International Journal of Science Engineering and Advance Technology

Multilevel Components to Improve Factor Revocability And Data Security Protection In Cloud

V.Siva Krishna Veni
Lecturer, Dept. of Computer Science,
Sri Durga Malleswara Siddhartha Mahila kalasala,
Vijayawada, A.P., India.

Abstract —The data stored in cloud environment can be accessed from anywhere and at anytime and by anyone. Many techniques effectively provide the security for cloud storage data. During transmission of data in cloud environment, encryption is an efficient and widely used technique for data security. Thought cloud service provides such services but security and privacy of owner's data is major concern in cloud storage. Therefore secure data access is critical issue in cloud storage. In this paper Proposed system an improve data security protection mechanism for cloud using two components. In this system sender sends an encrypted message to a receiver with the help of cloud system. The sender requires to know identity of receiver but no need of other information such as certificate or public key. To decrypt the cipher text, receiver needs two parts. The first thing is a unique personal security device or some hardware device connected to the computer system. Second one is private key or secrete key stored in the computer.

Without having these two things cipher text never decrypted. The important thing is the security device lost or stolen, then cipher text cannot be decrypted and hardware device is revoked or cancelled to decrypt cipher text. The efficiency and security analysis show that the system is secure as well as practically implemented. The system uses a new hardware device like pen drive etc. to decrypt the cipher text together with the private key.

Keywords — Access control,Security, Two-Components, factor revocability, public Cloud Storage.

1.INTRODUCTION

Security is by and large a coveted condition of being free from hurt. As characterized in data security, it is a condition in which a data resource is ensured against its classification, respectability and accessibility in the coveted state and at the opportune time. Security for the cloud is most vital viewpoint, there are various issues to be tended to if the cloud is to be impeccably secure. As distributed computing is accomplishing expanded prominence, concerns are being voiced about the security issues presented through reception of this new model. Different security instruments are perceived as the highlights of this imaginative sending model can vary generally from those of conventional structures. An option point of view on the theme of cloud security is this is yet another, albeit very expansive, instance of "connected security" and that comparative security rule that can be shared multi-client centralized computer security models apply with cloud security. Notwithstanding, in the distributed computing condition, cloud specialist co-ops can be assaulted by noxious aggressors. These assaults may release the classified data of clients for business interests as the information proprietors usually store unscrambled information in cloud servers. The most effective method to acknowledge get to control to the scrambled information and guarantee the privacy of information records of clients in an untrusted cloud condition are the significant issues. In addition, since the quantity of clients is vast in a distributed computing condition, how to acknowledge adaptable, adaptable and fine-grained get to control is unequivocally wanted in the administration arranged distributed computing model.

Distributed computing gives shared handling condition to information stockpiling and getting to otherwise called internetbased processing. It is a model which gives configurable processing assets, for example, systems, servers, stockpiling, applications and administrations. Distributed computing has a high calculation control, most minimal cost of administrations, higher execution, versatility, openness and accessibility therefore it is exceedingly requested. Information outsourcing carries with it many points of interest. metadata and information are put away in cloud database

and can access by customer through encoded database motor. Scrambled motor get expected metadata to execute SQL questions from cloud database and decode it through ace key which is with customer side application. Versatile encryption plot consider numerous SQL mindful encryption calculation, for example, Random, Deterministic which bolsters balance administrators, arrange safeguarding encryption, homomorphic entireties, plain and hunt. Versatile encryption conspire consider numerous SQL mindful encryption calculation, for example, Random,Deterministic which underpins balance administrators, arrange safeguarding encryption, homomorphic sums,plain and look. On the off chance that every section is encoded through just a single calculation then chairman needs to choose database operations at configuration time just for every section. Here encryption calculations are sorted out into structure called onions, where every onion is comprised of requested arrangement of encryption calculation called layer. Onions layers are utilized for fairness, examination, summation, string equity administrators.

Each plaintext section is encoded into at least one scrambled segment every one comparing to an onion. Each plain content is encoded through every one of the layers of its onion i.e.encrypted through more than on encryption calculation. Thought this approach gives more versatile instrument to getting to cloud database, get to arrangements are relegated by information proprietor or single expert no one but which can bring about framework bottleneck. Multi-User Encrypted SQL Operation on Cloud approach gives adaptable and secret access to cloud database. This engineering called MultiUser social Encrypted Data Base (Mute DB) that ensures information privacy by executing SQL operation on information by applying access control arrangements. The Mute DB does not depend on any transitional intermediary to keep away from single point bottleneck.

Here each datum and metadata is put away on cloud in scrambled arrangement. Here information oversaw and make by DBA, who is additionally dependable putting away scrambled information and metadata on the cloud. DBA is the trusted substance who possesses root qualifications, oversees client accounts and implements get to control approaches. This ACP characterizes which client can approach on which information. Every client will be given arrangement of accreditations including all the data that permits him/her to get to genuine information. For this situation get to strategies are likewise encoded and put away in cloud. The DBA is the main expert who can have control on all framework substance; this can leads toward DBA over-burdening and can resulton execution debasement.

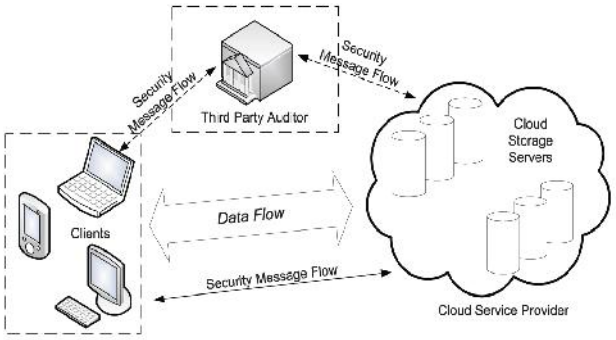


Fig : Architecture

2.LITERATURE SURVEY

Secure threshold multi authority attribute based encryption without a central authority

AUTHORS: H. Lin, Z. Cao, X. Liang, and J. Shao

An attribute based encryption scheme (ABE) is a cryptographic primitive in which each client is distinguished by an arrangement of traits, and some capacity of these credits is utilized to decide the capacity to unscramble each ciphertext. Pursue proposed the main multi expert ABE conspire in TCC 2007 as a response to an open issue displayed by Sahai and Waters in EUROCRYPT 2005. Be that as it may, her plan needs a completely trusted focal expert which can decode each ciphertext in the framework. This focal expert would jeopardize the entire framework if it's corrupted.This paper shows an edge multi specialist fluffy character based encryption (MA-FIBE) conspire without a focal specialist interestingly. An encrypter can encode a message to such an extent that a client could just unscramble on the off chance that he has in any event d k of the given characteristics about the message for in any event $t+1$, $t \leq n/2$ fair specialists of all the n quality experts in the proposed conspire. The security confirmation depends on the mystery of the hidden joint irregular mystery sharing convention and joint zero mystery sharing convention and the standard decisional bilinear Diffie-Hellman supposition. The proposed MA-FIBE could be reached out to the edge multi specialist trait based encryption (MA-ABE) conspire and be additionally stretched out to a proactive MA-ABE plot.

Multi-authority attribute-based encryption with honest-but-curious central authority

AUTHORS: V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi

An attribute-based encryption plot fit for dealing with various specialists was as of late proposed by Chase. The plan is based upon a solitary expert trait based encryption plot exhibited before by Sahai and Waters. Pursue's development utilizes a trusted focal expert that is innately equipped for unscrambling discretionary ciphertexts made inside the framework. We display a multi-specialist quality based encryption conspire in which just the arrangement of beneficiaries characterized by the scrambling gathering can decode a comparing ciphertext. The focal expert is seen as 'legitimate yet inquisitive': from one viewpoint, it sincerely takes after the convention, and then again, it is interested to decode discretionary ciphertexts consequently damaging the expectation of the encoding party. The proposed plot, which like its antecedents depends on the Bilinear Diffie– Hellman suspicion, has a many-sided quality practically identical to that of Chase's plan. We demonstrate that our plan is secure in the particular ID show and can endure a legitimate however inquisitive focal specialist.

Attribute-based secure data sharing with hidden policies in smart grid

AUTHORS: J. Hur

Shrewd matrix utilizes wise transmission and appropriation systems to convey power. It expects to enhance the electric framework's dependability, security, and productivity through two-path correspondence of utilization information and dynamic streamlining of electric-framework operations, support, and arranging. The savvy matrix frameworks utilize fine-grained control lattice estimations to give expanded network security and unwavering quality. Key to accomplishing this is safely sharing the estimations among framework substances over wide territory systems. Commonly, such sharing takes after arrangements that rely upon information generator and shopper inclinations and on time-delicate settings. In shrewd framework, and additionally the information, approaches for sharing the information might be touchy on the grounds that they straightforwardly contain delicate data, and uncover data about fundamental information ensured by the strategy, or about the information proprietor or beneficiaries. In this examination, we propose a trait based information sharing plan in brilliant matrix. The information as well as the entrance approaches are jumbled in matrix administrators' perspective amid the information sharing procedure. Therefore, the information security and strategy protection are saved in the proposed plot. The entrance arrangement can be communicated with any discretionary access equation. Accordingly, the expressiveness of the arrangement is improved. The security is additionally enhanced to such an extent that the unapproved key era focus or the matrix oversee frameworks that store the information can't decode the information to be shared. The calculation overhead of beneficiaries are additionally diminished by appointing a large portion of the difficult unscrambling operations to the all the more capable lattice oversee frameworks.

IMPLEMENTATION

Two-Factor Data Security Protection Mechanism For Cloud Storage System:

This algorithm allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the cipher text. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the cipher text without either piece.

Approach:

The encryption procedure is executed twice. In the first place encode the plaintext relating to people in general key or character of the client. At that point scramble it again comparing to the general population key or serial number of the security gadget. For the unscrambling stage, the security gadget initially decodes once. The halfway decoded ciphertext is then passed to the PC which utilizes the client mystery key to additionally unscramble it. Without either part (client mystery key or security gadget) one can't unscramble the ciphertext. In the event that the client has lost his security gadget, at that point his/her comparing ciphertext in the cloud can't be unscrambled until the end of time! That is, the approach can't bolster security gadget refresh/revocability. Certifiable executed case: At AT&T labs, in a druva framework, a message is first scrambled under a client key k1, and next transferred to a cloud server. The client key k1 is additionally scrambled by another client key k2, and put away in the server too. The key k2 is held by the client. While recovering the message, the client needs to utilize k2 to recoup k1

which is additionally used to recuperate m. It is irrefutable that this message-key scramble system is vastly improved than the mode just utilizing a solitary key to encode an outsourced information, and putting away the ciphertext alongside the key in the server. By and by, this instrument experiences a potential hazard practically speaking. Once the client loses the key k2, all information of the client put away in the cloud can't be recovered. The absence of revocability for encryption factor confines the adaptability of the framework

3. REALATED WORK

Our framework is an IBE (Identity-based encryption)-based system. That is, the sender just has to know the personality of the recipient keeping in mind the end goal to send an encoded information (ciphertext) to him/her. No other data of the collector (e.g. open key, testament and so on.) is required. At that point the sender sends the ciphertext to the cloud where the beneficiary can download it at whenever.

Our framework gives two-factor information encryption assurance. So as to decode the information put away in the cloud, the client needs to have two things. To start with, the client needs his/her mystery enter which is put away in the PC. Second, the client needs an extraordinary individual security gadget which will be utilized to associate with the PC (e.g. USB, Bluetooth and NFC). It is difficult to decode the ciphertext without either piece.

All the more significantly, our framework, interestingly, gives security gadget (one of the components) revocability. Once the security gadget is stolen or detailed as lost, this gadget is renounced. That is, utilizing this gadget can never again decode any ciphertext (comparing to the client) in any condition. The cloud will instantly execute a few calculations to change the current ciphertext to be un-decryptable by this gadget. While the client needs to utilize his new/substitution gadget (together with his mystery key) to unscramble his/her ciphertext. This procedure is totally straightforward to the sender.

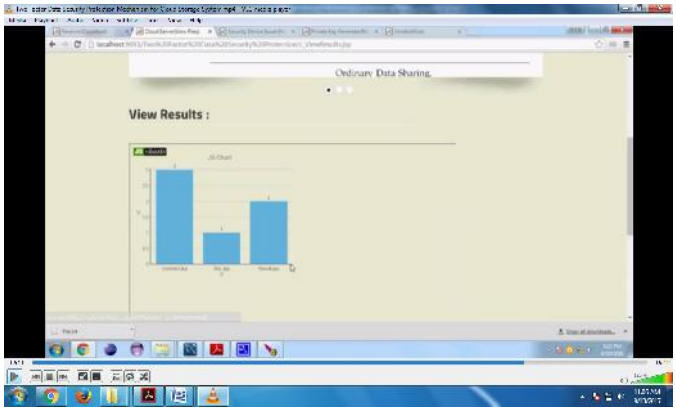
The cloud server can't decode any ciphertext whenever. We give an estimation of the running time of our model to demonstrate its common sense, utilizing some benchmark comes about. We additionally take note of that despite the fact that there exist some credulous methodologies that appear to accomplish our objective, that there are numerous restrictions by each of them and along these lines we trust our instrument is the first to accomplish all the previously mentioned includes in the writing.

User Revocation Based ABE ALGORITHM:

The concept of **attribute based encryption** is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent about attributes. In a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

Step 1: Select File attribute1 – say File name
Step 2: Convert the file name to Binary Codes
Step 3: Select File attribute 2 – say file size
Step 4 : Convert the file size to Binary Codes
Step 5: Perform AND Operation of File Attribute 1 and 2
Step 6: Perform OR Operation of File Attribute 1 and 2
Step 7: Result of AND Operation Stored as Secret Key
Step 8: Result of OR Operation Stored as Public Key

4.EXPERIMENTATION RESULTS



CONCLUSION

In this our solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked, the corresponding ciphertext will be updated automatically by the cloud server without any notice of the data owner. Furthermore, we presented the security proof and efficiency analysis for our system.

REFERENCES

[1]. Chen, H. C., Hu, Y., Lee, P. P., & Tang, Y. (2014). NCCloud: a network-coding-based storage system in a cloud-of-clouds. IEEE Transactions on Computers, 63(1), 31-44.

[2]. Chu, C. K., Chow, S. S., Tzeng, W. G., Zhou, J., & Deng, R. H. (2014). Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems, 25(2), 468-477.

[3]. Cloud Security Alliance, SecaaS Implementation Guidance, Category 8: Encryption. Version 1.0, CSA, 2012.

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang. Malicious kgc attacks in certificateless cryptography. In ASIACCS, pages 302–311. ACM, 2007.

[5] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In K. Nyberg, editor, EUROCRYPT, volume 1403 of LNCS, pages 127–144. Springer, 1998.

[6] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In P. Ning, P. F. Syverson, and S. Jha, editors, ACM Conference on Computer and Communications Security, pages 417–426. ACM, 2008.

[7] D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techn., 4(1):60–82, 2004.

[8] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In CRYPTO ’01, volume 2139 of LNCS, pages 213– 229. Springer, 2001.

[9] R. Canetti and S. Hohenberger. Chosen-ciphertext secure proxy re-encryption. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, ACM Conference on Computer and Communications Security, pages 185–194. ACM, 2007.

[10] D. Sudhadevi and K. Thilagavathy, “A novel approach to enhance cloud data defense,” Asian Journal of Information Technology, vol. 12, no. 9, pp. 305–311, 2013.

[11] Ferretti, L., Colajanni, M., & Marchetti, M. (2014). Distributed, concurrent, and independent access to encrypted cloud databases. IEEE transactions on parallel and distributed systems, 25(2), 437-446.

[12] Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y. (2016). Two-Factor Data Security Protection Mechanism for Cloud Storage System. IEEE Transactions on Computers, 65(6), 1992-2004.

About author:

V.SIVA KRISHNA VENI is presently working as Lecturer, Dept. of Computer Science, Sri Durga Malleswara Siddhartha Mahila kalasala,Vijayawada, A.P., India. She has more than ten years of experience in teaching field, her area of interests are cloud computing & Hadoop.

E-Mail: venivasantha@gmail.com