Pronika, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 12, Issue 12, December 2022, pp. 105-111

RESEARCH ARTICLE OPEN ACCESS

Performance of Fernet and Aes Algorithms with Existing Encryption Techniques

Pronika[1], Supriya P.Panda[2],S.S. Tyagi[3]
[1]*Research Scholar & Assistant Professor,*
[2] *Professor& Department of Computer Science & Engineering, MRIIRS, Faridabad*
[3]*Professor & Director, IIMT College of Engineering, Greater Noida*

Abstract
"Data" being a crucial and complicated means of information in the current technological era, it has been majorly accessed and utilized for varied purposes by people globally through 'cloud computing' via personal data storage, social platforms, research-based studies, etc. Researchers had focused cloud as storage in recent technological development since it offers more insight towards meta-data-based security and safety along with techniques in encryption and decryption of messages. Thus to protect data in the cloud, the researcher used symmetric and asymmetric algorithms.In this paper, symmetric algorithms are used, which are AES and FERNET algorithms. Different Sizes of files are encrypted with both algorithms and compared in terms of time. AES and FERNET algorithms are used with different sizes of data files, which are 1KB, 10KB, 100KB, and 1MB. From the comparison, it is concluded that the time taken by AES algorithms is almost half as compared to FERNET algorithm when file size is 1KB. This paper aims to provide a more secure cloud-computing model than existing encryptionmodels as using DES, ARC4, DES3, and Blowfish algorithms.

Keywords: AES Algorithm, Data Security, Data Storage, Encryption Scheme, FERNET Algorithm, Symmetric Algorithm.

Date of Submission: 10-12-2022 Date of Acceptance: 25-12-2022

I. INTRODUCTION

The information as a hotspot for some exploration and studies is viewed as "a major trend dark gold". In numerous nations as of now, the effect of pandemic circumstances had made scientists look for storing, getting to, and changing information according to their needs. Anyway, the security and safety norms of the metadata particularly in the cloud, and data cloud are at a huge risk, where, information theft, information control, and misinformation are at large. Thus getting the information in the cloud and encrypting the data or messages have been recently centered by scientists.

Cryptography is the act of tying down valuable data while communicating starting with one personal computerand then onto the next or putting away information on a personal computer. Cryptography manages the encryption of plaintext into the cipher text and the decoding of cipher text into plaintext. Cryptography used two methods for encrypting and decrypting information. Symmetric and asymmetric cryptographies are the methods or types of cryptography. Many authors used different algorithms for securing the data. Python upholds a cryptography bundle that helps us encode and decode information.

II. LITERATURE REVIEW

Cryptography plays an important role in the field of security of data. Many authors used symmetric and asymmetric algorithms for securing the data. This section deals with the related work in the field of cryptography and its related algorithms.

Siregar, R. (2018, April). Performance analysis of AES-Blowfish hybrid algorithm for the security of patient medical record data. In Journal of Physics: Conference Series (Vol. 1007, No. 1, p. 012018). IOP Publishing.

The authors proposed a hybrid cryptography method including both symmetric algorithms AES and Blowfish to secure the patient medical data with the help of encryption or decryption process. The authors used two types of approaches with the public and private keys with RSA and ECC. They found Blowfish technique is faster than AES and the hybrid method of Blowfish-AES provide better throughput when compared to Blowfish and AES. RSA method is less fast as compared to ECC. They conclude with the smaller size of the Key, which

provides the highest strength, faster calculation, and efficient and measurable methodology.

Chinnasamy, P., & Deepalakshmi, P. (2018, April). Design of secure storage for health-care cloud using hybrid cryptography. In 2018 second international conference on inventive communication and computational technologies (ICICCT) (pp. 1717-1720). IEEE.

The authors discussed a hybrid model related to healthcare data security in the cloud. With the help of a symmetric algorithm first, the data is encrypted then with the help of an asymmetric algorithm, the keys are encrypted. Using the Blowfish Algorithm data is encrypted related to health care data and stored in the cloud and the RSA algorithm manages keys. The proposed algorithm provides large prime numbers for keys, fast encryption, and effective key management. The authors also discussed that the proposed algorithm or hybrid algorithm with the help of results that decryption and encryption time is better as compared to AES and Blowfish algorithm.

B. Mehul, D. Prayas, R. Lalit & K. Rohini. (2018) Secure File Storage in Cloud Computing Using Hybrid Encryption Algorithm. International Journal of Computer Engineering and Applications,9(6),2018

The authors proposed a hybrid algorithm that includes four different encryption algorithms like DES, AES, Steganography, and RC4. It provides data privacy and security for the data in the cloud. Data is divided into three parts, RC4 encrypted the first part then DES encrypted the second part and AES encrypted the third part. The value of the key is hidden with the help of steganography, so the message sent by the sender will be encrypted by three different algorithms, and the key value be secured. Only the sender and receiver know the type of algorithm used in the proposed methods. The receiver using AES, RC4, DES and Steganography will receive data safely.

Zhang, F., Chen, Y., Meng, W., & Wu, Q. (2019). Hybrid encryption algorithms for medical data storage security in cloud database. International Journal of Database Management Systems (IJDMS) Vol, 11.

The authors proposed a hybrid algorithm to tackle the information security issue in the emergency clinic cloud data set. In the first place, the AES algorithm started at the first level. The improved calculation is called P-AES calculation or algorithm. The P-AES calculation is then joined with the RSA calculation, called a hybrid calculation. The trial results show that the hybrid encryption calculation enjoys the benefits of quick encryption and decoding speed, high security, great handling skill for longer information, and can partially tackle the information security issue in cloud data set. The calculation has been effectively applied to medical clinic data in the executive framework. They concluded that the P-AES algorithm has some limitations as it cannot encrypt images and pictures but can only encrypt text data.

Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. Sensors, 20(18), 5162.

The authors use different algorithms to secure the image data like symmetric and asymmetric algorithms. Many authors follow only symmetric algorithms for sensitive images and some used only asymmetric algorithms for the safety of image data. The authors used different hybrid algorithms for the safety of image data like Double Play fair Cipher Elgamal, AES ECC, and Hill Cipher ECC. With the help of the proposed algorithm, the authors calculated the decryption time, encryption time, squared Error, and entropy of the decrypted image and try to find out which one is the better technique. When compared to a single algorithm the entropy value is better in a hybrid algorithm and near eight. The authors discussed the squared error, which is also better in a hybrid algorithm. When the image size is large, AES ECC is not feasible. AES ECC is good for private communication or remote for small-size images. The authors conclude that Hill cipher with ECC is a good option for image encryption or decryption as compared to AES ECC.

Darwish, M. A., Yafi, E., Al Ghamdi, M. A., & Almasri, A. (2020). Decentralizing privacy implementation at cloud storage using blockchain-based hybrid algorithm. Arabian Journal for Science and Engineering, 45(4), 3369-3378.

In this paper, the authors discussed block-chain based hybrid algorithms that handle privacy issues in the cloud. With the help of the proposed algorithm data is first encrypted and outsourced to data centers then a digital signature that is unique is generated on the client side and stored. Integrity, data confidentiality, and authentication are important factors when a hybrid algorithm is implemented to access efficiency. Authors provide the privilege to users to control their private keys and their data are transparent and well formed with the help of the proposed method. Cloud auditors maintained the encrypted data from attackers and integrity is preserved at a decentralized level. The proposed model maintained data privacy inside the cloud and balance the requirement of the service provider and client. The authors showed that the privacy of user data is increased and reliability and integrity are preserved with help of the proposed model.

Kaur, R., & Singh, B. (2021). A hybrid algorithm

for robust image steganography. Multidimensional Systems and Signal Processing, 32(1), 1-23.
The authors proposed a novel hybrid algorithm for image steganography for secure data communication. First, the cover images changed into the frequency with the help of Discrete Cosine Transform then embed the secret data with frequency coefficients and maintained the quality of the image. Security against attacks is provided with coupled chaotic maps. The authors showed that the quality of the image is maintained using the proposed method.

Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.
The authors proposed an algorithm for maintaining the privacy, integrity, protection, and confidentiality of the data in the cloud from attackers. It is based on a cryptographic algorithm and used for enhancing the data security of the data in cloud computing. The proposed algorithm is a block cipher (16 bytes) and wants to encrypt the 16 bytes data. It is used to improve the complexity of the encryption and used substitution and feistal algorithms. The proposed model result shows a better security level and enhancement in the execution time when compared with others. The proposed model has the flexibility option in terms of the number of turns and secret key length.

Shanmugam, D. B., Vijayalakshmi, N., Sesubalan, S. A., Immanuel, D., & Shravan, V. R.(2022) SECURITY IMPROVEMENT OF CLOUD DATA USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY.
The authors combined two techniques: cryptography and steganography, for providing security in the cloud. The authors used a hybrid algorithm in which symmetric and asymmetric both techniques were used. AES part of the symmetric algorithm combined the RSA that belongs to asymmetric techniques for securing the cloud data. Different algorithms were used for the encryption and decryption process and the authors achieved better security and higher efficiency. The authors used the Triple DES algorithm for encryption purposes, providing better results and showing higher data security. The proposed system can be used in army databases, hospitals, banking, private sectors, etc. Encrypted data are hidden in the form of images using different algorithms and then compressed the data using steganography. The proposed system is more efficient and powerful when securing the data in the cloud. With the help of results, the authors showed the integrity of the data is also maintained using the proposed method.
Different authors used different algorithms for securing the data using cryptography. Comparisons of these algorithms are shown in Table 1.

Table 1: Comparison of Different Algorithms

Authors	Year	Algorithms	Strength	Weakness
Chowdhary et al.	2020	ECC with Hill Cipher, ECC with AES, and ElGamal with Double Playfair Cipher	Easy to implement with an increase in speed and improved security with hybrid algorithms.	ECC with AES hybrid algorithm is good for small size image but not suitable for larger size image because ECC required small bandwidth for the decryption process as compared to ECC and Hill Cipher.
Garima and Naveen	2014	DSA, AES, Steganography	The authentication process is done with the DSA algorithm, encryption with AES.	The one-to-one process's that's why takes more time.
Punam V Maitri, Aruna Verma	2016	AES, RC6, Blowfish	More security in block-wise cipher as compared to a stream cipher.	It provides low delay with low security for the encryption and decryption process.
Richa S. and Richa D.	2017	MD5 and AES	Tackle four phases: authentication, data integrity, data retrieval request, and verification using a hybrid algorithm.	Only AES is used for the cryptographic and hashing algorithms.
Bhale etal.	2016	RSA and MD5	Security features increased and better performance using RSA and MD5.	MD5 algorithm with cryptography secure is no longer used in this.
Yoshita etal.	2019	AES AND RSA	It provides different levels of encryption using the hybrid algorithm.	Issue of Data linage
Sarah and Depali	2016	ElGaman and SHA256	Hybrid algorithms provide integrity for outsourced data. Security for the cloud is provided on three different levels and it used cryptography to resolve	It takes more time in the decryption process as compared to other algorithms.

			security issues in the implicit cloud.	
Darwish et al.	2020	Elliptic-Curve Cryptography(ECC) and Advanced Encryption Standard(AES)	With this hybrid algorithm, users' data privacy and integrity increased. ECC and AES combined with blockchain to resolve privacy issues.	More than 100 requests from different users do not proceed at the same time.

III. COMPARATIVE ANALYSIS OF FERNET AND AES ALGORITHMS

This section deals with the comparative analysis of the FERNET and AES algorithms. Comparison by different sizes of files as 1KB, 10KB, 100KB, and 1MBand different time taken by both algorithms are shown in the form of tables and figures.

3.1 FERNET ENCRYPTION

The Fernet module of the cryptography bundle has inbuilt capabilities for the age of the key, encryption of plaintext into ciphertext, and unscrambling of ciphertext into plaintext utilizing the encode and decode techniques individually. The Fernet module ensures that information scrambled utilizing it cannot be additionally controlled or perused without the key.Different sizes of text are used and foundthat the total time taken to apply the Fernet encryption algorithmto the text as shown in Table 2.

Table 2: Total Time Taken to Encrypt the Different Sizes of Text (FERNET Encryption)

FERNET Encryption	
Size of Text	**Time Taken to Encrypt**
1 KB	0.003582239
10 KB	0.007000368
100 KB	0.00823307
1 MB	0.035600185

Fig 1 shows the time vs. size graph from which it can be clearly depicted that as the size of text increases it would take more time to encrypt.

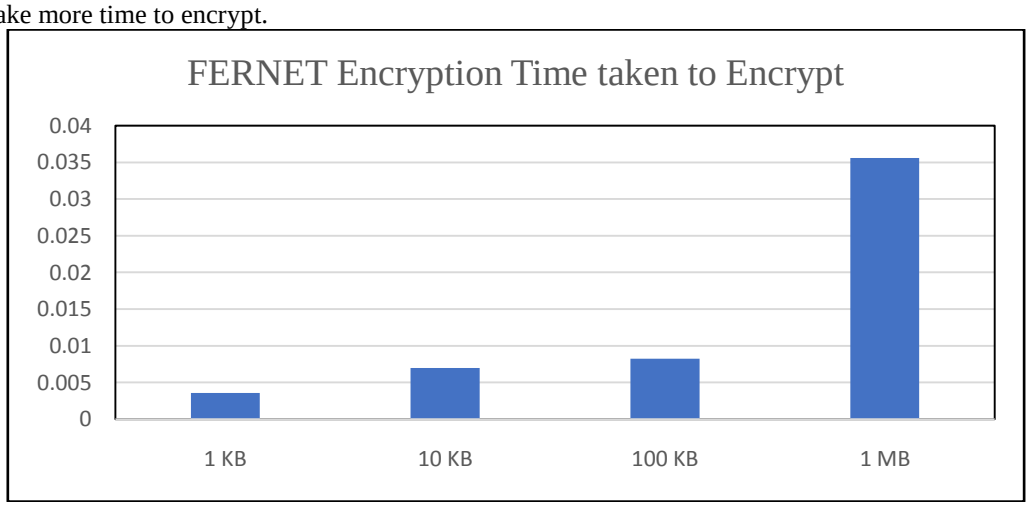

Fig 1: Time vs. Size Fernet Encryption Algorithm Graph

3.2 AES ENCRYPTION

High-level Advanced Encryption Standard (AES) is particular for the encryption of electronic information laid out by the U.S Public Foundation of Principles and Innovation,National Institute of Standards and Technology (NIST) in 2001. AES is broadly involved today as it is more grounded than Data Encryption Standard (DES) and triple DES in spite of being more enthusiastically to execute.

- AES is a block figure.
- The key size can be 128/192/256 pieces.
- Scrambles information in blocks of 128 pieces each.

That implies it accepts 128 pieces as information and results in 128 pieces of scrambled figure text as result. AES depends on replacement change network guidelines, which implies it is performed utilizing a progression of connected tasks, which includes supplanting and rearranging the information. Different sizes of text are used and foundthat the total time taken to apply the AES encryption algorithm to the text as shown in Table 2.

Table 3: Total Time Taken to Encrypt the Different Sizes of Text (AES Encryption)

AES Encryption	
Size of Text	**Time taken to Encrypt**
1 KB	0.00199604
10 KB	0.002985477
100 KB	0.007977724
1 MB	0.033907175

Fig. 2 shows the time vs. size graph from which it can be clearly depicted that as the size of text increases it would take more time to encrypt.

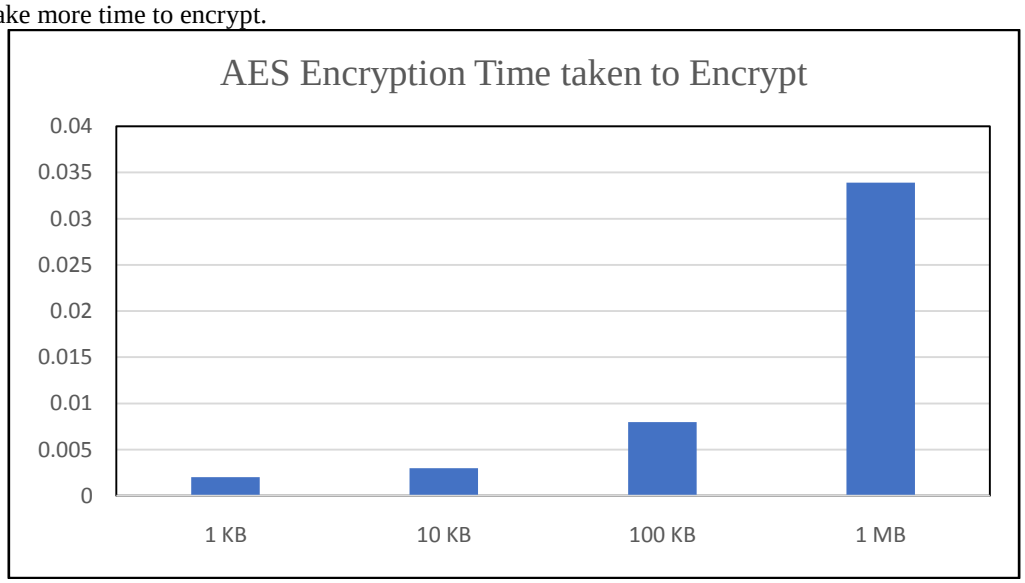

Fig. 2: Time vs. Size AES Encryption Algorithm Graph

3.3 COMPARISON OF FERNET AND AES ALGORITHMS

Table 4 shows the comparison of FERNET and AES Encryption algorithms on different sizes of data and Fig. 3 shows the graphical representation of the data.

Table 4: Total Time Taken To Encrypt the Different Size of Text (FERNET Encryption & AES Encryption)

FERNET Encryption		AES Encryption	
Size of Text	**Time taken to Encrypt**	**Size of Text**	**Time taken to Encrypt**
1 KB	0.003582239	1 KB	0.00199604
10 KB	0.007000368	10 KB	0.002985477
100 KB	0.00823307	100 KB	0.007977724
1 MB	0.035600185	1 MB	0.033907175

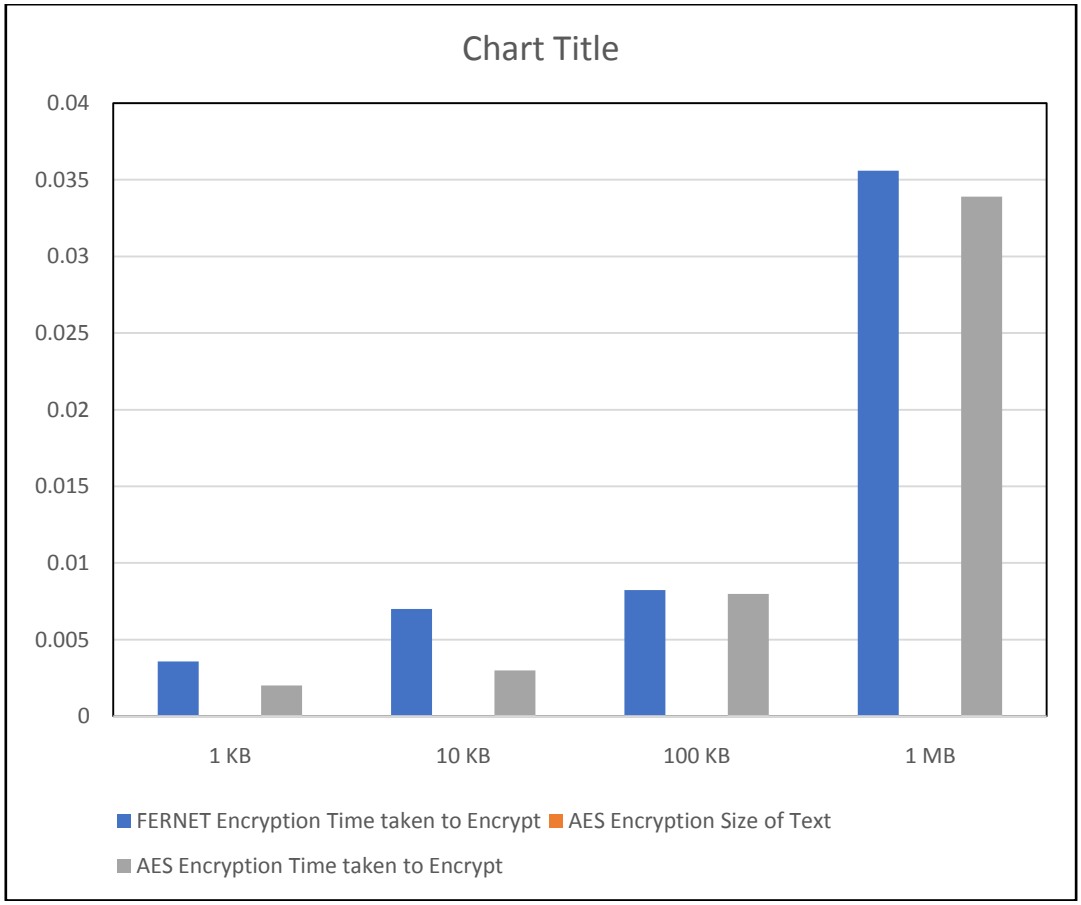

Fig 3: Time vs. Size AES & FERNETEncryption Algorithm Graph

Authors [10] used the same sizes of files for encryption using DES, ARC4, DES3, and Blowfish algorithms. The comparison shown in Table 5 with respect to file sizes is 1KB, 10KB, 100KB, and 1MB.

Table 5: Time Taken by Cryptography Algorithm for Encryption

Size/Algorithm	DES	Blowfish	ARC4	DES3	FERNET	AES
1KB	0.000996	0.0019965	0.000989	0.001995	0.00358223	0.0019960
10KB	0.001995	0.0019955	0.001996	0.0019941	0.00700036	0.0029854
100KB	0.009972	0.0079810	0.002984	0.0199472	0.00823307	0.0079777
1 MB	0.040885	0.0269279	0.017950	0.0957486	0.03560018	0.0339071

IV. CONCLUSION& FUTURE SCOPE

The Fernet and AES algorithms are crucial for data security. These algorithms were employed in the study of several authors. AES and FERNET algorithms, which are symmetric algorithms, are employed in this research. Both techniques are used to encrypt data of varying sizes, and their processing times are contrasted. In this study, multiple data file sizes—1KB, 10KB, 100KB, and 1MB—were employed using the AES and FERNET algorithms. Tables and figures are used to display the comparison as well. It may be inferred from the comparison that AES techniques take less time than the FERNET algorithm.

The time complexity of various data file sizes can be determined in the future by comparing the AES and FERNET algorithms with asymmetric techniques**.**

REFERENCES

[1]. Siregar, R. (2018, April). Performance analysis of AES-Blowfish hybrid algorithm for the security of patient medical record data. In Journal of Physics: Conference Series (Vol. 1007, No. 1, p. 012018). IOP Publishing.

[2]. Chinnasamy, P., & Deepalakshmi, P. (2018, April). Design of secure storage for health-care cloud using hybrid cryptography. In 2018 second international conference on inventive communication and computational technologies (ICICCT) (pp. 1717-1720). IEEE.

[3]. B. Mehul, D. Prayas, R. Lalit & K. Rohini. (2018) Secure File Storage in Cloud Computing Using Hybrid Encryption Algorithm. International Journal of Computer Engineering and Applications,9(6),2018

[4]. Zhang, F., Chen, Y., Meng, W., & Wu, Q. (2019). Hybrid encryption algorithms for medical data storage security in cloud database. International Journal of Database Management Systems (IJDMS) Vol, 11.

[5]. Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. Sensors, 20(18), 5162.

[6]. Darwish, M. A., Yafi, E., Al Ghamdi, M. A., & Almasri, A. (2020). Decentralizing privacy implementation at cloud storage using blockchain-based hybrid algorithm. Arabian Journal for Science and Engineering, 45(4), 3369-3378.

[7]. Kaur, R., & Singh, B. (2021). A hybrid algorithm for robust image steganography. Multidimensional Systems and Signal Processing, 32(1), 1-23.

[8]. Pronika, Tyagi, S. S. (2021). Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN). International Journal of Computer Networks and Applications, 8(4), 288-299.

[9]. Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.

[10]. Pronika, S., & Tyagi, S. (2021). Performance analysis of encryption and decryption algorithm. Indonesian Journal of Electrical Engineering and Computer Science, 23(2), 1030-1038.

[11]. Shanmugam, D. B., Vijayalakshmi, N., Sesubalan, S. A., Immanuel, D., & Shravan, V. R.(2022) Security Improvement Of Cloud Data Using Hybrid Cryptography And Steganography.

[12]. Kumar, M., Soni, A., Shekhawat, A. R. S., & Rawat, A. (2022, February). Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique. In 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS) (pp. 1453-1457). IEEE.