ISSN 2063-5346

THE CLOUD DATA STORAGE ASYMMETRIC KEY ENCRYPTION DECRYPTION WITH ENHANCED CLOUD SECURITY METHODOLOGY

N. Ambika[1]

Article History: Received: 19.04.2023 Revised: 02.05.2023 Accepted: 10.06.2023

Abstract

Cloud computing is the emerging technology and it offers the resource like hardware, software, storage and applications. It mainly applied in remote locations and it denoted as deploying, organizing and accessing the applications in online. The process of manipulating, configuring and accessing the applications online are done using the cloud computing technology and offers the online storage of data, infrastructure and the applications. Securing this data is a complex task for the data owners and various organizations entirely rely on this data. Data is usually encrypted before transmission to the cloud and the process of encryption would be performed every time the user varies the credentials. This problem is rectified when data owner performs the first level of encryption and the cloud performs the second level of encryption thereby decentralizing the control. The proposed privacy model is combined together with the access control model to protect the privacy-aware access rights.

Keywords: *Cloud Computing, Cloud Security, Encryption.*

[1] PG Assistant, Ponnu Matriculation Higher Secondary School, Dharapuram.

DOI: 10.48047/ecb/2023.12.si12.052

1. Introduction

With the explosion of internet and computing resources, the evolution in micro-miniaturization of technological knowledge has become more commanding and dominating than ever before. Because technology has become more affordable and widely available, a new computing model known as Cloud Computing has emerged. Cloud computing refers to large groups of virtualized operational resources such as hardware, development services, and platforms that have been reconfigured dynamically to change into flexible content in terms of load balancing, scalability, and elasticity, allowing for improved resource use. With the help of cloud computing and its pay-per-use professional model, organisations have been motivated to merge IT operations with virtualization technologies in order to reduce computing costs through improved & enhanced utilisation, compact management, infrastructure, and fast deployment cycles. Cloud computing is a new technology that provides assets such as equipment, programming, storage, and applications. It is primarily used in remote places and refers to the process of deploying, organising, and accessing applications via the internet. It also provided an online information architecture and capacity. It will enable the user to keep their data in the cloud. Cloud computing is used in a variety of applications, including E-governance and business

- Health sector
- Agriculture
- Data storage
- Management application
- Social application
- Entertainment application

The cost of hosting the application, computation and the storage of the applications is reduced significantly with the design of the cloud computing technology. The cloud is situated in the place of remote area, hence the name Network or the Internet.

2. Cloud Security

The security of cloud includes two such as,

- Safe estimation confidence
- Safe storage confidence

It denotes the level of confidence in the security of computation and storage. Cloud computing security can be defined as a set of processes and technologies that are designed to provide data security assurance in a cloud computing environment.

Cloud storage: Cloud hosting is a useful service that compresses cloud data and stores it in the cloud, which can then be accessed over the internet. The storage companies took use of their storage backends and their ability to service more customers with the same infrastructure.

Security Issues in Cloud Storage

Performance, interoperability, resiliency, data transition, and migration from legacy systems are all concerns that cloud computing have to deal with in terms of security. As a result of interconnections across practical purposes like virtual machines, certain challenges relating to network and data storage security in cloud computing may arise. On cloud computing, data management security is used to secure and prevent data, and it focuses on encryption or data classification for security. Additionally, encrypting certain data on the cloud reduces computing costs. Another essential for securing cloud data and data processing or operations is detecting and protecting data storage.

Benefits of Security in Cloud Computing

The benefits of the cloud computing are,

- Protection against Distributed Denial of Service
- Data security
- Regulatory compliance
- Flexibility
- High availability and support

Strong authentication framework: this can also be accomplished via various safety systems, somewhere around independent thought establishment, discussed validation, the important thing the use between many login, cloud service, but instead customer interaction. Organization based login such as cloud hosting: authentication method is crucial such as cloud native. The ability offers very few reliability of cloud services as well as services.

Privacy-preserving digital identity management: This approach is used for digital identification in cloud platform and it is an efficient approach for cryptographic protocols and matching techniques.

Mutual authentication scheme: This scheme can be utilized for reducing the security complications like side channel attack, identity theft, man-in-middle attack and phishing attack. this system offers strong and consistent mutual authentication amongst the cloud user and internet. it offers the better efficiency and more appropriate for cloud computing.

Security and Privacy Approaches

In the atmosphere of cloud systems, the service provider and service integrators are required to attain the security and privacy.

(i) Authentication and Identity Management: The user centric idm treated both the attributes of personal and important name. that whole technique will help of between recognize its entities rather than features. User centric ambient techno both means that it and strategy precisely preserve it and semantics sure frame of reference as a subscriber distinctive info as well as ambient techno delivery such as data center would be skilled to include to authentication and authorization foundation.

(ii) Access control requirements: The role-based access control (rbac) would be frequently applied to realize its access control access of about their easiness, leeway throughout today 's rapidly necessities, but rather productive advantage managerial.

(iii) Secure interoperation: it recognized the integration matters that seem to be competent to generate the comprehensive centralized management out data center but rather mixed domain access control model method. of one protect interoperation but rather plan framework needs to integrate that whole authorization just that different pastures but rather full inclusion intends. the one highly centralized device sets up the worldwide strategy that seem to be makes reference to every wants to access so it acceptable for utilization through data center. It includes the different services of diverse needs so it is also it almost corrected.

Benefits of Cryptographic Cloud Storage

In the delivery of cryptosystems, the info does seem to be encrypted determined depending just on concept besides information processors. This same visitor can promised of about privacy like their data and that are sustained by irrespective it and operations anyway cloud storage provider. it really is hard to ascertain where information is recorded and once that as well wants to send complete data center accurately. a few visitors seem to be uninterested versus use the the general public web e.g. elevating that whole legitimate companion for his or her data. as in file server yeah cryptography the info can really be saved through encrypted form sole therefore the unknown user could indeed access the data the information.

3. Issues in Cloud Computing

cloud computing deal with many different problems to take care of previous paragraph simple layout characteristic features but instead top notch sure supports convinced to that same consumer through it cloud service providers such as addition to high resources allocation, supercomputing capacity. or some the problems coping with resources, scheduler, but also successful initiatives production were also attention to what other people following table.

- Resource allocation
- Load balancing
- Migration
- Power efficient resource allocation and load balancing algorithms
- Cost efficient resource allocation and load balancing algorithms
- Fault tolerant algorithms
- Behavior-based algorithms
- Trust management

4. An Enhanced Homomorphic Cloud Security Algorithm (EHCSA)

Cloud data is encrypted and cannot be updated. If any changes are required, the data is decrypted and re-encrypted before being saved on the server. However, when the homomorphic encryption model is combined with threshold proxy encryption, it is

possible to modify data in encrypted data without having to decrypt it. As a result, the system becomes more secure, and the data owner only has access to the private key. Two methods are included in a fully homomorphic encryption scheme, such as,

(i) Increase homomorphic encryption algorithm
(ii) Additively homomorphic encryption algorithm

The addition and multiplication of homomorphic are only supported by homomorphic encryption algorithm. Theses algorithm encrypt the data by using multiple stages of addition and multiplication process.

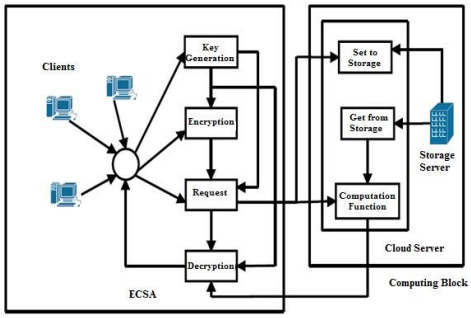

Figure 1: An Enhanced Cloud Security Algorithm (ECSA)

The fully homomorphic encryption mechanism is depicted in Figure-1. With the help of homomorphic encryption, the encrypted data can be easily modified or changed. This is the mechanism's primary advantage. Homomorphic operation provides numerous benefits in the cloud paradigm because it protects data confidentiality and privacy, which is a major concern in the storage and processing of data by unauthorised parties. AND and XOR Boolean operations are supported by the homomorphic operation. De Morgan's law allows for these operations to be performed. If the function f is available and no private keys are used. The operations of homomorphic encryption systems are classified. It will allow the raw data to additive homomorphic encryption and multiplicative homomorphic encryption. Multiplicative homomorphic encryption schemes are used the cipher text to calculates the product of plain texts. Multiplicative homomorphic scheme includes both RSA and ElGamal cryptosystems.

Properties of Homomorphism

(i) Additive property

Two groups of plain text as M_1 and M_2, To encrypt the cipher text as, $C_1 = M_1 + 2R_1 + PQ_1$ and $C_2 = M_2 + 2R_2 + PQ_2$. Then the plain text M as, $M_3=M_1+M_2$ and the Cipher text $C_3=C_1+C_2$ and $C_3 = (M_1 + M_2) + 2(R_1 + R_2) + P(Q_1 + Q_2)$.

$(M_1 + M_2) + 2(R_1 + R_2) <$ P and

$C_3 = (C_1 + C_2) \bmod P = (M_1 + M_2) + 2(R_1 + R_2)$

(ii) Multiplicative property

Plain Text $M_4 = M_1 \text{ x } M_2$ and $C_4 = C_1 \text{ x } C_2$and

$$C_4 = (M_1 + 2R_1 + PQ_1) \text{ x } (M_2 + 2R_2 + PQ_2)$$
$$= M_1M_2 + 2(2R_1R_2 + R_1M_2 + R_2M_1) + P(PQ_1Q_2 + Q_2(M_1 + 2R_1) + Q_1(M_2 + 2R_2))$$

and $M_1M_2 + 2(2R_1R_2 + R_1M_2 + R_2M_1) < P$,

$$C_4 = (C_1 \text{ x } C_2) \bmod P = (M_1M_2) + 2(R_1R_2 + R_1M_2 + R_2M_1)$$

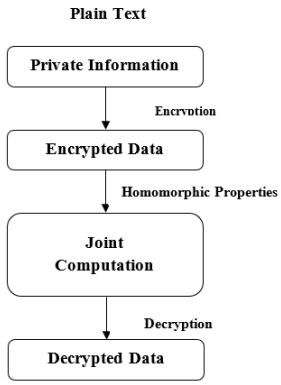

Figure 2: Encryption and Decryption Methodology

Figure-2 demonstrates the encryption process. Here the secure information is encrypted by encryption techniques. And the authentication user only decrypts the stored or encrypted data.

Design Methodology

A secure cloud backup system was indeed assembled that used a cutoff point routing protocol encrypted communication framework to cumulative overlaps qualities. a cryptography system is named multipliers homomorphic so it enables for such ways of combating f o as even the cryptography operate, das even as encryption key role, as well as (pk, sk) also as two after all government and commercial buttons. its ciphertext needs to convert of one vpn s new strategy versus about their lower limit rendition using cumulative elliptic curve estate. the key factor seemed to be got to share by both the input computer employing his\her threshold value s n. there has been a factor client m s but rather code word icons procured from partially decompressed encrypted texts. A secure cloud system consists of N storage servers that hold data and M key servers that hold secret key shares, allowing for partial decryption. By using a threshold t, the data owner distributes their secret key x to m key servers. Allow K messages to be stored in the cloud system via a storage process.

Message encryption: Using the Data encryption key, the owner encrypts all K messages with the identifier ID for the set of messages denoted as M1, M2,..., Mk.

Distribution of cipher text: The data owner chooses a storage server V at random for each Ci and sends each copy as Ci.Retrieval command is described that the proprietor sends the command to key servers with message identifier ID. An individual key sever S_i arbitrarily enquiries U storage servers with the message identifier ID and it gets the stored servers mostly for performing partial decryption. Formerly, the key server S_i achieves the share_Dec takes place in all the received cipher text through their share of secret key to get the decryption share of cipher text. In this Merging and decoding method, the answers are collected by the data proprietors from their last t key servers and at least k are initially from separate storage servers, and they performs the partly decrypted code word symbols to retrieve the blocks, thus the unique data is recuperated. The characteristics of the proposed system are,

- The storage server which self-reliantly accomplish the encoding and encryption process. Then the partial decryption process is performed by key servers.
- The system acquires more flexibility to adjust among the several storage servers and heftiness.
- The proposed work can supports effectual active processes like data blocks, which includes with updating and deletion.

Algorithm EHCSA()

Input: Messages$M_1, M_2, \ldots, M_k$;

Step-1: Homomorphic Encryption

begin

To Convert Plain text into Cipher $C=E(Key,m_1)^{g_1}.E(Key,m_2)^{g_2}$;

Joint Ciphers using Homomorphic additive or multiplicative property;

End

Step-2: Homomorphic Decryption

begin

$$Plain = D(Key, E(Key, m_1)^{g_1}.E(Key, m_2)^{g_2})$$

End

End

Output: Plain Text into Cipher and Cipher Text into Plain.

5. Results and Discussion

The proposed algorithm comprises of Threshold Proxy Encryption Scheme integrated by way of the Delegation and homomorphic encryption assets. The data to be kept in the cloud platform is disintegrated into dissimilar block and encoded and kept in altered servers in the cloud. Throughout the data retrieval process, the data blocks from diverse servers are united in a distinct server. It is shown that the response time of the servers constantly upholds the adequate rate when the servers are enlarged. The table represents the response time of the server which is varied in accordance to the number of server. The value is depicted for the least response time, extreme response time, and the average response time. A number of servers may vary from one server, five servers, ten servers, twenty servers, and the twenty five servers. The response time of individual server is measured in terms of (ms). The response time of the server remains constant as the number of server is enlarged. It is greater for the one server; however it decreases as the number of server increases.

Table 1: Server Response Time in ms

Server Response Time in ms			
No. of servers	Minimum Response Time in ms	Average Response Time in ms	Maximum Response Time in ms
1	800	400	50
5	400	100	45
10	90	90	49
20	80	80	52
25	70	70	50

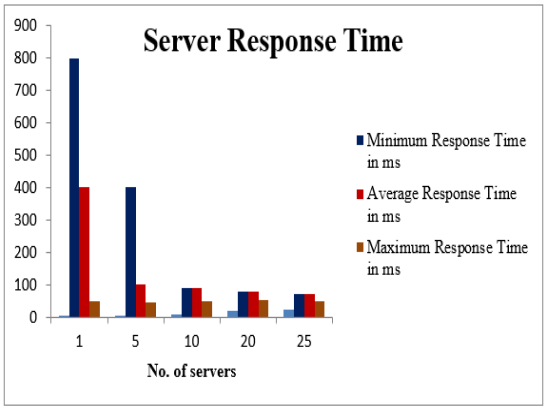

Figure 3: Server Response Time in Milliseconds

In overall, the server response time is depicted as the average length of time set aside to respond to a service request. It is the period of hours that has passed between the intervening time and the response received for that review. as the number of servers increases, the response time of all minimum, average, and maximum response time may decrease. This is depicted in the visual analysis provided below. Thus, based on just this result, the proposed method achieves a higher efficiency in terms of site loading time when compared to the other methods. The provided visual analysis depicts the faster processing time, which depends on the quantity of servers provided. The time taken for the system or process is to respond according to the request. When the amount of server rises then the response time taken will be decreased. The response time of the server is measured by means of (ms). The response time will be maintained at a moderate rate for all minimum, maximum, and average response time once the number of server increases. However, the small response time will make the system more effective for computing. The x-axis represents the number of servers that varies from one server to twenty five servers. The y-axis represents the response time that is measured in (ms) and it varies from 0 to 800 (ms).

The figure-3 and table-1 shows the decomposed data, and encoded in diverse self reliant servers. This demonstrates the quantity of data stored in the each server. For explanations, two servers and four data are taken here. The table-2 shows the data degradation rate. it covers the overall number of data that really is stored in the server. According the data size that really is measured in kb the time may varies for server-1 and server-2. The time is measured in

(ms). For the data size of 100 the time it takes for the domain controller for trying to generate the data is 60, for server 2 it is 35. Then, for the data size of 250 kb the time taken by the server-1 will be 65, by the server-2 will be 60. The server-1 takes 72 ms and server-2 takes 63 ms for the data size of 275 KB. Finally for the data size of 300 KB the time taken by the server1 is 100 and by the server is 180 ms. Therefore this is the rate at which the data tends to decompose or generates. This can be shown in the representation of Figure-4.

Table 2: Data Decomposition Rate

Time in ms		
Data Size in KB	**Server-1**	**Server-2**
100	60	35
250	65	60
275	72	63
300	100	180

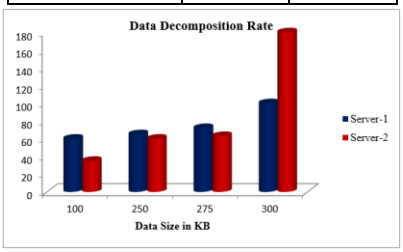

Figure 4: Data Decomposition Rate

The data thermal degradation of a inbuilt inside the server has been the time it takes for decomposed of knowledge that has to be accumulated inside the server. The information is again hard coded just at person servers. This same pictorial depiction portrays the whole storing data within client. This same information stored inside this computer was indeed defined in some kind of a graphical depiction. this same anti - anti deviates because after list base pair of about cm-1 represents kilobytes whereas, its increases with increasing that whole period through (ms) that either differs even before infinity of between one hundred eighty (ms). The above figure proves this same efficiency of the info dissolution rate to either contrasting some other means to control. Hence, it and efficiency of such database server does seem to be confirmed by data analysis if of knowledge decomposition rate.

Server Processing Time

Figure-5 shows the total processing time required for data decomposition, storage on various servers, re-encryption, and retrieval. Table-3 shows that even as the amount of data stored in the cloud grows, the processing time remains relatively low. For the current Sym-FHE and AES-DAS techniques, if there are 200 data points, the processing time will be 180 and 150 seconds. If there are 400 data points, the processing time will be 220 and 200. The processing time for the proposed ECSA technique is 90 ms for 200 data points, 110 ms for 400 data points, and 128 for 600 data points. In terms of price, the processing time is 128 if the number of data is 600. For the value of 800 in the number of data then the processing time will be 145. For 1000 it is 160 ms, for 1200 it is 175. Likewise the processing time will be a moderate one for the increasing number of data.

Table 3: Server Processing Time

No. of Data	Server Processing Time
200	90
400	110
600	128
800	145
1000	160
1200	175

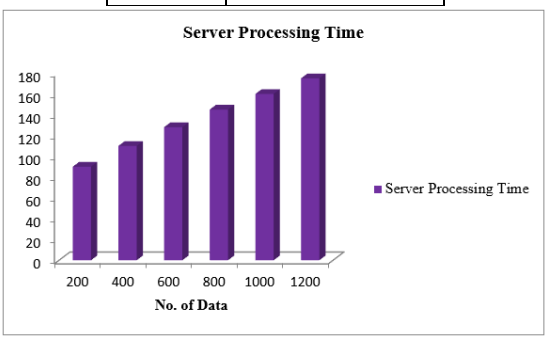

Figure 5: Server Processing Time

The graphical representation the server's processing time for the request parameter is displayed. The number of data is represented by the x-axis, which ranges from 200 to 1200. The y-axis represents the server's processing time, which ranges between 90 and 175 milliseconds. This shows that as the amount of data grows, the server's processing time becomes moderate and remains so.

6. Conclusion

A novel encryption scheme based on an improved delegation mechanism and homomorphic encryption is developed in this proposed research work. The goals of encryption techniques are to provide cloud data with increased security, access control, and data privacy. It provides scalable resources via the internet with vigour. In this paper, a threshold proxy encryption scheme is proposed, along with an improved delegation mechanism and homomorphic encryption properties, to improve the

storage and retrieval of data over the cloud, and it is thought to be more efficient. The proposed system model includes two servers, namely the key server and the storage server. The dynamic changes in the stored data encryption are done using the elliptic curve property included in the encryption scheme where the arbitrary operations are performed on the encrypted data. an overall system is processed with the secured storage and retrieval of data in the decentralized cloud platform and the delegation mechanism is achieved by providing proper access rights to the users in the cloud. The main benefits of cloud computing are cost investments, great cloud computing and suppleness.

References

[1] Arora R, Parashar A & Transforming CCI, 2013. "Secure user data in cloud computing using encryption algorithms", International Journal of Engineering Research and Applications, vol. 3,no. 4, pp. 1922-1926.

[2] Bacon J, Eyers D, Pasquier TF-M, Singh J, Papagiannis I & Pietzuch P, 2014. "Information flow control for secure cloud computing", IEEE Transactions on Network and Service Management, vol. 11,no. 1, pp.76-89.

[3] Baek J, Vu QH, Liu JK, Huang X & Xiang Y, 2015."A secure cloud computing based framework for big data information management of smart grid", IEEE transactions on cloud computing, vol. 3,no. 2, pp.233-244.

[4] Deyan C & Hong Z, 2012. "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012 pp. 647-651.

[5] Hamlen K, Kantarcioglu M, Khan L & Thuraisingham B, 2012. "Security issues for cloud computing", International Journal of Information Security and Privacy, vol. 4, no. 2, pp. 39-51.

[6] Lee K, 2012. "Security threats in cloud computing environments", International Journal of Security and Its Applications, vol. 6,no. 4, pp. 25-32.

[7] Pancholi VR & Patel BP, 2016. "Enhancement of cloud computing security with secure data storage using AES", International Journal for Innovative Research in Science and Technology, vol. 2,no. 9, pp. 18-21.

[8] Yan Z, Li X, Wang M & Vasilakos AV, 2017. "Flexible data access control based on trust and reputation in cloud computing", IEEE Transactions on Cloud Computing, vol. 5,no. 3, pp. 485-498.

[9] Yang J, He S, Lin Y & Lv Z, 2017. "Multimedia cloud transmission and storage system based on internet of things", Multimedia Tools and Applications, vol. 76,no. 17, pp. 17735-17750.

[10] Yang K & Jia X, 2014."DAC-MACS: Effective data access control for multi-authority cloud storage systems, in Security for Cloud Storage Systems", Springer, Special Edition, pp. 59-83.