A comprehensive performance empirical study of the symmetric algorithms:AES, 3DES, Blowfish and Twofish

Hasan Dibas
King Abdullah II School of Information Technology
The University of Jordan
Amman, Jordan
hsn8181559@ju.edu.jo

Khair Eddin Sabri
King Abdullah II School of Information Technology
The University of Jordan
Amman, Jordan
k.sabri@ju.edu.jo

2021 International Conference on Information Technology (ICIT) | 978-1-6654-2870-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICIT52682.2021.9491644

***Abstract*— Developing software applications that provide services in all business fields such as finance, health, education, real estate and social media etc., must maintain various quality attributes, such as security, performance, availability, reliability, scalability, maintainability, usability and so on. If we talk about security for example, then we must take care of couple of properties like confidentiality, integrity, availability, non-repudiation and accountability. To achieve these targets there are different ways, one of them is using cryptographic mechanism. Cryptography has two basic types of algorithms, symmetric and asymmetric. Each of them provides encryption and decryption processes. In this paper, we conducted a performance evaluation between four of the symmetric algorithms AES, 3DES, Blowfish and Twofish. We evaluated the execution time, memory utilization and ciphertext size on the encryption and decryption processes. We performed the comparison against different files size by building a .NET application using C#. By analyzing the result, we noticed that AES has the lowest execution time in encryption and decryption processes, while Twofish has the highest execution time. In the encryption process, AES and 3DES consumes less memory than the blowfish and Twofish and they used very close amount of memory. While AES utilized less memory in the decryption. Finally, Blowfish and Twofish have the biggest ciphertext size.**

Keywords*— *symmetric algorithm, AES, 3DES, Blowfish, Twofish, Security

I. INTRODUCTION

Security is one of the main quality attributes that we have to take care of while we building any software application. The security is involved in all of the application life cycle. In the design phase, we prepare the threat modeling and design a secure application, while in the development phase we implement and apply the security principles to provide a secure and robust application. We assess the application security in the testing phase, finally in the deployment phase we secure the host, network and the application. There are a lot of countermeasures that should be considered to build a secure application like input validation, authentication, authorization, session management and cryptography etc. Beside the security, the performance is one of the most important quality attributes that attracts end-users. There are a lot of theoretical analysis conducted to evaluate the symmetric algorithms and behaviors, but it’s necessary to evaluate them in practical way especially there are many factors could affect the result such that the operating systems, compiler and environment specs etc.

The purpose of this paper is to conduct a comprehensive empirical study to understand the performance impact between four of the symmetric cryptography algorithms.

1. Triple Data Encryption Standard (3DES)
2. Advanced Encryption Standard (AES)
3. Blowfish
4. Twofish

We measured the execution time, memory utilization and the size of the ciphertext compared to the size of the original text for those algorithms. The experimental executed against different files size. The remaining of this paper is organized as the following: in section II, we review the related works. In section III, we discuss the testing methodology. The results and discussion of the experimental are presented in section IV. Finally, in section V, we summarize the conclusion.

II. BACKGROUND

A. Cryptography

Cryptography aims to maintain the data confidentiality and integrity. How to keep secrets information, secret, protect and prevent the data from unauthorized change [1]. Cryptography involves two main operations encryption and decryption. Encryption is the process of converting plaintext to ciphertext by performing some operations like substitution, transformations and permutations on the original text. Decryption is the process of restoring the plaintext from the ciphertext. There are two basic types of the encryption algorithms [2]

1. Symmetric Algorithms (secret key): the same key is used for encryption and decryption.
2. Asymmetric Algorithms (public key): use different keys, one for encryption and one for decryption.

The main strength factor of any encryption algorithm is the Key size. The longer key size provides high-level of the security. Fig. 1 represents the encryption algorithms types and techniques.

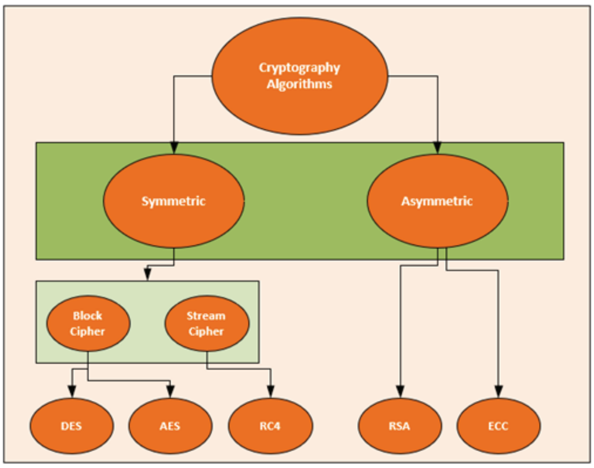


Figure 1. Encryption algorithms techniques

3DES: 3DES is the new version of DES algorithm. The key size in DES is 64 bits, 8 bits of them are used for parity check. Due to the availability of high-power computation, the DES become targeted to several kind of attacks like brute-force attack and cryptoanalysis which make it obsoleted and not secure anymore. 3DES is designed to solve the security issues in DES algorithm. 3DES is implemented by repeating the DES process three times with three different keys [3]. The block size is small in 3DES which could lead to a collision problem when we encrypt a big amount of data, especially if there is a chance to have two same ciphertext for different input. Then the attacker can apply XOR to get the plaintext. Therefore, it's not recommended by the US national institute to use the 3DES if block size exceeds 2^32 [4].

AES: in 2001, the National Institute of Standards and Technology (NIST) published the AES algorithm to overcome the security problems in 3DES. AES is a block cipher, it provides different key sizes 128, 192 and 256. It performs substitution and permutation operation number of rounds depends on the key size [5]. Table I shows the number of rounds per key size.

Table I. Number of rounds per key size

Key Size	*128*	*192*	*256*
Number of rounds	10	12	14

Blowfish: is one of the symmetric block cipher encryption algorithms that use feistel network structure, it is designed by Bruce Schneier in 1993. The block size in Blowfish is 64 bits, while the keys size ranges from 32 bits to 448 bits. The encryption function consists of 16 rounds [6].

Twofish: is considered as one of the symmetric block cipher algorithms that applied feistel structure. We can use it in smart cards due to its efficiency. It supports three key sizes 128,192 and 256 bits. The encryption and decryption process contains 16 rounds. Where the block size is 128 bits [7].

B. Literature Review

This section outlines the previous related works that discussed the various symmetric algorithm comparisons.

In [8], the authors provide a comparative analysis study between AES and RSA to explain that RSA has the ability to encrypt and decrypt the data more securely that AES.

In [9], the authors performed a performance comparison between the Tiny Encryption algorithm (TEA) and AES on an open-source android library called Cryptomator library. In [10], the authors provide a comprehensive study between symmetric (AES, DES, 3DES, Blowfish) and asymmetric (RSA, DSA, Diffie-Hellman and Elliptic Curve) algorithm by considering the algorithms speed and security.

In [11], a Java application is implemented to evaluate a performance comparison between symmetric (DES, AES) and asymmetric (RSA, ElGamal) algorithms using different file sizes. They covered multiple parameters such that encryption/ decryption time and key generation size.

In [12], the authors conducted a performance comparison between DES, 3DES and AES. They measured the encryption and decryption time, memory utilization and the throughput. The maximum used file size is 2MB. In [13], the authors investigated a hardware design that implements block cipher. They analyzed the power consumption for each of Blowfish, AES, IDEA and Rijndael.

In [14], a Java based application is developed to make a speed performance comparison between DES, AES and Blowfish using different data size using various cipher modes: Electronic Code Book (ECB), Cipher Feedback (CFB), Output Feedback (OFB) and Cipher Block Chaining (CBC). In [15], the authors analyzed the AES structure and design. They focused on resistance of AES against known attacks, performance and code compatibility on various environments and design simplicity, as well as the AES advantages against DES.

In [16], the authors presented a comparative analysis between AES and RC4. They used different block cipher mode on AES. The comparison considered the encryption, decryption time, CPU time, throughput and memory utilization. By using different key sizes and different data sizes.

In our research, we conducted a performance comparison between 3DES, AES, Blowfish and Twofish. We performed encryption and decryption process on different files sizes. We evaluated the execution time, memory utilization and ciphertext size. The comparison is implemented using C#.

III. EXPERIMENTAL TETSING METHODOLOGY

To conduct the performance comparison, we built a solution using C# under Microsoft Visual Studio Community 2019 IDE. For 3DES and AES, we used the cryptography library which is provided by Microsoft .NET framework [17]. For Blowfish and Twofish we used NetEncryptionLibrary which is provided by kellermansoftware [18]. The solution consists of four C# console applications as shown in Fig 2. Each of the console applications provides encryption and decryption services for the following symmetric cryptographic algorithms:

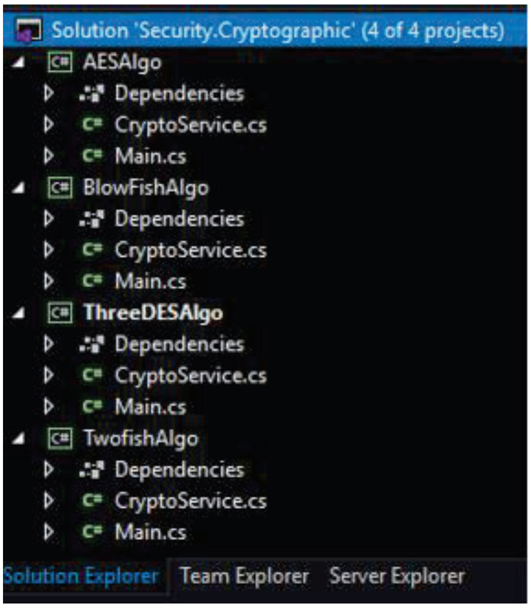
1. 3DES
2. AES

3. Blowfish
4. Twofish

Each console application contains two classes:

1. CryptoService.cs: provides the encryption and decryption operations.
2. Main.cs: is the entry point of the console application, which executes the encryption and decryption operations, log the execution time and capture the memory utilization.

We performed the encryption and decryption for each of the targeted algorithms five times. In each time, we captured the execution time and the memory utilization. Then we calculated the average of the results. The experimental is executed against different file sizes 1 KB, 100 KB, 1 MB, 10 MB and 100 MB.



Solution 'Security.Cryptographic' (4 of 4 projects)
- AESAlgo
  - Dependencies
  - CryptoService.cs
  - Main.cs
- BlowFishAlgo
  - Dependencies
  - CryptoService.cs
  - Main.cs
- ThreeDESAlgo
  - Dependencies
  - CryptoService.cs
  - Main.cs
- TwofishAlgo
  - Dependencies
  - CryptoService.cs
  - Main.cs

Figure 2. Testing project structure

We used cipher block chaining (CBC) mode in all algorithms. In Table II, we summarize the key and block size used in the experimental for all of 3DES, AES, Blowfish and Twofish.

Table II. Key and block size for all of 3DES, AES, Blowfish and Twofish

Factor	*3DES*	*AES*	*Blowfish*	*Twofish*
Key size	168 bits	256 bits	448 bits	256 bits
Block Size	64 bits	128 bits	64 bits	128 bits

All console applications experiments have been conducted on LENOVO Ideapad Y700 with Processor Intel(R) Core (TM) i7-6700HQ CPU @ 2.60GHz, 4 Core(s), 8 Logical Processor(s) and 32 GB RAM. The LENOVO is running Microsoft Windows 10 Enterprise LTSC.

IV. Results and Discussion

Cryptography is one of the security techniques that provide the integrity and confidentiality to our data. There are a lot of the cryptography algorithms in the market. Therefore, we have to be careful when we select any of them, and make sure that we choose the more efficient and secure algorithm. In this paper, we evaluate the execution time, memory utilization and ciphertext size for all of 3DES, AES, Blowfish and Twofish using CBC mode. We used those algorithms to perform encryption and decryption operations on different files size. We measured the execution time in millisecond (MS), and the memory utilization in Megabyte (MB).

A. Encryption

Reference to the result presented in Table III, and from encryption execution time point of view the most efficient cryptography algorithm is AES. The AES execution time is increased slightly when we encrypted bigger files, but it stays the more efficient with comparison to the other algorithms. For 3DES and Blowfish, we noticed that the file size 10MB is considered the threshold where the encryption execution time starts jumping to three times and above than the AES. Twofish shows the worst result and there is a big difference between its result and the others, especially when the file size exceeds 1MB.

Table III. Encryption time in MS

Algo/Size	1KB	100KB	1MB	10MB	100MB
AES	52.7	58.4	64.3	113.9	542.3
3DES	67.1	63.9	114.8	547.3	4734.1
Blowfish	159.2	165.6	194.2	398.9	2437.8
Twofish	176.1	270.8	614.0	3798.2	35174.0

Despite the good encryption performance for 3DES against the small files size, its execution time is increased drastically for the big files size as shown in Fig.3 The Y-axis represent the execution time in MS, while the X-axis represent the files size in MB.

To summarize, according to the encryption execution time results in Table III and Fig. 3, it appears that AES is considered the most efficient algorithm that we can use to perform encryption process, while Twofish is the worst. When the files size is less than 10MB, 3DES comes in the second level and Blowfish in the third, but when the file size exceed 10MB Blowfish gives a much better result than 3DES.

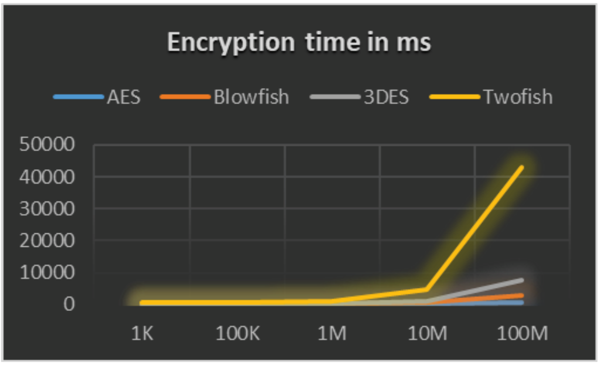


Figure 3. Encryption time in MS

Table IV illustrates the memory utilization result for the encryption processes. Reference to these results, we found that 3DES and AES consumed very close amount of memory, except that 3DES needs less amount of memory when the file size is greater than 10MB. Blowfish and Twofish give very closed results, and consume higher amount of memory than 3DES and AES.

Table IV. Encryption memory utilization in MB

Algo/Size	1KB	100KB	1MB	10MB	100MB
AES	6.88	7.8	10.62	71.38	840.6
3DES	7.28	7.78	12.92	83.72	674.9
Blowfish	8.74	9.1	16.24	118.02	1100
Twofish	8.78	12.86	17.38	107.52	1100

As shown in Fig. 4, the Blowfish and Twofish required double size of the memory than needed for 3DES when the file size 100 MB. In Fig. 4, the Y-axis represents the memory utilization in MB, while the X-axis represents the files size in MB.

General speaking, AES and 3DES required less amount of memory in the encryption process, while Blowfish and Twofish algorithms required a higher memory, especially in the large files.

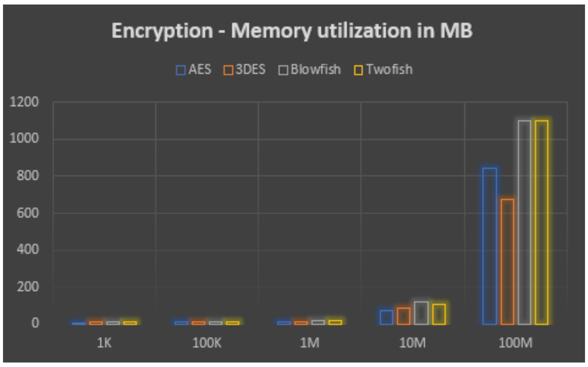


Figure 4. Encryption memory utilization in MB

B. *Decryption*

Table V presents the required execution time for the decryption process. It shows that AES is the most efficient. While Twofish has the worst result at all, its execution time starts jumping when the file size is 100 KB and above. As shown in Fig. 5, the execution time is significantly increased for 3DES and Blowfish when the file size exceeds 1 MB.

Table V. Decryption time in MS

Algo/Size	1KB	100KB	1MB	10MB	100MB
AES	2.2	3.0	7.9	58.2	549.2
3DES	12.1	15.3	49.9	315.3	2490.7
Blowfish	2.9	7.4	51.3	480.1	4833.9
Twofish	19.5	112.9	392.9	3755.1	35949. 3

3DES gives better execution time than Blowfish if the file size less than 100 KB, but when the file size is above 1 MB then Blowfish needs less time than 3DES. As a summary, the AES is the most efficient algorithm in both of the encryption and decryption. AES execution time is increased little bit against the big files size, but it remains very much less than the other algorithms. 3DES and Blowfish come between AES and Twofish. Finally, the Twofish needs more execution time in both encryption and deception.

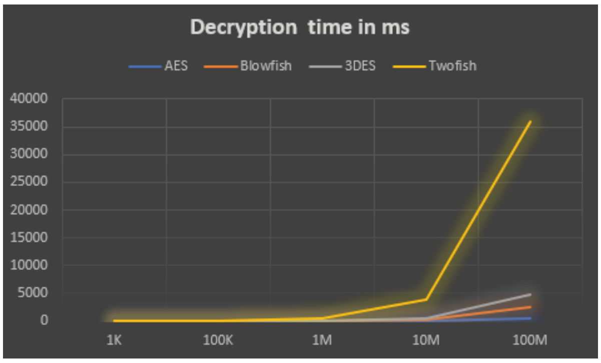


Figure 5. Decryption time in MS

Regarding the memory utilization in the decryption process, as shown in Table VI, AES requires less amount of memory. Then 3DES comes in the second level, Blowfish in the third and the Twofish in the last level. We can cluster 3DES and AES in one group since they have very close result, and Blowfish and Twofish in one group because also they have very similar results.

Table VI. Decryption memory utilization in MB

Algo/Size	1KB	100KB	1MB	10MB	100MB
AES	7	7.7	13.94	95.06	583.32
3DES	7.76	8.4	17.22	112.5	648.24
Blowfish	9.5	10.38	30.92	186.7	1053.8
Twofish	8.78	13.98	31.68	200.18	1240

Reference to Fig. 6, Blowfish and Twofish need the double size of memory with compare to AES when the file size exceeds 1 MB. Despite 3DES results are very close to AES in all files size, but AES memory utilization results stay the best in the decryption process. Basically, AES and 3DES give very similar results in both of encryption and decryption in memory consumption and much better than Blowfish and Twofish which they gained the higher memory consumption.

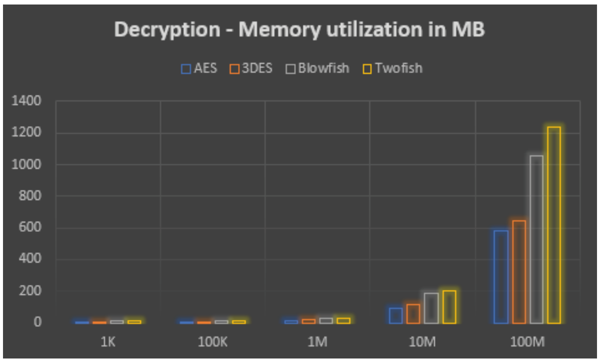


Figure 6. Decryption memory utilization in MB

C. *Encryption vs Decryption*

If we did a quick comparison between the encryption and decryption, we found that the encryption process required more execution time in most of the cases, while the decryption requires less time. Table VII contains the execution time for all encryption and decryption processes.

Table VII. encryption vs decryption execution time in MS

Algo/Size	1K	100K	1M	10M	100M
AES-Encryption	52.76	58.35	64.30	113.93	542.29
AES-Decryption	2.18	3.00	7.88	58.18	549.16
3DES-Encryption	67.12	63.92	114.78	547.33	4734.13
3DES-Decryption	2.89	7.42	51.33	480.12	4833.94
Blowfish-Encryption	159.19	165.63	194.21	398.89	2437.84
Blowfish-Decryption	12.12	15.25	49.99	315.29	2490.69
Twofish-Encryption	176.05	270.75	614.04	3798.2	35174.1
Twofish-Decryption	19.52	112.95	392.88	3755.1	35949.3

When we compared the utilized memory between the encryption and decryption, we can find a regular pattern. As shown in Table VIII, the utilized memory in the encryption process is less than the required amount of memory in the decryption process in all the cases, except when the file size exceeds 100 MB we noticed that 3DES, AES and Blowfish required more memory in the encryption process. In general, the utilized memory in both of encryption and decryption are very close, the different is very minor.

Table VIII. encryption vs decryption memory utilization in MB

Algo/Size	1K	100K	1M	10M	100M
AES-Encryption	6.88	7.8	10.62	71.38	840.6
AES-Decryption	7	7.7	13.94	95.06	583.32
3DES-Encryption	7.28	7.78	12.92	83.72	674.9
3DES-Decryption	7.76	8.4	17.22	112.5	648.24
Blowfish-Encryption	8.74	9.1	16.24	118.02	1100
Blowfish-Decryption	9.5	10.38	30.92	186.7	1053.8
Twofish-Encryption	8.78	12.86	17.38	107.52	1100
Twofish-Decryption	8.78	13.98	31.68	200.18	1240

D. *Ciphertext* size

We compared the encrypted files size against the original files, we noticed that the ciphertext size for AES and 3DES is very close to the original files size. To be accurate, the cipher size is increased by 10KB for each 10MB in the original file. For example, when the original file size is 100MB then the ciphertext is increased by 100 KB. But the situation in Blowfish and Twofish is different. We noticed that the ciphertext size is increased approximately by 3.3KB per each 10KB of the original size. For example, when the original file size is 100MB then the ciphertext reached to 133 MB and so on.

V. Conclution

In this paper, we conducted a performance comparison between symmetric cryptography algorithms 3DES, AES, Blowfish and Twofish. We evaluated the execution time, memory utilization and ciphertext size, by building a solution using C#. We performed the encryption and decryption for each of the targeted algorithms five times against different file sizes 1 KB, 100 KB, 1 MB, 10 MB and 100 MB. The result shows that AES is the most efficient in encryption and decryption form execution time point of view. When the files size is less than 10MB, 3DES comes in the second level and Blowfish in the third, but when the file size exceeds 10MB Blowfish gives a much better result than 3DES in both of the encryption and deception. Twofish gained the worst results at all. Regarding the encryption memory utilization, we noticed that AES and 3DES consumed less memory and relatively they utilized same amount of memory. While Blowfish and Twofish takes more memory, and they have the biggest ciphertext size.

References

[1] J. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamilla and A. Murukan,"Improving Web Application Security: Threats and Countermeasures",1st Edition, Microsoft Corporation.,2003

[2] W. Stallings, "cryptography and networksecurity princeples AND PRACTICE", 7th Edition, WILLIAM STALLINGS.2016

[3] N. Aleisa. A comparison of the 3DES and AES encryption standards. International Journal of Security and Its Applications. 9. 241-246.,2015

[4] G. Steel, The End of Triple DES. March 1, 2021. [Online], Available: https://cryptosense.com/blog/the-end-of-triple-des/ . Accessed March 1, 2021]

[5] M. Bishop , "Computer Security: Art and Science",2nd Edition, Addison-Wesley Professional, 2018

[6] A. Alabaichi, F. Ahmad and R. Mahmod, "Security analysis of blowfish algorithm," 2013 Second International Conference on Informatics & Applications (ICIA), Lodz, Poland, 2013, pp. 12-18

[7] M. Albahar, O. Olawumi, K. Haataja and P. Toivanen, "Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption". Journal of Information Security, Volume 9, Issue 2 (April 2018), PP. 168-176.

[8] A. Chandel, A. Aggarwal, A. Mittal and T. Choudhury, "Comparative Analysis of AES & RSA Cryptographic Techniques," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2019, pp. 410-414

[9] D. Budiyanto and P. A. W. Putro, "Comparison of Implementation Tiny Encryption Algorithm (TEA) and Advanced Encryption Standard (AES) Algorithm on Android Based Open Source Cryptomator Library," 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2018, pp. 136-139

[10] Maqsood, Faiqa & Ahmed, Muhammad & Mumtaz, Muhammad & Shah, Munam. “Cryptography: A Comparative Analysis for Modern Techniques”.2017 International Journal of Advanced Computer Science and Applications(IJACSA),2017, Volume 8, No. 6,.

[11] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," 2017 International Conference on Engineering and Technology (ICET), 2017, pp. 1-7

[12] S. Kansal and M. Mittal, "Performance evaluation of various symmetric encryption algorithms", International Conference on Parallel, Distributed and Grid Computing, Solan, India, 2014, pp. 105-109.

[13] D. Dakate and P. Dubey. "Performance Comparison of Symmetric Data Encryption Techniques", International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012

[14] J. Thakur and N. Kumar. "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis". International Journal of Emerging Technology and Advanced Engineering. Volume 1, Issue 2, December 2011.

[15] N. Penchalaiah and R. Seshadri. "Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)". International Journal on Computer Science and Engineering., Vol. 02, No. 05, 2010, 1641-1645.

[16] N. Singhal and J. Raina , "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, Issue 2011, pp. 177-181.

[17] D. Pine, .NET cryptography model , March 1,2021. [Online]. Available:https://docs.microsoft.com/en-us/dotnet/standard/security/cryptography-model . [Accessed March 1, 2021]

[18] NetEncryptionLibrary, Package info, March 1, 2021. [Online], Available:https://www.nuget.org/packages/NetEncryptionLibrary/.Accessed March 1, 2021]