TWO WAY PROTECTION IN CLOUD DATA SHARING ENVIRONMENT

[#1]**S.SHILPA**, *M.Tech Student,*
[#2]**K.SRINIVAS**, *Assistant Professor,*
Dept of CSE,
SCIENT INSTITUTE OF TECHNOLOGY, IBRAHIMPATNAM , RANGAREDDY TELANGANA.

Abstract—In that projected anenhance the data security protection mechanism for cloud using two components. During this system sender sends an encrypted message to a receiver with the assistance of cloud system. The sender needs knowing identity of receiver however no would like of different data like certificate or public key. To decode the cipher text, receiver desires two components. The primary issue may be a unique personal security device or some hardware device connected to the computer system. Second one is personal key or secretes key hold on within the computer. While not having these two factors cipher text ne'er decrypted the necessary thing is that the security device lost or stolen, then cipher text cannot be decoded and hardware device is revoked or cancelled to decoded the cipher text.

Index Terms-- Cloud Storage System, Cloud Security, Cloud Protection, Two-Factor Data Security Protection

I. INTRODUCTION

There are such an oversized variety of advantages, to store the data within the cloud storage. Data within the cloud storage server can be facilitated whenever and where as long as network access. Cloud service provider provides services to the cloud users; they can get any amount of a lot of resources any time. It provides no risk of data Storage maintenance tasks, like exploit further storage capability, is unloaded to the responsibility of a service provider easy to data sharing between numerous clients. in the event that sender needs to share a little of data, as an example, video, text, audio so forth to receiver it would be difficult for sender to send it by email as a result of the scale of data. Instead of that sender transfers the information into the cloud storage then receiver will easily transfer anytime from anywhere. Cloud storage usually refers to a proposal object storage services like Microsoft Azure and Amazon S3 Storage. There are totally different important challenges in cloud computing for securing information, provision of services and storage of data within the internet from differing kinds of attacks. Cloud computing provides an together with area for data storage, computer processing power, shared pool of resources, networks, user applications and specialized corporate. Cloud computing may be a lot of refined. it is simple to forecast that the protection for data protection within the cloud storage ought to be improved. In any cases, these applications go through a possible risk concerning component revocability that will limit their possibility. An expandable and flexible Two-Component encoding mechanism is actually a lot of appropriatewithin the term of cloud computing that prompt our System. Cloud computing may be a common term for anything that involves scalable services, delivering hosted services like accessing, information sharing, etc. over the online on demand basis. Generally, user shares numerous kinds of documents through cloud storage networking application like Drop box, cloud me, Google drive. Citrix Cloud computing is thought as an alternative to traditional technology as a result of its low-maintenance and better resource-sharing capabilities. the most goal of cloud computing is to provide high performance energy of computing for numerous field like military and analysis organization for performing billions of computations. The essential security demand is attained by combining each the cryptographically cloud storage together with searchable encoding scheme. In cloud system overall value of data storage is less because it does not need managing and maintaining expensive hardware. Within which information owner first encrypts all information before storing on a cloud in such approach that only user whom having decoding keys is decipher or fetch the data.

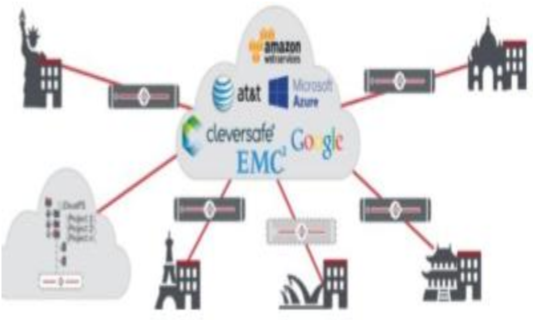


Figure 1: Architecture of Cloud Storage

II. RELATED WORK

In this scheme presents encoded cloud storage based on attribute-based encoded and a brand new keyword search notion: fine-grained access management aware keyword search. During this system initial group the decoded able files of users before execution the keyword search. It decreases data outpouring from the query method. A lot of system uses the easy search approach wherever for looking one encrypted keyword, the cloud server should look round all encrypted files on the storage to check that encrypted keyword to each keyword index, and this disadvantage is removed. Focused on drawback of Identity-Based proxy re-encryption, during which cipher-text are convert into one identity to a different. Proxy re-encryption scheme is used to convert the encrypted cipher-text into decrypted cipher text while not in behalf of underlying plaintext. This drawback removes in Inter-domain identity-based proxy reencryption. The authors share information and privacy protective auditing theme with massive groups within the cloud. They are utilizing group signature to cipher verification data on shared data. That is the TPA those able to audit correctness of shared data however cannot reveal the identity of the signers on every block. The original user will efficiently add new users to the group and close the identities of signers on all blocks. This paper describes a system Identity based encoding in commonplace model and has distinct disadvantage of existing system like specifically, computation capability, less public framework and a compact safety reduction. Stronger assumption is based on personal key generation quires created by attacker to reduce this disadvantage using linear diff-hellman Exponent assumption. This paper focuses on trace out information for security concern. Using a log based audit services that concentrate on privileged information utilize and additionally contemplate their period of time of utilization for this instance information trace go into the cloud storage. This technique overcome numerous operations on information, additionally repeated creation of tag and sampling. In planned cloud storage systems is used to hold on cipher-text existing access management strategy are not any longer helpful, disadvantage cipher text-Policy Attribute-Based encoding (CP-ABE) may be a technique for access management of encrypted information.

III. PROPOSED WORK

We propose a fine-grained two-factor access management protocol for web-based cloud computing services, employing a light-weight security device. The device has the subsequent properties: (1) it will work out some light-weight algorithms, e.g. hashing and exponentiation; and (2) it's tamper resistant, i.e., it's assumed that nobody will burgled it to induce the key info keep within.Advantages of Proposed System:1)Our protocol provides a 2FA security 2)Our protocol supports fine-grained attribute-based access that provides a good flexibility for the system to line completely different|completely different} access policies in step with different eventualities. At a similar time, the privacy of the user is additionally preserved. We seek advice from our approach because the SEM design. the essential plan is as follows: We introduce a brand new entity, mentioned as a SEM (Security Mediator): associate online semi-trusted server. To sign or decode a message, a consumer should 1st get a message-specific token from its SEM. while not this token, the user cannot accomplish the meant task. To revoke the user's ability to sign or decode, the security administrator instructs the SEM to prevent issue tokens for that user's future request. At that instant, the user's signature and/or cryptography capabilities are revoked. For quantifiability reasons, one SEM serves several users. We stress that the SEM design is clear to non-SEM users, i.e., a SEM is not concerned in cryptography or signature verification operations. With SEM's facilitate, a SEM consumer (Alice) will generate customary RSA signatures, and decode customary cipher text messages encrypted together with her RSA public key. while not SEM's facilitate, she cannot perform either of those operations. This backwards compatibility is one in every of our main style principles. Another notable feature is that a SEM isn't a completely trustworthy entity. It keeps no consumer secrets and every one SEM computations area unit checkable by its shoppers. However, a SEM is part trustworthy since every signature supporter implicitly trusts it to possess checked the signer's (SEM's client's) certificate standing at signature generation time. Similarly, every encryptor trusts a SEM to examine the decryptor's (SEM's client's) certificate standing at message cryptography time. we have a tendency to think about this level of trust cheap, especially since a SEM serves a large number of shoppers associated so represents an organization (or a group). In order to experiment and gain sensible expertise, we have a tendency to prototyped the SEM architecture exploitation the popular OpenSSL library. SEM is enforced as a daemon process running on a secure server. On the consumer aspect, we have a tendency to designed plug-ins for the Eudora and Outlook email shoppers for sign language outgoing, and decrypting incoming, emails. each of those tasks area unit performed with the SEM's facilitate. Consequently, signing and cryptography capabilities may be simply revoked. It is natural to raise whether or not constant practicality may be obtained with additional ancient security approaches to fine-grained management and quick written document revocation, such as Kerberos. Kerberos [25], after all, has been breathing since the mid- 80s and tends to figure fine in corporate-style settings. However, Kerberos is awkward in heterogeneous networks like the Internet; its inter-realm extensions are tough to use and need a definite quantity of manual setup. Moreover, Kerberos doesn't inter-operate with fashionable PKI-s and doesn't give universal origin authentication offered by public key signatures. On the opposite hand, the SEM design is totally compatible with existing PKI systems. additionally, the SEM is merely answerable for revocation. not like a Kerberos server, the SEM cannot forge user signatures or decode messages meant for users. As we have a tendency to discuss later in the paper, our approach isn't reciprocally exclusive with Kerberos-like intra-domain security architectures. we have a tendency to assert that the SEM design may be viewed as a group of complementary security services. Authority It is responsible to generate user secret key for each user according to their attributes. Authority which performs the function like Upload File And Provide Download Permission Cloud Server: It provides services to anonymous authorized users. It interacts with the user during the authentication process.

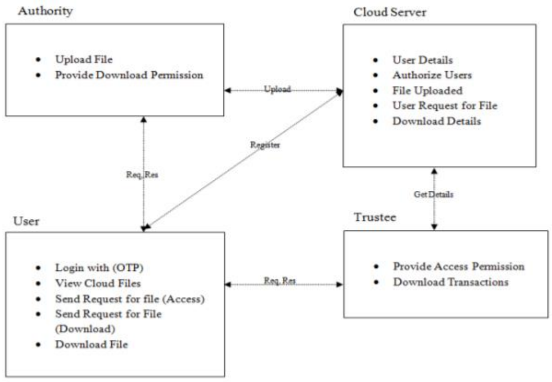


Fig:2 Architecture Diagram

Cloud Server which performs the function like User Details ,Authorize Users, File Uploaded, User Request for File, Download Details User: It is the player that makes authentication with the cloud server. Each user has a secret key issued by the attribute-issuing authority and a security device initialized by the trustee. User which performs the function like Login with (OTP),View Cloud Files, Send Request for file (Access),Send Request for File ,Download File.Trustee:It is responsible for generating all system parameters and initializes the security device. Trustee which performs the function like Provide Access Permission, Download Transactions.

IV. ALGORITHM

In this section, we formalize the system model and attack models considered in this paper, and identify the design goals

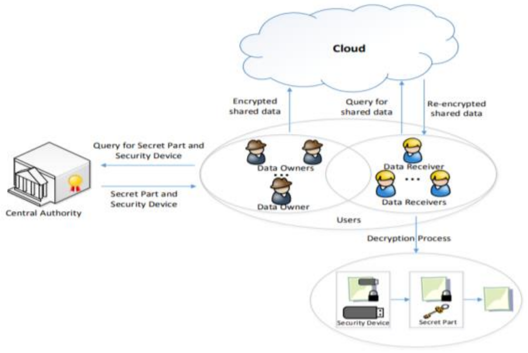
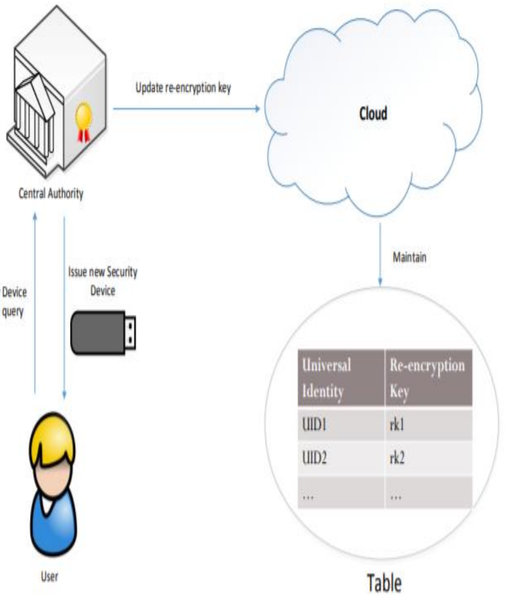


Fig. 3: Architecture of our framework

Fig. 3 shows the architecture of our CP-ABE based finegrained two-factor data protection framework. There are four main entities in our framework: Central Authority (CA), Cloud, Data Owners (DOs) and Data Receivers (DRs)1 .

• Central Authority (CA): The CA is a trusted party which is responsible for issuing the cryptographic key for every user according to their attribute set and then splitting it into two parts (two-factor): One, called as Secret Part Key (SPK), is assumed to be stored in a potential-insecure place (e.g., computer). The other, named as Security Device Key (SDK) is stored in a physically-secure but computationally limited device (security device). Furthermore, the CA is also responsible for updating every user's security device (and the corresponding SDK). Specially, in the SDK update phase, the CA generates a new SDK that is stored in a security device and the corresponding reencryption key that will be sent to the cloud. Fig. 2 shows the process of SDK update. We will give more details in Section IV.



Universal Identity	Re-encryption Key
UID1	rk1
UID2	rk2
...	...

Fig. 4: The process of SDK update

Note that the re-encryption key is used to update the cipher texts to make the new SDK work, while the generation of the re-encryption key requires the information of the old SDK. As mentioned before, one of the advantages of our proposal is that the CA does not need to store any secrets for users. In this case, the way that the CA simply issue an update key to update the old SDK cannot work due to the absent of the old SDK (the security device may be stolen or lost). To solve the problem, we use SPK to retrieve SDK instead. (See Section IV for more details.) • Cloud: The cloud is a semi-trust party that stores all encrypted shared data and maintains a table T able containing the users' universal identity (UID) and corresponding re-encryption key. When a DR queries for the shared data, the cloud acts as a proxy to re-encrypt the encrypted shared data by using DR's corresponding re-encryption key and returns the re-encrypted shared data to DR. • Data Owner (DO): A DO is a user who wants to share data with other users (DRs). All the shared data are encrypted by using CP-ABE according to the access policy. • Data Receiver (DR): A DR is a user who can receive the shared data from the cloud. When a DR wants to retrieve the shared data, be decrypted by using DR's own SPK and SDK, if DR's attribute set satisfies the access policy of the shared data. Note that SDK is never revealed out of the security device during the decryption, while a partial decryption process using SDK would be executed in the security device. Once the security device is lost or stolen, DR can revoke it and obtain a new security device through interacting with CA.

IV. RESULT

The numerical and experimental comparison between these two schemes Here modify LLS+15 from CCA-secure to CPA-secure by removing the parts related to the CCA security since our scheme is CPA-secure. Most of the related parts are due to the FO transformation, we can also use this method to make our scheme CCA-secure.We denote te, te1 and tp as the time for one exponentiation in G and G1, and one pairing, respectively. We also let jGj, jZpj and jG1j as the bit length of an element in G, Zp and G1, respectively. jWj denotes the bit length of the AND gate, and denotes the length of security parameter. Again, to make the comparison relatively fair, we set the attribute number in the system, the access structure and the private key to 1.The number of user's attributes are relatively small in real world.

V. CONCLUSION

In this paper, the proposal is a fine-grained two-factor data protection for cloud storage. The two-factor is realized by separating the secret key into two parts, one can be stored in a potential-insecure place, and the other is stored in a tamper resistant device. Only if one of them is kept secret, the proposal remains secure. Furthermore, with the help of CPABE and PRE, we obtained the fine-grained access control on encrypted. data and the revocability of tamper resistant device, respectively.

REFERENCES

1. J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for web-based cloud computing services," IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp.484–497, 2016.
2. C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, "Chosen cipher text secure attribute-based encryption with outsourced decryption" in Australasian Conference on Information Security and Privacy. Springer, 2016 , pp.495–6 based storage system in a cloud-of-clouds," Computers, IEEE Transactions on, vol. 63, no. 1, pp. 31–44, 2014
3. C.Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure. cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013
4. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," Services Computing, IEEE Transactions on, vol. 6, no. 2, pp. 227–238, 2013.
5. C., Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," Services Computing, IEEE Transactions on, vol. 5, no. 2, pp. 220–232, 2012.
6. L. Xu, X. Wu, and X. Zhang, "Cl-pre: a certificateless proxy re-encryption scheme for secure data sharing with public cloud," in Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012, pp. 87–88.
7. F. Zhang, Q. Li, and H. Xiong, "Efficient revocable key-policy attribute based encryption with full security," in Computational Intelligence and Security (CIS), 2012 Eighth International Conference on. IEEE, 2012, pp. 477–481.
8. A. De Caro and V. Iovino, "jpbc: Java pairing based cryptography," in Proceedings of the 16th IEEE Symposium on Computers and Communications ISCC 2011. Kerkyra, Corfu, Greece, June 28 - July 1: IEEE,2011, pp. 850–855
9. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography–PKC 2011. Springer, 2011, pp. 53–70.
10. J. Herranz, F. Laguillaumie, and C. R`afols, "Constant size ciphertexts in threshold attribute-based encryption," in Public Key Cryptography– PKC 2010. Springer, 2010, pp. 19–34.
11. N. Attrapadung, B. Libert, and E. De Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Public KeyCryptography–PKC 2011. Springer, 2011, pp. 90–108.
12. Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 463–474.
13. J.-l. Qian and X.-l. Dong, "Fully secure revocable attribute-based encryption,"Journal of Shanghai Jiaotong University (Science), vol. 16,pp. 490–496, 2011.
14. S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Securitymediated certificateless cryptography," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 508–524.
15. C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.
16. R. Cramer, I. Damgård, and P. D. MacKenzie, "Efficient zero-knowledge proofs of knowledge without intractability assumptions," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 1751, H. Imai and Y. Zheng, Eds. Berlin, Germany: Springer-Verlag, 2000, pp. 354–373.

17. Y. Dodis, J. Katz, S. Xu, and M. Yung, “Key-insulated public key cryptosystems,” in Proc. EUROCRYPT, 2002, pp. 65–82.
18. Y. Dodis and A. Yampolskiy, “A verifiable random function with short proofs and keys,” in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416–431.
19. M. K. Franklin, in Proc. 24th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 2004.
20. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attributebased encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.