2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) | 978-1-6654-7884-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICSCDS53736.2022.9760971

Classification of Security Levels to Enhance the Data Sharing Transmissions using Blowfish Algorithm In Comparison With Data Encryption Standard

Malli Mahendra
Research Scholar,
Department of Computer Science and Engineering,
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences,
Saveetha University, Chennai,
Tamilnadu, India, Pincode: 602105.
mallimahendra17@saveetha.com.

Ms.P. Shamuga Prabha
Project Guide, Corresponding Author,
Department of Computer Science and Engineering,
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences,
Saveetha University, Chennai,
Tamilnadu, India, Pincode: 602105.
shanmugaprabhap.sse@saveetha.com.

***Abstract*-- To ensure the information with limiting the spillage and loss of information, by fostering the privacy, integrity of information move through the cloud and improve the trust pace of the users. To give security in the cloud Novel Data Authentication is used. Materials and Methods: To guarantee security a critical plan is executed that is against the cipher attack. A total sample size of 20 is performed on two gatherings to accomplish the better encryption time. Result: The Blowfish algorithm produces a better execution time of (0.14 sec) than the Data Encryption Standard of (0.4 sec) with significance p-value of 0.012. Conclusion: Blowfish algorithm takes less encryption time than the Data Encryption Standard. Blowfish produces less Standard Error mean value (Standard Error Mean value = .01733) than Data Encryption Standard (Standard Error Mean value = .03005).**

Keywords: Cloud Computing, Data Encryption Standard, Blowfish, Encryption, Decryption, Novel Data Authentication.

I. INTRODUCTION

Cloud computing is the conveyance of various administrations through the web. These assets incorporate instruments and applications like information stockpiling, data sets, system administration and programming. Cloud based capacity makes it conceivable to save documents and recover them on request . The importance of cryptography is that it is a security tactic that protects the information from cyber threats and cipher attacks through the use of code. It protects the files, so that users can access and send the data safely [1]. Applications of cryptographic encryption are Electronic money and time stamping [2]. The other important application is securing email communications [3].

Cloud Security is carried out by researchers in which 20 research articles in IEEE digital xplore and 10 articles are published in research gate. The boom in computing, networking growth and threats extended the want for continuous controlled safety. Data safety enables the preservation of records privately [4]. Network protection is the most important thing in data protection, because it prevents information and network on hand assets from change and unauthorized use [5]. This paper yields the assessment of encryption algorithms such as Blowfish, AES, etc [5], [6]. Information is encoded utilizing blowfish which offers security to the data. It is estimated through normal encryption time, memory use and battery utilization [7]. Previously our team has rich experience in working on various research projects across multiple disciplines [8]. [9]–[13]. Now the growing trend in this area motivated us to pursue this research. We have collaborated with various authors across our institutions that has made us complete the project with ease and accuracy[14]–[30].Based on the literature survey, Data Encryption Standard does not provide better encryption time and security. The aim of the study is that Blowfish Algorithm provides better secrecy to the files. The keyword Novel Data Authentication is used to provide security to the content in the cloud server.

II. MATERIALS AND METHODS

The study setting of proposed work is done in Saveetha School of Engineering. The total number of groups for this research work are two, the first group is Blowfish and the second one is Data Encryption Standard. The sample size was calculated by using previous study results, by keeping threshold 0.05, G power 80%, confidence interval 95 %, and enrollment ratio as 1 [31].The procedure here follows the data encryption and decryption taken place in the cloud to provide better security. To start with, documents are encrypted to the system. Then the client needs to give the encrypted private key or an hexadecimal string. Further the encrypted documents are stored in the specified path. Clients from the other side need to provide the encrypted private key for accessing the original data. After that the document will be decrypted and shows the original information shown to the client.

A. Blowfish Algorithm

The delicate information and symmetric key are used inside the encryption calculation to transform the touchy information into cipher-text [32]. Blowfish alongside its replacement TwoFish, was in racing to supplant the Data Encryption Standard, however bombed because of the little size of its square. It has a block size of sixty four bits with key-length thirty two bits to Four forty eight bits multiple size [33]. The number of subkeys is eighteen with 16 rounds. Symmetric encryption implies that the key used to encode and decode information is something very similar [34]. In the Blowfish calculation, the encryption key encodes secret information into cipher text. Blowfish is the adoptive parent of the Twofish Encryption [3]. Table 1 shows pseudo code for Blowfish Algorithm.

TABLE 1. PSEUDO CODE FOR BLOWFISH ALGORITHM

```
INPUT: File from the system
1.Import the required packages.
2.Get the key or hexadecimal string from the user.
3.Access the document to be encoded from the framework.
4.Divide the 64-bit plain file into 32 bit parts with two
portions as left side portion(LSP) and Right side portion(RSP)
5.from i=0 to LSP is XOR with p[i];
  Find F(LSP):
  F(LSP) is XOR with RSP;
6.Exchange LSP and RSP.
7.RSP is XOR with p[16].
8.LSP is XOR with p[17].
9.Atlast merge RSP and LSP.
OUTPUT: Encryption Time
```

Table 3 shows Blowfish technique execution time based on key size (Blowfish-0.14 sec, 3.5MB)

TABLE 3. BLOWFISH TECHNIQUE EXECUTION TIME BASED ON KEY SIZE (BLOWFISH - 0.14 SEC ,3.5 MB)

S. No	Time	Size
1	0.29	2
2	0.28	2.2
3	0.26	2.3
4	0.24	2.4
5	0.23	2.6
6	0.2	2.8
7	0.19	3
8	0.17	3.2
9	0.15	3.3
10	0.14	3.5

B. Data Encryption Standard

It is one of the cryptographic algorithms. It provides security to the data without the spillage. It satisfies both the properties of block cipher [35]. One is the Avalanche effect which is a small change in plaintext results in good modification in the encrypted text. The other is completeness which means every part of encrypted text is based on multiple bits of plain text [36]. It depends on two central credits of cryptography: one is substitution and the other is transposition. Cipher Feedback utilizes the former cipher text that turns into contribution for the encryption calculation delivering pseudorandom yield [37]. Table 2 represents the pseudo code for Data Encryption Standard Algorithm.

TABLE 2. PSEUDO CODE FOR DATA ENCRYPTION STANDARD ALGORITHM

INPUT: File from the system
1.A 64-bit data file is given to method Early Permutation(EP).
2.Every step goes for the substitution and transposition process.
3.Early Permutation will be executed on the data file.
4.Then,EP generates 2 equivalent permuted portions called Left Text(LT) and Right Text(RT).
5.Then ,every LT value and RT value goes to a sixteen round process for encryption.
6.LT and RT are mixed and Last Permutation(LP) is executed on the mixed part.
7. Output of the task generates 64-bit plain-data.
OUTPUT: Encryption Time

Table 4 shows Data Encryption Standard execution time based on key size (DES-0.4 sec,3.5MB). The tool used to assess Blowfish algorithm and Data Encryption Standard is NetBeans 8.1 in Java Programming language. The language setup has an intel I5 processor with 8GB RAM. The framework used here is Windows 10 operating system.

C. *STATISTICAL ANALYSIS*

For statistical implementation the software tool used here is IBM SPSS V26.0. Statistical packages for social sciences are used for finding the statistical calculations such as mean, standard deviation and also the graphs. Dependent variables are time, security and Independent variables are keysize, plaintext, delegator. In SPSS, time values are prepared using iterating 10 times per each group and file sizes are taken differently for each iteration.

III. RESULTS

The outcomes are analyzed using the SPSS tool. For both proposed and existing algorithms 10 iterations were done with a sample size of 10-20 and for each iteration execution time was noted. Table 5 shows Group Statistics values of Data Encryption Standard (0.4 sec) and Blowfish algorithm (0.14 sec) and Std Error Mean for Blowfish is .01733 and Data Encryption Standard is .03005.

TABLE 4. Data Encryption Standard execution time based on keysize (DES - 0.4 sec, 3.5MB)

S. No	Time	Size
1	0.15	2
2	0.16	2.2
3	0.2	2.3
4	0.22	2.4
5	0.27	2.6
6	0.30	2.8
7	0.35	3
8	0.37	3.2
9	0.39	3.3
10	0.4	3.5

TABLE 5. Shows Group Statistics values of Data Encryption Standard (0.4 sec) and Blowfish algorithm (0.13 sec) and Std Error Mean for Blowfish is .01733 and Data Encryption Standard is .0305

	Algorithm	N	Mean	Std Deviation	Std.Error Mean
Time	Blowfish	10	.2140	.05481	.01733
	DES	10	.2810	.09504	.03005
Size	Blowfish	10	2.730	.5100	.16128
	DES	10	2.730	.5100	.16128

Table 6 represents the Independent sample test result that is applied for fixing confidence interval as 95% and level of significance as 0.05 of Blowfish and Data encryption standard. Table 7 represents the Independent sample test applied for sample T-Test result with 95% confidence interval of Blowfish algorithm has lower = -1.773 and upper = 0.67.A bar graph that is plotted by algorithm on X-axis and Time, Size on Y-axis shown in Fig. 1. From the graph it is clear that Blowfish Algorithm has less encryption time compared to the Data Encryption Standard. Also the Error bar shows less rate for Blowfish Algorithm compared to Data Encryption Standard.

TABLE 6 The Independent sample test result is applied for fixing confidence interval as 95% and level of significance as 0.05 of Blowfish and Data encryption standard .

		F	**Sig**	**t**	**df**	**sig(2-tailed)**	**Mean Difference**	**Std Error Difference**	**lower**	**upper**
Time	Equal Variances Assumed	5.114	.036	-1.93	18	.012	-.0670	.03469	-.1398	.005
	Equal variances not assumed			-1.93	14.39	.115	-.0670	.03469	-.1412	.007
Size	Equal variances assumed	.00	1.00	.00	18	1.00	.-00	.2280	-.4791	.479
	Equal variances not assumed			.00	18.00	1.00	.00	.2280	-.4791	.479

TABLE 7. Independent sample test is applied for sample T-Test result with 95% confidence interval of Blowfish algorithm has lower = -1.773 and upper = 0.67.

		Standardizer	**Point estimate**	**Lower**	**Upper**
Time	Cohen's d	.07758	-.864	-1.773	0.67
	Hedges correction	.08101	-.827	-1.698	0.65
	Glass's delta	.09504	-.705	-1.621	.245
Size	Cohen's d	.51001	.000	-.877	.877
	Hedges correction	.53257	.000	-.839	.839
	Glass's delta	.51001	.000	-.877	.877

IV. DISCUSSION

In this finding, the Blowfish algorithm generates less error rate and with less processing time (0.14 sec) compared to the Data Encryption Standard (p = 0.012, Independent sample t-test). These techniques are implemented using Java Programming language and outcomes have been analyzed by IBM SPSS V26.0 tool.To support this research, it offers security to information passed on at the product level, yet additionally at the equipment level, utilizing changed blowfish. It yields minimal latency, greater speed [31]. To increase the complexity of the method, this paper proposes adding numerous XOR operations in the f-function utilising filtering and striding techniques. Using average pooling, new key generation techniques are implemented [38]. This study focuses on RSA and Blowfish cryptographic algorithms based on educational data. Researchers enhanced the extended version of Blowfish [31]. This study used a symmetric key called 64-bit blowfish for picture encryption and decryption. Also employs a 448-byte variable key that is more dependable [39]. The goal of the study is to access the Blowfish method using various metrics such as quality of encryption, connection, key affectability and document size [40]. The factors affecting the Encryption are filename, filetype and file size [41].

Our organization is enthusiastic about top notch proof based exploration and has milestones in different fields. Here trust this investigation and add to this rich heritage. Information assurance is exceptionally intense and it has been hard for private enterprises to get the information from attacks. Using different cryptographic algorithms can provide security to them [37]. The limitation in the study is that the data protection is technologically neutral since it lacks definitions. However it is hard to implement. Information protection is impartial, it applies equally to a firm or to a multinational corporation. Although data operations are global, data security is remote. In future work, add the concept of Information replica. It is a type of data compression that eliminates redundant copies of the same data while also increasing the security of the data on the cloud. For information replicas take file size, file name and file type into account, so that space and money can be saved.

V. CONCLUSION

In this finding, the outcome shows that our proposed Blowfish Algorithm along with Novel Data Authentication distributes the data without any loss of information and cipher attacks, with less execution time (0.14 sec) compared to Data Encryption Standard.

REFERENCES

[1] G. Singh and M. Garg, "Enhanced Cloud Security using Hybrid Mechanism of RSA, AES and Blowfish Data Encryption with Secure OTP," *INTERNATIONAL JOURNAL OF COMPUTERS &*

TECHNOLOGY, vol. 18. pp. 7364–7380, 2018. doi: 10.24297/ijct.v18i0.7898.

[2] R. R. Corpuz, B. D. Gerardo, and R. P. Medina, “Using a Modified Approach of Blowfish Algorithm for Data Security in Cloud Computing,” *Proceedings of the 6th International Conference on Information Technology: IoT and Smart City - ICIT 2018*. 2018. doi: 10.1145/3301551.3301597.

[3] E. Dinesh and S. M. Ramesh, “Security Aware Data Transaction Using Optimized Blowfish Algorithm in Cloud Environment,” *Journal of Circuits, Systems and Computers*, vol. 30, no. 01. p. 2150004, 2021. doi: 10.1142/s0218126621500043.

[4] T. Hidayat, “ENCRYPTION SECURITY SHARING DATA CLOUD COMPUTING BY USING AES ALGORITHM: A SYSTEMATIC REVIEW,” *TEKNOKOM*, vol. 2, no. 2. pp. 11–16, 2019. doi: 10.31943/teknokom.v2i2.41.

[5] Z. Kasiran, H. F. Ali, and N. M. Noor, “Time performance analysis of advanced encryption standard and data encryption standard in data security transaction,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 2. p. 988, 2019. doi: 10.11591/ijeecs.v16.i2.pp988-994.

[6] D. A. Hema, A. Hema, and C. Dhanya, “A Survey on Cryptographic Algorithms for Secured Communication,” *Bonfring International Journal of Software Engineering and Soft Computing*, vol. 6, no. 1. pp. 01–04, 2016. doi: 10.9756/bijsesc.7123.

[7] S. S. and S. S., “Enhancing Security Issues in IoT based Smart Retail using Blowfish Algorithm,” *International Journal of Computer Applications*, vol. 171, no. 3. pp. 39–43, 2017. doi: 10.5120/ijca2017915006.

[8] E. Irick, “Development of a Model for Repurposing: A Case Study of TRAID.” 2016. doi: 10.31274/itaa_proceedings-180814-1383.

[9] S. Mudepalli, V. Srinivasa Rao, and R. Kiran Kumar, “An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing,” *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*. 2017. doi: 10.1109/iccons.2017.8250724.

[10] V. Krishnasamy and S. Venkatachalam, “An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm,” *Materials Today: Proceedings*. 2021. doi: 10.1016/j.matpr.2021.04.303.

[11] A. R. Wan, “A Robust Cloud Security Architecture based on Distributed Servers, User Authentication, and AES, Blowfish Encryption Techniques,” *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. SP3. pp. 1293–1300, 2020. doi: 10.5373/jardcs/v12sp3/20201378.

[12] “A Novel Encryption Algorithm by Fusion of Modified Blowfish Algorithm and Fermat’s Little Theorem for Data Security,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 4. pp. 1188–1192, 2020. doi: 10.35940/ijitee.c8684.029420.

[13] S. A. Salman, “New Method For Encryption Using Mixing Advanced Encryption Standard And Blowfish Algorithms,” المجلة العراقية لتكنولوجيا المعلومات. p. 33, 2018. doi: 10.34279/0923-008-002-007.

[14] S. Gheena and D. Ezhilarasan, “Syringic acid triggers reactive oxygen species-mediated cytotoxicity in HepG2 cells,” *Hum. Exp. Toxicol.*, vol. 38, no. 6, pp. 694–702, Jun. 2019.

[15] P. Neelakantan, D. Grotra, and S. Sharma, “Retreatability of 2 mineral trioxide aggregate-based root canal sealers: a cone-beam computed tomography analysis,” *J. Endod.*, vol. 39, no. 7, pp. 893–896, Jul. 2013.

[16] M. C. Putchala, P. Ramani, H. J. Sherlin, P. Premkumar, and A. Natesan, “Ascorbic acid and its pro-oxidant activity as a therapy for tumours of oral cavity -- a systematic review,” *Arch. Oral Biol.*, vol. 58, no. 6, pp. 563–574, Jun. 2013.

[17] P. U. A. Wahab, M. Madhulaxmi, P. Senthilnathan, M. R. Muthusekhar, Y. Vohra, and R. P. Abhinav, “Scalpel Versus Diathermy in Wound Healing After Mucosal Incisions: A Split-Mouth Study,” *J. Oral Maxillofac. Surg.*, vol. 76, no. 6, pp. 1160–1164, Jun. 2018.

[18] S. I. DeSouza, M. R. Rashmi, A. P. Vasanthi, S. M. Joseph, and R. Rodrigues, “Mobile phones: the next step towards healthcare delivery in rural India?,” *PLoS One*, vol. 9, no. 8, p. e104895, Aug. 2014.

[19] D. Sajan, K. Udaya Lakshmi, Y. Erdogdu, and I. H. Joe, “Molecular structure and vibrational spectra of 2,6-bis(benzylidene)cyclohexanone: a density functional theoretical study,” *Spectrochim. Acta A Mol. Biomol. Spectrosc.*, vol. 78, no. 1, pp. 113–121, Jan. 2011.

[20] A. K. Danda, “Comparison of a single noncompression miniplate versus 2 noncompression miniplates in the treatment of mandibular angle fractures: a prospective, randomized clinical trial,” *J. Oral Maxillofac. Surg.*, vol. 68, no. 7, pp. 1565–1567, Jul. 2010.

[21] A. K. Danda, M. R. Muthusekhar, V. Narayanan, M. F. Baig, and A. Siddareddi, “Open versus closed treatment of unilateral subcondylar and condylar neck fractures: a prospective, randomized clinical study,” *J. Oral Maxillofac. Surg.*, vol. 68, no. 6, pp. 1238–1241, Jun. 2010.

[22] R. Robert, C. Justin Raj, S. Krishnan, and S. Jerome Das, “Growth, theoretical and optical studies on potassium dihydrogen phosphate (KDP) single crystals by modified Sankaranarayanan–Ramasamy (mSR) method,” *Physica B Condens. Matter*, vol. 405, no. 1, pp. 20–24, Jan. 2010.

[23] M. S. Kumar, G. Vamsi, R. Sripriya, and P. K. Sehgal, “Expression of matrix metalloproteinases (MMP-8 and -9) in chronic periodontitis patients with and without diabetes mellitus,” *J. Periodontol.*, vol. 77, no. 11, pp. 1803–1808, Nov. 2006.

[24] A. S. Felicita, S. Chandrasekar, and K. K. Shanthasundari, “Determination of craniofacial relation among the subethnic Indian population: a modified approach - (Sagittal relation),” *Indian J. Dent. Res.*, vol. 23, no. 3, pp. 305–312, May 2012.

[25] R. A. Azeem and N. M. Sureshbabu, “Clinical performance of direct versus indirect composite restorations in posterior teeth: A systematic review,” *J. Conserv. Dent.*, vol. 21, no. 1, pp. 2–9, Jan. 2018.

[26] V. S. Devi and B. K. Gnanavel, “Properties of concrete manufactured using steel slag,” *Procedia Eng.*, vol. 97, pp. 95–104, 2014.

[27] P. Neelakantan, C. Subbarao, C. V. Subbarao, G. De-Deus, and M. Zehnder, “The impact of root dentine conditioning on sealing ability and push-out bond strength of an epoxy resin root canal sealer,” *Int. Endod. J.*, vol. 44, no. 6, pp. 491–498, Jun. 2011.

[28] V. Krishnan and T. Lakshmi, “Bioglass: A novel biocompatible innovation,” *J. Adv. Pharm. Technol. Res.*, vol. 4, no. 2, pp. 78–83, Apr. 2013.

[29] A. Mootha, S. Malaiappan, N. D. Jayakumar, S. S. Varghese, and J. Toby Thomas, “The Effect of Periodontitis on Expression of Interleukin-21: A Systematic Review,” *Int. J. Inflam.*, vol. 2016, p. 3507503, Feb. 2016.

[30] T. Lakshmi, V. Krishnan, R. Rajendran, and N. Madhusudhanan, “Azadirachta indica: A herbal panacea in dentistry - An update,” *Pharmacogn. Rev.*, vol. 9, no. 17, pp. 41–44, Jan. 2015.

[31] M. S. Radhakrishnan, “Securing Distributed Database Using RSA and Blowfish Algorithm,” *International Conference On Contemporary Researches in Engineering, Science, Management & Arts, 2020*. 2020. doi: 10.9756/bp2020.1002/07.

[32] Salma, Salma, R. F. Olanrewaju, K. Abdullah, Rusmala, and H. Darwis, “Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms,” *2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT)*. 2018. doi: 10.1109/eiconcit.2018.8878629.

[33] M. S. M., “Multi Cloud Secure Data Sharing Using Encryption and Decryption Algorithms,” *International Conference On Contemporary Researches in Engineering, Science, Management & Arts, 2020*. 2020. doi: 10.9756/bp2020.1002/09.

[34] P. P., S. S., S. M., and P. Mithari, “Hiding Data into Reserve Space before Image Encryption using Blowfish Algorithm,” *International Journal of Computer Applications*, vol. 140, no. 10. pp. 34–38, 2016. doi: 10.5120/ijca2016909474.

[35] Simran *et al.*, "Synthesis of 64-Bit Triple Data Encryption Standard Algorithm using VHDL," *International Journal of Trend in Scientific Research and Development*, vol. -2, no. -4. pp. 775–778, 2018. doi: 10.31142/ijtsrd14159.

[36] D. Commey, S. Griffith, and J. Dzisi, "Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage," *International Journal of Computer Applications*, vol. 177, no. 40. pp. 17–22, 2020. doi: 10.5120/ijca2020919897.

[37] M. A.Usha, M. A. Usha, Scholar, Department of Computer Science, Govt. Arts College, and – D., "Performance Study of Key Developer Data Encryption and Decryption Algorithm (KDDEDA) with AES, DES and BLOWFISH," *International Journal Of Engineering And Computer Science*. 2016. doi: 10.18535/ijecs/v5i12.62.

[38] R. V. Amorado, "Modified f – Function and Key Generation for Data Encryption Standard Algorithm based on Filtering and Striding Technique," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 01-Special. pp. 293–300, 2020. doi: 10.5373/jardcs/v12sp1/20201075.

[39] P. Thakur, A. Rana, and arni university, "A Symmetrical key Cryptography Analysis using Blowfish Algorithm," *International Journal of Engineering Research and*, vol. V5, no. 07. 2016. doi: 10.17577/ijertv5is070276.

[40] V. Poonia and N. S. Yadav, "Analysis of modified Blowfish algorithm in different cases with various parameters," *2015 International Conference on Advanced Computing and Communication Systems*. 2015. doi: 10.1109/icaccs.2015.7324114.

[41] M. Vekariya, "Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms," *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND SCIENCES*, vol. 1, no. 1. p. 1, 2015. doi: 10.26472/ijces.v1i1.20.