ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Unified Data Access Security on Revocable Multi Authority CP-ABE in Cloud

Suresh Kumar.P[1], Tamilselvan.D[2], Anuradha.C[3]

Assistant Professor, Department of Computer Science and Engineering, Bharath University, Chennai, India[3]

Student, Department of Computer Science and Engineering, Bharath University, Chennai, India[1,2]

ABSTRACT: The cloud information administrations, it is typical for information to be put away in the cloud, as well as imparted crosswise over various Users. A few systems have been intended to permit both information holders and open verifiers to proficiently review cloud information trustworthiness without recovering the whole information from the cloud server. Be that as it may, open examining on the respectability of imparted information to these current systems will definitely uncover classified data character protection to open verifiers. Information access control is a successful approach to guarantee the information security in the cloud. Because of information outsourcing and untrusted cloud servers, the information access control turns into a testing issue in distributed storage frameworks. Our property renouncement technique can effectively attain to both forward security and retrogressive security

KEYWORDS: Cloud Computing ,Cipher text-Policy Attribute-based Encryption, Cloud Security

I. INTRODUCTION

Cloud storage is a basic organization of appropriated processing which offers organizations for data chiefs to host their data in the cloud. This new perfect model of data encouraging and data access organizations familiarizes a staggering test with data access control. Since the cloud server can't be totally trusted by data administrators, they can no more depend on upon servers to do access control.

(CP-ABE) Cipher text-Policy Attribute-based Encryption is seen as a champion amongst the most suitable advances for data access control in dispersed stockpiling systems, in light of the fact that it gives the data chief more direct control on access methods. In CP-ABE arrangement, there is a power that is accountable for property organization and key scattering. The force can be the enlistment office in a school, the human resource division in an association, etc. We altogether upgrade the adequacy of the quality disavowal procedure. Specifically, in our new trademark denial system, simply the ciphertexts that joined with the revoked credit needs to be redesignd, while in all the ciphertexts that associated with any quality from the force (identifying with the denied property) should be upgraded.

II. DATA STORAGE IN CLOUD

Distributed storage is a model of information stockpiling where the computerized information is put away in coherent pools, the physical stockpiling degrees various servers and physical environment is ordinarily claimed and oversaw by a facilitating organization. The distributed storage suppliers are in charge of keeping the information accessible and available at all times, and the physical environment ensured and running. Associations and people purchase or lease stockpiling limit from the suppliers to store client, association, or application data.Security of put away information and information in travel may be a worry when putting away touchy information at a distributed storage supplier. Clients with particular records-keeping prerequisites, for example, open associations, that must safeguard electronic records as indicated by declaration, may experience confusions with utilizing distributed computing and storage.When an association decides to store information or host applications on general society cloud, it will lose physical access to servers facilitating its data. Because of this, possibly business delicate and classified information is at the danger of insider assaults. In light of a late Cloud Security Alliance Report, insider assaults is the third greatest danger to the distributed computing. In this manner, Cloud Service suppliers must guarantee that thorough historical verifications are directed for representatives who have physical access to the servers in the server farm. Notwithstanding that, server farms ought to be much of the time observed for fearful movement.

III. Related Work

In numerous access control frameworks, each bit of information may lawfully be gotten to by a few separate clients. Such a framework is regularly actualized by utilizing a trusted server which stores all the information in clear. A client would log into the server and after that the server would choose what information the client is allowed to get to. However such an answer accompanies an expense: imagine a scenario where the server is bargained. An aggressor who is fruitful in breaking into the server can see all the touchy information in clear. One regular answer for the above issue is to keep the information on the server scrambled with the private keys of the clients who are allowed to get to it. However taking care of a complex access control strategy utilizing customary open key encryption frameworks can be troublesome. This is on account of the entrance arrangement may be depicted as far as the properties or qualities that a legitimate client ought to have instead of as far as the real personalities of the clients. In this manner, from the earlier, one may not in any case know the accurate rundown of clients approved to get to a specific bit of information.[1][2]We frequently distinguish individuals by their properties. In 2005, Sahai andWaters proposed a framework (depicted in later phrasing as a key-arrangement quality based encryption (ABE) framework for edge strategies) in which a sender can encode a message indicating a characteristic set and a numbered, such that just a beneficiary with at any rate d of the given traits can decode the message. Then again, the sending ramifications of their plan may not be totally sensible, in that it expect the presence of a solitary trusted gathering who screens all properties and issues all decoding keys. Rather, we regularly have distinctive elements in charge of observing diverse qualities of a man, e.g. the Department of Motor Vehicles tests whether you can drive, a college can ensure that you are an understudy, and so forth. Hence, gave a multi-power ABE plan which underpins various powers working at the same time, every distributing mystery keys for an alternate arrangement of properties. Be that as it may, this arrangement was still not perfect.

There are two principle issues: one worry of security of the encryption, the other the protection of the clients.[2][3]Traditionally, we see encryption as a system for a client, Alice, to condentially encode information to a target beneficiary, Bob. Alice scrambles the information under the beneficiary's open key such that just Bob, with learning of his private key, can decode it. Be that as it may, in numerous applications, we and we have to impart information as indicated by an encryption approach without former learning of who will be getting the information. Assume an overseer needs to scramble a lesser employee's execution survey for all senior individuals from the software engineering division or anybody in the dignitary's and so forth. The overseer will need to encode the audit with the entrance arrangement (\Computer Science" AND \Tenured"). In this framework, just clients with properties (qualifications) that match this strategy ought to have the capacity to decode the record. The key test in building such frameworks is to acknowledge security against plotting clients. Case in point, the scrambled records ought not be open to a couple of unapproved clients, where one has the two accreditations of "Tenured".[3][4]The proposed framework comprises of Data holder, which is the client who needs to outsource her information into the cloud. Likewise she is in charge of scrambling _les and creating access structure approaches. Trusted power is the piece of the framework who is in charge of \issuing, disavowing, and overhauling trait keys for clients". The clients are all the clients who tries to get to the framework either approved or unapproved. At last is the administration supplier, which is a legit yet inquisitive framework that does what it should do yet needs to get to the plaintext for interest. The essential structure of the framework is the same as the first CP-ABE framework which was presented in a past paper, with an expansion of two new capacities. The principal capacity is KEKGen(U) which is utilized to create keys to scramble characteristics for gatherings.[4][5]Online applications are helpless against robbery of touchy data on the grounds that enemies can misuse programming bugs to obtain entrance to private information, and in light of the fact that inquisitive or malevolent heads may catch and break information. CryptDB is a framework that gives handy also provable privacy despite these assaults for applications supported by SQL databases. It lives up to expectations by executing SQL inquiries over encoded information utilizing an accumulation of effective SQL-mindful encryption plans. CryptDB can likewise affix encryption keys to client passwords, so that an information thing can be decoded just by utilizing the secret key of one of the clients with access to that information. Accordingly, a database director never becomes acquainted with decoded information, and regardless of the possibility that all servers are bargained, a foe can't unscramble the information of any client who is not logged in.[5][6]Distributed computing permits information managers to utilize huge information stockpiling and tremendous reckoning capacities at a low cost. Notwithstanding the profits, information outsourcing denies information holders of direct control over their outsourced information. To assuage concerns, information holders ought to scramble their information before outsourcing to the cloud. In any case, encryption can upset some helpful capacities for example, seeking over the outsourced encoded information while implementing an entrance control strategy. Besides, it is common to outsource the hunt operations to the cloud, while keeping the outsourced information private. There is a need to permit the information clients to confirm whether the cloud reliably executed the inquiry operations or not. To the best of our insight, existing arrangements can't accomplish these goals all the while.[6]

IV. EXISTING TECHNIQUE

Since the cloud server can't be completely trusted by information holders, they can no all the more depend on upon servers to do access control. (CP-ABE) Ciphertext Policy Attribute-based Encryption is seen as a champion amongst the most suitable progressions for information access control in coursed stockpiling structures, in light of the way that it gives the information chief all the more clear control on access strategies. It Cannot Store them in mixed format.each customer is deceitful and may interest to get unapproved access to data. each customer having the changed key. On the other hand, it is hard to unequivocally apply these multi-power CP-ABE plans to multi-power passed on limit frameworks as a result of the trait renouncement issue.

V. REVOCABLE MULTI AUTHORITY CP-ABE

To solve the existing security issue in this paper, we first propose a revocable multi authority CP-ABE plan, where an effective and secure renouncement system is proposed to take care of the trait disavowal issue in the framework. As portrayed in our quality disavowal technique is effective as in it acquires less correspondence expense and reckoning cost, and is secure as in it can attain to both retrogressive security (The repudiated client can't unscramble any new ciphertext that obliges the denied credit to decode) and forward security (The recently joined client can likewise decode the beforehand distributed ciphertexts1, in the event that it has sufficient characteristics). At that point, we apply our proposed revocable multi-power CP-ABE conspire as the hidden strategies to build the expressive and secure information access control plan for multi-power distributed storage frameworks.

There are five types of entities in the system: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). The CA is a global trusted certificate authority in the system.

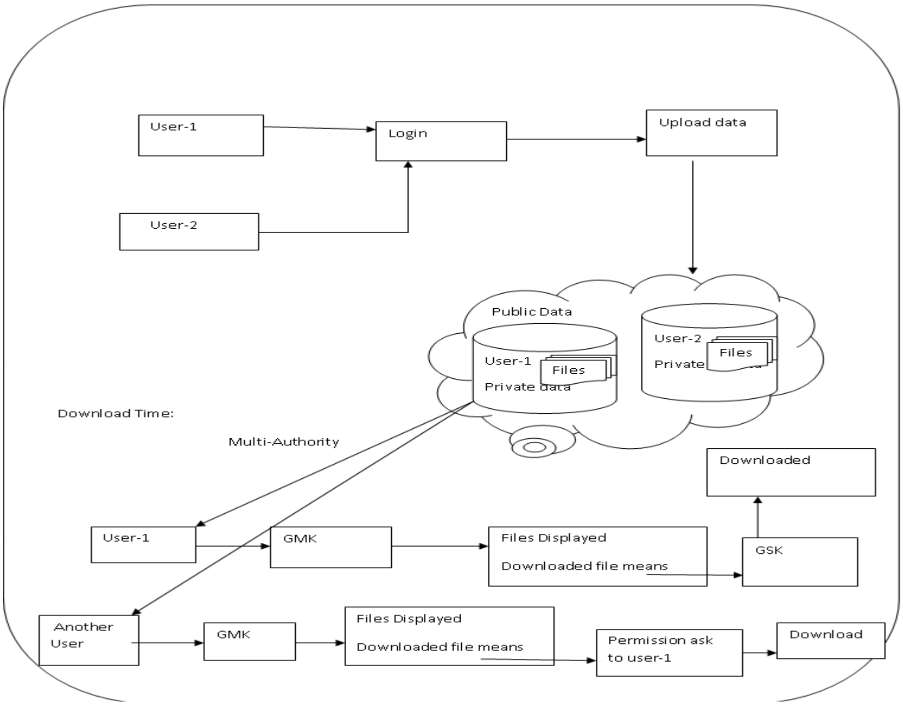
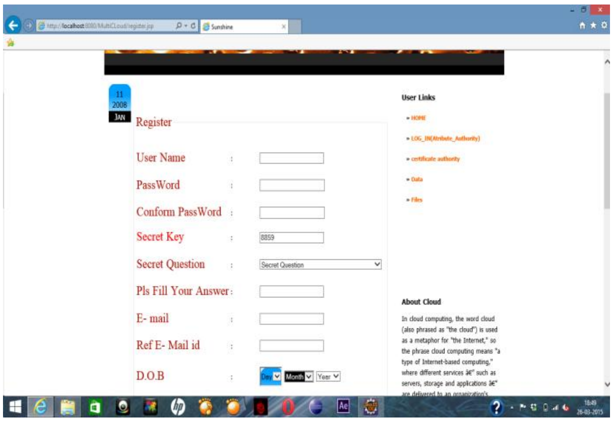


Fig. 1. Proposed System Architecture

VI. RESULTS

First the user is asked to register to the system with all the details regarding username, password, secret key, email id and date of birth.



Register

User Name :

PassWord :

Conform PassWord :

Secret Key : 8859

Secret Question : Secret Question

Pls Fill Your Answer :

E- mail :

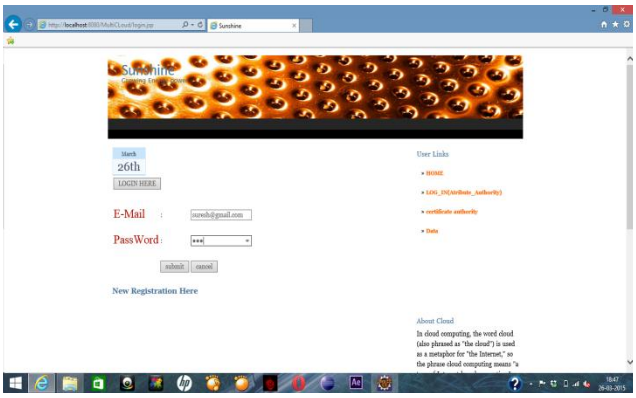
Ref E- Mail id :

D.O.B : Day Month Year

About Cloud

In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services â€" such as servers, storage and applications â€" are delivered to an organization's

Then the user can login using the registered email and password to access the cloud.



E-Mail : suresh@gmail.com

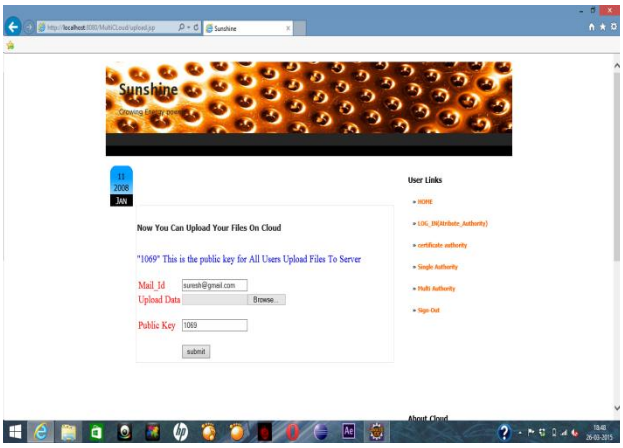
PassWord : •••

New Registration Here

About Cloud

In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a

Now the admin or first user can upload his/her file in the cloud storage along with the public key to authorize.



Now You Can Upload Your Files On Cloud

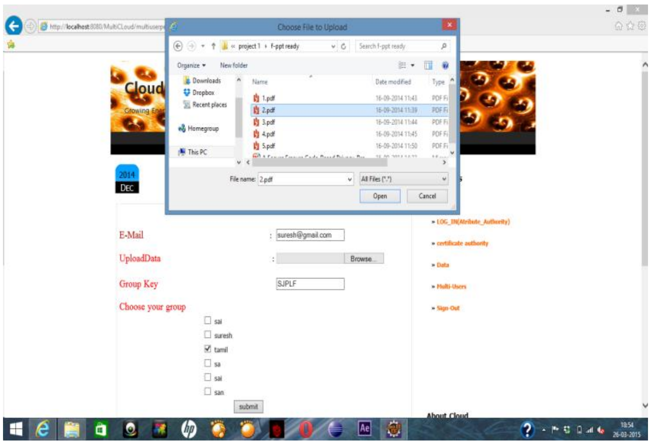
"1069" This is the public key for All Users Upload Files To Server

Mail_Id suresh@gmail.com

Upload Data

Public Key 1069

Now the user can upload data along with the group key for multiple users to access the file.



Name	Date modified	Type
1.pdf	16-09-2014 11:43	PDF Fi
2.pdf	16-09-2014 11:39	PDF Fi
3.pdf	16-09-2014 11:44	PDF Fi
4.pdf	16-09-2014 11:45	PDF Fi
5.pdf	16-09-2014 11:50	PDF Fi

File name: 2.pdf All Files (*.*)

E-Mail : suresh@gmail.com

UploadData : Browse...

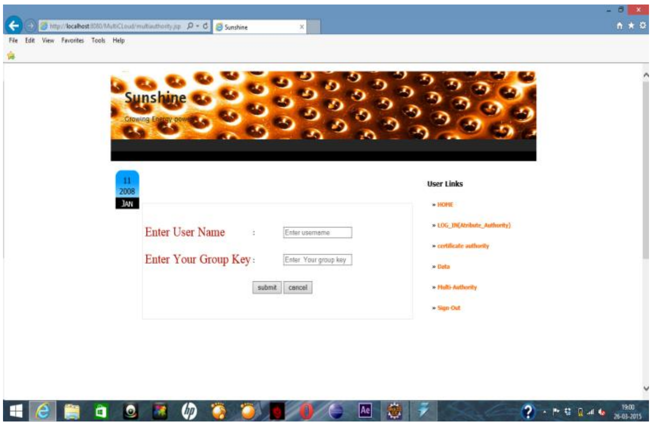
Group Key SJPLF

Choose your group

□ sai
□ suresh
☑ tamil
□ sa
□ sai
□ san

submit

Now other users in the cloud can access the files by first logging into their account and then getting to the group by using their group key

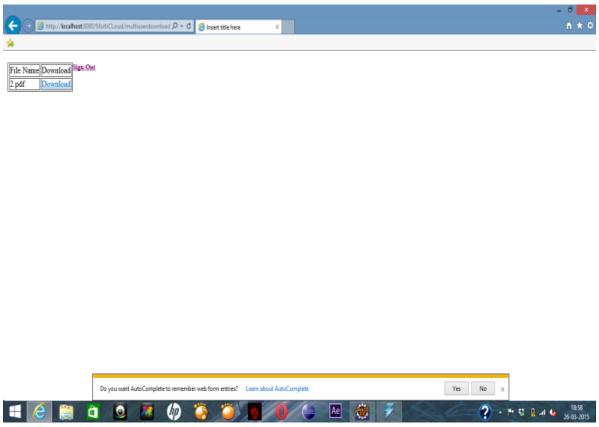


Enter User Name : Enter username

Enter Your Group Key : Enter Your group key

submit cancel

Once this is done the user gets the download link from where they can download the files.



File Name	Download
2.pdf	Download

Do you want AutoComplete to remember web form entries? Learn about AutoComplete

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

VII. CONCLUSION

During this paper, we have a tendency to projected a revocable multi-authority CPABE theme that may support economical attribute revocation. Then, we have a tendency to made a good information access management theme for multi-authority cloud storage systems. The revocable multi-authority CPABE may be a promising technique, which may be applied in any remote storage systems and on-line social networks etc.

REFERENCES

[1]C. Gentry, "Computing Arbitrary Functions of Encrypted Data,"Comm. ACM, vol. 53, no. 3, pp. 97-105, 2010.
[2] C. Gentry, "Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness," Proc. Advances in Cryptology (CRYPTO '10), pp. 116-137, 2010.
[3] C. Gentry and S. Halevi, "Implementing Gentry's Fully- Homomorphic Encryption Scheme," Proc. 30th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '11), pp. 129-148, 2011.
[4] D. Harris, D.M. Harris, and S.L. Harris, Digital Design and Computer Architecture. Morgan Kaufmann, 2007.
[5] D.J. Lilja and S.S. Sapatnekar, Designing Digital Computer Systems with Verilog. Cambridge Univ. Press, 2005.
[6] S. Ling and C.P. Xing, Coding Theory: A First Course. Cambridge Press, 2004.
[7] R. Ostrovsky and W. Skeith, "Private Searching on Streaming Data," Proc. Advances in Cryptology (CRYPTO '05), pp. 223-240, 2005.
[8] R. Ostrovsky and W. Skeith, "Private Searching on Streaming Data," J. Cryptology, vol. 20, no. 4, pp. 397-430, 2007.
[9] R. Ostrovsky and W. Skeith, "Algebraic Lower Bounds for Computing on Encrypted Data," Proc. Electronic Colloquium on Computational Complexity (ECCC '07), 2007.
[10] P. Paillier, "Public Key Cryptosystems Based on Composite Degree Residue Classes," Proc. 17th Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT '99),pp. 223-238, 1999.
[11] B. Parhami, Computer Arithmetic: Algorithms and Hardware Designs, second ed. Oxford Univ. Press, 2010.
[12] N. Smart and F. Vercauteren, "Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes," Proc. 13th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC '10), pp. 420-443, 2010.
[13] D. Stehle and R. Steinfeld, "Faster Fully Homomorphic Encryption," Proc. Advances in Cryptology (ASIACRYPT '10), pp. 377-394, 2010.
[14] J.F. Wakerly, Digital Design Principles and Practices, third ed. Prentice Hall, 2000.