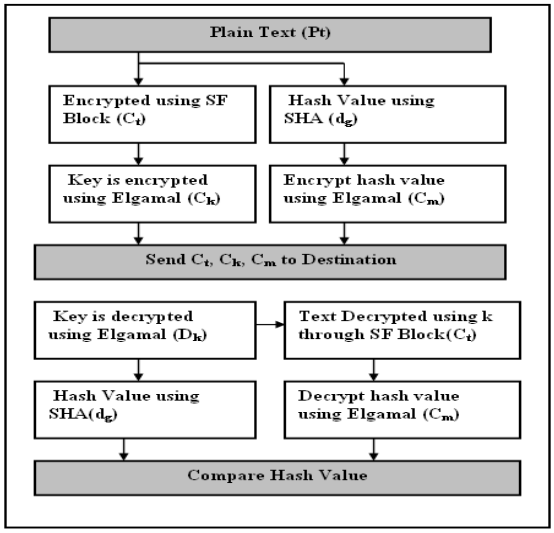

Figure 1 Security Architecture

Sender Side Algorithm

Step1: The data is encrypted using SF C_t = SF (P_t)
Step 2: The key_k is Encrypted using ELG C_k= ELG (k)
Step 3: Message digest for data using SHA d_g = SHA (P_t)
Step 4: Encrypt digest using ELG Cm= ELG (d_g)
Step 5: Send C_t, C_k, C_m to destination

Receiver Side Algorithm

Step 1: The key is decrypted using ELG D_k = ELG (C_k) = k
Step 2: The key_k is used to decrypt text D=SF (C_t)= P_t
Step 3: Message digest for data using SHA D_g = SHA (P_t) = dg
Step 4: Decrypt digest using ELG P_m = ELG (C_m) = d_g
Step 5: Compare d_g from Step 3 and Step 4.
Step 6: If equal data is accepted else rejected.

4. PERFORMANCE ANALYSIS

The performance of the proposed algorithm was compared with two commonly used symmetric encryption algorithms such as Blowfish and AES [16]. The performance measure of encryption schemes was conducted using several performance metrics such as energy consumption, changing data types such as text or document and images, changing packet size and changing key size for the selected cryptographic algorithms. The simulation setup was already tested with the work [17]. The experiments are performed several times to assure that the results are constant and are valid to compare the different algorithms with the proposed algorithm.

A. Encryption Process

The encryption time was calculated for the three algorithms namely AES, Blowfish and Proposed SF Block cipher. It is the aggregate time taken to deliver cipher content from plain-content. The computed encryption time is then used to ascertain the throughput of the scrambled calculation. Different file sizes ranging from 40 Kb to 8000 kb is used for the evaluation. It gives the rate of encryption. The formula for the calculation was given in 3.3.4.

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	AES	SF Block Cipher
1	49.00	59.0	36.0	56.0
2	59.10	39.0	36.0	38.0
3	100.09	94.0	61.0	90.0
4	247.12	121.0	90.0	112.0
5	321.24	167.0	134.0	164.0
6	694.45	234.0	256.0	210.0
7	899.12	254.0	256.0	258.0
8	963.09	213.0	187.0	208.0
9	5345.15	1324.0	1376.0	1237.0
10	7310.39	1432.0	1543.0	1366.0

Table 1. Time Consumption (Encryption)

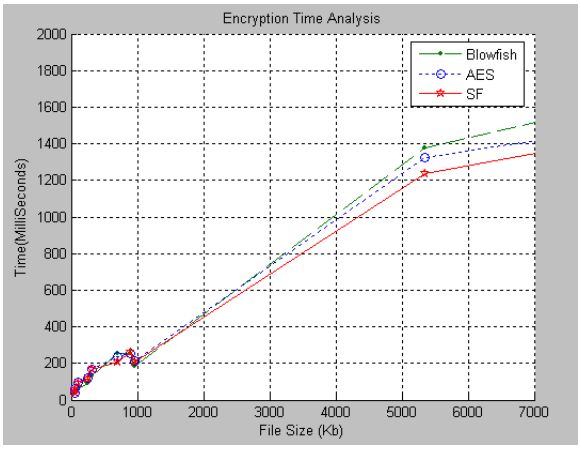

Figure 2. Time Consumption (Encryption)

B. Decryption Process

As in similar way of encryption, the time was calculated for the decryption process with the different file sizes. The table gives the time taken for decryption process.

Table 2. Time Consumption (Decryption)

S.No	Packet Size (KB)	Time Consumption(Decryption)		
		Blowfish	AES	SF Block Cipher
1	49.00	65.00	38.00	61.00
2	59.10	45.00	39.00	43.00
3	100.09	89.00	71.00	79.00
4	247.12	120.00	145.00	112.00
5	321.24	167.00	234.00	168.00
6	694.45	243.00	256.00	212.00
7	899.12	223.00	252.00	259.00
8	963.09	243.00	342.00	206.00
9	5345.15	1224.00	1371.00	1216.00
10	7310.39	1435.00	1443.00	1363.00

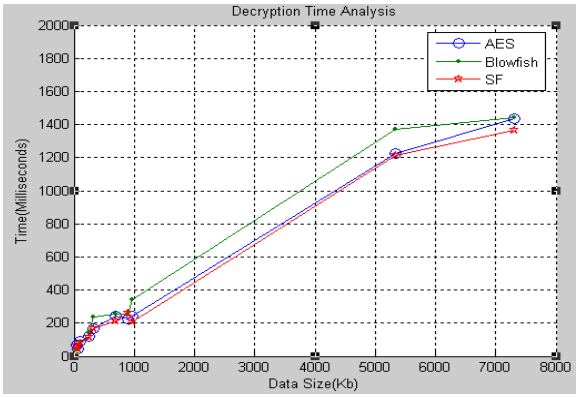

Figure 3. Time Consumption (Decryption)

C. Throughput analysis of Encryption and Decryption

The throughput of the encryption plot characterizes the speed of encryption. At the point when there is an expansion in the throughput of the encryption calculation, there is abatement in the power utilization calculation. Figure 6.16 means the throughput of encryption and figure 6.17 demonstrates the throughput of unscrambling. From the investigation it demonstrates that the proposed SF Block figure has preferable throughput over that of blowfish and AES calculations.

Table 3 Throughput (Encryption)

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	AES	SF Block Cipher
1	49	59	36	56
2	59	39	36	38
3	100	94	61	90
4	247	121	90	112
5	321	167	134	164
6	694	234	256	210
7	899	254	256	258
8	963	213	187	208
9	5345	1324	1376	1237
10	7310	1432	1543	1366
Average		**386**	**395**	**374**
Throughput		**4.29**	**3.34**	**4.59**

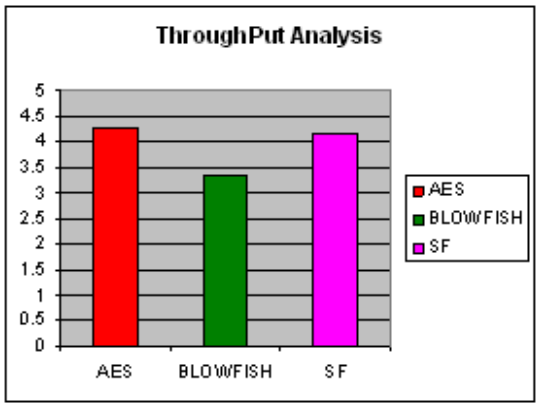

Figure 4. Throughput (Encryption)

Table 4. Throughput (Decryption)

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	AES	SF Block Cipher
1	49	65	36	61
2	59	45	36	43
3	100	89	61	79
4	247	120	90	112
5	321	167	134	168
6	694	243	256	212
7	899	223	256	259
8	963	243	187	206
9	5345	1224	1376	1216
10	7310	1435	1543	1363
Average		**388**	**395**	**377**
Throughput		**4.26**	**4.11**	**4.27**

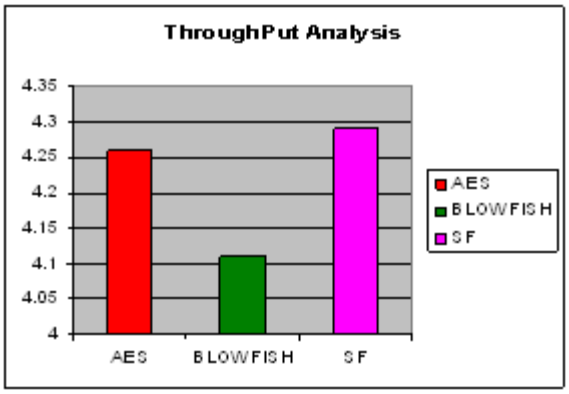

Figure 5 Throughput (Decryption)

5. CONCLUSION

In this work, the targets of planning new hybrid security design were accomplished. Another 512 piece cryptographic encryption, decoding and key administration calculation to improve the security of the TCP/IP convention suite was executed. A large portion of the accessible encryption and decoding strategies are not reasonable to be utilized to secure private information over an open system since they were initially planned before 10 years with restricted convenience. This exploration builds up another security structure that can be suited for content and additionally voice information with least over-burden regarding preparing. The proposed engineering has been executed and tried. The proposed framework utilizes 512-piece block and 512-piece key length for encryption and unscrambling process which was the primary favorable position over the current calculations. Because of the key size and square, it was difficult to execute the cryptanalysis.

6. REFERENCES

[1] Mingyuan Xin, "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System", International Conference on Cyber-Enabled Distributed

Computing and Knowledge Discovery. Vol 1, no 1, pp. 62-65, 2015

[2] Heesook Choi, Sencun Zhu, Guohong Cao, Raju Kumar, Thomas La Porta, and Patrick Traynor, "Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks", IEEE Transactions on Mobile Computing, vol. 6, no. 1 , pp. 663-677, 2007.

[3] Wentao Shang, Yingdi Yu, Ralph Droms, Lixia Zhang, "Challenges in IoT Networking via TCP/IP Architecture", NDN, Technical Report NDN-0038, February 10, 2016.

[4] Summit R. Tuladhar, James B.D. Joshi, Carlos E. Caicedo, "IPv6 Security Challenges", Computer, vol. 42, no.2 , pp. 36-42, 2009.

[5] Goth, G. "The End of IPv4 is Nearly Here 2014", IEEE Internet Computing, vol 6 no 2 pp. 7-11,2013

[6] N. Chuangchunsong, T. Kamolphiwong, T. Angchuan, "Performance of intra and inter communications of IPv4-in-IPv6 tunneling mechanisms", TENCON IEEE Region 10 Conference, pp. 1-6, 2014

[7] Mohammad Al-Jarrah, and Abdel-Karim R. Tamimi, "A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancement", Innovations in Information Technology. Vol 1 no 1 pp. 1-5, 2006

[8] Bhatt, D. V., S. Schulze, and G.P Hancke, "Secure Internet access to gateway using secure socket layer", IEEE Transactions on Instrumentation and Measurement, vol 55 o 3 pp. 793-800,2006.

[9] Thanuja, R., S. Dilip Kumar, "A Novel Cryptographic Architecture", Journal of Theoretical and Applied Information Technology, vol 38 no 1 pp. 74-78, 2012.

[10] Choudhary, A. R., and A. Sekelsky, "Securing IPv6 network infrastructure: A new security model", IEEE Technologies for Homeland Security, pp. 500-506, 2012

[11] Urbano Fullana, A., J. L. Ferrer Gomila, M. Payeras Capella, M. Hinarejos Campos, and L. Huguet Rotger, "Cross-Layer Secrecy Design on TCP/IP and 802.11 for Energy Saving", Proceedings of IEEE Conference on New Technologies, Mobility and Security (NTMS),pp 1-5, 2011.

[12] Shabnam Parveen, and Priyanka Gandhi," Enhanced Hybrid Encryption Algorithm for Security of Network", International Journal of Engineering Research and Applications, vol 2 no 4, pp. 873-876.,2012.

[13] Wang Tianfu, K., and Ramesh Babu, "Design of a Hybrid Cryptographic Algorithm", International Journal of Computer Science & Communication Networks, vol 2, no 2,pp. 277-283,2011

[14] Anand Kumar M., Dr. S. Karthikeyan, "Security Model for TCP/IP Protocol Suite", Journal of Advances in Information Technology, vol 2 no 2, pp. 87-91,2011.

[15] Anand Kumar.M and Dr. S. Karthikeyan," A New 512 Bit Cipher - SF Block Cipher" International. Journal of Computer Network and Information Security", vol 4 no 11, pp. 55-61, 2012.

[16] Mr.B.Bharathi , Mr.G.Manivasagam , Dr.M.Anand Kumar, "Metrics For Performance Evaluation of Encryption Algorithms", International Journal of Advance Research in Science and Engineering", vol 6 No 3, pp. 62-72, 2017

[17] Anand Kumar M.and Dr. S. Karthikeyan," Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms" International Journal of Computer Network and Information Security", vol 4 no 2, pp. 22-28, 2011

