Journal of Computing and Communication Vol.1 , No.1 , PP. 12-26 , 2022

FHE-Chaos NHCP: Developing a Novel Secure Framework for Cloud Computing Environment

Diaa Salama*[a,b], Elsayed Badr[b], Mostafa Farag[b]

[a]Department of data Science, Faculty of computers , Misr International , University, Cairo, Egypt

[b]Faculty of computer of Computer Science, Misr International University, Cairo, Egypt

*Corresponding author : Diaa Salama **[diaa.salama@fci.bu.edu.eg]**

ARTICLE DATA

Article history:
Received 26 Dec 2021
Revised 1 Feb 2022
Accepted 2 Feb 2022
Available online

Keywords:
Cloud Computing
Encryption,
AES
DES
Fast RSA
Blowfish
FHE.

ABSTRACT

Cloud computing has gained attention in recent years, and it is now used to support many aspects of human life. The amount of data transmitted via the internet is getting bigger and bigger every day. The increasing volume of essential data focuses on securing the stored data in cloud service providers' remote servers. The primary security obstacle in cloud computing is that the users can not directly control the remotely-stored data. Confidentiality is the most crucial problem in the cloud computing environment. Security has the most pressing concern in the cloud computing environment, and encryption plays a vital role in securing data. The existing methods encrypt the stored data using standard encryption algorithms without achieving the desired confidentiality level. Both symmetric and asymmetric encryption algorithms have some drawbacks. This paper proposes two-hybrid algorithms to overcome these drawbacks and ensure data confidentiality. The first is a hybrid between the Blowfish (symmetric) and Fully Homomorphic Encryption (FHE) symmetric algorithm. However, the second hybrid is the FastRSA (asymmetric) and the FHE symmetric algorithm. By comparing our proposed algorithms with other cryptographic methods, they have less encryption time than AES and Blowfish algorithms. A comparison is performed based on encryption time, throughput, and power consumption parameters. Compared with other encryption algorithms, the proposed method proved superior in processing time efficiency.

1. Introduction

Cloud computing is gaining steam, owing to a combination of factors related to the industry and technology. Rapidly changing market conditions are forcing many businesses to upgrade their computing infrastructure. The number of business resources and software is continuously growing, with new ones and eliminating old ones. Cloud computing is a type of Internet-based computing that provides shared computing resources and data to computers, servers, and other devices on demand. Cloud also utilizes a pay-as-you-go model to deliver services and support to many customers. Cloud computing is a preferred model for many organizations as it offers many benefits. These benefits include scalability, data security, and collaboration. Scalability means that cloud infrastructure scales on-demand to deliver many services. Data security means networked backups can prevent hardware failures in the cloud environment. The partnership means that teams can collaborate from popular locations. [1,2]

The cloud's three service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), are depicted in Figure 1. (SaaS). IaaS is a cloud computing service that enables the Management of all aspects of the cloud, from servers to storage and virtual machines. VMware and Hyper-V Hypervisor are both IaaS examples. PaaS is a software-as-a-service platform for executing, operating and deploying applications. It provides network-based services. Microsoft Azure is an example of PaaS. SaaS is a set of cloud-based software applications offered to customers and consumers. An example of SaaS is Google Apps. [1]

The cloud service models are alternative candidates to the traditional model. However, prove suggests that despite cloud computing being viewed as an essential business avenue for the coming years, security issues hamper migration to the cloud paradigm. Many financial institutes are attracted to cloud computing.

However, they are still in the early stages of adoption for security reasons. Around 50 million Dropbox user accounts were hacked in 2014 [2]. Recent cloud-based assaults demonstrate that cloud data security has risen to prominence. Al Awadhi et al.[3] have provided proof of the cloud's vulnerability to threats. They used honey pots to demonstrate the vulnerability of the cloud system and that it is the subject of several attacks from various countries. [4]

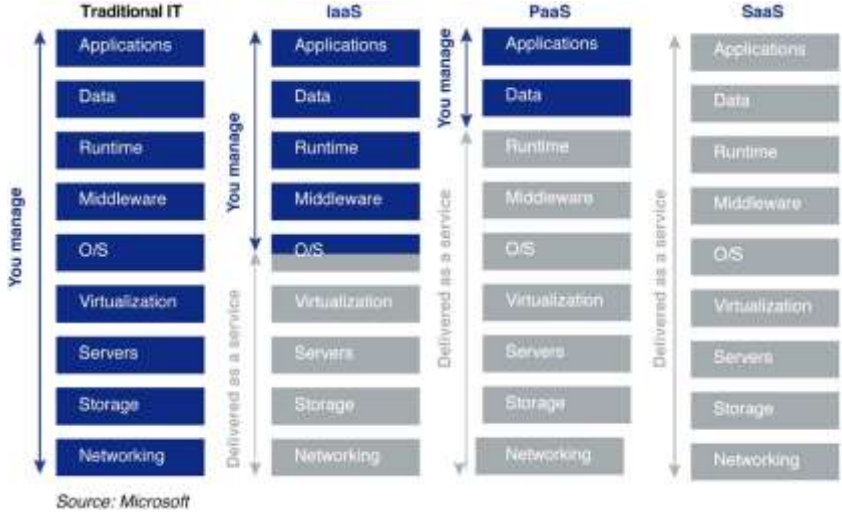


Figure 1. Cloud Service Models vs. Traditional Model

For cloud computing to be viewed as a feasible alternative, it must provide (at least) the same level of security as traditional IT models. To attain this goal, more attention is needed on tools and measures that are currently available to reverse malicious actions. Many works in the literature propose surveys of protection mechanisms implemented in cloud infrastructures [4-8]. To the best of our knowledge, however, they all give a partial view of the problem: some identify only the countermeasures taken by a particular provider and on a specific platform (i.e. [6]), others focus on security methods that can be used in different environments (i.e.[7]). In contrast, others limit their research to open-source cloud applications (i.e., [8]).

Data security is a growing concern for any technology. Yet when applied to an unregulated environment such as cloud computing, it becomes a significant challenge. This research focuses on a snapshot of cloud computing data protection problems. Its goal is to highlight the critical issues posed by the cloud environment relating to data protection. Issues related to data protection attributes are (confidentiality, integrity, and availability). [5] Confidentiality is necessary for cloud computing to ensure that authenticated users can get the right information. Confidentiality classifies information as top secret, confidential, personal, and public. Another area of concern is data location. This implies the storage of users' data on remote servers. Data location has a detrimental effect on data protection in the cloud computing environment, as it might reach all parties. This research aims to establish data secrecy by efficiently encrypting data using a hybrid encryption method. [6,7]

There are two types of encryption algorithms: symmetric and asymmetric key algorithms. Symmetric key algorithms, such as DES, AES, FHE, and Triple-DES employ the same key for encryption and decryption. [10]. Asymmetric key algorithms use two keys for encryption and decryption: public and private keys. Asymmetric key algorithms include the RSA, Diffie-Hellman, and Fast Cloud-RSA. Symmetric algorithms are faster than asymmetric algorithms and provide increased security because the secret key system can decrypt just one message. On the other hand, symmetric algorithms have several disadvantages, including key transportation, as the key is conveyed to the receiving system before sending the message. [9]

Homomorphic encryption performs computations on plaintext to obtain ciphertext, as well as it is a suitable encryption algorithm for the cloud computing environment.

Blowfish is a similar-looking encryption method to DES. It is a block cipher with a variable-length key that is symmetric. It is a Feistel cipher with a 16-round key and employs S-boxes. Five subkey arrays are present: one P-array with 18 entries and four S-boxes with 256 entries (S0, S1, S2, and S3). The Blowfish's anatomy is depicted in Figure 2 [11-12].

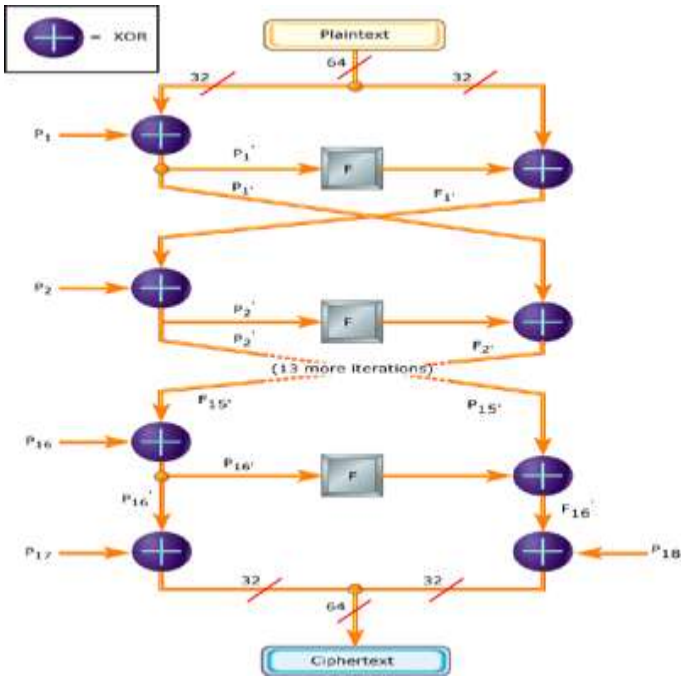
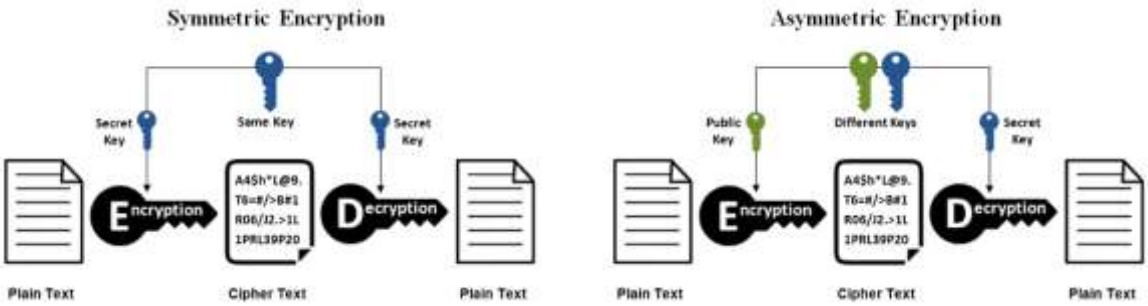


Figure 2. Structure of Blowfish

According to the cloud security perspective [13], insecure interfaces, data loss, and hardware failure are the three most significant concerns. One of the difficulties associated with symmetric key algorithms is the problem of trust. The term "trust" refers to the process of ascertaining the integrity of data. The data is hashed in this issue, and the resulting hash is encrypted with an asymmetric encryption technique utilizing a secret key. The recipient will receive the encrypted hash value and data. The recipient then decrypts the hash value using the shared key and compares the result to recalculating the hash value on the received data. This provides security, as only those with access to the secret key can correctly encrypt the hash of the original material.

Data loss is one of the threats that face asymmetric key algorithms. Data loss is any process that results in data being damaged, removed, and made unreadable by a user. Data loss is referred to as data leakage.

On the other side, asymmetric encryption was invented to overcome the inherent problem. The symmetric encryption method shares the key, leading to the need to share the key by using a private and public key. Figure 3 shows the two types of encryption algorithms.



(a) Symmetric Encryption (b) Asymmetric Encryption

Figure 3. Encryption algorithms types

2.1. Evaluation Metrics

its histogram is consistent. The logical XOR operation is used to mask pixels. The image is masked using a diffusion key XM in such a way that

$$X_M = X mod 256 \quad (1)$$

Confusion and diffusion are key properties of chaos theory, and any powerful cryptosystem should consider these elements. Chaotic synchronization is a particular kind of chaotic system. The shift map is denoted by the following:

$$x(t+1) = \mathrm{ax}(t)(mod1) \quad (2)$$

The phase space X = [0, 1] is the unit interval, and a>1 is an integer. 1-D chaotic maps can produce a chaotic sequence that can control the encryption process.

A permutation of plain-image pixels decreases the high correlation among the nearest pixels. The logistic map produces chaotic sequences and then sorts them ascendingly to generate a permutation key. The logistic map's remarkable simplicity is a great candidate for inclusion in the chaos theory notion.

The following equation can express a chaotic system:

$$\mathrm{X_{N+1}} = 10\mathrm{X_N}(mod1) \text{ where } 0 \leq \mathrm{X_N} \leq 1 \quad (3)$$

Due to its potential for encrypting digital multimedia, image encryption algorithms based on chaotic maps have garnered great interest. Numerous chaotic map-based picture encryption techniques have been presented. The Chaotic-Key-Based Algorithm (CKBA) is a one-dimensional logistic map-based algorithm. CKBA is a block cipher that performs value transformation.

The remainder of this article is structured as follows. The next section provides an overview of some relevant projects. Section 3 discusses our proposed method. In Section 4, we present the findings. Section 5 summarises our findings. Finally, we discuss our findings.

2. Literature review

In [14], the ciphertext encryption is accomplished using a Fully Homomorphic Encryption (FHE) technique. The technology was designed to provide data confidentiality and location for cloud-based data storage. The suggested system is composed of a cloud server, a node controller, and an admission controller. The suggested system's findings were compared to those obtained from CAST-128; the proposed system's results have lower complexity than those obtained from CAST-128.

In [15] suggested a straightforward and secure file upload and download technique based on AES. Encrypts the AES key using the RSA technique. The model proposed addresses the issues of data integrity and privacy. The suggested model comprises a cloud server, a host, and a host 2. When file upload and download times are compared, it is discovered that file upload takes less time than a file download.

In [16] presented a fast variant of the cloud RSA technique to reduce the time required for encryption and decoding significantly. The proposed technique was designed to address the problem of data secrecy by encrypting data with FastRSA. The suggested approach employs the form N = pr qs to generate decrypted data and uses the integers' multiplicative property.

Compared to cloud-RSA encryption, the proposed approach requires less time for encryption and decryption.

In [17] , The proposed approach addressed the problem of data localization for cloud-based data storage. To achieve data safety, uses a combination of the DES and CAST encryption algorithms. The suggested approach has a higher complexity and encryption time than the individual DES and CAST algorithms.

In [18], a novel symmetric encryption technique with the smallest computational overhead was suggested. Compared to AES results, the suggested approach requires less time to encrypt. The proposed system addressed the problems of data integrity and location. The system is comprised of a client that encrypts data and stores it in cloud storage, as well as a cloud server that acts as a bridge between the cloud platform and cloud storage.

In [19], a multi-cloud strategy was employed to address data loss and privacy breach issues. The proposed strategy addressed data confidentiality.Before data is sent to the cloud, the suggested approach encrypts it using RSA.Two clouds comprise the system: one for application logic and another for data logic. Compared to the conventional way, the new method provided increased security, integrity, and confidentiality.

In [20] conducts a comprehensive survey of cloud computing privacy issues. The system proposed that only authenticated users have access to private data, protecting against service attacks.

In [21], they established a security strategy that uses a capability-based access control method to ensure that only authorized users access outsourced data. However, the technique shared a symmetric key with users for safe data access.

The hybrid encryption algorithm established a novel fusion technique by integrating the vigenere and Base64 encryption algorithms [22]. The modified vigenere encryption algorithm is used, followed by the Base64 encryption

algorithm. By inputting plain text, the first encryption algorithm creates a ciphertext. Second, the improved Vigenere encryption technique requires the definition of a key. A second ciphertext will now be created using this key.

In [23]; authors use Blowfish with varying round counts to improve security and minimize hacking. The recursive blowfish algorithm provides greater security than the conventional blowfish approach. The suggested algorithm has a variable number of rounds for encrypting files.

[24] focuses on storing data encrypted in a completely homomorphic way on cloud computing. Amazon Web Service's DynamoDB is used to store the data (AWS). A user's computation is carried out on ciphertext in the public cloud.

In [25], system-level operations include system initialization, new file creation, new user grant, user revocation, file access, and file deletion. It incorporates three security techniques: Encryption based on key policy attributes, proxy re-encryption, and lazy re-encryption.

In [26], the SecCSIE flexible system architecture was developed for integrating multiple types of cloud storage providers with the employee's computer while maintaining data security. The proposed architecture is adaptable and centered on a proxy server that encrypts and distributes any outsourced files before leaving the internal network. Additionally, it ensures the security, integrity, and accessibility of data.

In [27] proposes a novel data security paradigm. The data is segmented into bits. Every two blocks of data are subjected to the genetic algorithm. Each genetic algorithm produces a ciphertext as its ultimate output, composed of two blocks of bits. Each ciphertext is uniquely saved in the cloud.

In [28] proposed a straightforward cloud computing security paradigm. It encrypted user data before launching in the cloud, using the AES method.

In [29], encryption operations on ciphertext are performed using private and public keys via the setup, keygen, and decrypt algorithms. It uses two-party computation (2PC) protocols to ensure security between the Key Generation Center and the data storage center.

In [30] Cloud security is enhanced by using the ElGamal algorithm, which enables two-level encryption of ciphertext (first and second levels). The encryption procedure occurs on the data owner's side; the CSP acts as an intermediary between the data owner and the data user; the CSP re-encrypts the ciphertext using the re-encryption key. This eliminates the possibility of collusion attacks.

Also , other related work can found in [46-56] have been proposed in recent years to address cryptography and security of cloud computing

3. Proposed Model

Our approach is based on the combination of two hybrid encryption techniques. A hybrid algorithm's purpose is to encrypt data, reducing encryption time efficiency. In a hybrid cryptography algorithm, four encryption techniques were combined. Two of these algorithms are hybrid and are used to increase the security and speed of encryption techniques. Because it encrypts data twice, a hybrid encryption algorithm protects. Because it separates plaintext into two halves, it has the advantage of lowering encryption time. We merged an asymmetric method with another asymmetric algorithm to ensure great security. The first proposed algorithm combines the symmetric Blowfish and fully homomorphic encryption (FHE). On the other hand, the second algorithm combines the FastRSA (asymmetric) and FHE (symmetric) algorithms. We first introduce the proposed algorithm for encrypting image files.

Proposed Encryption Algorithm for encrypting image files

Input: I an image
Output: $\bar{I}$ encrypted image
Method:

Step 1: The image I is treated as an array of bytes.
Step 2: Initialize key k with an integer number from 1 to 50
Step 3: for each *value i* in the *image I*
$\bar{I} = i$ XOR k
Step 4: Save the encrypted image $\bar{I}$ in a new file

Table 1: comparison between different security frameworks

	[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]	[40]	[41]	[42]	[43]	[44]	[45]
Parameter	FHE	Multi-cloud	Secure cloud model	probabilistic encryption	Fast RSA	Proposed symmetric algorithm	Proposed model	Hybrid DES&CAST	Recursive blowfish	Homomorphic Encryption	ElGamal	New security framework	Data splitting mechanism	homomorphic token and error-correcting codes	Protection model
Algorithm used	Homomorphic Encryption	RSA	AES and SHA	probabilistic encryption	Fast RSA	Symmetric algorithm	AES	DES&CAST	Enhanced Blowfish	Homomorphic Encryption	ElGamal	Genetic algorithm	AES	homomorphic token and error-correcting codes	AES
Applied security on cloud	Yes	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes
Used chaos theory	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Used hybrid algorithm	No	No	Yes	No	No	No	No	Yes	No	No	No	No	No	No	No
Performance	Complexity less than CAST-128	More secure when compared to regular system	Less processing time	Less encryption time when compared to AES and DES	Less encryption time when compared to cloud RSA	Less encryption time when compared to AES	file upload has less time than a file download	High encryption time when compared to DES	More secure than standard Blowfish	More secure	More secure	More secure and efficient	Safer than similar methods	Safer	More secure

Hashing

Hashing is described as converting a sequence of characters into a shorter fixed-length value that accurately replicates the original sequence. Figure 4 illustrates the principle of hashing..

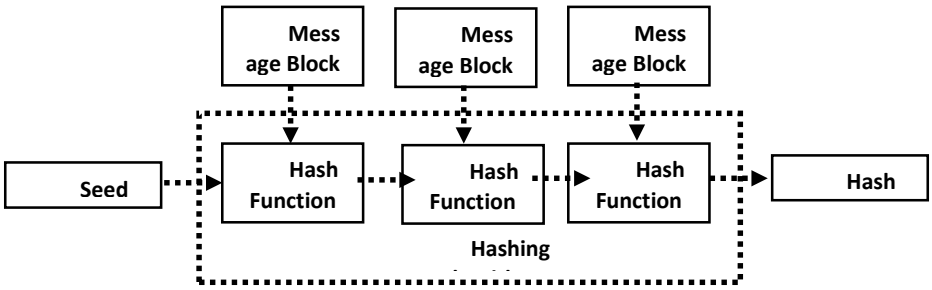


Figure 4. Hashing

Secure Hash Algorithm (SHA) is considered a robust hash algorithm that outputs a 160-bit message digest. This feature makes it a more secure algorithm.

1.1 First Hybrid algorithm using FHE & Blowfish (Fig.5)

1. the plaintext is divided into plaintext1 and plaintext2
2. FHE is used to encrypt plaintext1 generating ciphertext1
3. The MD5 hash function encrypts Ciphertext1
4. FastRSA encrypts the FHE key
5. Blowfish is used to encrypt plaintext2 generating ciphertext2
6. The MD5 hash function encrypts Ciphertext2
7. Dual RSA encrypts blowfish key
8. Ciphertext1 and ciphertext2 are combined into ciphertext

The proposed algorithm for the first hybrid algorithm is shown as follow

Proposed Encryption Algorithm

Input: *M (Plain text), k(secret key of Blowfish encryption), s(128-bit size of the block);*

Output: *C (Ciphertext), c_i (encrypted text using Blowfish), C_i (encrypted text using FHE), D (Hashing value of ciphertext);*

Method:

1. *n =M/s ;*
2. *le t i=0;*
3. *do{*
4. *$m = \sum_{i=0}^{i=\frac{n}{2}-1}(Bi)$ the first part of plain text; what is m and where it is used, what is B_i*
5. *for(j=0;j<= n-1;j++)*
6. *{*
7. *$K_j = FastRSA_{enc}\ (TC_{PK}, k_{i-1})$;*
8. *}*
9. *$c_i = E_{Blowfish}(K_j, B_i)$;*
10. *$d_i = MD5\ (c_i)$;*
11. *i++;*
12. *}*
13. *while(i<n/2);*
14. *i=(n/2)*
15. *let K be a private key of FHE*
16. *do{*
17. *$M = \sum_{i=n/2}^{i=n}(Bi)$ the second part of plain text which encrypted simultaneously with the first part;*
18. *for(j=0;j<= n-1;j++)*
19. *{*
20. *$K_j = DualRSA_{enc}\ (TC_{PK}, k_{i-1})$;*
21. *}*
22.
23. *$C_i = E_{FHE}(K_j, B_i)$;*
24. *$D_i = MD5\ (C_i)$;*
25.
26. *i++;*
27. *}*
28. *while(i< n);*
29. *$C = c_i + C_i$;*
30. *$D = d_i + D_i$;*

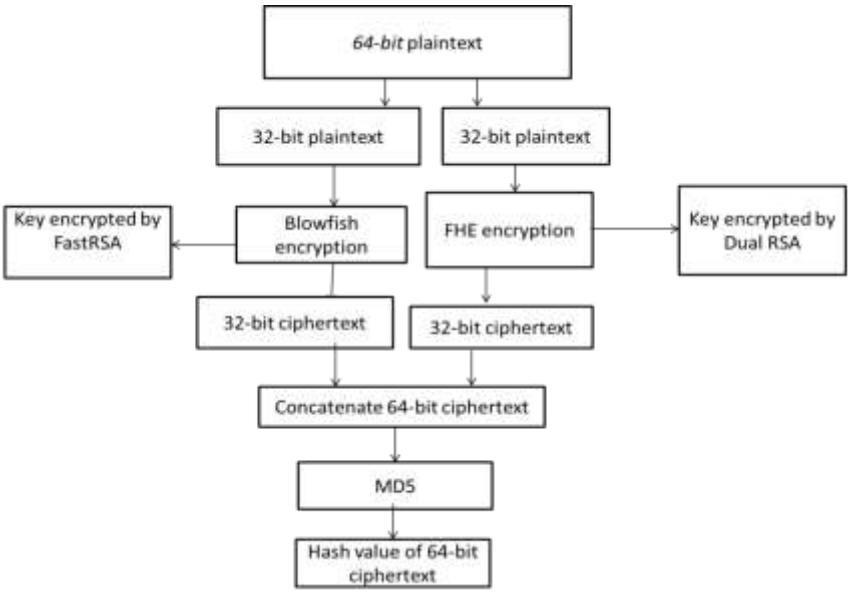


Figure 5. First Hybrid Algorithm using FHE and Blowfish

1.2 *Second Hybrid algorithm using FHE & FastRSA (Figure.6)*

1. the plaintext is divided into plaintext1 and plaintext2
2. FHE is used to encrypt plaintext1 and plaintext2, resulting in ciphertext1 and ciphertext2
3. FHE key is encrypted by Elliptical Curve Cryptography (ECC) and Dual RSA algorithms
4. FastRSA is used to encrypt ciphertext1 and ciphertext2, resulting in ciphertext3 and ciphertext4
5. Ciphertext3 and ciphertext4 are encrypted by Message Digest-5 (MD5) and SHA hash functions
6. Ciphertext3 and ciphertext4 are combined into ciphertext

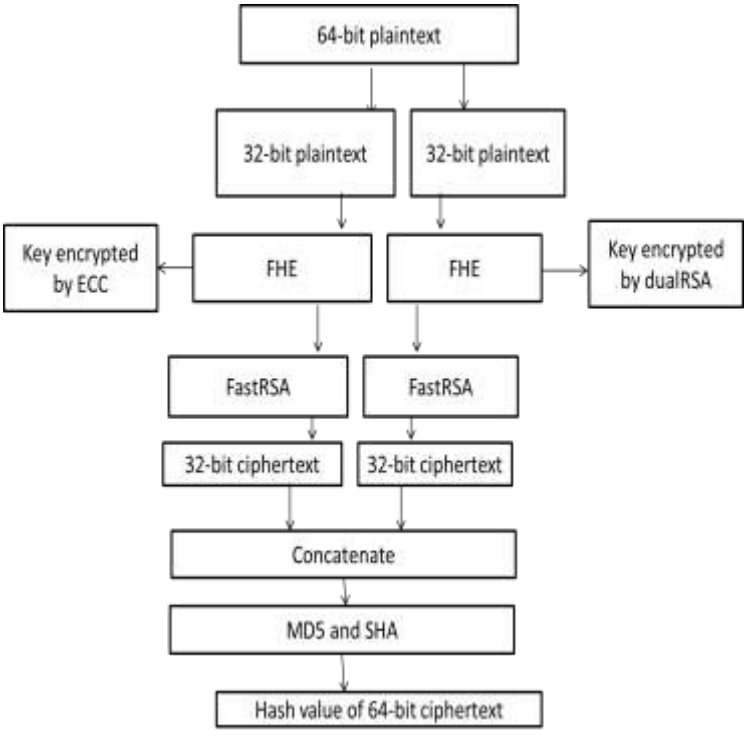


Figure 6. Second Hybrid Algorithm using FHE and FastRSA

4. Evaluation Metrics

Several performance criteria are utilized to evaluate the proposed technique, including encryption time, throughput, battery life, and accuracy.

- ***The encryption time*** is defined as the time required for an encryption algorithm to convert plaintext to ciphertext. The encryption time is employed to determine the throughput of an encryption technique. It represents the encryption's speed.

- ***The throughput*** *of the encryption scheme* is calculated as in equation (4).

$$\boldsymbol{Throughput} = \frac{T_p}{E_t} \quad \textbf{(4)}$$

Where T_p: total plain text (bytes) and E_t: encryption time (second)

• CPU process time is the amount of time that a CPU is dedicated exclusively to a single calculation activity. It reflects the CPU's burden. CPU clock cycles are a measure that indicates how much energy the CPU consumes when performing encryption processes. Each CPU cycle consumes a negligible amount of energy.

- **Measurement of Energy Consumption**
- ***Energy consumption***: There are numerous approaches to quantify the energy consumption of security primitives. The method utilized can be quantified by counting the number of processor cycles consumed by cryptographic computations. We employ the same procedures outlined in the following equations to determine the energy cost of encryption.

$$\mathbf{B_{cost\_encryption}\ (ampere\text{-}cycle) = \tau * I} \quad \textbf{(5)}$$

$$\mathbf{T_{energy\_cost}\ (ampere\text{-}seconds)} = \frac{B_{cost\_encryption}(\text{ampere - cycle})}{F(\text{cycles/sec})} \quad \textbf{(6)}$$

$$\mathbf{E_{cost}\ (Joule) = T_{energy\_cost}\ (ampere\text{-}seconds)*V} \quad \textbf{(7)}$$

Where

$\mathbf{B_{cost\_encryption}}$: a basic cost of encryption (*ampere-cycle*).
$\boldsymbol{\tau}$: the total number of *clock cycles*.
I: the *average current* is drawn by each CPU clock cycle.
T_{energy_cost}: the total energy cost (ampere-seconds).
F: clock frequency (cycles/sec).
$\mathbf{E_{cost}}$ **(Joule)**: the energy cost (consumed).

We can compute the energy consumption of cryptographic functions by considering the cycles, the CPU's operating voltage and the average current is drawn during each cycle. For example, on an Intel 486DX2 CPU, each cycle requires around 270 mA [46-50] or 180 mA on an Intel StrongARM processor [47]. According to a sample calculation, encryption with 20,000 cycles would require approximately 5.71 x 10-3 mA-second or 7.7 Joule on a 700 MHz CPU operating at 1.35 Volt. Thus, the quantity of energy consumed by program P to accomplish its objective (Encryption or decryption) is equal to.

$$\mathbf{E = V_{CC} \times I \times N \times \tau} \quad \textbf{(8)}$$

Where *N*: the number of clock cycles.
$\boldsymbol{\tau}$*:* the clock period.
$\boldsymbol{V_{CC}}$*:* the supply voltage of the system
I*:* the average current in amperes drawn from the power source for *T* seconds.

Because both VCC and are fixed for a given piece of hardware, E I N. At the application level, it is more meaningful to talk about T than it is to talk about N. Hence, we express energy as E I T. Because Vcc is fixed for a specific piece of hardware [51-56].

The accuracy of classification models is one of the metrics used to evaluate them. Accuracy is the percentage of correct predictions made by our model. Accuracy equals the number of correct predictions divided by the total number of forecasts (9)

- **Accuracy:** it measures the correctness according to the following

$$\mathbf{Accuracy = (TP+TN)/\ (TP+TN+FP+FN)} \quad \textbf{(9)}$$

Where TP = True Positives, TN = True Negatives, FP = False Positives, and FN = False Negatives.

Performance Evaluation

Algorithms are implemented using a python programming language in Windows-10, the 64-bit operating system on a 2.20 GHz processor using 8GB RAM to analyze their performance. Seven texts with different file sizes range from 50 KB to 5 MB. The

seven text files of various sizes are used to carry out the experiment, where we evaluate the performance of different algorithms AES, Blowfish, FastRSA, DES, and two hybrid algorithms. The experiments are conducted on the test system. These implementations are thoroughly tested and are optimized to give the maximum performance for each algorithm. The performance of these algorithms is evaluated based on parameters like encryption time, throughput, and power consumption.

4.1 Time of Encryption and Decryption Processes

The encryption time is required for an encryption algorithm to generate a ciphertext from plaintext. The decryption time is required for a decryption algorithm to reconstruct the plaintext from the ciphertext.

It is demonstrated that the first and second hybrid cryptography algorithms achieve more secure encryption than AES and DES. Table 2 and Figure 7 illustrate the time required to encrypt various chunks of plain text. Table 3 and Figure 8 illustrate the time required to decrypt various sizes of plain text. As with encryption, it is obvious that the first and second hybrid cryptography algorithms obtain a faster decryption time than AES and DES.

Table 2: Encryption time in seconds for text encryption

File size in KB	AES	Blowfish	FastRSA	DES	Hybrid (FHE+ Blowfish)	Hybrid (FHE+ FastRSA)
50	0.26	0.01	0.013	0.11	0.06	0.065
100	0.5	0.02	0.029	0.17	0.07	0.075
200	0.6	0.03	0.035	0.27	0.08	0.085
300	0.7	0.04	0.042	0.37	0.09	0.095
500	0.9	0.06	0.062	0.57	0.11	0.115
1 MB	1.3	0.08	0.082	0.9	0.13	0.135
3	3	0.1	0.12	2.6	0.16	0.165

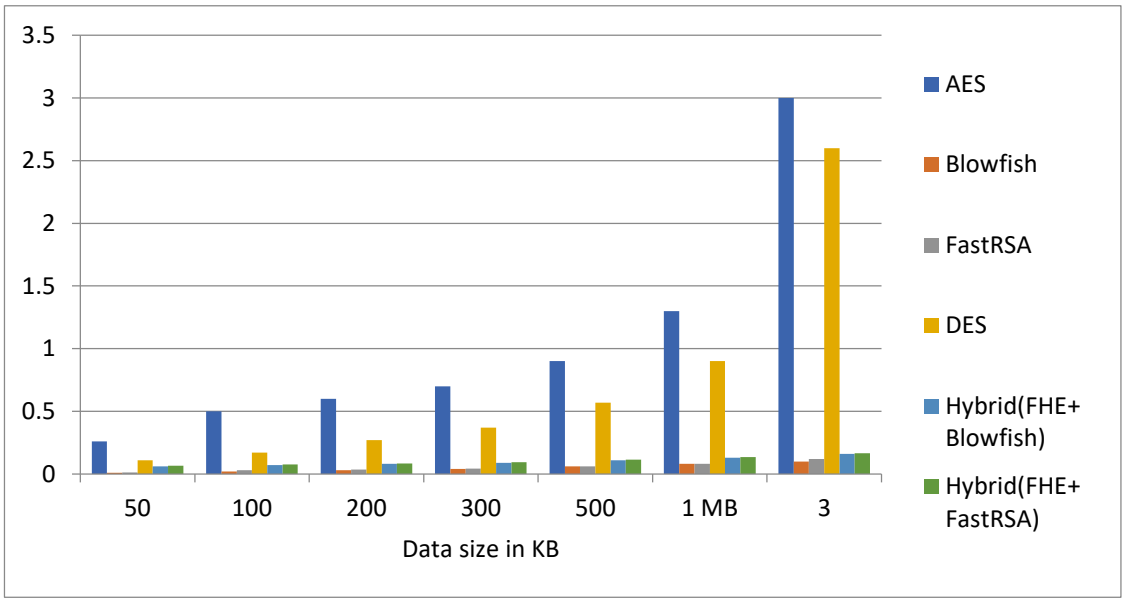


Figure 7: Encryption time of cryptographic algorithms

Table 1: Decryption time in seconds for text encryption

File size in KB	AES	Blowfish	FastRSA	DES	Hybrid(FHE+ Blowfish)	Hybrid(FHE+ FastRSA)
50	0.23	0.008	0.011	0.09	0.05	0.055
100	0.47	0.018	0.027	0.15	0.06	0.065
200	0.57	0.028	0.033	0.25	0.07	0.075
300	0.67	0.038	0.04	0.35	0.08	0.085
500	0.87	0.058	0.06	0.55	0.1	0.105
1 MB	1	0.078	0.08	0.88	0.12	0.125
3	2.7	0.08	0.1	2.58	0.15	0.155

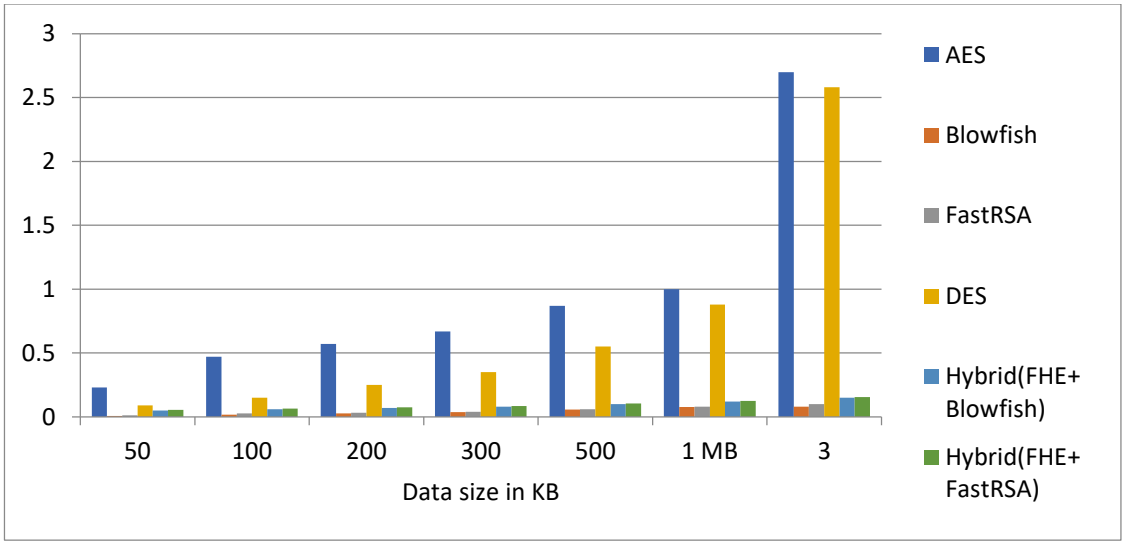


Figure 8: Decryption time of cryptographic algorithms

4.2 Throughput

Divide the file size in kilobytes by the average encryption time in seconds to find the encryption algorithm's throughput [34, 35]. The algorithm's performance is expressed in kilobytes per second.

The encryption time of a system is used to determine its throughput. It denotes the encryption's speed. The encryption throughput of the first hybrid cryptography method is shown in Table 4, and the second hybrid cryptography technique outperforms AES and DES for various amounts of plain text.

Table 4: Encryption Throughput (KB/second) of cryptographic algorithms for text encryption

File size in KB	AES	Blowfish	FastRSA	DES	Hybrid(FHE+ Blowfish)	Hybrid(FHE + FastRSA)
50	192	5000	3846	454	833	769
100	200	5000	3448	588	1428	1333
200	333	6667	5714	741	2500	2353
300	428	7500	7143	811	3333	3158
500	555	8333	8621	877	4545	4348
1 MB	769	12500	13513	1111	7692	7407
3	1000	30000	33333	1154	18750	18182

4.3 Power Consumption

Table 5 , and Figure. 9 shows the power consumption for different sizes of plain text. It is shown that the first hybrid cryptography algorithm and the second hybrid cryptography algorithm achieve power consumption less than AES and DES.

Table 5: Power consumption (watt) for encryption of different cryptographic algorithms

File size in KB	AES	Blowfish	FastRSA	DES	Hybrid(FHE + Blowfish)	Hybrid(FHE + FastRSA)
50	1.7	0.07	0.086	0.73	0.396	0.429
100	3.3	0.13	0.19	1.12	0.462	0.495
200	3.96	0.2	0.23	1.78	0.528	0.561
300	4.62	0.26	0.28	2.44	0.594	0.627
500	5.94	0.4	0.41	3.76	0.726	0.759
1 MB	8.6	0.53	0.54	5.94	0.858	0.891
3	19.8	0.66	0.79	17.16	1.056	1.089

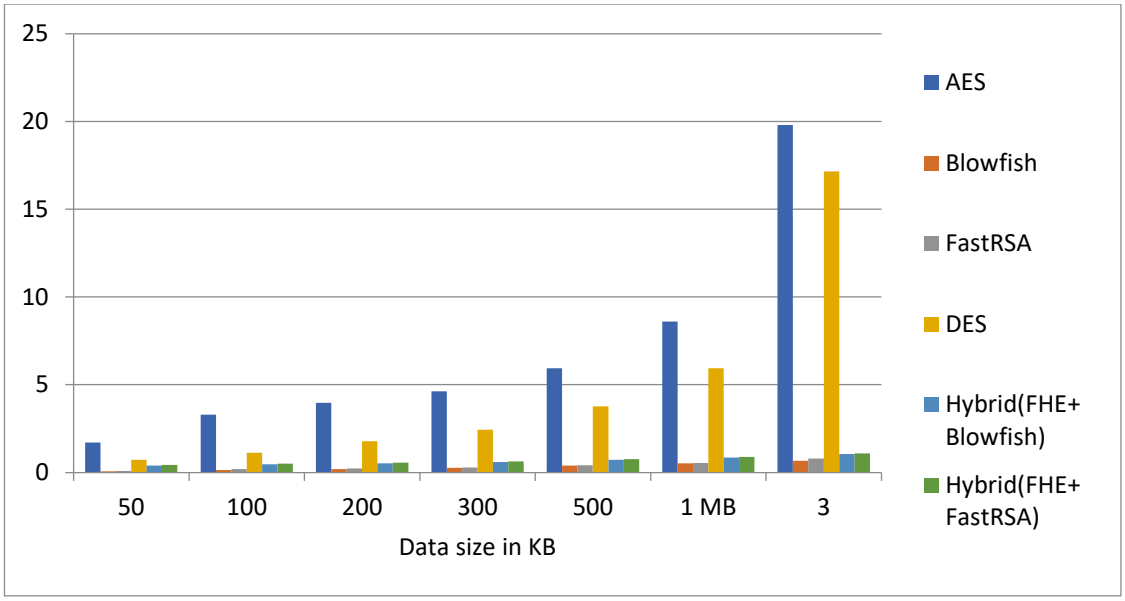


Figure 9: Power consumption of cryptographic algorithms

Table 6 shows the encryption time of cryptographic algorithms for encrypting images.

Table 6: Encryption time in seconds for image encryption

Image size in KB	AES	Chaotic	Proposed
10	10	0.02	0.01
20	12	0.03	0.015
30	14	0.04	0.02
50	16	0.05	0.025
60	18	0.06	0.03

Table 7: Throughput (KB/second) of cryptographic algorithms for image encryption

Image size in KB	AES	Chaotic	Proposed
10	1	500	1000
20	1.67	666	1333
30	2	750	1500
50	3	1000	2000
60	3.33	1000	2000

is how they come up with the diagnosis: The pathologists who do histopathology are the only ones who can help patients choose the right treatment plans. Because of the variety and complexity of the tests, breast cancer types, and the di erences in pathologists' skills, the histopathology process could lead to a lot of wrong conclusions [12]. Automating this complicated and time-consuming process is very important because it reduces opportunities of misdiagnosing people, prevents Patients to wait for a long time for the test and helps the pathologists have a lot of work to get the results and start the right treatment plans.

The fundamental contribution of this research is to present a method that uses Deep Learning techniques to automate the histology procedure. The worrisome lesion observed on the microscope biopsy images is detected using this method.These lesions are to be classified into Benign, Breast Cancer Invasive Ductal Carcinoma, or Ductal Carcinoma In Situ. To automate a system like our suggested approach, there have been a number of attempts and trial [13]. The paper's most significant contribution is as follows. A deep learning algorithm is first used to identify breast cancer from biopsy microscope pictures. Vgg16, Resnet50, Inception, Alexnet, Resnet101, and Densenet169 are some of the deep Convolution Neural networks (CNNs) that we use to analyse the data. We test our hypothesis on the BACH dataset, which contains 400 histopathological pictures divided into four

categories, Normal, Benign, Invasive Carcinoma, Carcinoma In-Situ [14].The images are first preprocessed using several approaches, such as data augmentation, segmentation, and Patching. We also present an ensemble strategy to improve the classifiers' accuracy.

This paper is organised as follows: Section 2 gives overview about CNN and classification evaluation metrics. Section 3 discusses related research e orts in breast cancer diagnosis. Section 4 discusses the research methodology. Section 5 discusses experimental results. Finally,section 6 concludes the paper.

5. Results analysis

It is shown from experimental results that the first hybrid algorithm (FHE & Blowfish) has an encryption time near Blowfish as it divides plaintext into two parts, reducing encryption time and data size. The first hybrid algorithm also provides high security.

The second hybrid algorithm (FHE & FastRSA) encrypts data by two algorithms and has encryption timeless than AES and DES. It is more secure than the first hybrid algorithm.

In the case of encryption (where the identical data is encrypted using DES and AES), it is discovered that the first hybrid method consumes approximately 23% of the time consumed by AES and 54% when compared to DES). Additionally, it is worth noting that the second hybrid method consumes around 25% of the time required for encryption compared to AES and 59% when compared to DES.

In the case of decryption, it is discovered that the first hybrid algorithm consumes around 22% of the time that AES consumes and 55% of the time that DES consumes in contrast). Additionally, it is worth noting that the second hybrid technique consumes around 24% of the time required by AES and 61% when compared by DES).

In terms of encryption throughput, it is determined that the first hybrid method consumes around 4.3 percent of the total throughput (compared to 1.8 percent for AES and 1.8 percent for DES). Additionally, it is worth noting that the second hybrid algorithm consumes around 4% of the throughput consumed by AES and 1.69 percent when compared to DES).

In terms of power consumption, it is discovered that the first hybrid algorithm consumes around 23% of the power consumed by AES and 54% when compared by DES). Additionally, it is worth noting that the second hybrid algorithm consumes around 25% of the power needed by AES and 58% when compared to DES).

6. Conclusion

This paper proposes a robust two-hybrid security algorithm for a cloud computing environment. They are designed to solve several issues as practical implementation, short response time, efficient computation, and the strength of the cryptosystem. Several cryptographic methods were studied to determine the most efficient one that gives more protection and less encryption time. An evaluation of the performance of different encryption algorithms is presented. The selected algorithms are AES, Blowfish, FastRSA, DES, and the proposed two-hybrid algorithms. By comparing the result of the proposed algorithm with other cryptographic methods, we can recommend the proposed algorithm to be used in securing data through cloud computing. We can apply the proposed algorithm to multimedia files such as sound files as part of our future work.

References

[1] AbdElminaam, D. S., Kader, H. M. A., Hadhoud, M. M., & El-Sayed, S. M. (2013, December). Elastic framework for augmenting the performance of mobile applications using cloud computing. In 2013 9th International Computer Engineering Conference (ICENCO) (pp. 134-141). IEEE.

[2] Kader, H. M. A., Hadhoud, M. M., El-Sayed, S. M., & AbdElminaam, D. S. (2014). Performance evaluation of new hybrid encryption algorithms to be used for mobile cloud computing. International Journal of Technology Enhancements and Emerging Engineering Research, 2(4).

[3] El-Sayed, S. M., Kader, H. M. A., Hadhoud, M. M., & AbdElminaam, D. (2014). Mobile cloud computing framework for elastic partitioned/modularized applications mobility. International Journal of Electronics and Information Engineering, 1(2), 53-63.

[4] AbdElminaam, D. S., Kader, H. M. A., Hadhoud, M. M., & El-Sayed, S. M. (2014). Increase the performance of mobile smartphones using partition and migration of mobile applications to cloud computing. International Journal of Electronics and Information Engineering, 1(1), 34-44.

[5] Abd Elminaam, D. S., Alanezi, F. T., & Hosny, K. M. (2019). SMCACC: Developing an Efficient Dynamic Secure Framework for Mobile Capabilities Augmentation Using Cloud Computing. IEEE Access, 7, 120214-120237.

[6] Taha, A. A., AbdElminaam, D. S., & Hosny, K. M. (2017). NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment. (IJACSA) International Journal of Advanced Computer Science and Applications, 8(11).

[7] AbdElminaam, D. S., Kader, H. M. A., Hadhoud, M. M., & El-Sayed, S. M. (2014). Increase the performance of mobile smartphones using partition and migration of mobile applications to cloud computing. International Journal of Electronics and Information Engineering, 1(1), 34-44.

[8] AbdElminaam, D. S., Toony, A. A., & Taha, M. (2020). Resource Allocation in the Cloud Environment Based On Quantum Genetic Algorithm Using Kalman Filter with ANFIS. IJCSNS, 20(10), 10.

[9] Al-Shabi, M. A. "A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security." *International Journal of Scientific and Research Publications (IJSRP)* 9.3 (2019).

[10] Maha Tebba, Saïd Haji Abdellatif Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security", Vol 2,no 3.World Congress on Engineering (2012)

[11] Mandal PC. Superiority of Blowfish algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. 2012 Sep;2(9).

[12] He X, Machanavajjhala A, Ding B. Blowfish privacy: Tuning privacy-utility trade-offs using policies. InProceedings of the 2014 ACM SIGMOD international conference on Management of data 2014 Jun 18 (pp. 1447-1458).

[13] ACM. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance.org,Vol ,3 no 2 (2009).

[14] P. Vijaya Bharati, T. Sita Mahalakshmi. Data Storage Security in Cloud Using a Functional Encryption Algorithm.Vol. 3, no 2.Springer (2016).

[15] Zaid Kartit, Ali Azougaghe, Applying Encryption Algorithm for Data Security in Cloud Storage, Vol. 3 no 3, Springer (2016)

[16] Khalid El Makkaoui, Abderrahim Beni-Hssane, Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing, Vol. 5 no 2, 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (2017)

[17] Nandita Sengupta and Ramya Chinnasamy, Contriving Hybrid DESCAST Algorithm for Cloud Security, Vol. 5 no 2, Eleventh International Multi-Conference on Information Processing (2015)

[18] Veeralakshmi Ponnuramu and Latha Tamilselvan, Encryption for Massive Data Storage in Cloud , Vol. 2 no 2, Computational Intelligence in Data Mining (2015)

[19] M. Sulochana ,Ojaswani Dubey, Preserving Data Confidentiality using Multi-Cloud Architecture. Vol. 3, no 4. 2nd International Symposium on Big Data and Cloud Computing ISBCC (2015)

[20] IC. Saravanakumar, and C. Arun, Survey on Interoperability, Security, Trust, Privacy Standardization of Cloud Computing. IEEE International Conference on Contemporary Computing and Informatics ,Vol 3 no 3 (2014)

[21] Sanka S, Hota C, Rajarajan M. Secure data access in cloud computing, in internet multimedia services architecture and application (IMSAA). 4th International Conference, IEEE, Vol 2,no 2 (2010)

[22] The Application of Hybrid Encryption Algorithm in Software Security, 4th International Conference on Computational Intelligence and Communication Networks (CICN), 2012 http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=6375216.

[23] Naziya Balkish, A.M. Prasad, and V. Suma, An Efficient Approach to Enhance Data Security in Cloud Using Recursive Blowfish Algorithm , Vol. 1 no 1, Springer (2014)

[24] Mr. Manish M Potey , Dr C A Dhote, Homomorphic Encryption for Security of Cloud Data,Vol. 1 no 1, 7th International Conference on Communication, Computing and Virtualization (2016)

[25] Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and fine-grained data access control in cloud computing,Vol. 1no 2 IEEE INFOCOM, San Diego, CA, USA (2010).

[26] Seiger R, Groß S, Schill A. SecCSIE: a secure cloud storage integrator for enterprises. IEEE 13th Conference on Commerce and Enterprise Computing (CEC); 252-255.

[27] ShaluMall , A New Security Framework for Cloud Data,Vol. 1 no 1, 8th International Conference on Advances in Computing and Communication (2018)

[28] M. B. Abha Sachdev, "Enhancing Cloud Computing Security using AES Algorithm," vol. 67, no. 9 International Journal of Computer Applications (2013)

[29] Junbeom Hur, "Improving security and efficiency in attribute-based data sharing," IEEE transactions on knowledge and data engineering, vol. 25, no. 10,pp. 2271{2282, 2011.

[30] Lizhi Xiong, Zhengquan Xu , A secure re-encryption scheme for data services in a cloud computing environment,Vol. 1 no 1, Wiley Online Library (2015)

[31] P. Vijaya Bharati, T. Sita Mahalakshmi. *Data Storage Security in Cloud Using a Functional Encryption Algorithm*.Vol. 3, no, 2.Springer (2016)

[32] M. Sulochana1 ,Ojaswani Dubey, Preserving Data Confidentiality using Multi-Cloud Architecture. Vol. 3, no 4. 2nd International Symposium on Big Data and Cloud Computing ISBCC (2015)

[33] Lo'ai Tawalbeh , Nour S. Darwazeh, A Secure Cloud Computing Model based on Data Classification. Vol. 4, no 4. *First International Workshop on Mobile Cloud Computing Systems, Management, and Security MCSMS* (2015)

[34] Paresh Ratha, Debabala Swain, An optimized encryption technique using an arbitrary matrix with probabilistic Encryption, Vol. 5, no 4. *3rd International Conference on Recent Trends in Computing ICTRC* (2015)

[35] Khalid El Makkaoui, Abderrahim Beni-Hssane, Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing, *8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks* (2017)

[36] Veeralakshmi Ponnuramu and Latha Tamilselvan, Encryption for Massive Data Storage in Cloud, Vol. 2 no 2, *Computational Intelligence in Data Mining* (2015)
[37] Zaid Kartit, Ali Azougaghe, Applying Encryption Algorithm for Data Security in Cloud Storage, Vol. 3 no 3, *Springer* (2016)
[38] Nandita Sengupta and Ramya Chinnasamy, Contriving Hybrid DESCAST Algorithm for Cloud Security, Vol. 5 no 2, Eleventh International Multi-Conference on Information Processing (2015)
[39] Naziya Balkish, A.M. Prasad, and V. Suma, An Efficient Approach to Enhance Data Security in Cloud Using Recursive Blowfish Algorithm, Vol. 1 no 1, Springer (2014)
[40] Mr Manish M Potey , Dr C A Dhote, Homomorphic Encryption for Security of Cloud Data, Vol. 1 no 1, 7th International Conference on Communication, Computing and Virtualization (2016)
[41] Lizhi Xiong, Zhengquan Xu, A secure re-encryption scheme for data services in a cloud computing environment, Vol. 1 no 1, Wiley Online Library (2015)
[42] ShaluMall , A New Security Framework for Cloud Data, Vol. 1 no 1, 8th International Conference on Advances in Computing and Communication (2018)
[43] Balasaraswathi V. R. and Manikandan S. "Enhanced security for multi-cloud storage using cryptographic data splitting witha dynamic approach.",Vol 2, no 3IEEE International Conference on Advanced Communications, Control and Computing Technologies:1190-1194(2014)
[44] Syam Kumar P., Subramanian R., An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing, Vol. 8, no 1,IJCSI International Journal of Computer Science Issues, (2011)
[45] M. B. Abha Sachdev, "Enhancing Cloud Computing Security using AES Algorithm," vol. 67, no. 9 International Journal of Computer Applications (2013)
[46] AbdElminaam, D. S., Kader, H. M. A., Hadhoud, M. M., & El-Sayed, S. M. (2013). GPS test performance: Elastic execution applications between mobile device and cloud to reduce power consumption. International Journal of Computer Science and Network Security (IJCSNS), 13(12),
[47] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2009). Energy efficiency of encryption schemes for wireless devices. *International Journal of Computer Theory and Engineering*, *1*(3), 302.
[48] Salama, D., Kader, H. A., & Hadhoud, M. (2011). Wireless network security still has no clothes. *International Arab Journal of e-Technology*, *2*(2), 112-123.
[49] Abd Elminaam, D. S., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *Int. J. Netw. Secur.*, *10*(3), 216-222.
[50] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2009). Tradeoffs between energy consumption and security of symmetric encryption algorithms. *International Journal of Computer Theory and Engineering*, *1*(3), 325.
[51] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2009). Analyzing the energy consumption of security algorithms for wireless lans. *International Journal of Computer Theory and Engineering*, *1*(4), 334.
[52] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2009). Measuring and Reducing Energy Consumption of Cryptographic Schemes for Different Data Types. *International Journal of Computer Theory and Engineering*, *1*(3), 1793-8201.
[53] Elminaam, D. A., Kader, H. A., & Hadhoud, M. M. (2009). Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices. *International Journal of Computer Theory and Engineering*, *1*(3), 1793-8201
[54] Taha, A. A., Elminaam, D. S. A., & Hosny, K. M. (2018). An improved security schema for mobile cloud computing using hybrid cryptographic algorithms. *Far East Journal of Electronics and Communications*, *18*(4), 521-546.
[55] Abdul, D. S. (2018). 'Reliable the resources of mobile devices in cloud computing. Int. J. Adv. Comput. Technol., 10(1), 61-70.
[56] AbdElminaam, D. S., Toony, A. A., & Taha, M. (2020). Resource Allocation in the Cloud Environment Based On Quantum Genetic Algorithm Using Kalman Filter with ANFIS. IJCSNS, 20(10), 10.