Secure and Efficient Access of Cipher Text for Mobile Cloud Computing

Eldhose Peter, Eldo P Elias

Abstract*: With the fame of distributed computing, cell phones can stack/recover individual information from anyplace whenever. Thus, the information security issue in versatile cloud turns out to be increasingly serious and forestalls further advancement of portable cloud. To ensure information security, clients normally encode their touchy information before transferring to cloud servers, which renders the information usage to be troublesome. In any case, there is no solid examinations for getting to cipher texts in mobile cloud. In this paper, we propose a safe and proficient information get to technique for versatile distributed computing. Consolidating proficient Mobile distributed computing system dependent on CP-ABE and presenting characteristic sprout channel for quicker cipher text access in versatile cloud. This plan has straight intricacy and depends for the most part on proficient symmetric key tasks. At long last, security examination and effectiveness correlation show that the proposition is successful for the proficient access of scrambled information in distributed computing.

Keywords: Cloud Bloom Filter (CBF), Mobile Cloud Computing, Attribute Based Encryption (ABE), Personal Digital Assistant (PDA).

I. INTRODUCTION

Disseminated registering has been executed and gotten to by right around 89 percent of local people on the planet today. The cloud has been gotten in every single industry and the ideal conditions have been acquired by attempts and people. Different affiliations have settled on cloud administrations to store their basic but sensitive information since they at present recognize how secure cloud can be [1][2]. Prior, there were different solicitations raised against the turn of events and its application in relationship as everyone was cautious as for the confirmation of information in the cloud. Routinely, cloud alteration has negated everyone and set up how feasibly cloud can profit putting away and get to to information from any place and from any gadget. A specific space on the server grants you to store nuances and recoup it at whatever point it is required. This advancement has spared a lot of costs, improved business efficiencies, and gave a goliath high ground over affiliations that don't utilize cloud administrations. Information on the cloud can be gotten to remotely through any gadget which is connected with the web which is one of the basic focal points of this headway.

A generally new term which is Mobile Cloud Computing is on a rising and their execution and reputation on each side of it may be revolt [1][3]. That specific closeness of telephones will run the flexible cloud enlisting plan. Nowadays essentially every self-administering has a wireless and perceives how to utilize each part of it. As PDAs can run distinctive awesome quality requesting, cloud-set up demands are in like manner available concerning the phone and it cooperate with your appropriated accumulating to stock and recoup information. Adaptable scattered preparing utilizes scattered enlisting to offer deals to specific telephones. PDAs were not famous like cloud structure but rather they at any rate give a phase which can utilize a cloud system to utilize shocking getting ready power and storerooms which are none of a PDA. Adaptable based cloud requesting is used coincidentally using flexibility and rate by the help of the scattered figuring's capacity and data putting away limits.

These days, the number of mobile phones and mobile users is expanding quickly. The wide utilization of mobile gadgets has brought the idea of cloud computing in spotlight. The term mobile cloud computing is a procedure of integrating cloud computing within the versatile condition. A portable cloud approach empowers engineers to construct applications structured explicitly for versatile clients without being limited by the portable working framework and the processing or memory limit of the cell phone. Portable distributed computing focused are for the most part gotten to by means of a versatile program from a remote webserver, regularly without the requirement for introducing a customer application on the beneficiary telephone. Individuals are getting increasingly reliant on portable or mobile devices. Mobile cloud computing extends distributed computing by offering upgraded assistance accessibility and by misusing data about a client's area, setting and system knowledge, along these lines consider capably improving client experience. Utilizing the cell phone stockpiling, detecting and handling assets for advancing cloud-based application additionally includes to better client experience. Be that as it may, versatile cloud isn't liberated from blemishes. There had been issues in regards to security and protection of information redistributed. There have been considerable examines on the issue of information get to command over cipher text.

Revised Manuscript Received on June 25, 2020.

* Correspondence Author

Eldhose Peter*, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India. E-mail: petereldhose77@gmail.com

Eldo P Elias, Assistant Professor, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India.

Getting to and recovering of cipher text may get troublesome the same number of records put away under a similar proprietor. In this paper we introduce a effective access and retrieval of cipher text in versatile cloud. Section II portrays the system. In section III, consequence of study is showed.

Section IV depicts the exhibition and section V finishes up the paper.

II. METHODOLOGY

Investigating protection guaranteed and successful pursuit administration over scrambled cloud information is of central significance. Thinking about the huge number of on-request information clients and tremendous measure of re-appropriated information records in the cloud, this issue is especially testing as it is incredibly hard to meet additionally the prerequisites of useful presentation and worthy framework convenience. Here we use Cloud Bloom Filter for productive information access in LDSS framework [5].

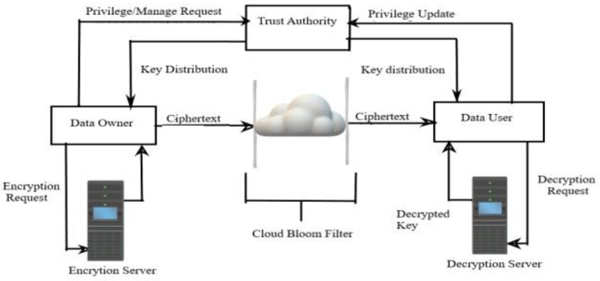

Fig. 2. Architecture

In the wake of enrolling on trust authority information owner encodes the plain content utilizing AES encryption. The key is encoded with the assistance of Encryption server utilizing get to arrangement and open key dispersed from trust authority. Information Owner sends the cipher text (encrypted plain content) to the portable cloud. When cipher text is sent to cloud it go through CBF and a hash function takes information and yields an extraordinary identifier of fixed length which is utilized for ID of information at the point when a client demand a document this one of a kind identifier present in the hash table is made valuable for quicker retrieval of cipher texts in the mobile cloud. The client at that point decodes the record.

Rather than utilizing a variety of bits in traditional Bloom Filter, the Cloud Bloom Filter utilizes a variety of l-bit, where l is the security parameter.[6] Unique in relation to the customary Bloom Filter the false positive is a lot of lower. Since it not just relies upon the collision likelihood of hash capacities, yet additionally relies upon the likelihood of string coordinating. So as to unequivocally find ascribe to comparing cipher text in Mobile cloud, a particular string as the component of the Bloom Filter.

The element of CBF is a two defined string relation, where the two strings refer to the cipher text file property. The CBF can be created by calling the Garbled Bloom Filter algorithm by accepting component arrangements as details [6]. This element is shared with secret sharing and generates sharing irregular strings to include an element in the set to the CBF.

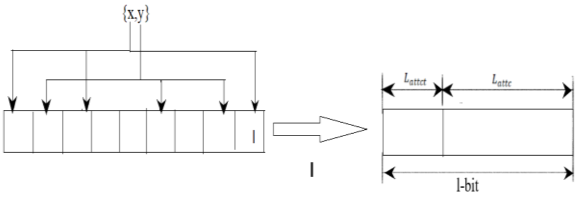

Fig. 2. Cloud Bloom Filter

The element is hashed with various hash functions at that point. Instead of placing a significant hash on the CBF's position record, the element offer will be stored. For Querying, it takes characteristic of information client and processes the positon indices by taking care of the attribute with k hash function to produce the one of a kind hash esteem. At that point it gets the relating strings from the position indexed in the CBF. After it recreates the element and mapped to the file stored.

III. PERFORMANCE ANALYSIS

A. Security Analysis

As per the examination of GBF in [6], the false positive of CBF is an immaterial likelihood. Explicitly a false positive happens just when element isn't in set yet the yield of CBF of equivalent string. Each incentive in CBF will be share of specific element or arbitrary string. Consequently, in the event of element in the input set isn't equivalent to portions of the element, the yield will not equivalent to element. The consequence of XOR will must be an arbitrary string. Anybody can't acquire the attribute except if he is information client.

B. Efficiency Analysis

To assess the proficiency of the proposed arrangement, we direct a few examinations. The trial of CBF is done on an AMD Athlon machine, which has 2.0GHz CPU with the Microsoft operating system (Windows10) installed.

In the strategy proposed, CBF prevails with regards to superseding the customary record document to diminish disk access to 15%. At the point when an information purchaser requests a document, the program tests whether a record exists with the name of the mentioned object, at that point it sidetracks to the position characterized in that object. This decreases the time of access required for the mentioned record.

Table- I: Efficiency Comparison

No. of files	Present Scheme	Proposed Scheme	Time difference
200 files	654.04ms	408.92ms	245.12ms
400 files	767.48ms	508.83ms	258.65ms
600 files	1031.81ms	749.62ms	282.19ms

Retrieval Number: E9969069520/2020©BEIESP
DOI: 10.35940/ijeat.E9969.069520
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication
© Copyright: All rights reserved.

The above table shows the efficiency of data lookup in mobile cloud using proposed method and existing method.

IV. CONCLUSION

Although LDSS explains secure information partaking in versatile cloud, ie, conventional ABE isn't appropriate for mobile cloud since it is computationally serious and cell phones just have restricted assets but not cipher text retrieval. Yet, access of cipher text can be troublesome as the greatest number of information can be there in name of same proprietor. The proposed strategy focuses on proficient cipher text access of mobile cloud by presenting a cloud Bloom Filter. This assists with lessening the disk accesses to as it utilizes a littler hash territory yet at the same time disposes of most superfluous gets to. By lessening disk access during turn upward, the cipher text can recovered quicker from mobile cloud.

REFERENCES

1. D. Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud: Asecure mobile cloud framework for pervasive mobile computing and communication. in: Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering. Nanjing,China: IEEE, pp. 90-98, 2010.
2. P. K. Tysowski and M. A.Hasan. Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds. IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172-186, Nov. 2013.
3. Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010.
4. Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66,2009.
5. Li, R., Shen, C., He, H., Gu, X., Xu, Z., Xu, C.-Z. (2018). A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. IEEE Transactions on Cloud Computing, 6(2), 344–357, 2017.
6. Changyu Dong, Liqun Chen, Zikai Wen, When Private Set Intersection Meets Big Data: An Efficient and Scalable Protocol, In ACM SIGSA conference on Computer communications security, pages 789–800, 2013.
7. Shamir A. How to share a secret. Communications of the ACM,1979, 22 (11): 612-613.
8. Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure keypolicy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2017.

AUTHORS PROFILE

Eldhose Peter received Bachelor of Technology in Computer Science and Engineering from MGM College of Engineering Pambakkuda, Ernakulam in 2017 and currently pursuing Master of Technology in Computer Science and Engineering from Mar Athanasius College of Engineering, Kothamangalam affiliated to APJ Abdul Kalam Technological University. His research interest is in Cryptography Cloud Computing, Deep Learning and Data Mining.

Eldo P Elias is currently a professor in the Department of Computer Science and Engineering of Mar Athanasius College of Engineering, Kothamangalam, Kerala, India. He received her BE Degree in Computer Science and Engineering in 2003 from Bharathiar University and MTech in Software Engineering from CUSAT University, Kerala in 2013. . He has around 7 years of teaching and research experience.