Using the principle of algorithm hybridization to maintain a high level of security in cloud storage

Rasha Muhseen Hadi[1]	, [1]Al-Muthanna University / Agriculture Collage / Iraq rasha.muhseen@mu.edu.iq
Barakat Saad Ibrahim[2]	[2]Al-Muthanna University / Electronic computer center / Iraq barakat.alobaidy@mu.edu.iq
Seror Manea Bahloos[3]	[3]Al-Muthanna University / Iraq seror.manea@mu.edu.iq

ABSTRACT

If the level of security is not in the process of protecting the stored data, then cloud computing security is one of the best options. Quite a few algorithms have been used in many researches for the purpose of cloud computing security. In this manuscript, a hybrid algorithm based on the working principle of an algorithm (ECC) and an algorithm (AES) was used in order to obtain a high amount of protection. In the first part of this manuscript, the study of the concepts of obfuscation and the safety of this technique was discussed, and then we conducted an evaluation process for this algorithm, where the results of hybridization of the algorithms used and when they work together provide additional features that ensure high performance and excellent data protection.

Keywords: cloud computing, algorithm hybridization, data security.

1. Introduction:

One of the technologies that have been used recently is cloud computing technology, which is considered one of the most advanced and most reliable technologies. The nature of this computing can be summarized as follows: it is the possibility of obtaining and accessing information from anywhere and at any time as a central storage swab. This technology can provide a set of services that have been created based on the needs of users[1]. These models mainly include infrastructure, platforms, and software [2]. Although cloud computing is considered a flexible and convenient solution, it still faces some limitations due to security related issues. [3], [4]. There are three basic dimensions related to cloud computing, and they mainly include security (computer, network, information). A computer-related security issue also involves the process of protecting information, hardware, and software as well. Can the system face serious security challenges such as the ability to gain unauthorized access to information, and this is one of the most important challenges facing cloud technology also there is the ability to change customer related data. In addition, the data must be provided to the customer every time without any problem affecting the data storage. [5] He mentioned that the main issue with cloud adoption is security as well as privacy. Obfuscation service providers must ensure the protection of the infrastructure and implement an effective mechanism for the security of customer and application data. [6] It has been stated that the acceptance of the obfuscation technique among different users depends on the level of security. The level of quality assessment of the security of obfuscation service providers is a critical issue.

Security challenges in data obfuscation can lead to a loss of economy and an invalid reputation. For these reasons, users should be more careful when storing information using cloud technology, before transferring data to cloud storage, it must be encrypted [7].

2. Clouding Models:

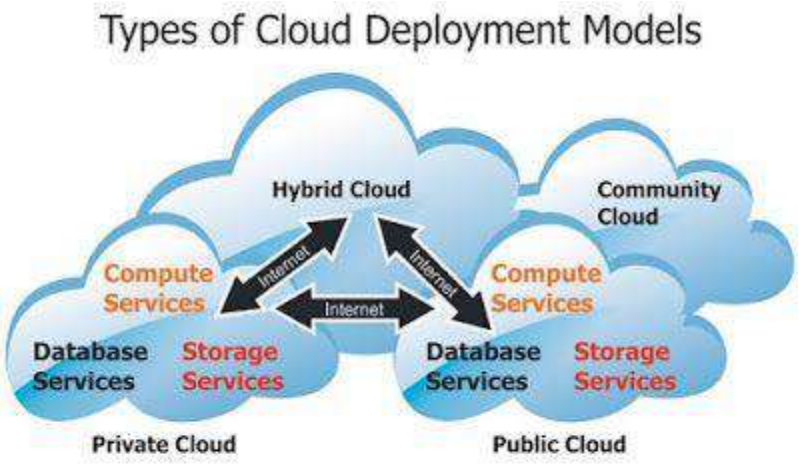
The cloud system has three different model which are commonly used:

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.

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[8].



Fig(1) : The basic models of cloud computing

3. Hybrid encryption 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.

3.1 - Level 1 Advance 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(128,192,256 bit) with (rounds of 10,12,14 keys). The key of privacy

could share only among sender and receiver to access the encrypted information.

3.2- Level 2 ECC algorithm: It protect the data which stored in the cloud environment from eavesdropper and the hackers. It is a public-key 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:

$y^2 + a_1xy + a_3y = x^3 + a_2^2 + a_4x + a_6$ 1

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

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

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. $Rand\ k \coloneqq [1, n-1] \forall k\ \epsilon\ Z$

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.

$Assume\ Ahmad\ sends\ an\ encrypted\ message\ to\ Basi$

ii. $Ahmad\ Plian\_text \coloneqq f(message\ m\ with\ points\ from\ the\ elliptic\ group$

iii. $Ahmad \coloneqq Rand\ k\ [1, p-1] \forall\ k\ \epsilon\ Z$

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

v. $Basil \coloneqq Cipher\_text$

$Encryption\ Algorithm$

$Basil\ decrypts\ ciph\_text$

i= $Basil \coloneqq kB * yB$

$\{pub\_key\ and\ its\ pri\_key\ yB\}$

ii. $Basil \coloneqq (pm + k * PB) - kB * yB, since\ PB: = yB * B, so\ the\ difference\ is\ pm$

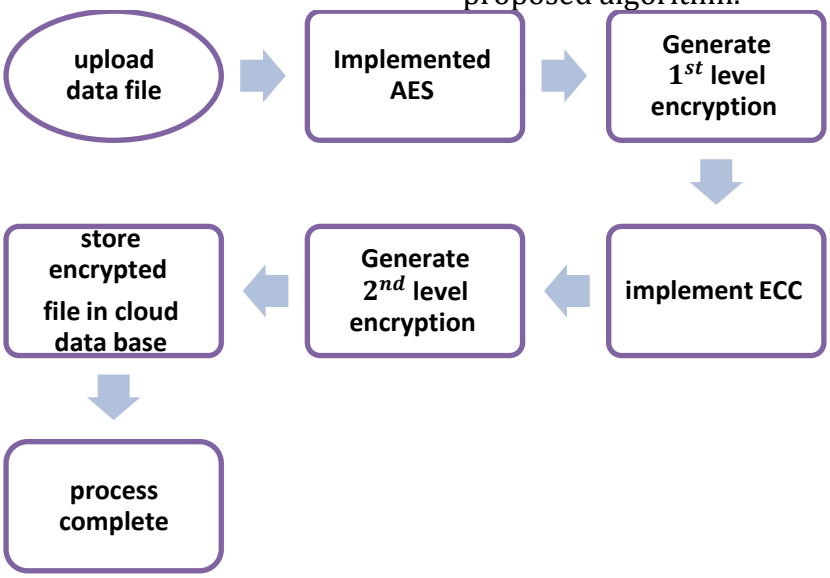
iii.

$finally, Basil\_message\{which\ is\ the\ AES\ cipher\ text$

$decode\ (pm)$

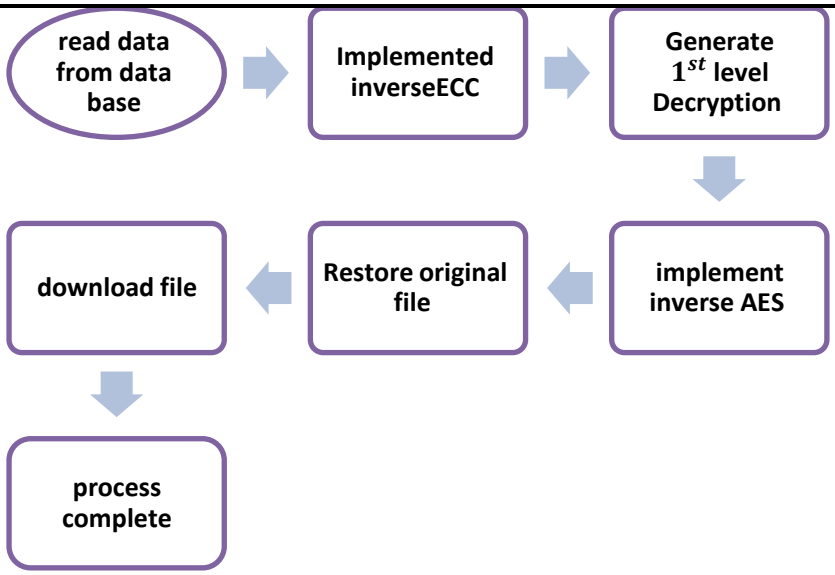
The combination of the two various process ensure the security and mitigate losing the data due to the hackers.

The algorithm AES firstly is implemented and the figure (2) illustrate the block diagram of the proposed algorithm.



fig(2): 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(3) illustrates the block diagram of the process of decryption.



Fig(3): block diagram of the proposed decryption algorithm

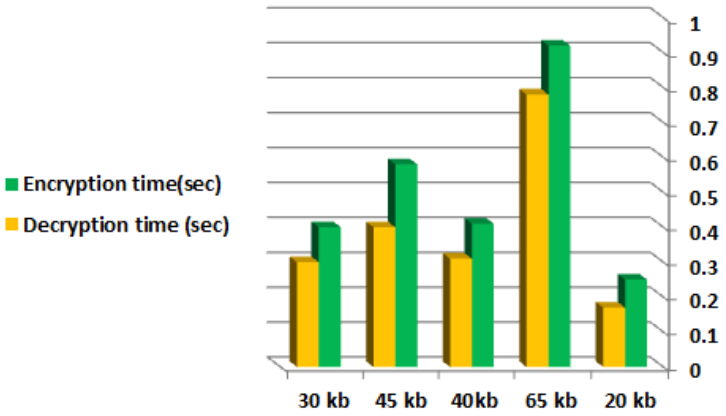
4. The Results of Hybrid algorithm

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 (4) it could be seen that the time is required for encryption is higher than the time which is required for decryption.



Fig(4): Time of encryption, decryption

Table (2) had presented the required time for AES, ECC, and the hybrid for comparison. Fig(5) 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
65 kb	0.90	1.9	1.60
40 kb	0.40	0.8	0.72
45 kb	0.55	1.12	0.98
30 kb	0.40	0.79	0.70
Average-time	0.5	1.046	0.88
Average-size	40	40	40
Throughput	80	38.2	45.4

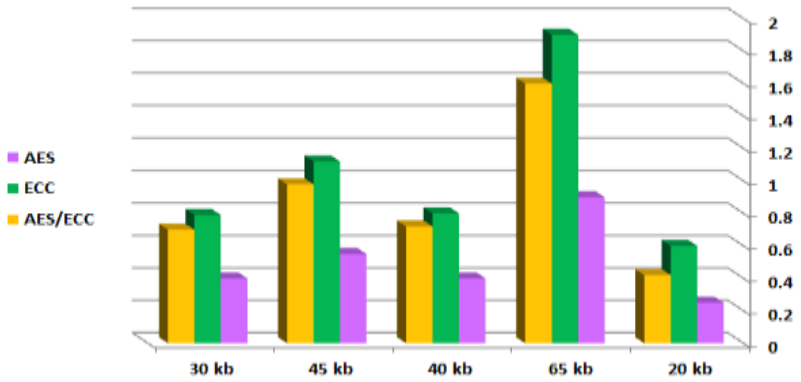


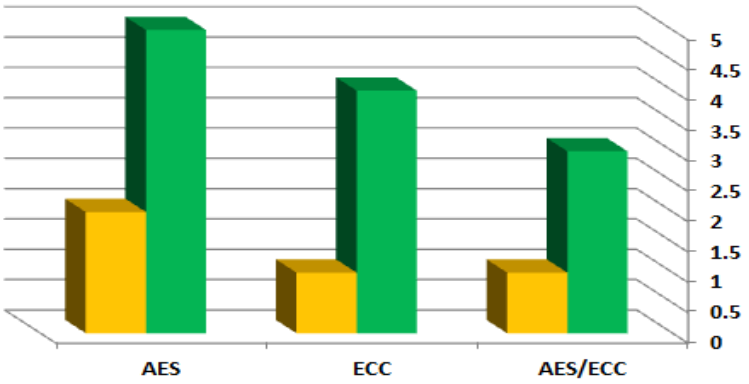
Fig (5): comparison of the required time for the three studied algorithms

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 ECC and higher than AES.

Table 3

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

The results which is summarized by table(3) is represented by fig (6) to show the ratio of each studied algorithm.



Fig(6): The ratio ciphertext/plaintext

Conclusion:

The cloud application is a convenient place to save data, users can access data from anywhere and at any time when data is needed. It is important to pay attention to the issue of security, and this is done by improving the tools and algorithms that we need for this. The results that we obtained in this manuscript show the strength of using the hybrid algorithm as well as obtaining more reliability and efficiency, as well as there is a significant difference in the execution time of operations when using the proposed hybrid algorithm. These results were presented in the form of tables and graphs to compare the difference in the time taken to implement encryption as well as decryption. The proposed algorithm has proven its effectiveness and reliability to protect data from all hackers.

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. Rasmi, M., Multilevel Security in Cloud Computing, International Journal of Engineering Research & Technology (IJERT), 2016.