A Comparative Study of Twofish, Blowfish, and Advanced Encryption Standard for Secured Data Transmission

Article *in* International Journal of Advanced Computer Science and Applications · January 2023

DOI: 10.14569/IJACSA.2023.0140344

CITATIONS
5

READS
64

2 authors:

Kwame Assa-Agyei
Nottingham Trent University
10 PUBLICATIONS **13** CITATIONS
SEE PROFILE

Funminiyi Olajide
University of Westminster
48 PUBLICATIONS **191** CITATIONS
SEE PROFILE

A Comparative Study of Twofish, Blowfish, and Advanced Encryption Standard for Secured Data Transmission

Kwame Assa-Agyei, Funminiyi Olajide
Department of Computer Science, Nottingham Trent University, Nottingham, United Kingdom

***Abstract*—Now-a-days, network security is becoming an increasingly significant and demanding research area of interest. Threats and attacks on information and Internet security are getting increasingly difficult to detect. As a result, encryption has emerged as a solution and now plays a critical role in information security systems. Many techniques are required to safeguard shared data. In this work, the encryption, decryption times, and throughput (speed) of the three most commonly used block cipher algorithms: Twofish, Blowfish, and AES were investigated using different file types. Comparison of symmetric encryption techniques of experiments on these types of algorithms uses a lot of computer resources including CPU time, memory, and battery power. Previous research has yielded diverse results in terms of time complexity, speed, space complexity, power consumption, and security. However, this research evaluated the effectiveness of each algorithm based on the following parameters: process time and speed. An application was developed for data simulation to test different file formats and for the encryption process and speed using Python 3.10.**

***Keywords*—Cryptography; twofish; blowfish; advanced encryption standard; throughput; data encryption; decryption**

I. INTRODUCTION

Due to the increasing number of incidents in which personal data between two parties is taken by intruders, it is critical to protect data communicated over the Internet nowadays[1]. People spend so much time connected to a network that network security has become an extremely important part of data communication. These are vulnerable to security attacks such as unauthorized access to a file or alterations to its contents. One of the main reasons invaders succeed is that most of the information obtained from a system is in a form that can be read and comprehended. The solution to this dilemma is to utilize Cryptography. This is the art and science of securing information from unwanted individuals by changing it into an indiscernible form to its attackers while it is stored and transported [2]. There are numerous encryption methods that are widely available and utilized in information security. They are classified as Symmetric (private) or Asymmetric (public) Key Encryption. Only one key is needed to encrypt and decrypt data in symmetric keys encryption or secret key encryption. Asymmetric keys employ two keys: private and public keys. The public key is used to encrypt data, while the private key is used to decrypt it (e.g. RSA and ECC) [3]. A block cipher algorithm is a symmetric key cryptosystem whose security is based on sophisticated non-linear transformations and whose encryption speed is quite fast. As a result, the block cipher algorithm has evolved into a vital encryption technique that is widely utilized in applications such as secure data transfer, storage encryption, digital signing, and entity certification [4]. The primary purpose of the security mechanism is to give message privacy while also ensuring data confidentiality, integrity, and non-repetition. The primary function of network security is to enable efficient data authentication and authorization through the use of cryptographic algorithms [5]. A cryptographic algorithm is typically computationally heavy and thereby, consumes a lot of computing power such as CPU time, memory usage, and power consumption [6].

Previous research has revealed inconsistencies in the efficacy of various encryption methods. The current work analyzed symmetric (AES, Twofish, and Blowfish) cryptographic algorithms using multiple file types such as binary, text, and image files with a unique key bit size of 128. These encryption methods were compared based on three different parameters: encryption time, decryption time, and throughput. The effectiveness of each technique is demonstrated using simulation data. This study addresses the following research questions.

RQ 1: What is the performance difference between the various algorithms using a constant key bit size of 128?

RQ2: Which block cipher technique works better in the context of process time and throughput using different file types? Hence, the current study makes the following key contributions.

1) To perform an extensive evaluation of the encryption, decryption times, and speed using a unique key bit size of 128.

2) To analyze the performance using different file types.

3) To perform an extensive analysis of the performance of selected algorithms, namely: AES (Rijndael), Twofish, and Blowfish

The rest of the paper is organized as follows: Section II presents the related work. The experimental analysis and setup is presented in Section III. Section IV and V present the performance results and discussion of this research. Finally, the conclusion is drawn in Section VI.

II. RELATED WORK

In recent years, several surveys based on various cryptographic techniques, such as the Blowfish, Twofish, and

AES algorithms, have been published. Various researchers discuss network security and cryptography challenges. This research explains and analyses earlier work in the field of data encryption to provide a broader perspective on the performance of the encryption methods.

Nema and Rizvi [7] conducted a critical analysis of various Symmetric Key Cryptographic algorithms. The objective is to identify the strengths and weaknesses of cryptographic algorithms. During the analysis, the research work observed that Blowfish was the best among all in terms of Security, Flexibility, Memory usage, and Encryption performance. Tyagi and Ganpati [8] evaluated the performance of Symmetric Key Encryption Algorithms to have a deeper understanding of the cryptography process and to perform a comparative analysis of symmetric encryption algorithms of cryptography. Blowfish algorithm runs faster than other popular symmetric key encryption algorithms: DES, 3DES, and AES. It also concluded that Blowfish gives better performance than DES, 3DES, and AES in terms of encryption time, decryption time, and throughput. 3DES has the least performance among all mentioned algorithms. The authors in [9] analysed an approach to identifying cryptographic algorithms from the cipher text. The focus of the study is to identify the performance of the cryptographic algorithm on cipher text only. The unique research work concluded that the identification rate can obtain around 90% if keys are the same for training and testing cipher texts. When they use different keys for training and testing cipher texts, it identifies AES from any one of the other four cryptographic algorithms with a high identification rate in one-to-one identification. A study conducted to assess the performance of encryption algorithms based on execution time, memory required for implementation, and throughput across two different operating systems. Based on the simulation results, AES and Salsa20 are preferable to Blowfish for plain text data encryption [6]. Singh et al., [10] presented a fair comparison between the most common four encryption algorithms namely; AES, DES, 3DES, and Blowfish in terms of security and power consumption. The simulation results showed that AES had a better performance than other common algorithms. Singh and Supriya [11] reviewed in-depth the well-known encryption methods such as RSA, DES, 3DES, and AES. They added that a variety of encryption techniques are available and that the advantages and disadvantages of each algorithm will determine which method is optimal for encrypting plain text. Each method is effective for real-time encryption. Each technique is distinctive in its own way, may be appropriate for various purposes, and has advantages and disadvantages of its own. The AES algorithm has been shown to be the most effective in terms of speed, time, throughput, and the avalanche effect, according to studies and a literature review. Ramesh and Suruliandi [12] evaluated the efficacy of some few particular symmetric algorithms in 2013. The experimental findings and input text file size led to the conclusion that the Blowfish method generates higher throughput while requiring less execution time and memory. In comparison to AES and DES, B1owfish performed around four times faster. Comparing Blowfish to AES and DES, memory usage is lower. Since AES required more computing resources than other algorithms, its performance results were subpar. Blowfish is not only the quickest encryption algorithm, but it also offers excellent security because of its large key size, making it suitable for usage in a wide range of applications, including packet encryption, random bit generation, internet-based security, and many more. Gautam et al., [13] conducted an experiment on cryptographic algorithms to analyze their performance and usage. The outcomes of the research on AES and TWOFISH are regarded as the two top candidates for achieving the aims of the study focus. These two outperform the other encryption methods in terms of speed, entropy, and optimal encoding, however, AES still has an advantage over TWOFISH due to its higher efficiency. The authors in [14] evaluated the performance of DES and Blowfish using different memory sizes. Both algorithms have high security to resist differential cryptanalysis and linear cryptanalysis attacks. They evaluated encryption function speed based on different memory sizes. The experimental results showed Blowfish is much faster than DES but as the speed increase for Blowfish, it is slower compared to DES. This was because of the needs to have more memory for sub-key and S boxes initialization. Kuma and Karthikeyan [15] conducted a comparison study on the effectiveness of the Blowfish and Rejindael (AES) algorithms for the chosen cryptographic algorithms in terms of energy consumption, changing data types like text or documents and images, power consumption, changing packet size, and changing key size. The simulation findings revealed that Blowfish surpasses AES in almost all of the test scenarios. The study found that while AES is better for image encryption, blowfish is better for text-based encryption. It is also shown that performance changes when the AES algorithm's key size is altered. Overall, the study found that AES can be used in circumstances needing a high level of security. Blowfish, however, is a performance-wise viable option. Suresh and Neema [16] explored hardware implementation of Blowfish algorithm for the secure data transmission in Internet of Things. It concluded that of all the cryptographic algorithms, the Blowfish algorithm is the best in terms of execution time, memory usage, throughput, power consumption, and security, and thus, well suited for IoT. The authors in [17] analysed the parameters of various cryptographic techniques, including AES and Blowfish, for performance, including encryption speed, CPU usage over time, and battery consumption. The outcomes showed that in terms of processing speed and throughput, the Blowfish approach performed better than the AES algorithm. The algorithm has a higher throughput while running more quickly and with less energy. According to the study, blowfish is the best option. AES, 3DES, Blowfish, and Twofish were the focus of an empirical investigation by Dibas and Sabri. The outcome demonstrated that, in terms of execution time, AES is the most effective encryption and decryption algorithm. In terms of encryption and decryption, Blowfish performed far better than 3DES. The findings obtained by Twofish were the worst. The authors found that, in terms of memory usage for encryption, AES and 3DES used less memory whereas Blowfish and Twofish used more memory and had the largest ciphertext sizes [18]. In 2020, Gosh conducted a side-by-side comparison of the three algorithms AES, Blowfish, and Twofish while taking into account various factors like speed and computation time. Conclusion: In terms of the evaluated

evaluation measures, such as encryption time, decryption time, and throughput, Twofish clearly outperformed AES and Blowfish [19]. Raigoza and Jituri [20] evaluated the performance of symmetric encryption algorithms. The aim of this paper is to assess and contrast the performance of the Blowfish algorithm and the widely used Advanced Encryption Standard (AES). The AES algorithm outperformed Blowfish in terms of speed, with a difference of around 200 to 300 milliseconds. And, when the data size was altered, there were minor changes between the methods evaluated, such that the encrypted data for the AES and Blowfish algorithms tended to be roughly the same length. When the authors changed the ASCII value range, both the AES and the Blowfish algorithms increased overall execution time as the ASCII value increased, but the regression line slope for the Blowfish was more than the AES. Given the same rising ASCII values, the encrypted data from the Blowfish algorithm tended to be greater in size than the AES-encrypted data. The authors in [21] conducted an experiment to evaluate the effectiveness of the most widely used symmetric algorithms in terms of Security, Architecture, Limitations, and Efficiency and to draw attention to the shortcomings of various algorithms. AES was discovered to be the best algorithm in terms of security, efficiency, and architecture. The authors in [22] examined AES and Twofish encryption schemes. The simulation's findings were as follows: (1) for text encryption, AES is faster than Twofish, but as RAM is increased, Twofish overtakes AES. (2) AES is faster for image encryption, although Twofish performs equally well with more RAM. (3) Twofish works better for sound encryption, and its speed increases even more with more RAM. The authors in [23] evaluated the various encryption methods for secure data transmission. The study came to the conclusion that Blowfish outperformed AES, DES, and 3DES in terms of encryption and decryption times, power use, memory utilisation, latency, jitter, and security level. The authors in [24] investigated performance of selected security algorithms in cloud computing to evaluate and contrast the effectiveness of AES (Rijndael), Blowfish, and RSA. Result of the simulated outcomes, indicated that Blowfish performed better than the AES and RSA algorithms. According to Yegireddi and Kumar [25] conducted a survey to assess the efficiency of well-known conventional encryption techniques. It concluded that AES and Blowfish are the only algorithms that give speed and security due to their variable key.

III. Experimental Analysis

We have implemented the various symmetric encryptions in Python. Our performance evaluation is based on the implementation of three symmetric algorithms AES, Twofish and blowfish for encryption and decryption, and throughput. The following criteria were used: a) encryption and decryption time; b) throughput; and c) 128 key bit size for AES, Twofish, and Blowfish. To show the outcomes for the conclusion, the values for each criterion were logged and graphically plotted. The simulation was run on a laptop with an Intel® CoreTM i5-10210U CPU running at 2.40 GHz and 16 GB of RAM. Version 21H2 of Windows 11 Pro for Workstations was used. A key size of 128 bits was utilised as the benchmark in this experiment to acquire trustworthy values for evaluating the efficiency of AES, Blowfish, and Twofish cryptographic algorithms. The experiment was run three times and the mean execution time was recorded. The three block-cipher methods—AES, Blowfish, and Twofish—are also listed in Table I as a summary.

TABLE I. Key and Block Size

Factors	AES	Blowfish	Twofish
Key sizes	128	128	128
Block size	128 bits	64 bits	128 bits

IV. Performance Evaluation

A. Process Time (Encryption and Decryption Time)

Tables II to VII show the comparison of results. It is worth noting that AES-128 key bit size has the quickest encryption and decryption time on average.

TABLE II. AES – Encryption (128 Key Bit)

File format	File size (in kb)	MEAN
file_example_TXT	9	0.037459
file-example_PDF_1MB	1,018	0.368214
file_example_MP3_5MG	5,166	1.182518
file_example_MP4_1280_10MG	9,610	2.218504
file-sample_1MB_DOCX	1,003	0.247889
file_example_XLS_5000	657	0.171259
file_example_PPT_250kB	243	0.105667
file_example_JPG_2500kB	2,446	0.569065

TABLE III. Blowfish – Encryption (128 Key Bit)

File format	File size (in kb)	MEAN
file_example_TXT	9	0.010809
file-example_PDF_1MB	1,018	0.304263
file_example_MP3_5MG	5,166	1.436277
file_example_MP4_1280_10MG	9,610	2.874504
file-sample_1MB_DOCX	1,003	0.306568
file_example_XLS_5000	657	0.218169
file_example_PPT_250kB	243	0.111124
file_example_JPG_2500kB	2,446	0.718191

TABLE IV. Twofish – Encryption (128 Key Bit)

File format	File size (in kb)	MEAN
file_example_TXT	9	0.25
file-example_PDF_1MB	1,018	26.34
file_example_MP3_5MG	5,166	131.50
file_example_MP4_1280_10MG	9,610	244.11
file-sample_1MB_DOCX	1,003	25.39
file_example_XLS_5000	657	16.59
file_example_PPT_250kB	243	6.20
file_example_JPG_2500kB	2,446	63.02

TABLE V. AES – DECRYPTION (128 KEY BIT)

File format	File size (in kb)	MEAN
file_example_TXT	9	0.01238
file-example_PDF_1MB	1,018	0.288262
file_example_MP3_5MG	5,166	1.213215
file_example_MP4_1280_10MG	9,610	2.238994
file-sample_1MB_DOCX	1,003	0.298465
file_example_XLS_5000	657	0.200942
file_example_PPT_250kB	243	0.076602
file_example_JPG_2500kB	2,446	0.615148

TABLE VI. BLOWFISH – DECRYPTION (128 KEY BIT)

File format	File size (in kb)	MEAN
file_example_TXT	9	0.016267
file-example_PDF_1MB	1,018	0.298124
file_example_MP3_5MG	5,166	1.504732
file_example_MP4_1280_10MG	9,610	2.703225
file-sample_1MB_DOCX	1,003	0.298391
file_example_XLS_5000	657	0.21287
file_example_PPT_250kB	243	0.092704
file_example_JPG_2500kB	2,446	0.735764

TABLE VII. TWOFISH – DECRYPTION (128 KEY BIT)

File format	File size (in kb)	MEAN
file_example_TXT	9	0.244043
file-example_PDF_1MB	1,018	25.60037
file_example_MP3_5MG	5,166	135.4913
file_example_MP4_1280_10MG	9,610	245.67
file-sample_1MB_DOCX	1,003	25.33303
file_example_XLS_5000	657	16.62755
file_example_PPT_250kB	243	6.150904
file_example_JPG_2500kB	2,446	62.01268

B. Throughput

The throughput of an encryption scheme defines the speed of encryption. The encryption scheme's throughput is calculated by dividing the total plaintext in bytes encrypted by the encryption time [14]. In this experiment, the throughput is derived from calculated as the total plaintext in Kilobytes encrypted/encryption time (KB/sec) divided by their mean time generated. AES has the highest throughput making it the fastest of the three followed by blowfish. The results are shown in Tables VIII to X.

TABLE VIII. AES THROUGHPUT IN KILOBYTES/SECONDS (128 KEY BIT)

File Name	File Size (in kb)	Encryption Throughput	Decryption Throughput
	KB	KB/Sec	KB/Sec
file_example_TXT	9	240.2626872	726.9789984
file_example_PDF_1MB	1,018	2764.696617	3531.50953
file_example_MP3_5MG	5,166	4368.64386	4258.10759
file_example_MP4_1280_10MG	9,610	4331.747881	4292.106187
file_example_1MB_DOCX	1,003	4046.165824	3360.528035
file_example_XLS_5000	657	3836.294735	3269.600183
file_example_PPT_250kB	243	2299.677288	3172.240934
file_example_JPG_2500kB	2,446	4298.278756	3976.278879

TABLE IX. BLOWFISH THROUGHPUT IN KILOBYTES/SECONDS 128 KEY BIT)

File Name	File Size (in kb)	Encryption Throughput	Decryption Throughput
		KB/Sec	KB/Sec
file_example_TXT	9	832.6394671	553.2673511
file_example_PDF_1MB	1,018	3345.789662	3414.686506
file_example_MP3_5MG	5,166	3596.799225	3433.169495
file_example_MP4_1280_10MG	9,610	3343.185468	3555.012994
file_example_1MB_DOCX	1,003	3271.704809	3361.361435
file_example_XLS_5000	657	3011.426921	3086.390755
file_example_PPT_250kB	243	2186.746337	2621.246117
file_example_JPG_2500kB	2,446	3405.779243	3324.435553

TABLE X. TWOFISH THROUGHPUT IN KILOBYTES/SECONDS (128 KEY BIT)

File Name	File Size (in kb)	Encryption Throughput	Decryption Throughput
		KB/Sec	KB/Sec
file_example_TXT	9	36	36.87874678
file_example_PDF_1MB	1,018	38.64844343	39.76505027
file_example_MP3_5MG	5,166	39.2851711	38.12790932
file_example_MP4_1280_10MG	9,610	39.36749826	39.11751537
file_example_1MB_DOCX	1,003	39.50374163	39.59257933
file_example_XLS_5000	657	39.60216998	39.51273639
file_example_PPT_250kB	243	39.19354839	39.506388
file_example_JPG_2500kB	2,446	38.81307521	39.44354606

V. DISCUSSION OF RESULTS

Tables I to IX show the encryption time, decryption time, and throughput. Performance analysis varies based on a particular file type, but on average, AES outperforms Blowfish and Twofish in terms of speed and process time. Furthermore, the figures in Fig. 1 and Fig. 2 are based on the average of total encryption/decryption and throughput of AES,

Blowfish, and Twofish. An overview of all the comparisons can be summarized into the following Table XI. The summary in Table XI is based on values from Fig. 1 and Fig. 2. AES-128 produced fast encryption, decryption times and speed than Blowfish and Twofish. The results show that Blowfish can match the encryption and decryption speeds of AES.

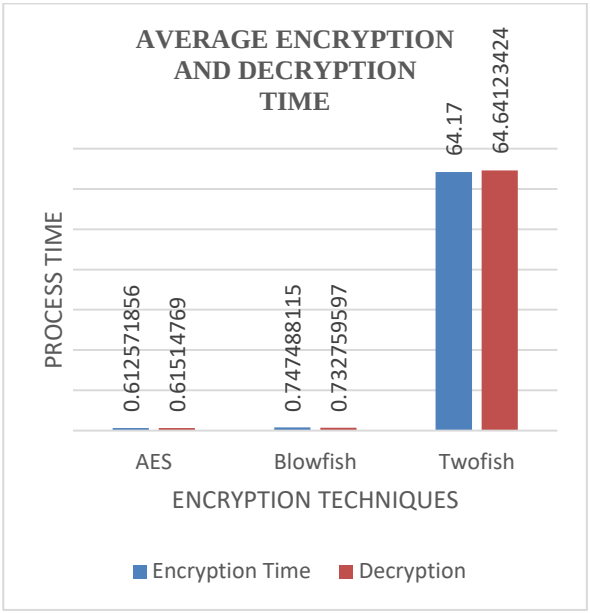

Fig. 1. Average process for AES, blowfish and twofish.

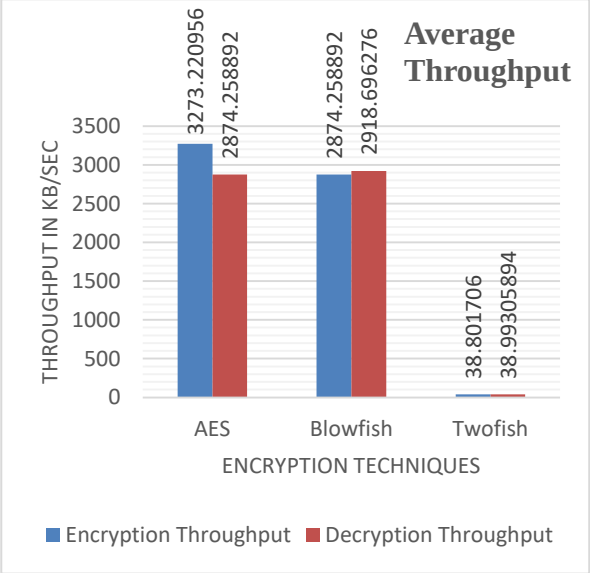

Fig. 2. Average throughput for AES, blowfish, and twofish.

TABLE XI. AES, BLOWFISH, AND TWOFISH AN OVERALL COMPARISON

Parameters	AES	Blowfish	Twofish
Key bit size	128	128	128
Encryption	Very fast	Fast	Too slow
Decryption	Very fast	Fast	Too slow
Throughput (Speed)	Very high	High	Low

VI. CONCLUSION

In today's rapidly expanding Internet and network applications, encryption algorithms play a critical role in ensuring information security. Based on a key bit size of 128 in this study, we evaluated three symmetric key encryption algorithms: AES, Twofish, and Blowfish. Based on the experimental results, the 128 key bit of AES algorithm has the shortest process time and runs quicker than Twofish and Blowfish. Overall results proved that the AES algorithm is more suitable for secure data transfer.

REFERENCES

[1] P. K. Ghosh, S. K. Ghosh, and L. M. Khan, "Current trend of bank selection criteria of retail customers in Bangladesh: An investigation," Glob. Bus. Financ. Rev., vol. 20, no. 2, pp. 27–34, 2015, doi: 10.17549/gbfr.2015.20.2.27.

[2] M. Panda, "Performance analysis of encryption algorithms for security," in International Conference on Signal Processing, Communication, Power and Embedded System, SCOPES 2016 - Proceedings, 2017, pp. 278–284, doi: 10.1109/SCOPES.2016.7955835.

[3] D. S. Abd Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms," Int. J. Netw. Secur., vol. 10, no. 3, pp. 213–219, 2010.

[4] B. Xing, D. D. Wang, Y. Yang, Z. Wei, J. Wu, and C. He, "Accelerating DES and AES Algorithms for a Heterogeneous Many-core Processor," Int. J. Parallel Program., vol. 49, no. 3, pp. 463–486, 2021, doi: 10.1007/s10766-021-00692-4.

[5] S. N. Karale, K. Pendke, and P. Dahiwale, "The survey of various techniques & algorithms for SMS security," ICIIECS 2015 - 2015 IEEE Int. Conf. Innov. Information, Embed. Commun. Syst., 2015, doi: 10.1109/ICIIECS.2015.7192943.

[6] M. Panda and A. Nag, "Plain Text Encryption Using AES, DES and SALSA20 by Java Based Bouncy Castle API on Windows and Linux," Proc. - 2015 2nd IEEE Int. Conf. Adv. Comput. Commun. Eng. ICACCE 2015, pp. 541–548, 2015, doi: 10.1109/ICACCE.2015.130.

[7] P. Nema and M. A. Rizvi, "Critical Analysis of Various Symmetric Key Cryptographic Algorithms," Int. J. Recent Innov. Trends Comput. Commun., vol. 3, no. 6, pp. 4301–4306, 2015.

[8] N. Tyagi and A. Ganpati, "Comparative Analysis of Symmetric Key Encryption Algorithms," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 6, pp. 94–99, 2014.

[9] C. Tan and Q. Ji, "An approach to identifying cryptographic algorithm from ciphertext," in Proceedings of 2016 8th IEEE International Conference on Communication Software and Networks, ICCSN 2016, 2016, pp. 19–23, doi: 10.1109/ICCSN.2016.7586649.

[10] G. Singh, A. Kumar, and K. S. Sandha, "A Study of New Trends in Blowfish Algorithm," Int. J. Eng. Res. Appl. www.ijera.com, vol. 1, no. 2, pp. 321–326, 2015, [Online]. Available: www.ijera.com.

[11] G. Singh and S. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," Int. J. Comput. Appl., vol. 67, no. 19, pp. 33–38, 2013, doi: 10.5120/11507-7224.

[12] A. Ramesh and A. Suruliandi, "Performance analysis of encryption algorithms for information security," Proc. IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT 2013, pp. 840–844, 2013, doi: 10.1109/ICCPCT.2013.6528957.

[13] S. Gautam, S. Singh, and H. Singh, "A Comparative Study and Analysis of Cryptographic Algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH," Int. J. Res. Electron. Comput. Eng., vol. 7, no. 1, 2019, [Online]. Available: https://www. researchgate.net/publication/ 334724160.

[14] T. Nie, C. Song, and X. Zhi, "Performance evaluation of DES and Blowfish algorithms," 2010 Int. Conf. Biomed. Eng. Comput. Sci. ICBECS 2010, pp. 16–19, 2010, doi: 10.1109/ICBECS.2010.5462398.

[15] M. Anand Kumar and S. Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms," Int. J. Comput. Netw. Inf. Secur., vol. 4, no. 2, pp. 22–28, 2012, doi: 10.5815/ijcnis.2012.02.04.

[16] M. Suresh and M. Neema, "Hardware Implementation of Blowfish Algorithm for the Secure Data Transmission in Internet of Things," Procedia Technol., vol. 25, no. Raerest, pp. 248–255, 2016, doi: 10.1016/j.protcy.2016.08.104.

[17] C. Haldankar and S. Kuwelkar, "Implementation of Aes and Blowfish Algorithm," Int. J. Res. Eng. Technol., vol. 03, no. 15, pp. 143–146, 2014, doi: 10.15623/ijret.2014.0315026.

[18] H. Dibas and K. E. Sabri, "A comprehensive performance empirical study of the symmetric algorithms:AES, 3DES, Blowfish and Twofish," 2021 Int. Conf. Inf. Technol. ICIT 2021 - Proc., pp. 344–349, 2021, doi: 10.1109/ICIT52682.2021.9491644.

[19] A. Ghosh, "Comparison of Encryption Algorithms : AES , Blowfish and Twofish for Security of Wireless Networks," Int. Res. J. Eng. Technol., no. June, pp. 4656–4659, 2020, doi: 10.13140/RG.2.2.31024.38401.

[20] J. Raigoza and K. Jituri, "Evaluating Performance of Symmetric Encryption Algorithms," Proc. - 2016 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2016, pp. 1378–1379, 2017, doi: 10.1109/CSCI.2016.0258.

[21] S. S. Ghosh, H. Parmar, P. Shah, and K. Samdani, "A Comprehensive Analysis between Popular Symmetric Encryption Algorithms," 1st Int. Conf. Data Sci. Anal. PuneCon 2018 - Proc., 2018, doi: 10.1109/PUNECON.2018.8745324.

[22] S. A. M. Rizvi, S. Z. Hussain, and N. Wadhwa, "Performance analysis of AES and Twofish encryption schemes," Proc. - 2011 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2011, pp. 76–79, 2011, doi: 10.1109/CSNT.2011.160.

[23] A. V. Mota, A. Sami, K. C. Shanmugam, Bharanidharan Yeo, and K. Krishnan, "Comparative Analysis of Different Techniques of Encryption for Secured Data Transmission," IEEE Int. Conf. Power, Control. Signals Instrum. Eng., vol. 54, no. 4, pp. 847–860, 2017.

[24] R. S. Cordova, R. L. R. Maata, A. S. Halibas, and R. Al-Azawi, "Comparative analysis on the performance of selected security algorithms in cloud computing," 2017 Int. Conf. Electr. Comput. Technol. Appl. ICECTA 2017, vol. 2018-Janua, pp. 1–4, 2017, doi: 10.1109/ICECTA.2017.8252030.

[25] R. Yegireddi and R. K. Kumar, "A survey on conventional encryption algorithms of Cryptography," Proc. 2016 Int. Conf. ICT Business, Ind. Gov. ICTBIG 2016, pp. 6–9, 2017, doi: 10.1109/ICTBIG.2016.7892684.