JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PROVIDING A ENCRYPTED DATA SHARING MECHANISM BETWEEN DATA OWNER AND DATA USER IN CLOUD COMPUTING

[1]N. Sivanagamani, ,[2]M.Sailaja
[1] Associate professor,,[2]PG Scholar, Department Of C.S.E
[1,2]Geethanjali Institute of Science And Technology, Kovur, S.P.S.R Nellore Dt,A.P

ABSTRACT

Individuals underwrite the incredible intensity of distributed computing, however can't completely believe the cloud suppliers to have protection delicate information, because of the nonattendance of client to-cloud controllability. To guarantee privacy, information proprietors redistribute encrypted information rather than plaintexts. To impart the encrypted records to different clients, Cipher text-Policy Attribute-based Encryption (CP-ABE) can be used to lead fine-grained and proprietor driven access control. But this does not adequately become secure against different assaults. A malignant aggressor can download a great many records to dispatch Economic Denial of Sustainability (EDoS) assaults, which will to a great extent devour the cloud asset. The payer of the cloud administration bears the cost. In addition, the cloud supplier serves both as the bookkeeper and the payee of asset utilization expense, coming up short on the straightforwardness to information proprietors.

I.INTRODUCTION

Distributed storage has numerous benefits, for example, constantly on the web, pay-as-you-go, and modest [1]. During these years, more information are re-appropriated to open cloud for industrious capacity, including individual and business documents. It brings a security worry to information proprietors [2]–[4]: the open cloud isn't trusted, and the redistributed information ought not be spilled to the cloud supplier without the consent from information proprietors. Numerous capacity frameworks use server-overwhelmed access control, similar to secret word based [5] and certificate-based verification [6]. They excessively trust the cloud supplier to ensure their delicate information. The cloud suppliers and their representatives can peruse any report paying little mind to information proprietors' entrance approach. Additionally, the cloud supplier can overstate the asset utilization of the file stockpiling and charge the payers more without giving verifiable records [2], [7], [8], since we do not have a framework for verifiable calculation of the asset usage.

Relying on the current server-overwhelmed access control isn't verify. Information proprietors who store files on cloud servers still need to control the entrance alone hands and keep the information confidential against the cloud supplier and vindictive clients. Encryption isn't sufficient. To include the confidentiality ensure, information proprietors can encrypt the files and set an entrance arrangement with the goal that just qualified clients can decrypt the archive. With Cipher text-Policy Attribute-based Encryption (CP-ABE) [9], [10], we can have both fine-grained access control and solid confidentiality . In any case, this entrance control is accessible for information proprietors, which ends up being insufficient. In the event that the cloud supplier can't verify clients before downloading, as in many existing CP-ABE distributed storage frameworks [14], [15], the cloud needs to enable everybody to download to guarantee accessibility. This makes the capacity framework defenseless against the asset fatigue assaults. As far as we could possibly know, this is the first work to guarantee that insufficient cloud-side access control in encrypted distributed storage will prompt EDoS assaults and gives a reasonable arrangement. The arrangement can be good with numerous CP-ABE plans. 2) For various information proprietor online examples and execution concern, we give two conventions to confirmation and asset utilization bookkeeping. We likewise present the blossom filter and the probabilistic check to improve the efficiency yet at the same time ensure the security. 3) Compared with many condition of-expressions developments of encrypted distributed storage that accept the presence of a semihonest cloud supplier, we utilize a progressively handy risk model where we expect the cloud supplier to be a secretive foe [24], which gives higher security guarantee.

II.LITERATURE SURVEY

A. Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner

A few plans for k-closest neighbors (k-NN) inquiry over encrypted information in cloud have been proposed as of late. By and by, existing plans either assume each question client is completely trusted, or need information proprietor to be online for each inquiry. A completely confided in question client is accepted to get the decryption key of information proprietor's re-appropriated dataset, subsequently, cloud server could altogether break the redistributed dataset after picking up the decryption key from some deceitful inquiry client. In view of the online necessity, information proprietor still needs to load such a large number of computational errands during the k-NN questions, which in this way is illogical. In this paper, we propose another plan to perform k-NN question over encrypted information in cloud while securing the protection of the two information proprietor and inquiry clients from cloud. Our new strategy just uncovers constrained information about information proprietors critical to question clients, and has no need of an online information proprietor. For picking up the properties, we present another scalar item convention, at that point the new convention and some other change methodologies are converted into our safe k-NN inquiry framework. Furthermore, we affirm our security and productivity through hypothetical examination and broad reenactment tests.

B. Online/offline attribute-based encryption

Quality based encryption (ABE) is a kind of open key encryption that enables clients to encrypt and decrypt messages dependent on client characteristics. For example, one can encrypt a message to any client fulfilling the boolean recipe ("crypto meeting participant" AND "PhD understudy") OR "IACR part". One disadvantage is that encryption and key age computational costs scale with the unpredictability of the entrance approach or number of characteristics. Practically speaking, this makes encryption and client key age a conceivable bottleneck for certain applications. To address this issue, we grow new procedures for ABE that split the calculation for these calculations into two stages: a readiness stage that does most by far of the work to encrypt a message or make a mystery key before it knows the message or the quality rundown/get to control strategy that will be utilized (or even the size of the rundown or arrangement). A subsequent stage can then quickly gather an ABE cipher text or key when the points of interest become known.

C.TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage

Quality based Encryption (ABE) is viewed as a promising cryptographic leading instrument to ensure information proprietors' immediate power over their information in open distributed storage. The prior ABE plans include just a single expert to keep up the entire characteristic set, which can bring a solitary point bottleneck on both security and execution. In this manner, some multi-specialist plans are proposed, in which different experts independently keep up disjoint quality subsets. In any case, the single-point bottleneck issue stays unsolved. In this paper, from another point of view, we lead an edge multi-specialist CP-ABE access control plot for open distributed storage, named TMACS, in which different experts mutually deal with a uniform quality set. In TMACS, exploiting (t, n) limit mystery sharing, the ace key can be shared among different specialists, and a lawful client can produce his/her mystery key by communicating with any t experts.

D.TAFC: Time and attribute factors combined access control for time sensitive data in public cloud

The new worldview of re-appropriating information to the cloud is a twofold edged sword. From one perspective, it liberates information proprietors from the specialized administration, and is simpler for information proprietors to impart their information to proposed clients. Then again, it presents new difficulties on protection and security assurance. To secure information secrecy against the fair however inquisitive cloud specialist organization, various works have been proposed to help fine-grained information access control. In any case, till now, no plans can bolster both fine-grained access control and time-delicate information distributing. In this paper, by implanting coordinated discharge encryption into CP-ABE (Cipher text-Policy Attribute-based Encryption), we propose another time and trait variables joined access control on time-touchy information for open distributed storage (named TAFC). In view of the proposed plan, we further propose an effective way to deal with configuration get to arrangements looked with different access necessities for time-touchy information. Broad security and execution investigation demonstrates that our proposed plan is profoundly productive and fulfills the security necessities for time sensitive information stockpiling in open cloud.

III.EXISTING SYSTEM

Distributed stockpiling has various favorable circumstances, for instance, always on the web, pay-as-you-go, and unobtrusive . In the midst of these years, more information are re-appropriated to open cloud for steady limit, including individual and business reports. It passes on a security stress to information owners individuals when all is said in done cloud isn't trusted, and the redistributed information should not be spilled to the cloud provider without the approval from information owners. Various limit systems use server-ruled access control, like mystery key based and underwriting based affirmation . They too much trust the cloud provider to guarantee their fragile information. The cloud providers and their agents can scrutinize any report paying little regard to information owners' passageway methodology.

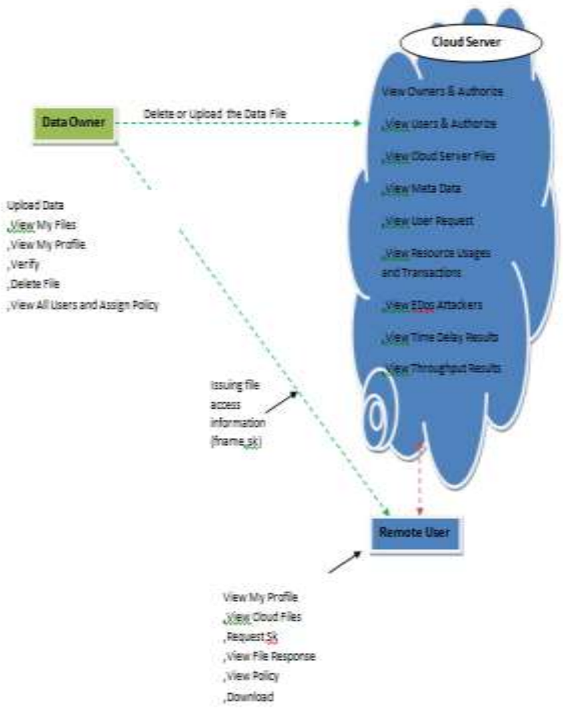
In expansion, the cloud provider can distort the benefit use of the archive storing and charge the payers more without giving certain records, since we miss the mark on a structure for verifiable computation of the advantage usage. Relying on the present server-ruled access control isn't grapple. Information owners who store reports on cloud servers still need to control the passage exclusively hands and keep the information ordered against the cloud provider and harmful customers.

IV.PROPOSED SYSTEM

We join the cloud-side access control and the present information owner side CP-ABE based access control, to decide the recently referenced security issues in insurance sparing dispersed capacity. Our methodology can keep the EDoS attacks by enabling the cloud server to check whether the customer is endorsed in CP-ABE based arrangement, without discharging other information.

For our cloud-side access control, we use CP-ABE encryption/unscrambling delight as test response. While move an encoded archive, the information owner immediately makes some unpredictable test plaintexts and the contrasting cipher texts. The cipher texts are related to a comparable access course of action with the express record. For a moving toward information customer, the cloud server asks him/her to disentangle subjectively picked test cipher text. In case the customer shows a correct result, which suggests he/she is endorsed in CP-ABE, the cloud-side access control allows the record download.

A. Architecture Diagram



V.MODULES

1.Data Owners

DATA Owners are the proprietor and distributer of records and pay for the asset utilization on document sharing. As the payers for cloud benefits, the information proprietors need the straightforwardness of asset utilization to guarantee reasonable charging. The information proprietors require the cloud supplier to legitimize the asset utilization. In our framework, the information proprietor isn't constantly on the web.

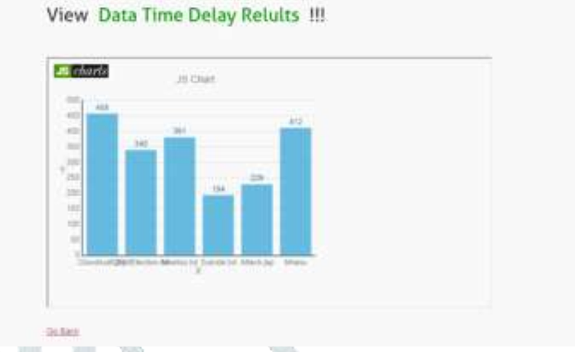
2.Data Users

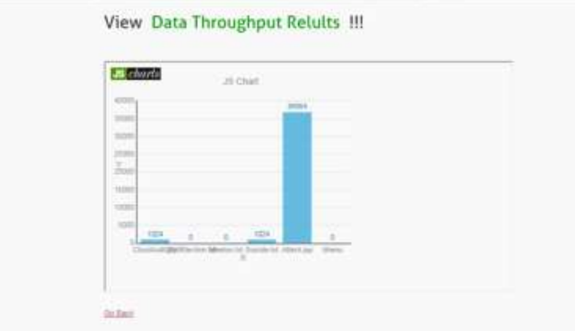
DATA users need to acquire a few records from the cloud supplier put away on the distributed storage. They should be verified by the cloud supplier before the download (to obstruct EDoS assaults). The approved clients at that point affirm (and sign for) the asset utilization for this download to the cloud supplier.

3.Cloud Server

Cloud supplier has the encrypted stockpiling and is constantly on the web. It records the asset utilization and charges information proprietors dependent on that record. The cloud isn't open available in our framework as it has a confirmation based access control. Just information clients fulfilling the entrance approach can download the relating records. The cloud supplier likewise gathers the verification of the asset utilization to legitimize the charging.

VI.RESULTS:


View Data Time Delay Relults !!!


View Data Throughput Relults !!!

V.CONCLUSIONS

In this paper, we propose a consolidated the cloud-side and information proprietor side access control in encrypted distributed storage, which is impervious to DDoS/EDoS assaults and gives asset utilization bookkeeping. Our framework underpins subjective CP-ABE developments. The development is secure against malignant information clients and an undercover cloud supplier. We loosen up the security necessity of the cloud supplier to secretive enemies, which is a more functional and loosened up thought than that with semi-legitimate foes. To utilize the undercover security, we use blossom filter and probabilistic check in the asset utilization bookkeeping to decrease the overhead. Execution investigation demonstrates that the overhead of our development is little over existing frameworks.

REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1,

no. 1, pp. 7–18, 2010.

[2] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, no. 1, pp. 69–73, 2012.

[3] L. Zhou, Y. Zhu, and A. Castiglione, “Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner,” Computers & Security, vol. 69, pp. 84–96, 2017.

[4] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, “Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data,” IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.

[5] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, “oPass: A user authentication protocol resistant to password stealing and password reuse attacks,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, 2012.

[6] L. Harn and J. Ren, “Generalized digital certificate for user authentication and key establishment for secure communications,” IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.

[7] V. Sekar and P. Maniatis, “Verifiable resource accounting for cloud computing services,” in Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM, 2011, pp. 21–26.

[8] C. Chen, P. Maniatis, A. Perrig, A. Vasudevan, and V. Sekar, “Towards verifiable resource accounting for outsourced computation,” in ACM SIGPLAN Notices, vol. 48, no. 7. ACM, 2013, pp. 167–178.

[9] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in 2007 IEEE Symposium on Security and Privacy (SP’07). IEEE, 2007, pp. 321–334.

[10] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography–PKC 2011. Springer, 2011, pp. 53–70.

[11] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[12] S. Yu, K. Ren, and W. Lou, “Attribute-based content distribution with hidden policy,” in Proceedings of 4th Workshop on Secure Network Protocols (NPSec2008). IEEE, 2008, pp. 39–44.

[13] S. Hohenberger and B. Waters, “Online/offline attribute-based encryption,” in Public-Key Cryptography–PKC 2014. Springer, 2014, pp. 293–310.

[14] W. Li, K. Xue, Y. Xue, and J. Hong, “TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484–1496, 2016.

[15] J. Hong, K. Xue, Y. Xue, W. Chen, D. S. Wei, N. Yu, and P. Hong, “TAFC: Time and attribute factors combined access control for timesensitive data in public cloud,” IEEE Transactions on Services Computing, Online, 2017.