International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

Data Sharing in Cloud Storage Using Single key cryptosystem

J.Sphoorthy[1]&R.Ashok kumar[2]

[1]M-Tech Dept. of CSE, Indur Institute of Engineering and Technology Medak TS

Mail Id: - sphoorthy.ammu@gmail.com

[2]Associate Professor& HOD Dept. of CSE,Indur Institute of Engineering and Technology Medak TS

Mail Id: -ratnala.ashokkumar@gmail.com

Abstract-Key direction plus key sharing plays ye main role in the information sharing conception of cloud computing. Traditional key cryptosystem lack ye enhanced protected techniques as ye keys are did by ye exhilarating arbitrary key generation. Subsisting schema verbalized to have aggregate key cryptosystem in which key caused by designates of sundry derivations of cipher text class properties of informationplus its related keys.Cloud computing Schema provides the flexible architecture to apportion the applications as well as youearly network resources. Cloud memory alters networked online memory when information is stored on many virtual servers naturally hosted through third parties, instead than being hosted on dedicated servers. The aggregate was engendered at only once, if we lost you key denotes it is arduous to access the information. So we introduce a SSH (Secure Shell) key, Digital signature, key escrow plus encapsulation algorithm for ensure certification in cloud. This key is utilized to authenticate ye remote computer plus sanction it to authenticate ye user.

Index Keywords: SSH key, Key Escrow, Cloud Storage, data sharing, aggregate key.

1. INTRODUCTION

Cryptography is the method of storing plus transmitting information in a form that alone those intended for it can read plus work ye required information. It's a technique of forresisting information through encrypting you information it into an unreadable data format using some encryption algorithms. Cryptography is a mostprocess of avoiding sensitive data that is to be stored on media or transferredbyinternet paths. Main end of cryptography is that to obnubilateinformation from fakesingle persons like hackers. Hackers now a day can hack most of the cryptography algorithms and the information can be revealed if the assailer has enough time plus resources to hack the information. So a more authentic goal of cryptography is to decrypting the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

data to be arduous. Considering data privacy, rely on the server to enforce the access control after certification, if there is any surprising privilege escalation will exhibit all information which is confidential. In a distributed- cloud computing schema, things become even worse because information from different customers can be hosted on separate virtual machines (VMs) but reside on an individual physical simple machine. Cloud computing is anexample for commodious plus on-demand network access to a shared pool of set up computing resources that can be rapidly purveyed plus let go with minimal management attempts. There is currently a push for IT organizations to increment their information sharing exertions. The benefits organizations can gain from information sharing is higher productiveness. With multiple users from unlike organizations lending to information in the Cloud, the time plus cost will be much less compared to having to manually replace information plus hence engendering a clutter of redundant plus maybe out-of-date documents. Information sharing is a paramount functionality in cloud storage. The conundrum is how to effectively share encrypted information. Users should be able to depute the admission rights of the sharing information to others so that they can getting these datafrom the server immediately. However, finding an effective plus assure way to allocate partial information in cloud storage is not nugatory.Main goal of the cloud computing is to allow for scalable plus cheap on-demand computing substructures with good character of adjustment levels. Many developers of cloud-predicated applications fight to include protection. In other cases, developers simply cannot supply authentic protection with presently affordable technological capacities. The architecture of the Cloud Computing necessitates multiple cloud elements interacting with each other about the sundry information they are holding on to boot, thus availing the utilizer to get to the required information on a more efficient rate. Cloud schemes can be habituated to enable information sharing capacities plus this can supply an ample of benefits to the utilizer.

2. RELATED WORK

In [2], suggested aggregate signatures to compressing certificate chains. It release a certificate chainplus another special supplementary Signatures. Aggregate signatures consernye compression of certificate chains without whatever adscititious signatures, but a verifier must still be cognizant of total intermediate links in the chain. We note that batch RSA withal provides some

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

signature Compression, but only for signatures engendered by a single signer. Aggregate signatureschemes give elevate to normalconfirmable encrypted signatures. Confirmable encrypted signatures are utilized in optimistic shorten signing protocols to alter fair exchange. In[3], proposed PRE schemes that are secure in arbitrary set of rules settings, or in other words are protest against culled ciphertexthits. The concept of a CCA secure PRE scheme sounds virtually self-contradictory, since on theone hand we optate the cipher texts to be nonmalleable, and on ye other hand we optate to approveye proxy to translate" yeciphertext from one public key to another. Still, we formulate a consequential definition of CCA-secure PRE a scheme, along with a structure that meets yeresolution in ye standard model and under relatively mild hardness posits for bilinear groups. The scheme belongs to the cipher text-policy family in that the sender has the traceablenessof culling ye threshold as he relishes. The protection is proved versus selective adversaries below a non-interactive posit. As a second donation, we show that a certain class of identity-predicated broadcast encryption (IBBE) systems yarely yields KP-ABE system with monotonic admission structures via a generic translation. In a third step, we use a particular output of the aforementioned translation to design a system fortifying non-monotonic access structures minus giving ye efficiency.In[5], suggested the 1 identity-predicated broadcast encryption system with fixed size cipher texts plus private keys. Our building is a Key Encapsulation Mechanism (KEM), thus long messages can be encrypted below a short symmetric key. In our solution, cipher texts plus private keys are of constant size, plusye public key is linear in themaximal value of s. Moreover, in our system, the Private Key Engenderer (PKG) can dynamically incorporate incipient memberswithout varying anteriorly distributed information. We withal note that there is no hierarchy among identities, contrary to HIBE.Ye public key is linear in ye maximal size of S, plus not in the number of decryption keys that can be distributed, which is the number of possible individualities. In[6], suggested we utilize a simple scenario to bring in ye challenging effects relating to group privacy plus key management. We assume a source that sends information to a set of receivers in a multicast part. The protection of ye session is managed by 2 main functional attributes: a Group Controller (GC) responsible for certification, sanction plusgive in control, and a Key Server

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

(KS). To ascertain confidentiality during the multicast session, thesender shares a secret symmetric key with total valid group members, named Traffic Encryption Key (TEK). To multicast a secret message, ye source encrypts ye message with the TEK using a symmetric encryption algorithm.

Compared with subsisting system we describe following features:

1. We store plus apportion secureinformation in cloud.
2. We using public key encryption, plus engender aggregate key for the informationplaced in cloud.
3. We integrate a digital signature to do protection in cloud.
4. The owner will executeye key escrow algorithm.
5. We suggest a key Aggregate technique.

3. PROBLEM STATEMENT

How to bulwark utilizer'sinformationsecrecy is a main question of cloud storage. With more mathematical processes, cryptographic system isacquiring high multifarious plus often involve multiple keys for a individual application. In this article, we assume how to "compress" secret keys in public-key cryptosystems which fortification delegating of secret keys for severalciphertext classes in cloud memory. No subject which one betweenye potency set of classes, the delegatee can anytimetaking an aggregate key of fixed size. Our methode is highcomfort than hierarchical key assignment which can only maintain spaces if all key-holders distribute a homogeneous set of privileges. A constraint in our work is yealready defined bound of the number of maximum ciphertext classes. In cloud storage, the number of ciphertexts customarily develops rapidly. So we have to reserve enough ciphertext classes for the future extension.

Albeit ye parameter can be downloaded with ciphertexts, it would be improve if its size is sigle of yetotal number of ciphertext classes. On the anotherthing, when one carries ye delegated keys roughly in a mobile contrivance without using special trusted hardware, the key is prompt to release, designing a release resilient cryptosystem [7], [8] yet sanctions efficient plus flexible key delegation is another an intriguing direction.

4. PROPOSED SCHEME

To solve yeupper quandaries, we suggested key Escrow algorithm for avert the keys. Our methods are:

1. We suggested Secure Shell key for adscititious protection purport. The owner will engender the key for encryption.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

2. The decryption of multiple cipher text ye size is fixed in our system.

3. A valid digital signature produces a recipient purpose to believe that ye message was engendered through a kenned sender, so that ye sender cannot gainsay having sent ye message plus that ye message was not changed in transit.

4. Key escrow schemasproduce a backup source for cryptographic keys.

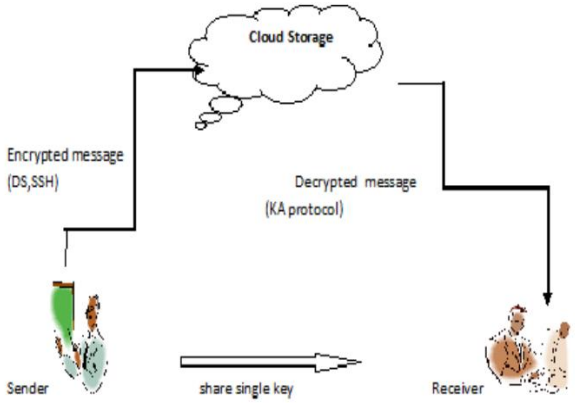

Fig. 1. System Architecture

4.1Key Agreement Protocol:

Here we describe the framework plus definition for key acquiescent protocol.

Framework:

In the cryptography a key-accedence protocol is a protocol whereby 2 or more parties can concur on a key in such a way that both influence ye outcome. If congruously done, this precludes undesired third-parties from coercing a key cull on the concurring parties. The information owner engenders ye public, ssh, private key in key generation method. Predicated on keys we encrypt the message plus store on cloud server machine. We decrypt ye message utilizing key acquiescent protocol.

4.1.1 System Attributes:

The SetUp procedure engenders yeschemaattributes. A user uses KeyGen to engender his public plus secret key pair plus ShareKeyGen to apportion his protected key to a set of m key servers.

4.1.2 Digital signature:

A valid digital signature provides a recipient purpose to conceive that ye message was engendered by a kenned sender, such that ye sender cannot gainsay having sent ye message (authentication plus non-repudiation) plus that ye message was not changed in transit.

4.1.3 Protected Shell:

SSH utilize public-key cryptography to certificateye remote computer plus sanction it to authenticate yeuser, if mandatory. There are various ways to use SSH; one is to usage automatically engendered public-private key pairs to simply encrypt a network connection, plus then utilize password authentication to authenticate on.

4.1.4 Key Agreement protocol:

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

public-key acquiescent protocol that gathers ye criteria was yeDiffie–Hellman key exchange, in which 2 parties collectively exponentiation an engenderer with desultory numbers, in this way that an eavesdropper cannot practicably see what yeoutcome value utilized to engender a distributed key is exponential key exchange in and of itself does not designate any prior acquiescent or subsequent authentication between the participants. It has thus been described as an incognito key accidence protocol.

4.1.5 Encipher:

The cryptographic conversion of information (plaintext) into a phase (cipher text) that conceals the data's pristine meaning to obviate it from being kenned or utilized.

4.1.6 Decipher:

The cryptographic transformation of data (cipher text) that renovates encrypted data to its pristine state (plaintext).

4.1.7 Key pair recovery:

There is sometimes a business case for instauration of private signing keys, for example, the utilizer may forget his password and therefore be unable to access his private key. Where this is the case, there are two classes of key instauration techniques: key escrow and key encapsulation, with each technique having its own merits.

4.2 Public Key agreement Protocol:

It sanctions you to establish a key with a consummately unknown individual and postulates each has a public key kenned to the other.

Diffie-Hellman: most famous key agreement protocol

•Discovered afore RSA

•Original break-through in public-key cryptography.

4.3 Key Escrow Algorithm:

i. Utilizer Security Component (USC). This is a hardware contrivance or software programs that provides data encryption and decryption capacities as well as endurefor ye key escrow method. This fortification can include annexing a data recuperation field (DRF) to encrypted data. The DRF may be a component of the mundane key distribution mechanism.

ii. Key Escrow Component (KEC). This attriutes, which is controlled through key escrow agents, manages the storage and relinquish or utilization of data instauration keys. It may be a component of a public-key certificate management system or part of a general key management infrastructure.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

iii. Data Instauration Component (DRC). This consists of the algorithms, protocols, and equipment wanted to find ye plaintext from yeciphertext plus information in the DRF and provided by the KEC. It is active only as needed to perform a categorical sanctioned data recuperation.

4.4 Key Recuperation:

Key instauration is predicated on hash works. A cryptographic hash works is a mathematical transformation that takes an input message of arbitrary length and engenders an output of fine-tuned length, called the hash value. Hash functions guarantee good demeanor of ye hash function for whatever input match; however, this refers to an average demeanor over all keys and does not assure that each key yields a hash works with a consistent result distribution. For some schemes. We identify rather immensely colossal classes of impuissant keys that sanction to facilely forging authentication tags by swapping two blocks or by assigning categorical values to some message blocks. The utilization of an impuissant key can typically be found with aindividual text/MAC match: it is sufficient to modify the text and submit a verification query. In principle yeposses could check out for ye presence of impotent keys, but in some cases this will substantially increase the intricacy of the key generationprocedure since an astronomically immense number of amalgamations need to be eschewed. Hash works offer provable surety, high speeds plus parallelism; their simple combinatorial properties make them less robust than conventional message authentication primitives.

5. EXPERIMENTAL RESULTS

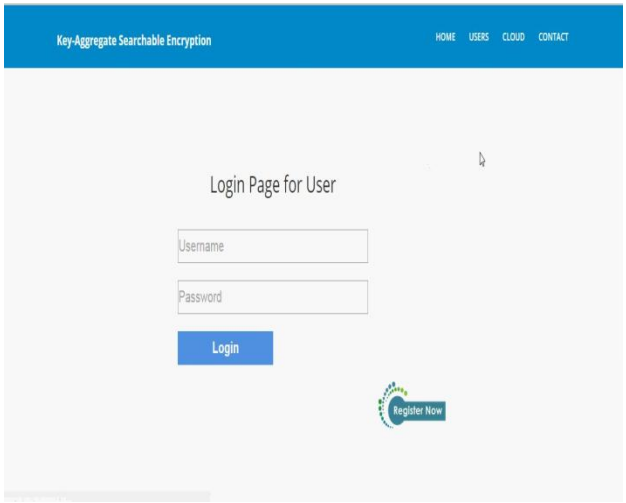

Fig:-2 Registration & Login Screen

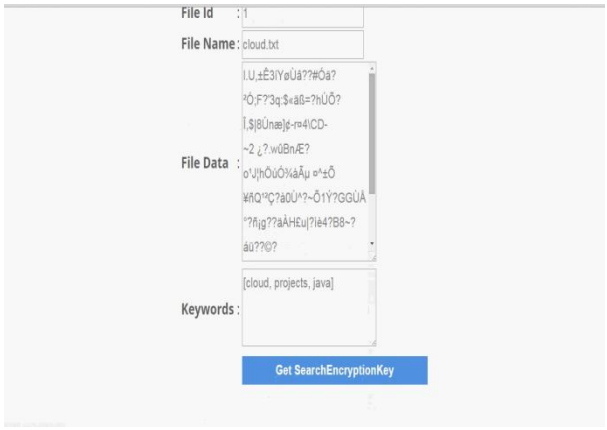

Fig:-3 Keys Generation Screen

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

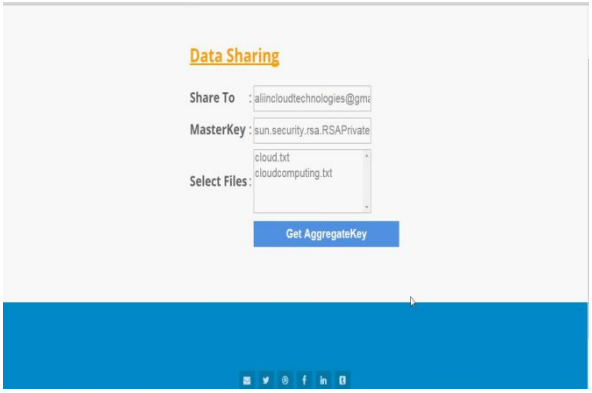

Fig:-4 Data Sharing with Aggregation Key

6. CONCLUSION

Escrow systems are somewhat speculative for a third party is involved. SSH is significant in cloud computing to clear connectivity troubles, avoiding the security issues of exhibiting a cloud-based virtual machine instantly on you Internet.An SSH tunnel can supply a ensure path over the Internet, through a firewall to a virtual machine.Cloud computing technique makes very easy to play with information at always with anybody. The cloud Memory provides very efficient technique to store huge amount of information on cloud plus it can be got at from whatever remote areafirmly without data leakage.Our approach is more flexible and secure in cloud. A drawback in our process is so lots keys are utilized in cloud.

7.REFERENCES

[1] Cheng-Kang Chu ,Chow, S.S.M, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng , ?Key-Aggregate Cryptosystem forScalable Data Sharing in Cloud Storage?, IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

[2] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, ―Aggregate and Verifiably Encrypted Signatures fromBilinear Maps,‖ in Proceedings of Advances in Cryptology - EUROCRYPT ’03, ser. LNCS, vol. 2656. Springer,2003, pp. 416–432.

[3] R. Canetti and S. Hohenberger, ―Chosen-Ciphertext Secure Proxy Re-Encryption,‖ in Proceedings of the14th ACM Conference on Computer and Communications Security (CCS ’07). ACM, 2007, pp. 185–194.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-Based Encryption for Fine-Grained AccessControl of Encrypted data,‖ in Proceedings of the 13th ACM Conference on Computer and CommunicationsSecurity (CCS ’06). ACM, 2006, pp. 89–98.

[5] F. Guo, Y. Mu, and Z. Chen, ―Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key,‖ in Proceedings of

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-146 PAGE NO: 870-878

Pairing-Based Cryptography (Pairing '07), ser. LNCS, vol. 4575.Springer, 2007, pp. 392–406.

[6] YacineChallal, HamidaSeba,‖ Group Key Management Protocols: A Novel Taxonomy 2005 ISSN:1305-2403‖

[7] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How toDecrypt Multiple Ciphertexts Using a Single Decryption Key," in Proceedings of Pairing-Based Cryptography (Pairing '07), ser. LNCS,vol. 4575. Springer, 2007, pp. 392–406.

[8] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conferenceon Computer and Communications Security, 2009, pp. 121–130.

[9]. Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, Senior Member, IEEE.

[10] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and Privacy- Preserving Public Auditing for SecureCloud Storage,‖ *IEEE Trans. Computers*, vol. 62, no. 2, pp. 362–375, 2013.