International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups In the Cloud

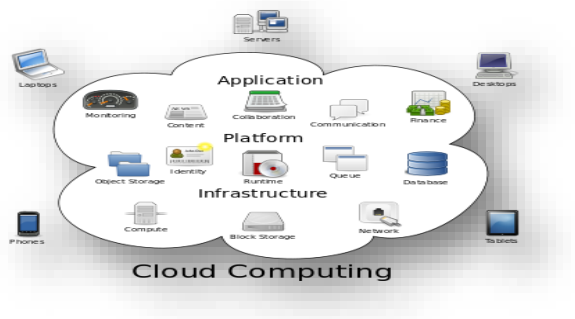
Bharathi
Email Id:-Bharathig250@Gmail.Com
Sir Vishveshwaraiah Institute Of Science And Technology

ABSTRACT

Profited from spread enrolling, clients can complete a persuading and compelling methodology for information sharing among group individuals in the cloud with the characters of low upkeep and little association cost. Meanwhile, we should give security affirmations to the sharing information reports since they are outsourced. Unfortunately, in light of the unremitting qualification in the selection, sharing information while surrendering security saving is 'before a testing issue, particularly for an unfrosted cloud because of the intrigue assault. Similarly, to exist outlines, the security of key distribution depends upon the guaranteed correspondence channel, in any case, to have such channel is a solid supposition and is troublesome for getting ready. In this paper, we propose a protected information sharing game plan for dynamic individuals. In any case, we propose a guaranteed course for key stream with no ensured correspondence channels, and the clients can safely obtain their private keys from add up to official. Second, our course of action can accomplish fine-grained find the opportunity to control, any client in the party can utilize the source in the cloud and disavowed clients can't get to the cloud again after they are denied. Third, we can shield the course of action from conspiracy assault, which deduces that denied clients can't get the fundamental information record paying little regard to whether they scheme with the unfrosted cloud. In our approach, by utilizing polynomial farthest point, we can complete a secured client renouncement conspire. At last, our course of action can complete fine capacity, which proposes past clients require not resuscitating their private keys for the condition either another client appreciates the party or a client is renounced from the get-together.

INTRODUCTION

What is distributed computing:-Cloud processing is the utilization of dealing with assets (rigging and programming) that are passed on as an association over a system (routinely the Internet). The name starts from the ordinary utilization of a cloud-framed picture as a reflection for the dumbfounding foundation it contains in framework diagrams. Appropriated figuring favours remote associations with a client's information, programming and estimation. Scattered preparing contains rigging and programming assets made accessible on The Internet as oversaw untouchable associations. These associations routinely offer access to cutting edge programming applications **and first rate structures of server PCs**



Structure of cloud computing

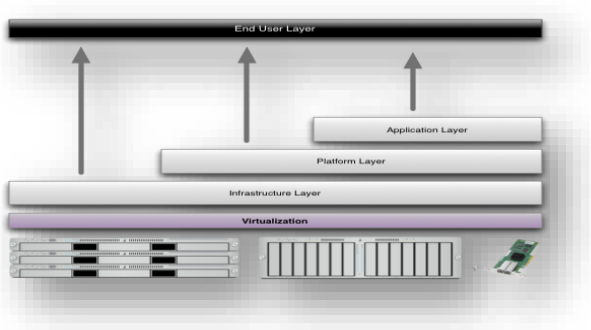
How Cloud Computing Works:-The goal of circulated processing is to apply standard supercomputing, or world class enlisting power, commonly used by military and research workplaces, to perform a large number of figuring's for consistently, in purchaser organized applications, for instance, money related portfolios, to pass on tweaked information, to give data accumulating or to control tremendous, immersive

PC diversions. The conveyed processing uses frameworks of gigantic social affairs of servers conventionally running negligible exertion purchaser PC advancement with specific relationship with spread data getting ready errands transversely finished them. This shared IT establishment contains extensive pools of systems that are associated together. Much of the time, virtualization systems are used to enlarge the vitality of dispersed registering.

Qualities and Services Models:-The striking qualities of distributed computing in view of the definitions gave by the National Institute of Standards and Terminology (NIST) are illustrated beneath: On-request self-benefit: A buyer can uniquely plan enrolling capacities, for instance, server time and framework accumulating, as required thus without requiring human joint effort with every expert co-op's.

Characteristics of cloud computing

ServicesModels: Distributedcomputinginvolvesthre e diverse administration models, to be specific Infrastructure-asaService(IaaS), PlatformasaService (PaaS), and Software-as-a-Service (SaaS). The three administration models or layer are finished by an end client layer that typifies the end client point of view on cloud administrations. The model is appeared in figure underneath. In the event that a cloud client gets to administrations on the framework layer, for example, she can run her own particular applications on the assets of a cloud foundation and stay in charge of the help, support, and security of these applications herself. In the event that she gets to an administration on the application layer, these assignments are regularly dealt with by the cloudspecialistorganization.



Structure of service models

What is Secure Computing: - security (Also known as digital security or IT Security) is data security as connected to PCs and systems. The field covers every one of the procedures and components by which PC based gear, data and administrations are shielded from unintended or unapproved access, change or obliteration. PC security likewise incorporates insurance from impromptu occasions and cataclysmic events. Something else, in the PC business, the term security - or the expression PC security - alludes to strategies for guaranteeing that information put away in a PC can't be perused or traded off by any people without approval. Most PC safety efforts include information encryption and passwords. Information encryption is the interpretation of information into a shape that is incoherent without a disentangling instrument. A watchword is a mystery word or expression that gives a client access to a specific program or framework. Diagram clearly explain the about the secure computing.

What is Secure Computing:-PC security (Also known as digital security or IT Security) is data security as connected to PCs and systems. The field covers every one of the procedures and components by which PC based gear, data and administrations are shielded from unintended or unapproved access, change or obliteration. PC security likewise incorporates insurance from impromptu occasions and cataclysmic events. Something else, in the PC business, the term security - or the expression PC security - alludes to strategies for guaranteeing that information put away in a PC can't be perused or traded off by any people without approval. Most PC safety efforts include information encryption and passwords. Information encryption is the interpretation of information into a shape that is

incoherent without a disentangling instrument. A watchword is a mystery word or expression that gives a client access to a specific program or framework. Diagram clearly explain the about the secure computing

LITERATURE SURVEY

"Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," AUTHORS: B. Wang, B. Li, and H. Li, With cloud data organizations, it is standard for data to be secured in the cloud, and additionally shared over various customers. Tragically, the genuineness of cloud data is at risk to question on account of the nearnessof hardware/programming disillusionments and human slip-ups. A couple of segments have been proposed to allow the two data proprietors and open verifiers to capably survey cloud data genuineness without recouping the entire data from the cloud server. Regardless, open analyzing on the dependability of conferred data to these present frameworks will reveal arranged information identity security to open verifiers. In this paper, we propose a novel assurance sparing instrument that sponsorships open checking on shared data set away in the cloud. In particular, we abuse ring imprints to enrol check metadata anticipated that would audit the precision of shared data. With our instrument, the character of the endorser on each square in shared data is kept private from open verifiers, who can viably check shared data dependability without recuperating the entire record. In like manner, our part can play out various exploring assignments in the meantime rather than checking them one by one. Our test comes to fruition demonstrate the suitability and capability of our part while looking at shared data reliability.

"Security Challenges for the Public Cloud," Makers: K. Ren, C. Wang, and Q. Wang, In this exchange, I will at first discuss different crushing security challenges in Cloud Computing, including data advantage outsourcing security and secure figuring outsourcing. By then, I will focus on data amassing security in Cloud Computing. As one of the unrefined organizations, disseminated capacity empowers data proprietors to outsource their data to cloud for its drawing in favourable circumstances. In any case, the way that proprietors never again have physical responsibility for outsourced data raises huge security stresses on the limit rightness. Thusly, engaging secure limit examining in the cloud condition with new strategies twists up perceptibly essential and testing. In this talk, I will display our flow investigate attempts towards limit outsourcing security in appropriated figuring and depict both our particular strategies and security and execution evaluations.

SYSTEM ANALYSIS

Existing system:-Kallahalla et al presented a cryptographic accumulating structure that enables secure data sharing on deceptive servers in light of the frameworks that dividing reports into record social events and encoding each record hoard with a record square key. Yu et al abused and united frameworks of key course of action property based encryption, delegate re-encryption and unresponsive re-encryption to achieve fine-grained data get the chance to control without uncovering data substance.

Inconveniences of existing system:- The report piece keys ought to be invigorated and passed on for a customer denial; in like manner, the system had a mind-boggling key assignment overhead. The complexities of customer venture and denial in these plans are sprightly growing with the amount of datproprietors and the disavowed customers. The single-proprietor way may discourage the execution of employments, where any part in the social occasion can use the cloud organization to store and offer data records with others.

Proposed system:- In this paper, we propose a protected data sharing arrangement, which can achieve secure key allotment and data sharing for dynamic social affair. We give a secured strategy to key movement with no protected correspondence channels. The customers can securely get their private keys from amass executive with no Certificate Authorities on account of the check for the overall public key of the customer. Our plan can achieve fine-grained get the chance to control, with the help of the social event customer list, any customer in the get-together can use the source in the cloud and disavowed customers can't get to the cloud again after they are denied. We propose a sheltered data sharing arrangement which can be protected from understanding ambush. The denied customers can not have the ability to get the main data archives once they are repudiated paying little mind to whether they design with the untreated cloud. Our arrangement can finish secure customer repudiation with the help of polynomial limit. Our plan can reinforce dynamic social occasions capably, when another customer takes an interest in the get-together or a customer is repudiated from the get-together, the private keys of interchange customers don't ought to be recomputed and invigorated. We give security examination to exhibit the security of our arrangement.

Great circumstances of proposed system:-The computation cost is immaterial to the amount of renounced customers in RBAC contrive. The reason is that paying little respect to what number of customers is denied, the operations for people to translate the data reports about proceed as some time recently. The cost is unessential to the amount of the denied customers. The reason is that the computation cost of the cloud for record move in our arrangement includes two affirmations for signature, which is immaterial to the amount of the denied customers. The reason behind the little count cost of the cloud in the time of record move in RBAC plot is that the checks between correspondence substances are not stressed in this arrangement. In our arrangement, the customers can securely get their private keys from assemble boss Certificate Authorities and secure correspondence channels. Also, our arrangement can support dynamic social events beneficially, when another customer partakes in the get-together or a customer is repudiated from the get-together, the private keys of exchange customers ought not to be recomputed and invigorated.

SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:-

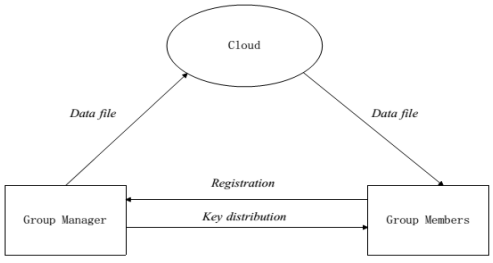
System	:	PentiumIV2.4GHz.
Hard Disk	:	40 GB.
Floppy Drive	:	1.44 Mb.
Monitor	:	15 VGA Colour.
Mouse	:	Logitech.
Ram	:	512 Mb.

SOFTWARE REQUIREMENTS:-

Operating framework	:	Windows XP/7.
Coding Language	:	JAVA/J2EE.
IDE	:	Eclipse IDÉE.
Database	:	MYSQL

SYSTEM DESIGN

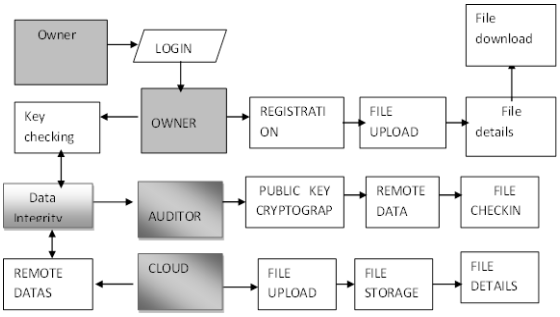
System architecture:-



Data flow diagram:-The DFD is also called as air stash graph. It is a direct graphical formalism that can be used to address a system to the extent data to the structure, diverse getting ready did on this data, and the yield data is made by this system. The data stream diagram (DFD) is a champion among the most fundamental showing mechanical assemblies. It is used to show the structure

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

fragments. These parts are the system technique, the data used by the methodology, an external component that speaks with the structure and the information streams in the structure. DFD demonstrates how the information goes through the structure and how it is modified by a movement of changes. It is a graphical method that depicts information stream and the progressions that are associated as data moves from commitment to yield DFD is generally called bubble diagram. A DFD may be used to address a system at any level of reflection. DFD may be allotted into levels that address growing information stream and utilitarian detail.



Uml diagrams:-

UML stays for Unified Modelling Language. UML is a systematized comprehensively helpful showing tongue in the field of question orchestrated programming building. The standard is directed, and was made by, the Object Management Group. The goal is for UML to wind up recognizably a normal tongue for making models of question arranged PC programming. In its present casing UML is incorporated two imperative parts: a Meta-show and documentation. Later on, some kind of methodology or process may in like manner be added to; or associated with, UML. The Unified Modelling Language is a standard vernacular for deciding, Visualization, Constructing and revealing the relics of programming system, and moreover for business showing and other non-programming structures. The UML addresses an amassing of best planning hones that have exhibited productive in the showing of broad and complex systems. The UML is a basic bit of making objects orchestrated programming and the item headway process. The UML uses generally graphical documentations to express the arrangement of programming wanders.

MODULES

1. Cloud Module
2.Group Manager Module
3.Group Member Module
4.File Security Module
5.Group Signature Module
6. Client Revocation Module .

MODULES DESCRIPTION:

1.Cloud Module :-In this module, we make a neighborhood Cloud and give evaluated inexhaustible capacity administrations. The clients can transfer their information in the cloud. We build up this module, where the distributed storage can be made secure. In any case, the cloud isn't completely trusted by clients since the CSPs are probably going to be outside of the cloud clients' put stock in area. Like we accept that the cloud server is straightforward yet inquisitive. That is, the cloud server won't malignantly erase or alter client information because of the security of information evaluating plans, however will attempt to take in the substance of the put away information and the personalities of cloud clients.

2.GroupManagerModule:-Gatheringadministrator assumes responsibility of followings:

1. Framework parameters age,
2. Client enlistment,
3. Client denial, and
4. Uncovering the genuine personality of a question information proprietor.

In this manner, we expect that the gathering chief is completely trusted by alternate gatherings. The Group supervisor is the administrator. The gathering director has the logs of every last procedure in the cloud. The gathering director is in charge of client enrollment and furthermore client denial as well.

3.Group Member Module :

Gathering individuals are an arrangement of enrolled clients that will

1. Store their private information into the cloud server and
2. Share them with others in the gathering.

Note that, the gathering enrollment is progressively changed, because of the staff acquiescence and new representative interest in the organization. The gathering part has the responsibility for the records in the gathering. Whoever in the gathering can see the records which are transferred in their gathering and furthermore change it.

4.File Security Module :

1. Scrambling the information document.
2. Document put away in the cloud can be erased by either the gathering administrator or the information proprietor.
(i.e., the part who transferred the document into the server).

5.Group Signature Module :- A gathering mark plot enables any individual from the gathering to sign messages while keeping the character mystery from verifiers. Furthermore, the assigned gathering director can uncover the character of the mark's originator when a question happens, which is meant as traceability.

6. Client Revocation Module :- Client repudiation is performed by the gathering director by means of an open accessible denial list (RL), in light of which aggregate individuals can encode their information records and guarantee the secrecy against the renounced clients.

SYSTEM TESTING

The explanation behind testing is to discover bungles. Testing is the route toward trying to locate every conceivable fault or deficiency in a work thing. It gives a way to deal with check the convenience of parts, sub assemblages, social events and moreover a finished thing It is the path toward working on programming with the arrangement of ensuring that the Programming system satisfies its requirements and customer wants and does not flounder in an unsatisfactory way. There are diverse sorts of test. Each test compose addresses a specific testing need.

KINDS OF TESTS

Unit testing:- Unit testing incorporates the arrangement of examinations that support that the internal program method of reasoning is working suitably, and that program inputs make significant yields. All decision branches and inside code stream should be affirmed. It is the attempting of individual programming units of the application .it is done after the completing of an individual unit before consolidation. This is a fundamental testing, that relies upon data of its improvement and is prominent.

Blend testing:-Blend tests are planned to test fused programming sections to choose whether they truly continue running as one program. Testing is event driven and is more stressed over the basic consequence of screens or fields. Coordination tests show that regardless of the way that the parts were autonomously satisfaction, as showed up by adequately unit testing, the blend of sections is correct and solid. Blend testing is especially away to uncover the issues that rise up out of the blend of sections.

Structure Test: - Structure testing ensures that the entire consolidated programming system meets requirements. It tests a setup to ensure known and obvious results. An instance of system testing is the game plan arranged structure joining test. Structure testing relies upon process portrayals and streams, focusing on pre-driven process associations and blend centres.

White Box Testing: -White Box Testing is an attempting in which in which the item analyzer thinks about the interior workings, structure and vernacular of the item, or if nothing else its inspiration. It is reason. It is used to test districts that can't be come to from a revelation level.

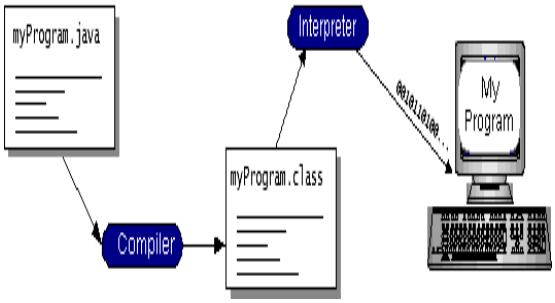
Revelation Testing:-Revelation Testing will attempt the item with no data of the internal workings, structure or tongue of the module being attempted. Revelation tests, as most unique sorts of tests, must be made from a definitive source chronicle, for instance, detail or necessities report, for instance, assurance or essentials record. It is an attempting in which the item under test is managed, as a disclosure .you can't "see" into it. The test gives wellsprings of information and responds to yields without considering how the item capacities.

SOFTWAREENVIRONMET

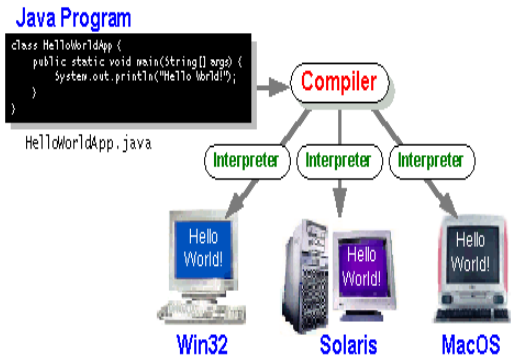
Java Technology:-The Java programming language is a high-level language that can be characterized by all of the following buzzwords With most programming vernaculars, you either join or interpret a program so you can run it on your PC. The Java programming vernacular is strange in that a program is both gathered and deciphered. With the compiler, first you make an elucidation of a program into a centreVernacular called Java byte codes the stage self-ruling codes deciphered by the interpreter on the Java organize. The go between parses and runs each Java byte

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

code heading on the PC. Course of action happens just once; understanding happens each time the program is executed. The going with figure depicts how this capacities.



You can consider Java byte codes as the machine code bearings for the Java Virtual Machine (Java VM). Every Java interpreter, paying little respect to whether it's a change instrument or a Web program that can run applets, is an execution of the Java VM. Java byte codes empower make "to create once, run wherever" possible. You can gather your program into byte codes on any phase that has a Java compiler. The byte codes would then have the capacity to be continue running on any use of the Java VM. That suggests that as long as a PC has a Java VM, a comparative program written in the Java programming tongue can continue running on Windows 2000, a Solaris workstation, or on an iMac.



ODBC:-Microsoft Open Database Connectivity (ODBC) is a standard programming interface for application organizers and database frameworks suppliers. Before ODBC changed into a veritable standard for Windows dares to interface with database frameworks, planners anticipated that would utilize select tongues for every database they anticipated that would associate with. Before long, ODBC has settled on the decision of the database structure in every way that really matters unessential from a coding point of view, which is as it ought to be.

JDBC:-With an extreme target to set an independent database standard API for Java; Sun Microsystems made Java Database Connectivity, or JDBC. JDBC offers a non specific SQL database get to structure that gives a foreseen interface to a course of action of RDBMSs. This reliable interface is refined using "module" database openness modules, or drivers. On the off chance that a database shipper wishes to have JDBC support, he or she should give the driver to each stage that the database and Java continue running on. To get a more wide assertion of JDBC, Sun build up JDBC's structure in light of ODBC. As you found before around there, ODBC has regardless of what you look like at it fortify on an assortment of stages.

SYSTEM STUDY

FEASIBILITY STUDY:-The common sense of the wander is inspected in this stage and business suggestion is progressed with a greatly expansive course of action for the endeavour and some cost gages. In the midst of structure examination the achievability examination of the proposed system is to be finished. This is to ensure that the proposed structure isn't a weight to the association. For feasibility examination, some appreciation of the huge necessities for the system is fundamental. Three key thoughts related with the credibility examination are

• ECONOMICAL FEASIBILITY
• TECHNICAL FEASIBILITY
• SOCIAL FEASIBILITY

ECONOMICALFEASIBILITY:

Thisexamination is finished to check the money related impact that the structure will have on the

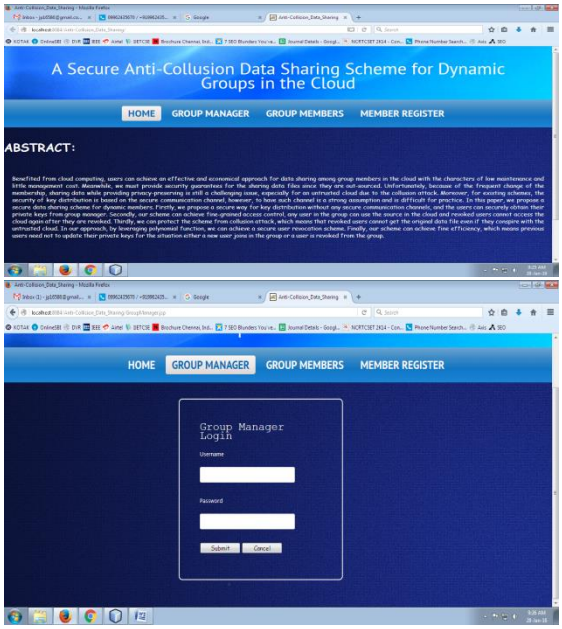
affiliation. The measure of store that the association can fill the creative work of the system is obliged. The utilizations must be upheld. Likewise the made structure too inside the monetary arrangement and this was proficient in light of the way that by far most of the advances used are energetically available. Simply the changed things must be purchased.

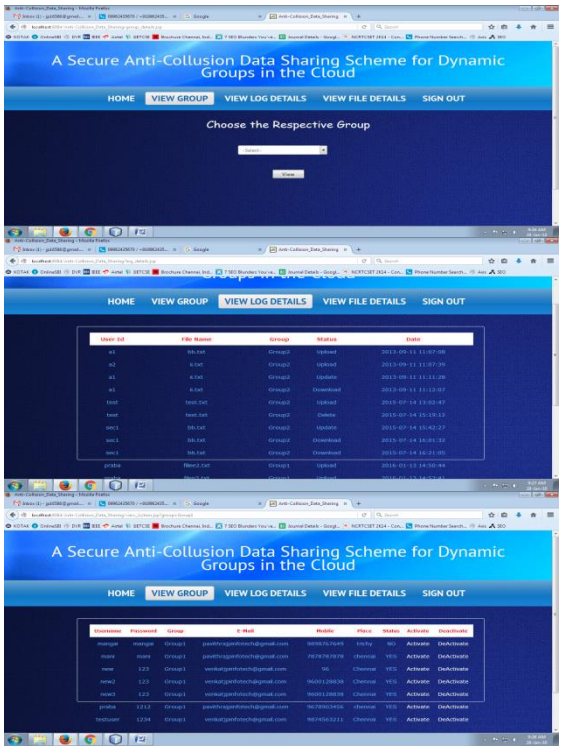
.

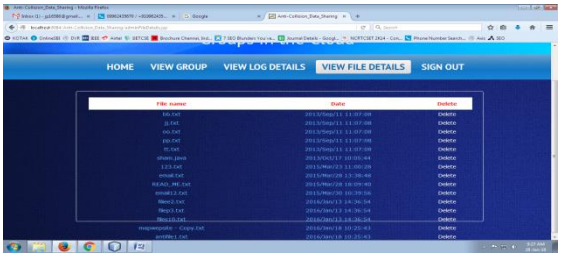
TECHNICAL FEASIBILITY:-This examination is finished to check the specific common sense, that is, the particular requirements of the system. Any structure made must not have an interest on the open specific resources. This will incite levels of prominence on the open particular resources. This will incite levels of ubiquity being determined to the client. The made structure must have an unassuming need, as simply insignificant or invalid changes are required for completing this system.

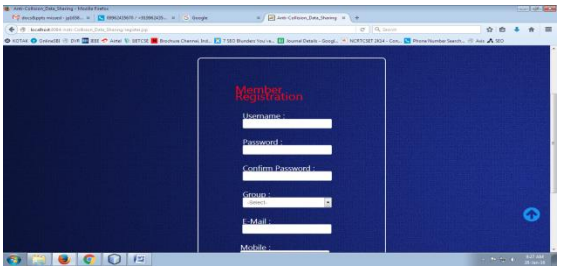
SOCIAL FEASIBILITY:-The piece of study is to check the level of affirmation of the structure by the customer. This consolidates the route toward setting up the customer to use the structure capably. The customer must not feel crippled by the structure, rather ought to recognize it as a need. The level of affirmation by the customers only depends upon the techniques that are used to educate the customer about the structure and to make him alright with it. His level of sureness must be raised with the objective that he is moreover prepared to make some supportive criticism, which is welcomed, as he is the last customer of the system.

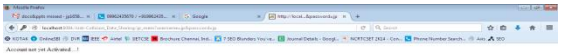
SCREEN SHOTS

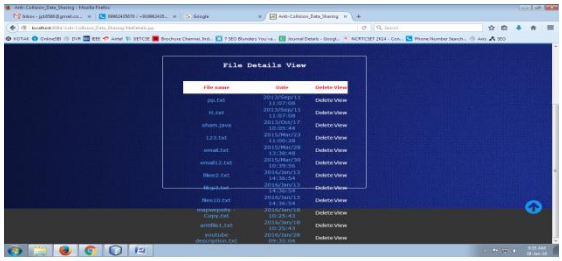












CONCLUSION

In this paper, we diagram an ensured unfriendly to trick data sharing arrangement for dynamic get-togethers in the cloud. In our arrangement, the clients can securely get their private keys from total supervisor Certificate Authorities and secure correspondence channels. In like manner, our arrangement can reinforce dynamic social occasions capably, when another customer takes an interest in the get-together or a customer is renounced from the get-together, the private keys of exchange customers don't ought to be recomputed and revived. Furthermore, our arrangement can finish secure customer disavowal, the revoked customers can not have the ability to get the principal data records once they are

BIBILIOGRAPHY

[1] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz, A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.Zaharia. "A View of Cloud Computing,"Comm. ACM, vol. 53,no.4, pp.50-58, Apr.2010.

[2] S.Kamara and K.Lauter,"Cryptographic Cloud Storage," Proc.Int'l Conf. Money related Cryptography and Data Security (FC), pp.136-149, Jan. 2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. Report and Storage Technologies, pp. 29-42, 2003.

[4] E.Goh, H. Sachem, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Framework and DistributedSystems Security Seem. (NDSS), pp. 131-145, 2003.

[5] G. Agenise, K. Fu, M. Green, and S. Hohenberger,"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed

Storage," Proc. Framework and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

[6] Shushing Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. PC and Comm. Security (CCS), pp. 89-98, 2006

[8] R. Lu, X. Lin, X. Liang, and X. Shin, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Sump. Information, Computer and Comm. Security, pp. 282-292, 2010.

[9] B. Waters, "Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Open Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008

[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[11] D.Boneh, X. Boyen, and E. Goh, "Different leveled IdentityBasedEncryption with Constant Size Cipher text," Proc. Ann. Int'l Conf.Theory and Applications of Cryptographic Techniques (EUROCRYPT),pp. 440-456, 2005.

[12] C. Delerablee, P. Paillier, and D. Point cheval, "FullyCollusionSecure Dynamic Broadcast Encryption with Constant-SizeCi-phertexts or Decryption Keys," Proc.First Int'l Conf. Mixing Based Cryptography, pp. 39-59, 2007.

[13] Zhongma Zhu, Zelman Jiang, Ruin Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, "Proceedings of2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou,Dec.7,2013,pp. 185-189.

[14] Lang Zhou, Vijay Varadharajan, and Michael Hitchens, "Fulfilling Secure Role-Based Access Control on Encrypted Data in Cloud Storage,"IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[15]Xukai Zou, Yuan-sundial, and ElisaBertino, "A practical and versatile keymanagement segment for trusted group situated computing,"INFOCOM 2008, pp. 1211-1219.

[16] M. Nabeel, N. Shang, and E. Bettino, "Security ensuring policy based content sharing straightforwardly clouds,"IEEE Trans. on Know. And Data Eng., vol. 25, no. 11, pp. 2602-2614, 2013.

[17] Dolev,D.,Yao A. C'mon the security of open key protocols",IEEE trans. on Information Theory,vol. IT-29, no. 2, pp.198– 208, 1983

[18] Bonehead, Franklin Matt, "Identity based encryption from the weil coordinating

[19] B. sanctuary Boer,Diffie– Hellman is as strong as discrete log for certain primesin Advances in Cryptology– CRYPTO88, Lecture Notes in Computer Science 403, Springer, p.530, 1988.

[20] D. Boneh, X. Boyen, H. shacham, "Short assembling mark," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp.41-55, 2004.

[21] D. Boneh, X. Boyen, and E. Goh, "Different leveled IdentityBasedEncryption with Constant Size Cipher text," Proc. Ann. Int'l Conf.Theory and Applications of Cryptographic Functions