International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

A Secure Anti-Collusion Data Sharing Framework for Cloud-Based Dynamic Groups

Ms.M.ANITHA[1], Ms. K. PAVANI [2], CH. SWATHI [3]

#1 Assistant professor in the Master of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

#2 Assistant professor in the Master of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

#3 MCA student in the Master of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

ABSTRACT_ Profited from distributed computing, clients can accomplish a successful and affordable methodology for information dividing between bunch individuals in the cloud with the characters of low support and little administration cost. In the interim, here should give security assurances to the sharing information documents since they are rethought. Sadly, due to the frequent membership changes, sharing data while maintaining privacy is still a difficult problem, especially for an untrusted cloud affected by the collusion attack. Besides, for existing plans, the security of key circulation depends on the protected correspondence channel, in any case, to have such channel is major areas of strength for an and is hard for training. In this venture, I propose a protected information sharing plan for dynamic individuals. In the first place, here I propose a safe way for key dispersion with next to no solid correspondence channels, and the clients can safely get their confidential keys. Second, our plan can accomplish fine-grained admittance control, any client in the gathering can involve the source in the cloud and denied clients can't get to the cloud again after they are repudiated. Third, I can shield the plan from arrangement assault, and that implies that denied clients can't get the first information document regardless of whether they scheme with the untrusted cloud. Using the polynomial function, I am able to implement a secure user revocation scheme in our strategy. At last, our plan can accomplish fine proficiency, and that implies past clients need not to refresh their confidential keys for the circumstance either another client participates in the gathering or a client is disavowed from the gathering

1.INTRODUCTION

Data sharing has become an increasingly important topic in the business world. Traditionally defined as a concept in the world of academic research, data sharing as a technology has become highly relevant for businesses of all sizes, whether they need to disseminate data across a large, global organization or need to augment internal data with broader market data to gain better insights. The sharing of data securely in cloud computing is a very crucial method. The information is stored in cloud data centers. To access data from or store data into data centers through the internet, the intruders may attack our data. Users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacypreserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice...

2.LITERATURE SURVEY

1. "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,"

AUTHORS: B. Wang, B. Li, and H. Li,

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

2. "Security Challenges for the Public Cloud,"

AUTHORS: K. Ren, C. Wang, and Q. Wang,

In this talk, I will first discuss a number of pressing security challenges in Cloud Computing, including data service outsourcing security and secure computation outsourcing. Then, I will focus on data storage security in Cloud Computing. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging. In this talk, I will present our recent research efforts towards storage outsourcing security in cloud computing and describe both our technical approaches and security & performance evaluations.

3. "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,"

AUTHORS: C. Wang, Q. Wang, K. Ren, and W. Lou

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

3.PROPOSED SYSTEM

□ In this undertaking, I propose a protected information sharing plan, which can accomplish secure key dissemination and information sharing for dynamic gathering.

I supply a secure method for the distribution of keys in the absence of secure communication channels. Due to user verification of the user's public key, users can securely obtain their private keys from group manager without the need for Certificate Authorities.

Any user in the group can use the source in the cloud with the assistance of the group user list, and revoked users cannot access the cloud again after being revoked. Our scheme can achieve fine-grained access control.

□ I propose a safe information sharing plan which can be shielded from plot assault. The denied clients can not have the option to get the first information records whenever they are disavowed regardless of whether they plan with the untrusted cloud. With the assistance of a polynomial function, our strategy is capable of achieving secure user revocation.

□ Our plan can uphold dynamic gatherings productively, when another client participates in the gathering or a client is denied from the gathering, the confidential keys of different clients needn't bother with to be recomputed and refreshed.

 I give security examination to demonstrate the security of our plan.

3.1 IMPLEMENTATION

1. Group Manager Module :

Group manager takes charge of followings:

- ➢ System parameters generation
- ➢ User registration
- ➢ User revocation
- ➢ Revealing the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

2. Group Member Module :

Group members are a set of registered users that will

- ➢ Store their private data into the cloud server and
- ➢ Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it.

File Security Module :

- ➢ Encrypting the data file.
- ➢ File stored in the cloud can be deleted by either the group manager or the data owner.

(i.e., the member who uploaded the file into the server).

Group Signature Module :

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

User Revocation Module :

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

3. Member Registration Module

In this module, registration can be done by the members who wants to join in the particular group by giving their details like,

- ➢ User name
- ➢ Password
- ➢ Respective Group
- ➢ Email
- ➢ Mobile number
- ➢ Place

These details are mandatory and enter the details with required specifications.

.

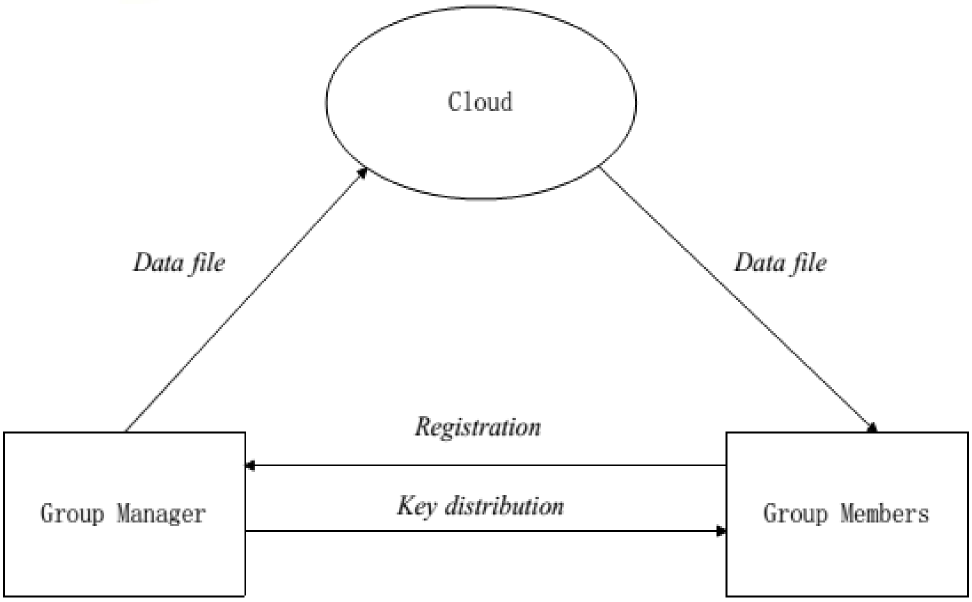
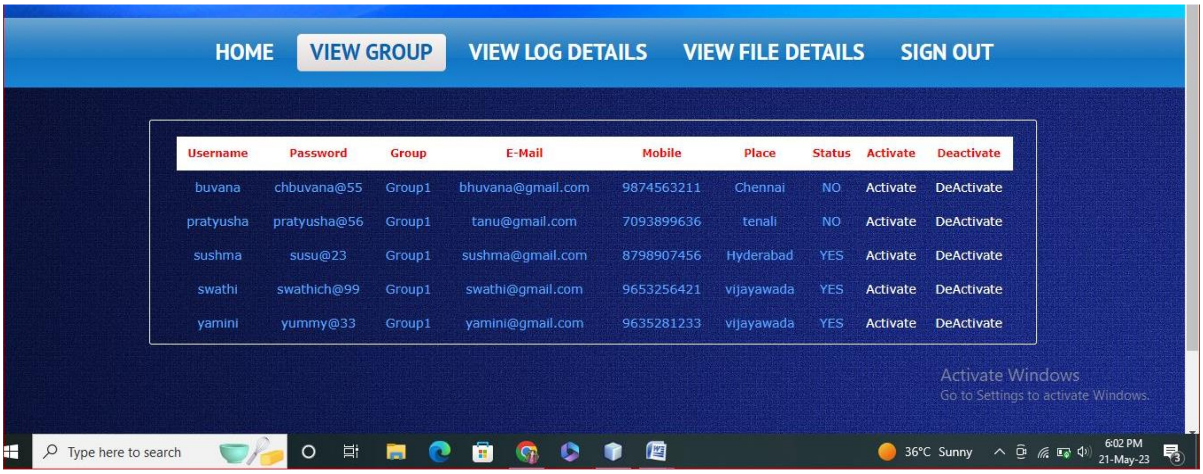


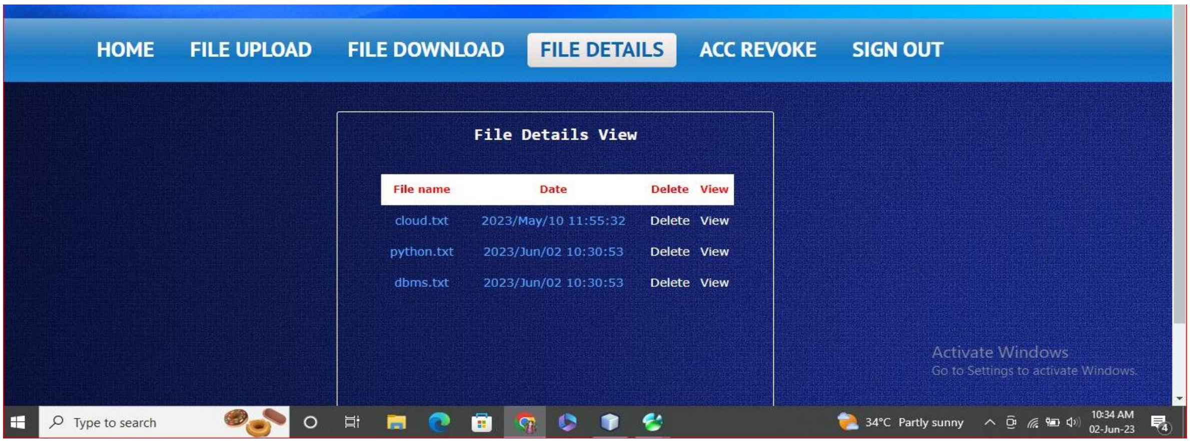
Fig 1:Architecture

4.RESULTS AND DISCUSSION



Username	Password	Group	E-Mail	Mobile	Place	Status	Activate	Deactivate
buvana	chbuvana@55	Group1	bhuvana@gmail.com	9874563211	Chennai	NO	Activate	DeActivate
pratyusha	pratyusha@56	Group1	tanu@gmail.com	7093899636	tenali	NO	Activate	DeActivate
sushma	susu@23	Group1	sushma@gmail.com	8798907456	Hyderabad	YES	Activate	DeActivate
swathi	swathich@99	Group1	swathi@gmail.com	9653256421	vijayawada	YES	Activate	DeActivate
yamini	yummy@33	Group1	yamini@gmail.com	9635281233	vijayawada	YES	Activate	DeActivate

Fig 2:After view a respective group, the group contains the group member username, passwords which group they are belonging to and their e-mail addresses mobile number, place and as well active statuses.



File Details View

File name	Date	Delete	View
cloud.txt	2023/May/10 11:55:32	Delete	View
python.txt	2023/Jun/02 10:30:53	Delete	View
dbms.txt	2023/Jun/02 10:30:53	Delete	View

Fig 3: After file download and then we can see the file details file uploaded date and file delete and view files option. When we want to delete or to view the files it asks the signature key of the file as shown below.

5.CONCLUSION

We create a safe anti-collusion data exchange system for active organisations online. In our system, the group manager Certificate Authorities and secure communication channels allow the users to safely receive their private keys. The private keys of the other users do not need to be recalculated and updated when a new user enters the group or a user is removed from the group thanks to the efficient dynamic group support provided by our scheme. Furthermore, our system enables secure user revocation; revoked users are unable to access the original data files after their access has been terminated, even if they work with an unreliable 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.

AUTHOR PROFILES

Ms. M. ANITHA completed her Master of Computer Applications and Masters of Technology. Currently working as an Assistant professor in the Department of Masters of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Ms. K. PAVANI completed her Master of Computer Applications. Currently working as an Assistant professor in the department of MCA at SRK Institute of Technology, Enikepadu, NTR District. His areas of interest include Artificial Intelligence and Machine Learning.

CH. SWATHI is an MCA student in the Department of Master of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. She has Completed Degree in B.Sc (computers) from ASN Degree College(Affiliated to Acharya Nagarajuna University), Tenali. Her areas of interest are Cloud Computing, DBMS, JavaScript, Machine Learning with Python, HTML, CSS.