International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

Mitigation the Challenges of Cloud Storage Security Using Hybrid Algorithms

Sokiyna Mohammad Glilat*

**Master's Student in Computer Science. German Jordanian University Information Technology Collage, Jordan.*

*Corresponding Email: *mohdsoukena@gmail.com*

Received: 05 June 2022 **Accepted:** 21 August 2022 **Published:** 29 September 2022

Abstract: Security of the cloud computing is one of the most challenge which limit the idea of adopting the technology of clouding if the level of the security is not significant to protect the stored data, many researches had implemented several algorithms for this purpose. This paper implemented a hybrid algorithm based on AES and ECC to give high level of security. A theoretical study is presented in the first part of this search to explain the basic concepts of clouding as well as the security of this technique. After that the performance of the proposed scheme had been evaluated. The result showed that the AES combined with ECC offer extra feature which ensure high level of protection for the data.

Keywords: Cloud, Hybrid, Security, Data, Hacker, Attacks, Encryption, Decryption.

1. INTRODUCTION

Nowadays, Cloud computing had been grown rapidly as an emerging technical. The concept of Cloud Computing could summarized by the possibility of access to high amount of data from anywhere and at any time. This concept reduces the function of local device such as computers. Cloud computing could provide many models of service based on users' requirement[1]. This models include basically infrastructure, electronic platforms and software[2]. Although cloud computing is flexible and convenient solution, it still experiences some restrictions due to the issues related to security. [3],[4]. There are three basic dimensions related to cloud-computing, they basically include the security of (computer, network, information). The security issue related to computer also include the protection process of information, hardware and also software. Could system has serious challenges related to security such as the ability of unsanctioned access to the information, this is one of the most important challenge for cloud technology also there are the

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

ability to vary the data related to the client. Additionally, the availability of data for client every time should be achieved without any issue which impact on the storage of the data. [5] had stated that the basic issue in adopting the cloud is the security as well as the privacy. The providers of the clouding service should ensure the protective of the infrastructure and implemented effective mechanism of security of the clients data and application. [6] had mentioned that accept the clouding technology among the various users is depending on the level of security. Evaluation quality level of the security of the clouding providers is a critical issue. The challenges related to the security in clouding the data could lead to economy loss and an invalid reputation. For these reasons, users should be more careful when the store the information using the cloud technical, before transmitting the data to the cloud- storage, it had to encrypted[7].

Previous searches and works about clouding storage

[8] presented the characteristics of cloud and applied several algorithm to encrypt the data. Encryption based on symmetric and asymmetric algorithms was investigated. The studied algorithm had been tested using various attacks and the tests showed that there is no possibility attack the information in the cloud storage. [9] presented a study to enhance the security by combining RSA and MD5 encryption algorithm which provide communication secure also ensure the hiding of data to prevent the not allowed users access. [10] implemented encryption to protect the data transmission SSL,RSA integrated with a magic square. [11] had mentioned that the rapid advance of information technology and the limitation related to transmit the information leading to the requirement to find powerful cryptosystem which taking small space after encrypting for the ciphering text. The proposed method taking the least amount of spaces between other algorithm such as Two-fish, AES. [12] the proposed technique based on combining AES, RC5. This made the level of the security and the improve the performance. [13] offered security to transmit the information through various reliable channels which achieved by encryption. The used algorithm is BFT. It provided vitality and safe performance. [14] changed the information and worked to improve the integrity the information and audit it. The encryption is done by Secure-Hash algorithm SHA combined with the AES scheme. It also detected the repetition of information as well as reducing the bandwidth.

Literature Review

In this part, it will be introduced a brief review about cloud systems(modes, challenges) and the conception of security of the cloud system and the basic categories of algorithms which used to ensure protection to the data stored in the cloud environment.

Clouding Models

The cloud system has three different model which are commonly used:

A. Public: it represent the external clouding and the ability to access is openly, in this way the client could access to the resources. This model could host the individual in addition groups of services.

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

B. Private: this model offers a limiting access to the its services and resources to the client who belong to the organization of the cloud, this is called internal clouding. The infrastructure of this model could be operated and managed for one only organization. Therefore, the control level and privacy and also governance should be maintained.

C. Hybrid: by this model, public model is combined with private. This could provide extra advantages. This could enable the management of the workload in the private model of the cloud system. if the workload had increased, it could be asking the public model clouding for heavy resources of computing and return when the need is no longer.

D. Community:
This model is sharing the resources with multiple organizations in the community which share commonly interests such as security, governance, compliance. It typically implies special-purpose environments of cloud computing which managed and shared through set of relating organizations participating in a commonly domain[15].

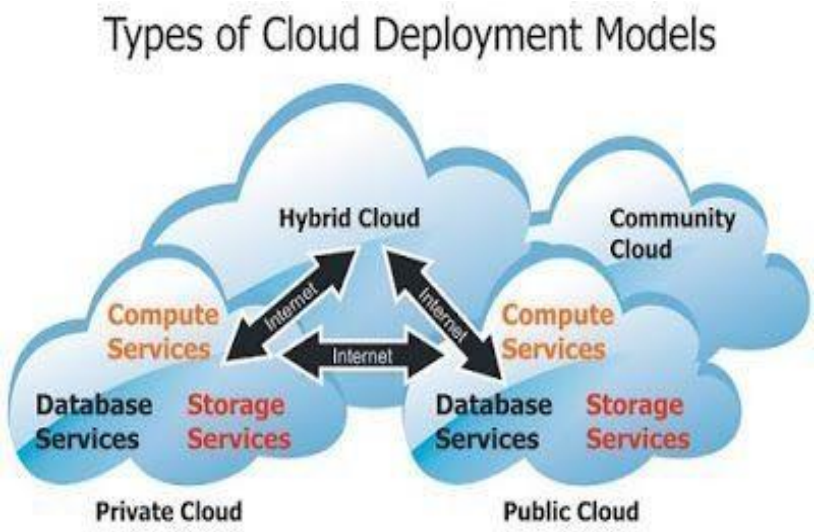

Fig (1): The basic models of cloud computing

Challenges related to cloud computing
There are different restrictions to adopt cloud computing on a large scale[16] such as the following issues:

A. participation of the data without warrant
Here, It should allow the owner of information to be permitting in the privacy police that users should agree before the using of models of cloud service. The life- threatening condition which

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

generally there is no enough time for waiting the police to get a warrant. Therefore, majority of clouding providers could share the data immediately to police for getting warrant for the sensitive information.

B. security:
This is a desired condition ensure the freedom from the harm where the information is protecting from the integrity, confidentiality as well as the availability in the wanted state also at the desired time. If the security of the cloud system is achieved, this could open the scale to more challenges for addressing.

C. the client and the storage:
The diverse using of cloud computing lead to reduce the demand of the consumer devices with high capacity of storage because the low cost of low capacity storage equipment. Despite of this features that by outsourcing information storage could menace the sensitive information of clients. Due to the physical unauthorized accessing to the information. In this case, the encryption is one of the most powerful method to ensure transmitting the sensitive information in the clouding environment.

D. Sustainability
Despite cloud computing is supposed to be a form of the green computing, currently it is unable for measuring how "green" the computers [16]. Cyber-security Ventures had been predicted that in 2025, it will be keeping the data in the cloud environment for over one hundred (100) zettabytes, (trillion gigabytes), it also predicted that more than 200 Zettabytes of data could store by all over the world [17]

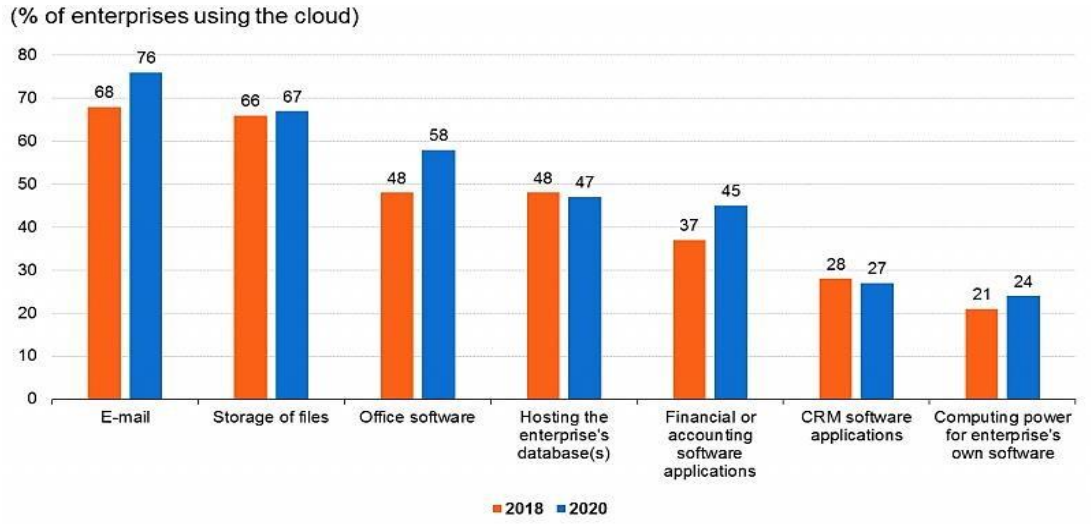

Fig (2): The use of clouding services in the enterprises (2018-2020)[18]

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

The aims of cryptography:
The cryptography aims basically in the cloud system to the following goals:

A. confidentiality: this mean that the ability to access of the message content is only for the sender and the receiver.

B. Authentication: It is necessary because multiple users depend on encryption using to secure their data.

C. Integrity: this feature ensure that the messages contents should reach to the receiver as it had been sent by the sender exactly.

D. Non- repudiation: this feature prevent the sender from repudiation of posting the messages.
E. access-control: this feature is stated that who could access the content of the message.

F. Availability: this means that the services have to be available for all time. and have convenient backup.

Classification of the Algorithms used for encryption:
A. Symmetric: by this algorithm, a commonly key is used for the encryption process and decryption of the information such as Data Standard (DES), Data (IDEA), encryption standard(AES)[19]

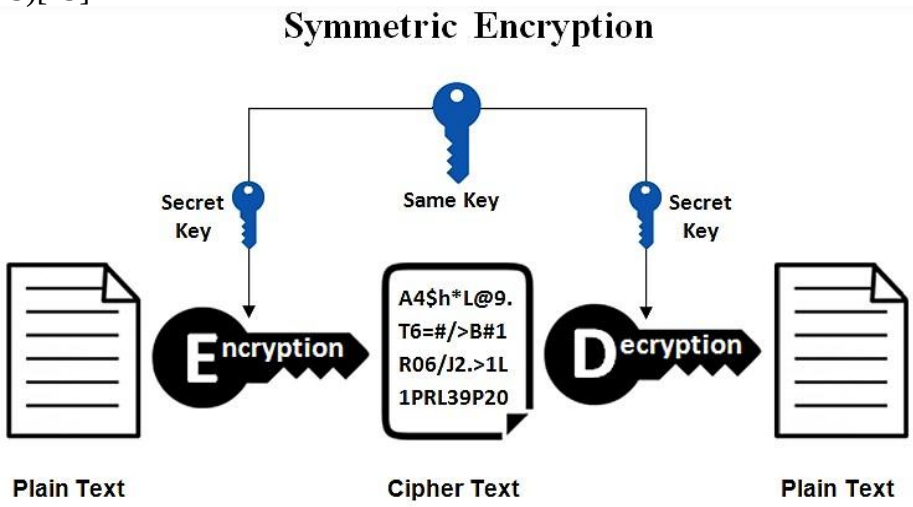

Fig (3): The symmetric encryption principle

b. Asymmetric: By this type, two various keys are used for the encryption process and decryption of the information. Such as: RSA, ElHamal, Diffe-Hellman [19],[20].

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

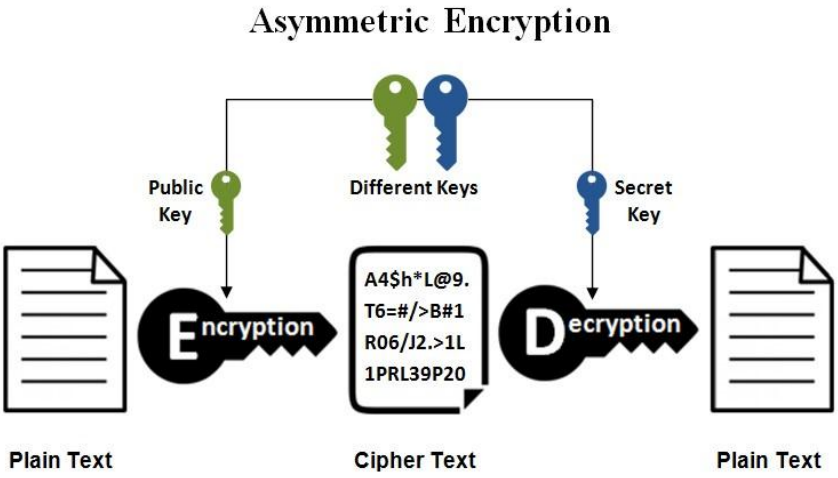

Fig (4): The Asymmetric encryption principle

c. Hybrid: This type is achieved by combination between over two algorithms. The same or various algorithms are used to encrypt messages which had been already encrypted more times. The encryption of data and decryption provide a possibility for using several encryptions. The most important uses of the multiple-encryptions to secure the information by preventing Brute-Force attacks. The same file or text could be encrypted several times, These encryptions offer good level of protection from the attacks and make the ciphering powerful. (AES) combined with (RSA) is one of the examples about hybrid algorithms.

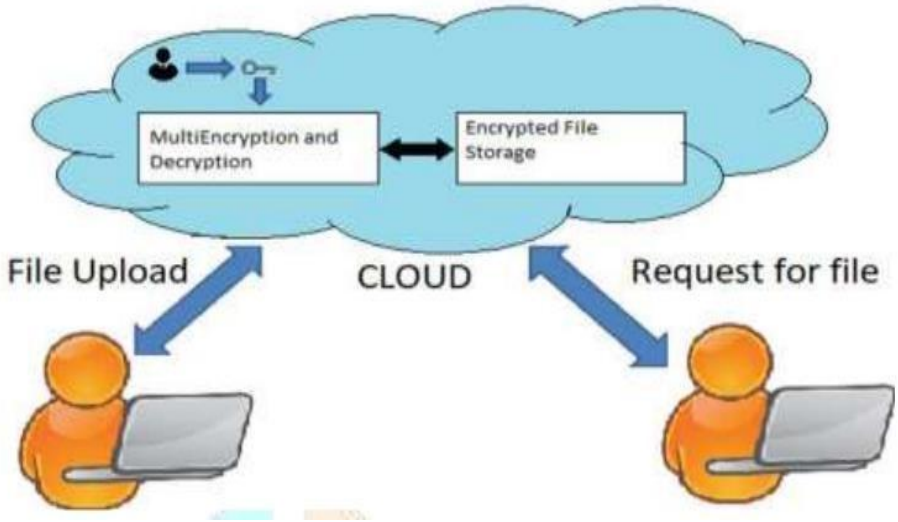

Fig (5): The hybrid encryption principle

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

Proposed Algorithm:
In this study Hybrid encryption algorithm had implemented. One of the symmetric algorithms (AES) is combined with an asymmetric (ECC). AES is characterized by its fast, and adopted for a wide scale. (ECC) are characterized by its robust as well as enhancing the performance of the computing power.

Level 1 encryption standard (AES): The components of the encryption have a series of operations which are linked each other. Substitutions is the concept of blending operation for establishing a relation among plain-text , cipher-text , the key. Permutation determines each bit related to the cipher-text base on each bit of plain-text with key. The procedures related to the network of substitutions-Permutation include transformation of (sub-bytes, shift-row, mix-columns, as well as round-key). In this case the procedure will use the produced output from prior stage as input for the following stage. AES is a fast algorithm and offer a good level of security. It could be used in different modes. Additionally, it backs key length and data combination like) with the key of privacy.
Could share only among sender and receiver to access the encrypted information.

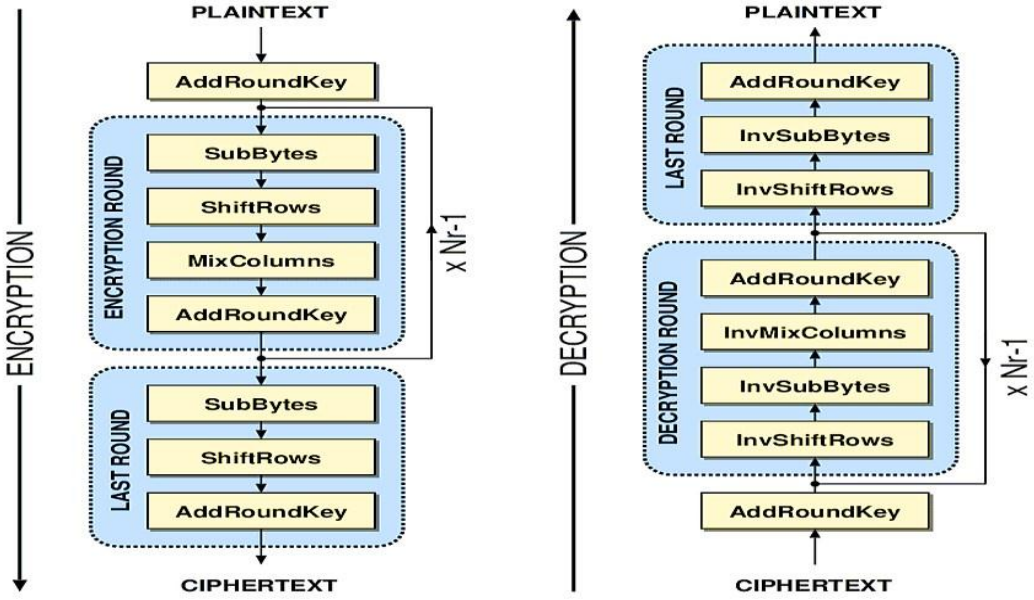

Fig (6): The structure of algorithm

Level 2 ECC algorithm: It protect the data which stored in the cloud environment from eavesdropper and the hackers. It is a cryptography technique. The symmetry in ECC is horizontal which are points located on X-axis, any line which is non-vertical will intersect the curve by three points at most. ECC basically depending on the theory of elliptic-curve. The equation of this curve is given as following:

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

$$y^2 + a_1xy + a_3y = x^3 + a_2^2 + a_4x + a_6$$

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + a_4x + (a_3^2 + a_6)$$

$$y^2 = x^3 + Ax + B$$

The key generation of ECC:

Signature-generation:

i. *For signing a message m, using Ahmad's pr_key yA*

ii. $e \coloneqq HASH\ (m)\ s.t.\ HASH\ is\ a\ f(SHA-1,\dots)$

iii. $Rand\ k \coloneqq [1, n-1] \forall k\ \in \mathbb{Z}$

iv. $r \coloneqq i_1 (mod\ n), where\ (i_1, j_1) = k *$

$B. If\ r = 0, then\ step\ III$

v. $s \coloneqq k - 1(e + yA * r)(mod\ n). If\ s = 0,\ then\ step\ III$

vi. $Signature \coloneqq f(r, s)$

vii. $Finally, Basil \leftarrow signature(r, s)$

Encryption Algorithm

i. *Assume Ahmad sends an encrypted message to Basil*

ii. *Ahmad Plian_text* :=

$f(message\ m\ with\ points\ from\ the\ elliptic\ group$

iii. $Ahmad \coloneqq Rand\ k\ [1, p-1] \forall\ k \in \mathbf{Z}$

iv. $Cipher\_text \coloneqq [\ (kB), (pm + k * PB)]$

The combination of the two various process ensure the security and mitigate losing the data due to the hackers.
The algorithm AES firstly is implemented and the figure (6) illustrate the block diagram of the proposed algorithm.

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

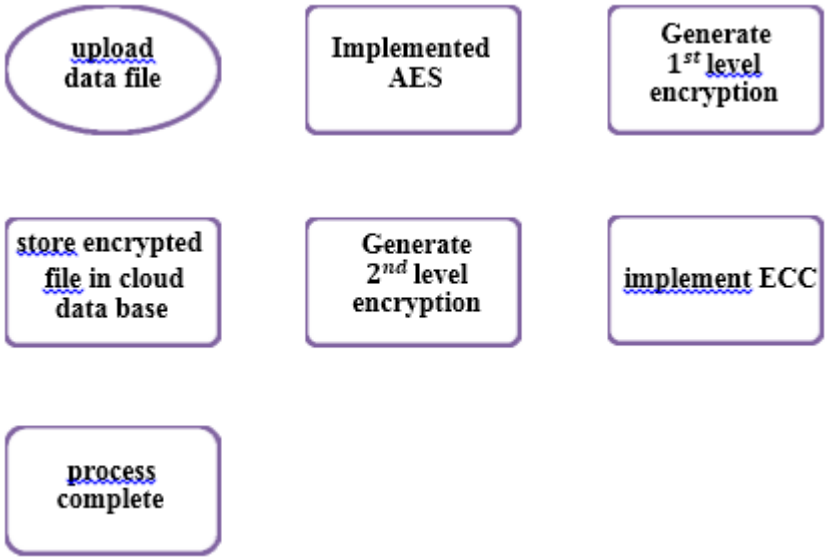

Fig (7): block diagram of the proposed encryption algorithm

When the file is downloading, the ECC will decrypt the key of AES, this will be implemented on the text which it is cipher for decrypting the data. Fig(7) illustrates the block diagram of the process of decryption.

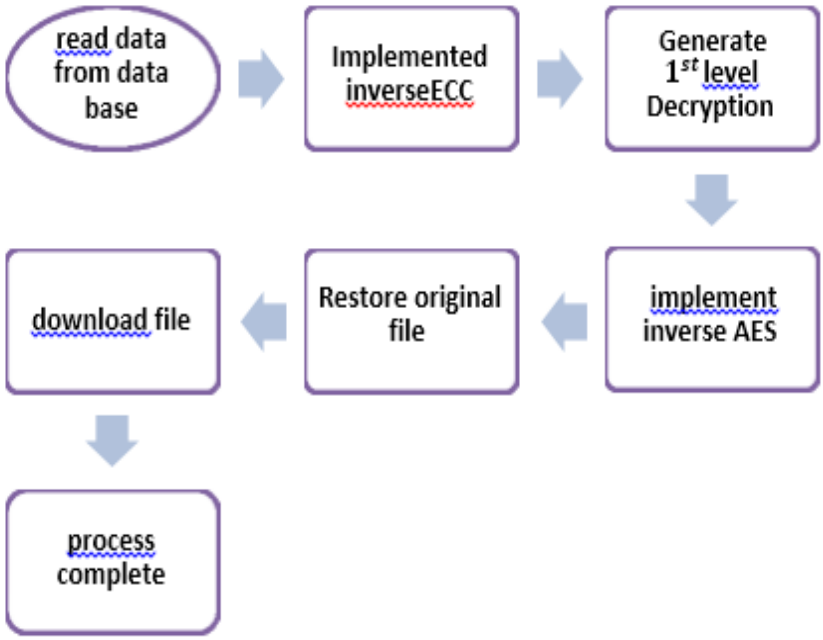

Fig (8): block diagram of the proposed decryption algorithm

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

Evaluation of the proposed Algorithm performance:

The evaluation of the privacy model performance is computed to investigate the affectivity of the proposed algorithm which blended between symmetric and asymmetric algorithms. Table (1) presented the runtime of the encryption as well as the decryption of the data which is transferred between Ahmad and Mohammad.

Table 1

Size	Encryption time(sec)	Decryption time (sec)
20 kb	0.25	0.17
65 kb	0.92	0.78
40kb	0.41	0.31
45 kb	0.58	0.40
30 kb	0.4	0.30

From table (1) and figure (8) it could be seen that the time is required for encryption is higher than the time which is required for decryption.

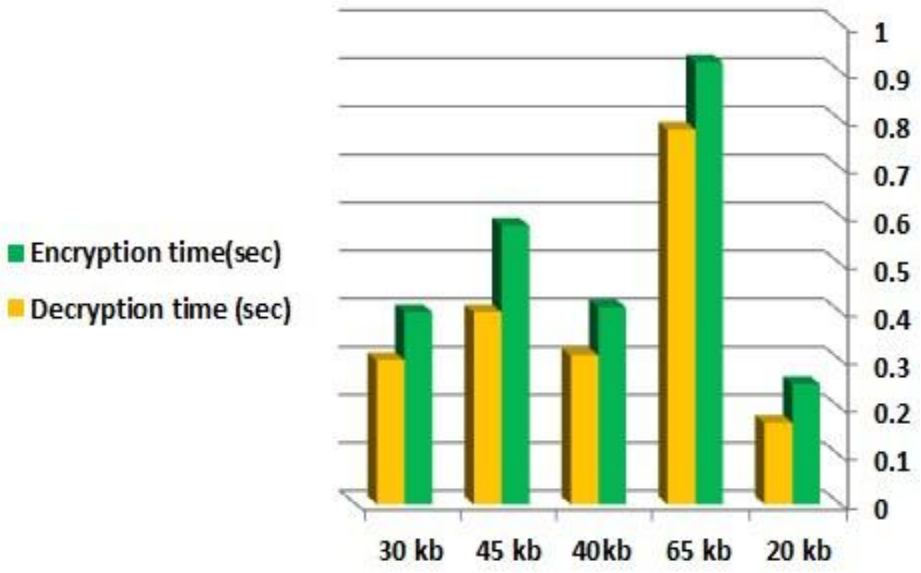

Fig (9): Time of encryption, decryption

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

Table (2) had presented the required time for AES, ECC, and the hybrid for comparison. Fig(9) showed that the required time for encryption by using ECC is higher than the proposed algorithm. However, the required time for AES implementation is smaller than the proposed algorithm. Despite this proposed algorithm better than the individual algorithm in the issues related to security. If the hacker had decrypt the first level, it would be complex to decrypt the second level.

Table 2

Size	Time (sec)		
	AES	ECC	AES/ECC
20 kb	0.25	0.6	0.42 1.60
65 kb	0.90	1.9	0.72 0.98
40 kb	0.40	0.8	0.70 0.88
45 kb	0.55	1.12	40
30 kb	0.40	0.79	45.4
Average-time	0.5	1.046	
Average-size	40	40	
Throughput	80	38.2	

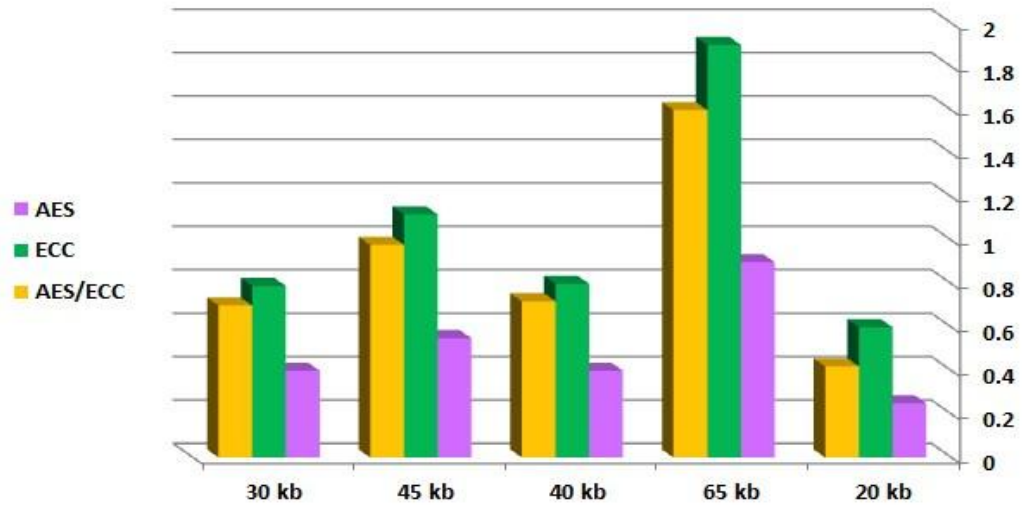

Fig (10): comparison of the required time for the three studied algorithms

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

The speed of the encryption is specified by: $\frac{\text{Plaintexx(kb)}}{\text{encryption time (sec)}}$

Increasing the value of throughput indicated an increase in the functionality. The performance evaluated depending on the time required to send the data as well as the throughput. Table(3) presented the ratio of the cipher-text to the plain-text, it had found that the ratio for the proposed algorithm is smaller than and higher than.

Table 3

Algorithm	**Ratio of cipher to plain-text 5:2**
AES	4:1
ECC	3:1
AES/ECC	

The results which is summarized by table(3) is represented by fig (10) to show the ratio of each studied algorithm.

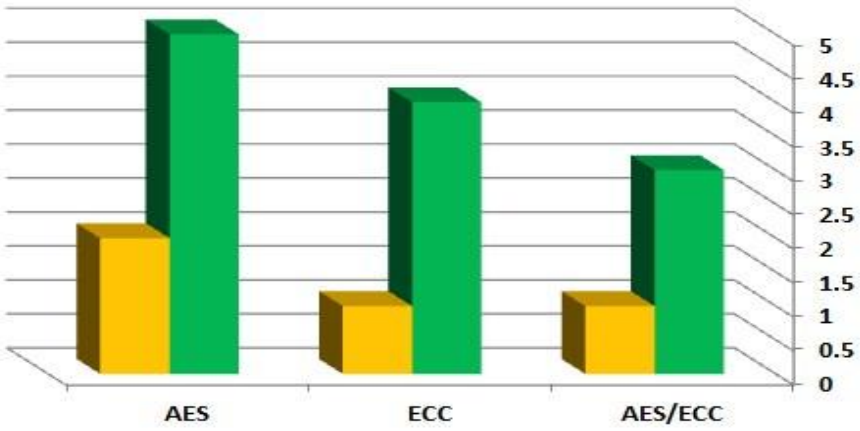

Fig (11): The ratio/

2. CONCLUSION

Cloud application offer a suitable environment for data storage, it facilitate the access to the own data of users from anywhere as well as at the time which the client need his data. Therefore, it

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

should be interested in the security issues by improving the algorithms which used for this purpose. The results which extracted from this detailed study showed the powerful of using AES combined with ECC to get more reliable and efficiency, It had found that the desired time for encryption implementation using ECC is higher than AES/ECC, and the desired time for AES implementation is smaller than AES/ECC. These results are presented graphically to compare the required time to implement the encryption as well as the decryption by every studied algorithm. The proposed algorithm had proved its affectivity and reliability for protection the data from both hackers and attaches.

3. REFERENCE

1. Sun, X. , Critical Security Issues in Cloud Computing: A Survey , IEEE International Conference on Big Data Security on Cloud 2018).
2. Qian, L. Luo, Z. Du, Y. and Guo. L., Cloud computing: An overview. Cloud computing, pages 626–631, 2009.
3. Dinh, T. Xuan, Y. Thai, M. Pardalos, P. and Znati. T. On new approaches of assessing network vulnerability: hardness and approximation. IEEE/ACM Transactions on Networking, 20(2):609–619, 2012.
4. Khorshed, T. Ali, A. and Wasimi, S. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems, 28(6):833– 851, 2012.
5. Sajay, K., Babu, S., Vijayalakshmi, Y., Enhancing the security of cloud data using hybrid encryption algorithm, Journal of Ambient Intelligence and Humanized Computing, 2019.
6. Shinde, M., Taur, R., Encryption algorithm for data security and privacy in cloud storage. Am J Comput Sci Eng Surv , 2015 ,34–39.
7. Arockiam, L ., Monikandan S., Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. Int J Adv Res Comput Commun Eng 2014, 3064–3069.
8. Bangar, A., Shinde, S. Study and comparison of cryptographic methods for cloud security. Int J Comput Sci Eng Inf Technol. 2014,205– 213
9. Lenka S., Nayak B., Enhancing data security in cloud computing using RSA encryption and MD5 algorithm. Int J Comput Sci Trends Technol . 2014, 60–64.
10. Dharini A., Saranya Devi R., Chandrasekar I., Data security for cloud computing using RSA with magic square algorithm. Int J Innov Sci, 2014,439–444.
11. Mushtaque M., Dhiman H., Hussain S., Maheshwari S., Evaluation of DES, TDES, AES, bowfsh and twofsh encryption algorithm: based on space complexity. Int J Eng Res Technol (IJERT) ,2014, 1922–1933.
12. Khorsheed N., Khorsheed O., Rashad M., Hamza T. , Proposed encryption technique for cloud applications. Int J Sci Eng), 2015. 693– 698.
13. Thimma B., Bala K., Raghunath S. Cloud security using blowfsh and key management encryption algorithm. Int J Eng Appl Sci (IJEAS) , 2016, 59–62.
14. Salem M., Sabbeh S., EL-Shishtawy T., An efcient privacy preserving public auditing

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.25.41.54

mechanism for secure cloud storage. Int J Appl Eng ,2017,1093–110.
15. Rasmi, M., Multilevel Security in Cloud Computing, International Journal of Engineering Research & Technology (IJERT), 2016
16. Tasleem, S., Vijayaraghavulu, P., A Multi-Level Security Mechanism for Cloud Storage System, October IJIRT Vol. 7, 2020.
17. https://www.eescorporation.com/cloud-computing-statistics/
18. https://ec.europa.eu/eurostat/statisticsexplained/index.php?title=File:Use_of_cloud_computing_services_in_enterprises,_by_purpose,_EU27,_2018_and_2020_(%25_of_enterprises_using_the_cloud).png
19. Noha M., Fatma, O., Nahla, F., A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing, International Journal of Computer Science and Information Security (IJCSIS), 2016.
20. https://msdn.microsoft.com/en-us/library/ff650720.aspx.
21. Gupta, U., Saluja, S., Tiwari, T., Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms, Utkarsh Gupta et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, 2018.
22. Kumar, U., Prakash, J., Secure File Storage on Cloud Using Hybrid Cryptography Algorithm, IJCRT ,Vol 8,2020
23. Thangapandiyan, M., Anand, R., Sakthidasan, K., Enhanced Cloud Security Implementation using Modified ECC Algorithm, International Conference on Communication and Signal Processing, 2018.
24. Santhisri, K., Lakshmi, P., Comparative Study on Various Security Algorithms in Cloud Computing, Recent Trends in Programming Languages, 2015.
25. Khan, S., Yadav, C., Khare, M., Implementing Cryptographic Method for Ensuring Data Security In Cloud Computing Based On Hybrid Cloud, IJSRST, 2018.
26. Timothy, D., Santra, A., A Hybrid Cryptography Algorithm for Cloud Computing Security, IEEE, 2017.
27. Ahmed, Q., Garg, S., Energetic Data Security Management Scheme using Hybrid Encryption Algorithm over Cloud Environment, Turkish Journal of Computer and Mathematics Education, 2021.
28. Issa, N., Cloud Computing Security and Privacy Preservation: Using multi-level encryption, IJEIT on Engineering and Information Technology, 2021.
29. Ramachandran, B., Subramaniam, K., Multilevel Security Framework Based Resource Sharing Using Bilinear Mapping in Cloud Environment, Intelligent Engineering & systems, 2017.
30. Ahmad, N., Cloud Computing: Technology, Security Issues and Solutions, IEEE,2017.
31. Arockiam, L., Monikandan, S., Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm, International Journal of Advanced Research in Computer and Communication Engineering, 2013.