Research Journal of Computer Systems and Engineering

ISSN: 2230-8571, 2230-8563

Volume 03 Issue 01 - 2022 (January to June)

Page 78:83

Access Control-Based Cloud Storage Using Role-Fully Homomorphic Encryption Scheme

Dr.Neha Verma
Green Energy Technology
SSIPMT,Raipur
ORCHID ID-0000-0001-9091-4428
n.verma@ssipmt.com

Article History

Received: 22 January 2022
Revised: 14 April 2022
Accepted: 19 May 2022

Abstract

The gigantic creation of computerized information and the intricacy of the basic information the executives persuade people and ventures to re-appropriate their computational necessities to cloud. Cloud processing has become progressively well known in IT world as the following framework for putting away information and deploying software and administrations. It gives clients a not insignificant rundown of benefits, like on-request self-administration; broad, heterogeneous network access; asset pooling and rapid elasticity with estimated administrations. One of the significant administrations presented in distributed computing is cloud information storage, in which, supporters don't need to store their own information on their servers, rather their information will be put away on CSP's servers. In this research, essentially center around information capacity in cloud.
Keywords: digital data, heterogeneous network access, resource pooling, cloud computing, data storage.

1 INTRODUCTION

The expression "cloud" implies system of giving propertiesover the web. The propertiespresent in cloud can be utilized unendingly by client at whatever point required. In cloud computing, clients normally wanted to outsider supplier for administration of web rather than setup their very own physical framework. Highlights of cloud computing incorporate on interest self-administrations, measure administrations, expansive system territory, quick flexibility, lessen pooling, multi-determination and shared framework [1].

Lately, the handling and the limit of tremendous volumes of information have been redesigned enormously in these keep going seemingly forever in light of the improvement of Distributed computing. This thought is portrayed as a processing perspective, where a significant pool of structures are related in private, open or half and half frameworks, to give continuously flexible establishment to figuring property [2]. On-demand self-benefit suggests that affiliations can get to and manage their own figuring resources. Extensive frameworks will empowers organizations to be presented over the Web or confidential frameworks [3,4].

2 LITERATURE SURVEY

Homomorphic encryption is the reasonable response for comprehend distributed computing security issues, since its arrangements engage to perform computations on mixed information without sharing secret key expected to unscramble information [5].

Work [6] showsHomomorphic encryption, went for enabling estimation in the scrambled space, is becoming crucial to a wide and creating extent of uses, from distributed computing to fitting distinguishing. Creator in [7] said that homomorphic encryption is kind of encryption that empowers a few certain kinds of estimations to be finished on figure texts and make a scrambled result which, on unscrambled, matches outcome of undertakings performed on plaintexts. Work in [8] have examined that the distributed computing security subject to totally homomorphic encryption, is novel thought of safety which enables us to give outcomes of depends on the scrambled information without knowing rough information by which assessments was performed, concerning the information secretly.

Creator in [9] expressed that in distributed computing, information is placed on untouchable servers, and client is absolutely ignorant about region of server. Work [10] said that the most FHE plans rely upon Upper class' layout that including first fostering a SHE and after that using Nobility's bootstrapping system to change over it into again FHE plot.

2.1 Problem Identification:

- The client have zero control over the progression of deal with the information and the client can't guarantee the information security free from any other individual. The information storing and action and organization change also deals with the cloud system. The key information resource and insurance information are incredibly import for the client. The cloud should give information control system to the client.

- In the cloud computing, the cloud provider system has various clients in a powerful response to changing organization needs. The clients don't understand what position the information and don't know which servers are handling the information. The client don't perceive what organization are communicating the information because the flexibility and adaptability of cloud system. The client can't guarantee information security worked by the cloud secretly.

- The cloud system can convey the cloud a center in different area and the information can be taken care of in different cloud center point. The unmistakable region has different regulation so the security organization can meet the law peril. Distributed computing organization should be improved in legal security.

3 RESEARCH METHODOLOGY

The proposed procedure utilizing FHE encryption method for scramble the first data and encrypted data is put away in cloud server. The key age is utilized for client and cloud server for producing the mystery key. The proposed work process design is demonstrated as follows.

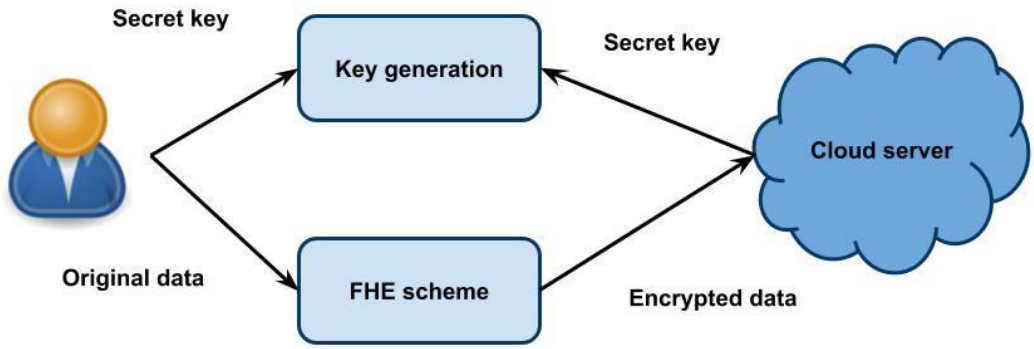

Figure 1 *Proposed system architecture*

3.1 Fully Homomorphic Encryption

For an extensive variety of rely on the information set aside in the cloud, we ought to choose the totally Homomorphic encryption which can execute a large number of undertakings on encoded information without unscrambling.

The use of totally Homomorphic encryption is a fundamental stone in Distributed computing security; all the something else generally, we could reallocate calculations on ordered information to Cloud server, keeping secret key that can unscramble eventual outcome of assessment.

3.2 Symmetric homomorphic encrypt scheme:

Select encrypt parameter: a, b and c, $c \sim 2^n$, $a \sim 2^{n2}$, $b \sim 2^{n5}$ and p is prime

A is the secret key

Encrypt: for plain text m

Compute d=ab+2c+l where c is the cipher text

Decrypt: l= (d mod a) mod 2

Correctness: because ab is larger than 2c+l so (d mod a) =2c+l

Finally (d mod a) mod 2= (2c+l) mod 2=l

Homomorphic: for two cipher text

D1=b1a+2c1+L1

D2=b2a+2c2+L2

Compute: D1+ D2= (b1+b2) a+2(c1+c2) +L1+L2

So if 2(c1+c2) +L1+L2<<a

Then (d1+d2) mod a=2(c1+c2) +L1+L2

So its additive homomorphic.

And d1*d2= [b1*b2a+ (2c1+L1) + (2c2+L2)] a+2(2c1 c2+c1L1+c2 L1) +L1 L2

So if 2(2c1 c2+c1L1+c2 L1) +L1 L2<<a

Then (d1*d2) mod a=2(2c1 c2+c1L1+c2 L1) +L1 L2

With this arrangement, the set aside information as well as the sent information is scrambled, so we don't worry about information is listened covertly or taken. It similarly can give secure information audit benefit considering way that third survey get-together can deal with encoded information explicitly. Besides, the encryption we use is balance so we can enroll it with less MIPS which are basic for dainty client.The usage of totally homomorphic encryption estimation application is especially expansive, generally in the going with 3 viewpoints.

Data processing· completely homomorphic encryption instrument can influence clients or confided in outsider to scramble data straightforwardly, rather than the first data, the clients decrypt the consequence of processing and get the handled data.

Defense protection· the client data is to be transmitted by cipher text shape to the cloud of data stockpiling, not just guarantee the wellbeing of data amid transmission, yet additionally guarantee the security of data stockpiling. Regardless of whether the cloud computing specialist organizations can't without much of a stretch acquire plaintext data.

Cipher content retrieval· cipher content recovery dependent on fullyhomomorphic encryption innovation utilized for recovering on ciphertext straightforwardly, which cannot just guarantee investigating security and enhance the recovery proficiency yet in addition can do the expansion and augmentation activity to the recovered data without changing the relating plaintext.

4 EXPERIMENTAL RESULTS

Performance analysis of proposed work is data encryption based on Fully Homomorphic Encryption (FHE) scheme. Secret key is generated as well as provided to cloud server and user for identification of data.

Fig 2: creating the login ID and password

The above figure 2 shows the user login page for accessing the data. After submitting the ID and password, secret key is generated to E-mail ID using fully homomorphic technique.

Fig 3: Key is generated and user can login

The above figure 3 secret key generation for individual user to login and access the data in cloud server.

Fig 4: After getting the security key. One can log in to view the confidential files

The above figure 4 shows the user accessing the cloud once the user getting the secret key. He / she can access the confidential file.

Fig 5.A user can upload the files with homomorphic authentication

The above figure 5 shows the user upload the data files to the server. at point when client send data to server in scrambled structure to play out any computational activity to that encoded data server need private key from client. This is an encryption process.

5 CONCLUSION

Security of cloud computing assisted completely homomorphic encoding could be another idea of security that is to alter to supply aftereffects of counts on encrypted learning while not knowing crude passages on that figuring was connected regarding the privacy of data. In this paper, principally aims around data stockpiling in cloud, in view of the mystery key the data is put away on cloud. The execution should be possible and getting proper yield results.

REFERENCE

[1] Wang, S., Wang, X., & Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. *IEEE access*, *7*, 112713-112725.

[2] Xue, Y., Xue, K., Gai, N., Hong, J., Wei, D. S., & Hong, P. (2019). An attribute-based controlled collaborative access control scheme for public cloud storage. *IEEE Transactions on Information Forensics and Security*, *14*(11), 2927-2942.

[3] Ning, J., Cao, Z., Dong, X., Liang, K., Wei, L., &Choo, K. K. R. (2018). CryptCloud $^+ $+: secure and expressive data access control for cloud storage. *IEEE Transactions on Services Computing*, *14*(1), 111-124.

[4] Xu, S., Yang, G., Mu, Y., & Liu, X. (2019). A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. *Future Generation Computer Systems*, *97*, 284-294.

[5] Sukhodolskiy, I., &Zapechnikov, S. (2018, January). A blockchain-based access control system for cloud storage. In *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)* (pp. 1575-1578). IEEE.

[6] A. Chaturvedi, A. Kapoor and V. Kumar, "A review of homomorphic encryption of data in cloud computing," International Journal of Computer Trends and Technology (IJCTT), Volume 43, Number 2, January 2017, pp. 75-80.

[7] K. Benzekki et al., "A Secure Cloud Computing Architecture Using Homomorphic Encryption," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 7, No. 2, 2016 pp. 293-298.

[8] Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *Ieee Access*, *6*, 38437-38450.

[9] Xue, K., Chen, W., Li, W., Hong, J., & Hong, P. (2018). Combining data owner-side and cloud-side access control for encrypted cloud storage. *IEEE Transactions on Information Forensics and Security*, *13*(8), 2062-2074.

[10] Selvakumar, K., SaiRamesh, L., Sabena, S., &Kannayaram, G. (2019). CLOUD COMPUTING-TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage. In *Smart Intelligent Computing and Applications* (pp. 365-373). Springer, Singapore.