International Journal of Science Engineering and Advance Technology, IJSEAT, Vol. 5, Issue 7 | ISSN 2321-6905 JULY -2017

International Journal of Science Engineering and Advance Technology

Key Distribution And Privacy Preserving In An Access Controlled Cloud Computing

[1]A. Anuradha, [2]Ch.Karthik
[1]H.O.D ,Dept. of M.C.A, Dr. C.S.N Degree & P.G College, Industrial Estate, Bhimavaram, W.G.DT,AP, India
[2]Student ,Dept. of M.C.A, Dr. C.S.N Degree & P.G College, Industrial Estate, Bhimavaram, W.G.DT,AP, India

ABSTRACT:
We propose a safe information sharing plan for dynamic individuals. Initially, we propose a protected path for key conveyance with no safe correspondence channels, and the clients can safely get their private keys from gathering director. Second, our plan can accomplish fine-grained get to control, any client in the gathering can utilize the source in the cloud and denied clients can't get to the cloud again after they are renounced. Third, we can shield the plan from conspiracy assault, which implies that renounced clients can't get the first information document regardless of the possibility that they scheme with the untrusted cloud. In our approach, by utilizing polynomial capacity, we can accomplish a safe client denial plot. At long last, our plan can accomplish fine proficiency.

KEYWORDS: Access control, privacy-preserving, key distribution, cloud computing

I. INTRODUCTION:

A protected multi-proprietor information sharing plan, named Mona. It is asserted that the plan can accomplish fine-grained get to control and renounced clients won't have the capacity to get to the sharing information again once they are repudiated. Be that as it may, the plan will effortlessly experience the ill effects of the intrigue assault by the renounced client and the cloud. The renounced client can utilize his private key to decode the scrambled information record and get the mystery information after his repudiation by plotting with the cloud. In the period of document get to, as a matter of first importance, the denied client sends his demand to the cloud, then the cloud reacts the comparing scrambled information record and renouncement rundown to the repudiated client without checks. Next, the renounced client can figure the decoding key with the assistance of the assault calculation. At long last, this assault can prompt the denied clients getting the sharing information and unveiling different privileged insights of true blue individuals.

LITERATURE SURVEY:

[1],we build up another cryptosystem for fine-grained sharing of encoded information that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are named with sets of characteristics and private keys are related with get to structures that control which ciphertexts a client can unscramble. We exhibit the relevance of our development to sharing of review log data and communicate encryption. Our development bolsters assignment of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

[2],we display three developments inside our system. Our first framework is demonstrated specifically secure under a supposition that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) presumption which can be seen as a speculation of the BDHE suspicion. Our next two developments give execution tradeoffs to accomplish provable security individually under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear DiffieHellman suspicions.

PROBLEM DEFINITION

Kallahalla et al exhibited a cryptographic stockpiling framework that empowers secure information sharing on deceitful servers in view of the methods that isolating documents into record gatherings and scrambling each record assemble with a record square key.

Yu et al misused and consolidated methods of key strategy trait based encryption, intermediary re-encryption and apathetic re-encryption to accomplish fine-grained information get to control without uncovering information substance

PROPOSED APPROACH

We propose a safe information sharing plan, which can accomplish secure key appropriation and information sharing for dynamic gathering.

We give a protected approach to key dissemination with no safe correspondence channels. The clients can safely acquire their private keys from gathering supervisor with no Certificate Authorities because

of the confirmation for the general population key of the client.

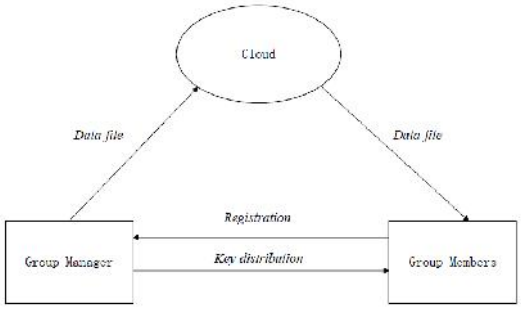
Our plan can accomplish fine-grained get to control, with the assistance of the gathering client list, any client in the gathering can utilize the source in the cloud and disavowed clients can't get to the cloud again after they are renounced.

We propose a safe information sharing plan which can be shielded from conspiracy assault. The renounced clients can not have the capacity to get the first information documents once they are denied regardless of the possibility that they plan with the untrusted cloud. Our plan can accomplish secure client denial with the assistance of polynomial capacity.

Our plan can bolster dynamic gatherings proficiently, when another client participates in the gathering or a client is disavowed from the gathering, the private keys of alternate clients don't should be recomputed and refreshed.

We give security investigation to demonstrate the security of our plan.

SYSTEM ARCHITECTURE:



PROPOSED METHODOLOGY:

DATA OWNER(GROUP MEMBER)

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

CLOUD SERVER

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

DATA INTEGRITY

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

GROUP MANAGER

The Group Manager who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data. The Group Manager will perform the revocation and un revocation of the remote user if he is the attacker or malicious user over the cloud data.

DATA CONSUMER(END USER / GROUP MEMBER)

In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the GM authority and the Data user's are controlled by the GM Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges.

ALGORITHM:

SECURE DATA SHARING SCHEME:

INPUT: GROUP MANAGER, GMEMBER, SIGNATURE, FILE, PUBKEY, SECKEY

STEP1: Group manager take charge of secure symmetric encryption algorithm with secret key k. and it will be kept secret as the master key of the group manager.

STEP2: The group manager adds the group user list, which will be used in the traceability phase. After the registration, user i obtains a private key which will be used for group signature generation and file decryption.

STEP3: User revocation is performed by the group manager via a public available revocation list ðRLÞ, based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

step4: Uploading the data into the cloud server and adding the data into the local shared data list maintained by the manager.

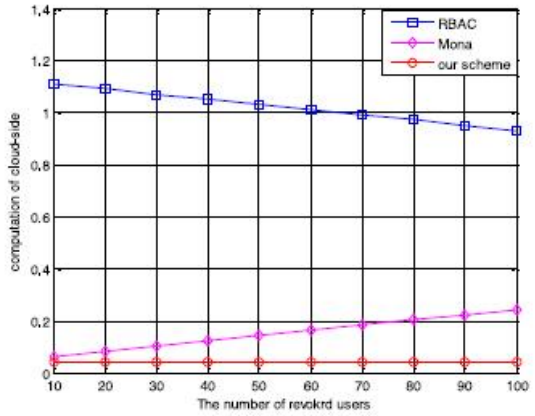
Step5: Group members in different groups sharing data is validated by Group manager based on signature validation.

STEP6: On receiving the data, the cloud first invokes signature generation technique to check its validity. If the algorithm returns true, the group signature is valid; otherwise, the cloud abandons the data.

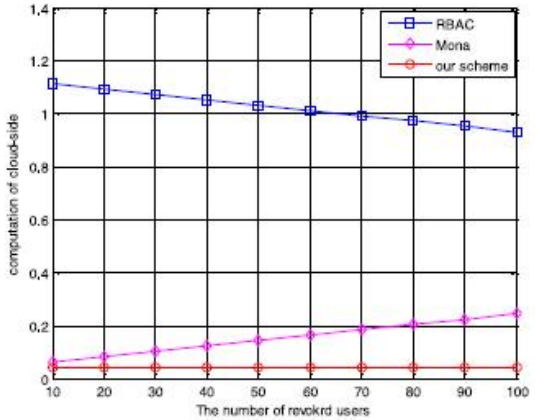
STEP7: Obtaining the tuple data from his local storage. Invoking signature generation to compute a group signature on data.

STEP8: Sending data and the signature as a deletion request to the cloud.

RESULTS:



(a) Downloading a 10 MB file



(b) Downloading a 100 MB file

Comparison on computation cost of the cloud for file download among RBAC, Mona and our scheme

CONCLUSION:

We outline a protected against intrigue information sharing plan for dynamic gatherings in the cloud. In our plan, the clients can safely get their private keys from gathering supervisor Certificate Authorities and secure correspondence channels. Likewise, our plan can bolster dynamic gatherings proficiently, when another client participates in the gathering or a client is repudiated from the gathering, the private keys of alternate clients don't should be recomputed and refreshed. Also, our plan can accomplish secure client disavowal, the denied clients cannot have the capacity to get the first information records once they are repudiated regardless of the possibility that they scheme with the un confided in cloud.

REFERENCES:

[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. Financial 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. File and Storage Technologies, pp. 29-42, 2003.

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

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

[6] Shucheng Yu, Cong Wang, KuiRen, 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. Computer and Comm. Security (CCS), pp. 89-98, 2006

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

[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public 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, "Hierarchical IdentityBasedEncryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf.Theory and Applications of Cryptographic Techniques (EUROCRYPT),pp. 440-456, 2005.

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

[13] Zhongma Zhu, Zemin Jiang, Rui 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] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving 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]XukaiZou, Yuan-shunDai, and ElisaBertino, "A practical and flexible keymanagement mechanism for trusted collaborative computing,"INFOCOM 2008, pp. 1211-1219.

AUTHOR BIOGRAPHIES

Smt. A. ANURADHA, **MCA, M.Phil, M.tech, (PHD)** well known Author and excellent teacher Received M.C.A from Sri Venkateswara University, Nellore., M.Phil form Alagappa University, M.Tech(IT) form Andhra University and PHD from Nagarjuna University. Presently she is working as Asst. Professor & HOD in the department M.C.A, Dr. C.S.N Degree & P.G College – Bhimavaram. She has 13 years of teaching experience in various P.G colleges. To her credit couple of publications both national and international Conferences /Journals. Her area of Interest includes Data Warehouse, Data Mining, Neural Networks, flavors of Unix Operating systems and other advances in computer Applications.

Mr. CH.KARTHIK is a student of Dr.C.S.N Degree& PG College Industrial Estate Bhimavaram. Presently he is pursuing his MCA [Master of Computer Applications] from this college. His area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.