IJMTST is UGC Approved Journal with Journal Id: 43137

International Journal for Modern Trends in Science and Technology, 8(S03):167-172, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST08S0338
Available online at: https://www.ijmtst.com/vol8si03.html

Group Key Management Protocol for File Sharing on Cloud Storage using Verification Scheme

T. Srinivasarao, Dr. N. Leelavathy

Department of Computer Science and Engineering, Godavari Institute of Engineering and Technology (A), JNTUK, Kakinada.

To Cite this Article
T. Srinivasarao and Dr. N. Leelavathy. Group Key Management Protocol for File Sharing on Cloud Storage using Verification Scheme. International Journal for Modern Trends in Science and Technology 2022, 8(S03), pp. 167-172.https://doi.org/10.46501/IJMTST08S0338

Article Info
Received: 26 April 2022; Accepted: 24 May 2022; Published: 30 May 2022.

ABSTRACT

The advancement of distributed storage is supported by numerous organizations huge scope sharing necessities. The assumptions and worries for document security are expanding as distributed computing keeps up with shared records past the trust zone of the proprietor. This work utilizes a check strategy to offer a Group Key Management Protocol for document sharing on distributed storage. A gathering key age framework in view of mixture encryption innovation is introduced because of organization dangers from public channels. A verification scheme is additionally used to shield shared documents from cloud suppliers and gathering individuals intriguing to go after them. The proposed system is both secure and productive for information trade in distributed computing, as per security and execution assessments. To safeguard the records from meddlesome eyes, we utilize the Double Encryption Technique from data spillage.

Keywords — Cloud Computing, Data Base, Authentication, Security, File Sharing.

1.INTRODUCTION

Revamping administrations as far as cloud has developed more famous considering the present creative blast of cloud innovations. Information from various clients can be put away on a solitary actual framework, which can be facilitated on different virtual machines, in a common occupancy distributed computing climate. Since the cloud supplier has unlimited oversight over information capacity and organization, information proprietors are left defenseless and should depend just on the cloud supplier to safeguard their information under this worldview. As indicated by ongoing reports, in the wake of getting a court order, Google gave up every one of one of its clients' records to the FBI, however the clients knew nothing about the pursuit until they were kept. [9] Since the cloud supplier has total admittance to the information, the protection of the information could be imperiled assuming that the cloud supplier blocks or adjusts the client's information. Encoding and confirming shared information is a regular way to deal with guarantee privacy.A number of cryptographic arrangements exist that permit an outsider inspector to validate the accessibility of documents without uncovering any data about the record.[10] Likewise, cloud clients are probably not going to have serious areas of strength for an in the cloud server's capacity to keep up with secrecy. Prior to transferring documents to the cloud server, cloud clients are urged to scramble them utilizing their own keys. The last test is sorting out some way to share and oversee cryptographic keys. A simple method for agreeing with the gathering paper organizing prerequisites is to involve this record as a layout and just sort your text into it.

2. RELATED WORKS

Storage System security has forever been an interesting issue of discussion all over the worlf. CFS and NASD are two instances of authentic frameworks. CFS is intended for single-client workstations and scrambles information utilizing client provided passwords. NASD gives a circulated framework shrewd circles and client provided keys as approval evidences. NASD and SNAD are two methodologies that attention on defending organization traffic and forestalling outside interruptions. For the safe correspondence of individual wellbeing data through distributed computing, Rao proposed a ciphertext-strategy ascribed based [CP-ABE] signcryption framework. It centers around preventing individuals from having unapproved admittance to delicate data. Liu et al. introduced a CP-ABE-based admittance control system for individual records in distributed computing. In the framework, only one completely believed focal power handles key administration and creating keys. Huang et al. came up an original public-key encryption model with approved fairness assurance on all or a predefined ciphertext for the sake of security. Wu et al.. came up with an effective and security based data encryption type with correspondence test in distributed computing to fulfill the developing security need.

Xu et al. introduced a Ciphertext Policy Attribute Based Encryption that utilizes bi-linear matching to give clients ciphertext looking and fine-grained admittance control.. He and his associates fostered the ACPC approach, which endeavors to give secure, effective, and fine grained information access-control in a P2P stockpiling cloud. RAAC, a progressive structure for public distributed storage access control that settles the single-point execution imperative of traditional CP-ABE based admittance control frameworks, was presented by Xue et al. While these frameworks utilize trait based systems to guarantee personality protection, they neglect to get client property security. Pervez et al. recommended a protection mindful information sharing framework SAPDS in their latest review tending to security challenges in cloud-based capacity. It consolidates quality based encryption method with intermediary re-encryption and mystery key update without requiring the utilization of a confided in outsider. Be that as it may, the capacity and correspondence upward of SAPDS is chosen by characteristic encryption plot. The accompanying frameworks allocate similar information access approval to gatherings of clients, and any client who has the entrance consent can get to the common documents. These gathering authorizations are usually used to safeguard information encryption keys. We can see that securely sharing information records with numerous proprietors for bunches while keeping up with personality protection in a doubt cloud stays a troublesome issue.

3. PROTOCOLS MODEL

1] GOAL'S - Our overall objective is to foster a productive gathering key administration convention for record sharing on distributed storage, the subsequent strategies ought to have the option to stand up to two principal issues. One is guaranteeing that the substance of the common documents can't be advanced by the Unapproved people groups. Another one is safeguarding the records against abuse by the cloud-supplier and block attempt by the organizations.

2] SHARING - A sharing gathering is comprised of clients who wish to trade documents, and each sharing gathering is constrained by the cloud supplier. Every sharer in the gathering has a couple of keys that are utilized to deal with the correspondence message. The cloud supplier deals with the public key, while the sharers just approach the private key. Prior to sending a record to the cloud, a sharer ought to deliver a gathering key and encode it with it. Then, at that point, without including the cloud supplier, he uses a key circulation instrument to scatter the gathering key to the next bunch sharers. All individuals from the assemble should attempt to recuperate the gathering key.

3] COMMUNICATION - To be focus on the gathering key administration, we worked on a group communication method. Accepting that all file sharers utilize normal organization to communicate message, the document sharers might communicate a message to the next bunch sharers straightforwardly.

4] THREAT-MODEL - Three methods of adversaries could represent a threat to our convention. The first is the cloud supplier, who is usually alluded to as a "aloof adversary" since he gathers information however

significantly affects how bunch individuals convey. The second is an agreeable adversary who, as a document sharer, may modify the result information. The last sort is a versatile foe equipped for compromising at least one gathering sharers and assembling and changing the result information of the individuals who have been compromised. At the point when a detached or positive rival is recognized, we want to have our convention stopped, while the versatile enemy should think twice about bunch individuals to overcome our convention, where, n is quantity of gathering individuals.

5] ALGORITHM - Acknowledge a sharing gathering G & each gathering member Pi with a transmission message B. D is an individual key offer convention if : [i] for any gathering part Ui not entirely settled by K and B [ii] all individuals in the sharing gathering can't learn anything about K. [c] no data of mi is gained from either the transmission data or the mystery 'K' key alone.

4. GKMP

Consider a sharing model G and each social event part 'Pi' with a transmission data B. D is a singular key proposition show if : [i] for any get-together part Ui not totally settled by K and B [ii] all people in the sharing social affair can't learn anything about K. [iii] No information of mi is acquired from the transmission data or the private key K alone.

i] ***KEY-SHARING PROTOCOL*** - The motivation behind key offer convention is to appropriate a gathering key to bunch individuals, and different individuals can't access any data of the key. In our methodology, the document proprietor communicates a message, and all the gathering individuals can get the key from the original data. We propose a methodology with the mix of Advanced Encryption Standard and RSA , Advanced Encryption Standard is utilized to scramble the common record and RSA is utilized to encode the transmission data. Assume that P1 wishes to share a record R to P2, P3, ...Pn. .

1] INITILIZATION

The cloud supplier makes a sharing gathering G containing P1, P2, . . , Pn. Each Pi produces a couple of key [Pi, Si] and Ui sends Pi to the cloud supplier through the public channel. The part's open keys are sent by the cloud supplier to the document proprietor P1. P1 secretly creates a gathering key K and encodes F with Equation. Crypt [F] is sent and put away on the distributed storage framework.

2] ENCRYPITON

P1 utilizes the public keys P2 , P3 , . . , Pn of P2, P3, . . , Pn which have been gotten from the cloud supplier to create the transmission data SK. P1, first and foremost, computes d = fracsize [K] [n-1] and produces an irregular worth p, taking m pieces of K [record as Kmod] from the [p + 1] digit to [p+d] piece furtively and parts the rest chomps of K[record as Ksub] into [n-1] piece k2, k3, . .. , kn similarly.

3] DECRYPTION

All of the people from sharing social event G could get the transmission data from the public channel that had SK.The next task for the get-together people is reproducing the get-together key from SK.Stage 0] Ui, I = 2.....n gets the data from P1 through the public channel and the encryption part cipher[ki] from SK then decodes it utilizing its private key Si .

Stage I] Pi unscrambles cipher[Ki] utilizing its secret key Si . Then encryption (Ki)with the public key of Pi+1 produce Ki,1 by supplanting cipher[ki+1] with the scrambled ENC [RSA, Pi, ki] in SK and send Ki, 1 to Pi+1[Pn communicate it to P2].

Stage II to n-1] At step j, j = 2, 3, . . ,n-1 Pi gets Ki, j−1 which has been gotten from Pi−1[P2 gets it from Pn] and does the estimation steps displayed as below. Then, at that point, Ui sends Ki,j to Pi+1 [Pn send it to P2]. At long last, after n−1 steps, each gathering individuals figures ki, I = 1, 2, . . , n then gets one duplicate of Kmod ,Ki = k2 K3...kn. The middle data Pi has sent and gotten.

ii] VERIFICATION PROTOCOL **-** Key offer convention is a proficient convention to circulate bunch key to bunch individuals. Here we further extended it to empower the gathering individuals to confirm their own halfway data. During the key dissemination, each gathering part Ui gets the data from the public channel and figures a duplicate of Ksub. Confirmation conventions comprises of three stages to really look at Ki .

1] INITIALIZATION

This methodology picks a single-way hash work HASH() to compute the hash worth of Ksub. Using Piblic Channel P1 communicates HASH(Ksub).

2] CALCULATE VERIFY VALUE OF KI

Every Pi registers the hash esteem Ki and broadcast their check esteem Yi on the public channel.

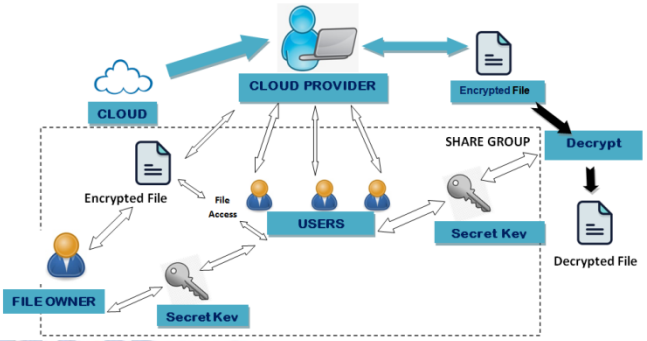
3] VERIFICATION P1

It processes the sum up of Yi , s = Pn i=2 Yi and broadcasts the outcome as per following advances: 1] If [S 6= n-1], P1 reports key appropriation falls flat and the convention ends. 2] If [S = n-1], P1 declares that key offer succeeds and it distributes Kmod , m. In confirmation convention, on the off chance that a gathering part sends wrong transitional data to our gathering individuals, it might identified by P1. The key offer convention is utilized to convey bunch keys to sharing gathering individuals without including the cloud supplier. The Protocol of Verification is utilized to decide if there is any cheating in the key offer convention and to guarantee key sharing security. The gathering key is scattered to the gathering participation's watchfully through open channels by playing out these conventions bit by bit.

5. EXISTING METHOD

CFS is intended for single-client workstations and scrambles information utilizing client provided passwords, while NASD is intended for multi-client workstations. NASD offers an appropriated framework in view of shrewd circles and client provided keys as evidences of approval. While these frameworks utilize property based answers for defend character security, they miss the mark concerning protecting client characteristic protection. The Encryption, CFS and NASD are not fitting for exceptionally enormous data sets because of their low exhibition, intricacy, and failure to recuperate from information base defilement. These two can't give satisfactory information security and insurance security. For this Purpose we are moving to the proposed framework.

6. PROPOSED METHOD



The recommended arrangement utilizes a confirmation plan to shield shared information from agreement assaults by cloud suppliers and gathering individuals. The recommended convention is both secure and productive for information trade in distributed computing, as per security and execution assessments. A gathering key age framework in light of twofold encryption innovation is introduced because of organization dangers from public channels. We introduced a critical age and twofold encryption methodology for document security and protection to defeat the issue from the current framework. The vital age for this situation, in the feeling of creating a key to get the information, will be achieved by sending an OTP to the client through email. The key will be created after the OTP confirmation as been finished. The information will be free from even a hint of harm with high security after the OTP check key is created.

7. RESULTS AND EVALUATION

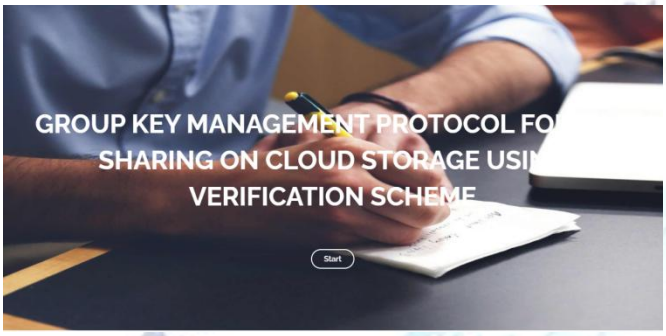
The exhibition of the proposed plan is assessed in this part. Our assessment centers around GKMP's stockpiling and computational upward specifically.

A. PERFORMANCE

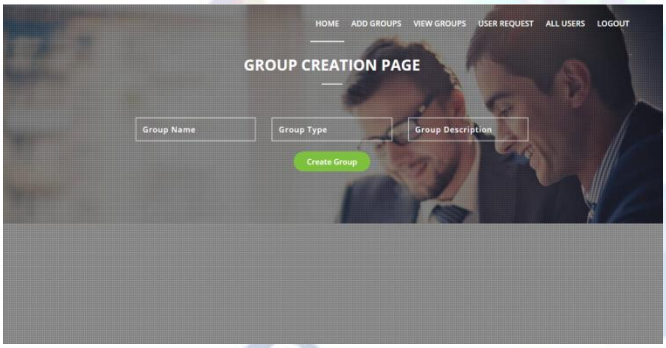
GKMP's productivity is being researched through an assortment of studies. Similarly as with distributed storage, a server with a Core 8 Dual Intel 2.93GHz processor and 8GB of RAM is used to store data. Furthermore, fluctuated measures of strings working on a PC with an Intel Core 2 Dual 2.93GHz processor and 2GB of RAM .

B. STORAGE OVER-HEAD

The storage upward of GKMP and SAPDS are thought about in this part. The ciphertext length, public & private key size, and ciphertext length between the most recent CP-ABE conspire and GKMP were totally analyzed. We accept in our paper that the length of gathering numbers is n and the key size is. The accompanying thing surveys GKMP's adequacy. Ciphertext length Implied the



correspondence cost that the document proprietor expected to ship off the cloud [SAPDS] or the information proprietor expected to ship off bunch individuals. In GKMP and SADPS, the common documents and encoded key were sent through the record proprietor to the cloud.



8. CONCLISON

We utilized a verification scheme to make an original gathering key administration convention for document sharing on distributed storage in this examination. GKMP utilizes public keys to guarantee that gathering keys are conveyed fairly and to shield against assaults from the compromised cloud-supplier. We give a definite investigation of potential security assaults and their connected guards, showing that GKMP is secure in any event, when more vulnerable suppositions are utilized. We likewise show that the convention is less complicated regarding stockpiling and calculation. We can add secure verification methods for information trade from here on out, as well as information inspecting plans

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] S. Zhang, S. Han, B. Zheng, K. Han and E. Pang, "Group Key Management Protocol for File Sharing on Cloud Storage," in IEEE Access, vol. 8, pp. 123614-123622, 2020, doi: 10.1109/ACCESS.2019.2963782.

[2] J.Wu, Y.Li, T.Wang, et al. CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing, IEEE Access, vol.7, pp.160482-160497, 2019

[3] Po-Wen. C, Chin L, "Audit-Free Cloud Storage via Deniable AttributeBased Encryption", IEEE Transactions on Cloud Computing,vol.6, no.2, pp. 414-427, 2018.

[4] J. Zhou et al., "Securing outsourced data in the multi-authority cloud with fine- grained access control and efficient attribute revocation", Comput. J., vol. 60, no. 8, pp. 1210-1222, Aug. 2017.

[5] Hu.X, Jianfei.S, "Comments on Verifiable and Exculpable Outsourced Attribute- Based Encryption for Access Control in Cloud Computing", IEEE Transactions on Dependable and Secure Computing., vol. 14, no.4, pp. 461-462, Aug.2017.

[6] Z. Fu X. Sun S. Ji G. Xie "Towards efficient content-aware search over encrypted outsourced data in cloud" Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM) pp. 1-9 Apr. 2016.

[7] Y. S. Rao "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing" Future Gener. Comput. Syst. vol. 67 pp. 133-151 Feb. 2017.

[8] H. liu Y. huang J. K. Liu "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute- Based Signcryption" Future Gener. Comput. Syst. vol. 52 pp. 67-76 Nov. 2015.

[9] Parvathi, D. S. L., Leelavathi, N., Ravikumar, J. M. S. V., & Sujatha, B. (2020, July). Emotion Analysis Using Deep Learning. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 593-598). IEEE.

[10] Kumar, J. R., Sujatha, B., & Leelavathi, N. (2021, February). Automatic Vehicle Number Plate Recognition System Using Machine Learning. In IOP Conference Series: Materials Science and Engineering (Vol. 1074, No. 1, p. 012012). IOP Publishing."