# Secure Data Validation in Cloud Using Trusted Third Party Module

Mr.M.Ayyapa Chakaravarthi[1],K.Naga Preethi[2], K.Siva Nageswarao[3], I.Divya Jyothi[4], N.Ganesh[5]
*[1]Assoc.Prof, Dept of CSE, Tirumala Engineering College, Narasaropet, Guntur, A.P., India*
*[2,3,4,5] B. Tech Students, Dept of CSE, Tirumala Engineering College, Narasaropet, Guntur, A.P., India*

Abstract: Information sharing today is not an easy task if the data is accessible to the cloud and if the access authorization is needed depending on the position of the information. If the Data Owner Program Module uploads a specific document, the file is authenticated by the Data Owner and provided with an attribute dependent protection. This is particularly important for any broad information sharing network, since it is challenging for single-and multi-user users to protect the data, then the data owner becomes difficult. This paper calls for a practical and efficient instantiation of the scheme offered for the main purpose, illustrates the protection based on its characteristics and offers a functional implementation component. The transfer of cloud data from the already accessible network using a different technique in order to solve security problems has become more complicated for data owners. Existing approaches for solving this problem are becoming very necessary to manage and share information with the key dependent data security. This article would present the Trusted Third Party to authenticate those who have links to cloud data. Trusted Third Party generates the key with theMd-5 algorithm which allows users and owner to share. The Trusted third party module accepts encrypted file F from data owner using a RSA algorithm and calculates a MD-5 hash key. It store keys in its data base that are used to evaluate the tricker in the cloud service provider and storage owner for the evolving operations. Trustworthy Third Party transfers data F to the Provider node of the cloud service to save.

Keywords: Attribute Based Security; Cloud Service Provider; Authentication Service; data sharing system;

## I. INTRODUCTION

The internet now has many innovations to help. Cloud computing is one of the most common technologies. The cloud computing environment creates the massive storage center. Cloud computing is now a tool for the consumer to use in remote cloud access to data. The website, which is compensated for by use at the request site, can be easily and quickly accessed. Cloud computing is used mostly by companies and industries and provides immense room for low-cost data sharing. Most cloud vendors such as the Aws, Google App Engine, Drop Box, etc. offer cloud services. Cloud provides data management as one of the most important services. There are several issues involved in data sharing between two participants or party of representatives. It is performance, data integrity and data proprietor protection. The most difficult activities for complex organizations are to provide anonymity and honesty. The current system offers diverse participants with a secure data sharing scheme [1]. This method utilizes key sharing in a secure way so that community administrators provide the users with private keys without using secure communication networks. The program should maintain a comprehensive monitoring of entry. This provides security against coordination attacks with the use of a community signature that guarantees secure app revokes. Collusion assault includes decrypting data using a secret key by the revoked person and sharing secret files with the web. Secure deletion of users ensures the relocated users will not be able to obtain the original data file if they conspire with the server. The program will offer outstanding reliability, which ensures that former members do not need to change their private keys when a new user enters the party or a user is deleted. Safe and efficient procedures are required to provide cloud-specified data integrity and privacy [2].

Community signature [3] enables members of a group to sign a document on behalf of the party as a whole without sharing their own identities. Group signature has two features: 1) traceability and confidentiality 2). Anonymity ensures that the specific group leaders who make up the signature do not show. As in any systems that protect privacy, consumer secrecy is preserved as far as it is practicable, but we must also make sure that a mechanism exists to misinterpret group members. With the aid of a traceability domain, the community signature recognizes the mis conducting members. Nevertheless, there is certain compliance situations in which a signatory identification cannot be revealed. It violates the community signature's anonymity rights. This paper suggests a Ring Signature on Identity in order to resolve this downside. This program helps to provide protection for huge cloud data sharing. Code verification for cloud data exchange guarantees secure data sharing through the group's identity-based code signature. The legitimacy and confidentiality of end users are also given. As is the case with a standard public key infrastructure environment, which is a limitation, the proposed system eliminates costly registration keys. Leaking of a user's secret key does not invalidate all previously created signatures of identity-based ring signatures. In particular, the assets are vital for every huge quantity of data sharing schemes as all data owners cannot be required to re-authenticate their data even if there is one user's hidden key.

## II. RELATED WORK

Liu et al. [5] suggested a stable multi-owner system called Mona for data sharing. This system will accomplish advanced access control and remove the rights of users to share data once they are revoked. Nonetheless, a conspiracy assault on the relocated user and the server will be quickly endured in the scheme [6]. The consumer revoked will decrypt the encrypted data and retrieve the secret data by coordinating with the cloud using his personal key. The revoked consumer submits his request to the cloud during the process of database access, and then the cloud replies to the respective encoded logs. After that, the revoked user can use the attack algorithm to determine the decryption key. This attack will ultimately cause the revoked users to gain data sharing and to expose certain secrets of legitimate members.

Zhou et al. [7] have suggested a secure access control system in cloud storage using a role-based encryption technology to encrypt data. That method, the account can be removed well-organized and incorporates roll-based access control controls with encryption to guarantee large cloud storage. Regrettably, tests between organizations are not afraid. The system is easily attacked by conspiracy, for example. Finally, this assault will contribute to sensitive data files being revealed.

Zou etal. [8] Also suggested a trustworthy shared programming practical and scalable key management framework. It is structured to effectively handle connectivity for complex classes. Unfortunately, the safe solution to the exchange of the member's specific permanent portable secret and the hidden key will not be accepted until disclosed after the intruder has accessed the personally permanent portable information.

Nabeel et al. [9] suggested a method of data sharing focused on privacy protection in public clouds. Yet, for the sake of inadequate security of involvement in the identity token issuance, this device cannot be protected.

## III. PROPOSED METHOD

Identity Based Ring Authentication proposed to improve safety by offering fine grain access control and raising overheads for main generation. Signature of the ring is group-oriented privacy-related signature [10]. This signature is one of the physical. The credibility and privacy of the consumer is given by this system. In comparison to traditional methods, an identity based ring signature cannot carry out certificate authentication. The ring signature on identity-based systems incorporates the cryptosystem and ring signature.

There are 3 algorithms in the ring signature scheme: **KeyGen;** Sign and Check. Once the protection parameter 1k is accessed, the user implements KeyGen independently in this algorithm and generates a key-pair (pk, sk). The algorithm for the Sign requires a secret key sk on the entry, the ring R includes a list of public keys that correspond to ring members, a signature a and a message m, the output is μ on m. The Verify Algorithm, the Ring R, the signature μ, and the message m are taken from the input, the output is 1 if some R participant generated the signature − on m and the output is 0.

### A. Framework

The following four protocols include an ID-based ring signature scheme: Preferences, keygenes, signatures, and verifications.

**Setup:** When k is a protection parameter with an unary input strings 1k, it generates the main secret key s and the public parameters that include the definition of a finite signature space and the description of a finite message area. Setup:

**KeyGen:** It returns the hidden SID key for Signer by taking an ID{ 0,1} and a master secret s entry of signer identification. Sign: on input of a message m, group of the n user identity S{ IDi}, where 1~I{ n} and the hidden keys of the SID members where 1{ s} is a message n, outputs an identity-based ring signature on the message m. (All the users can determine the corresponding public authentication key QID).

**Verifying:** It collects feedback as the ring signature¨, the m message and the S{IDi} community of signatories, it releases 1 to' true' or 0 to' false' based on if¨is a legitimate signature of a certain S{IDi} representatives in the m message category. These algorithms are required to meet the ID-based ring signature standard restriction, i.e. if S −Sign(m, S{IDi},SIDs) and IDs{ IDi}, we have to have Verify(τ,S{IDi},m)=1, and the performance is otherwise0.

Enforceability and signatories should also be a stable ID-based ring signature scheme.

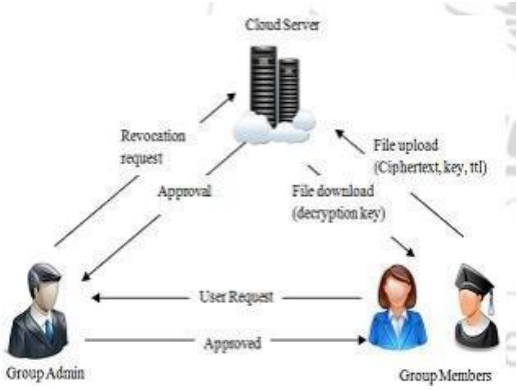

**Figure 1**: Architecture of cloud data Sharing Scheme

The architecture of the structure comprises of three different entities: A project manager and three group members.

**Cloud Server:** Cloud manages information tremendously. Cloud saves all team holders and accesses the file for other groups participants within a group based on the publicly available cancelation list the Community Admin retains. We might picture a truthful yet interested cloud service. That is, because of the protection of computer auditing scheme Group **Admin:** Group Admin is working by the Company's owner, the cloud service does not deliberately remove or change user data. They assume, however, that the other parties would support Team Admin in full. Community Administrators perform different operations, such as generating device parameters, registrying members, establishing the community, assigning ring signatures, generating a private key using bilinear map and assigning it to the requested person.

**Group Members:** Group members are a community of registered users who store and share their personal data with other owners in the team on the cloud server. Team administrators and group members are able to log in via their login information. Upon effective login, Group Admin unlocks cloud newly added users by creating keys for each participant and sending them to their respective group members through bilinear mapping. He may also check the details of group and appoint signature of group. The signature of Group Members shall be confirmed upon effective login. The user is able to upload, update and edit the files after a positive review. Until uploading to the server, Group Member will crypt data file. Upon entering the cloud by the Group Manager, the Group Members identity may be revoked.

**User registration:** Participants want to be enrolled with the network via their user registration process following effective development of their cloud setup. Members must apply their personal information to complete the registration process during enrollment. The customer with his / her ID (user name, mobile no and e-mail-id), registered with them. Users have a special name and permission mechanism during the registration process. This gives the leaders a secret key. A registered user uses the hidden key for encrypting and decrypting the file.

**User Authentication:** After proper insertion of user I d and password, users can only login successfully. Login is not feasible if the user enters the wrong user I d or incorrect password. This helps to avoid unauthorized access.

**Key distribution:** Way of transferring secret keys through the Admin Committee which is only true if Group members are not removed. By generating new key from an old key, the key can be modified.

Account cancellation: account cancellation is the account elimination process that is achieved by community admin from a device user list. Community admin will revoke multiple users directly at any time via public revocation list without impacting any unrevoked account. If the user defined login credentials suit the revoke list data, access is refused.

**File Upload:** File upload is a cloud storage system for defined data files. Until the date defined for uploading the file, uploaded data stay in the cloud. The file must be secured and compacted before the file is submitted to guarantee the file's safety and privacy. The relevant decryption key and TTL value for the file is encapsulated and sent to the server.

**Download File:** Group members submit as team I d, user I d, in order to access the data stored in the cloud. If the group member in the same community will access the code, the Cloud server can validate the signature. Group members are entitled to access data, but not to remove or alter any data stored in the cloud.

## IV. RESULTS

### A. Security Analysis

**Table 1:** Security performance comparison

| | RBAC | Mona | Proposed method |
|---|---|---|---|
| Secure key distribution | | ✓ | ✓ |
| Access control | ✓ | ✓ | ✓ |
| Secure user revocation | | | ✓ |
| Anti-collusion attack | | | ✓ |
| Data confidentiality | | ✓ | ✓ |

The suggested agreements will achieve protected dissemination of key data, comprehensive access control, conspiracy security, data secrecy, and a stable user revocation in contrast to RBCA and Mona.

B. Performance analysis the identity-based ring signature is related on the overall time taken to upload and retrieve a file from / to the cloud. The total time consists of the duration that the data has been sent to the cloud server until the file is uploaded / downloaded from / to the system.

**Table 2:** Comparison of Turnaround Time

| File size (KB) | Existing Method | | Proposed method | |
|---|---|---|---|---|
| | Upload | Down-load | Upload | Down-Load |
| 150 | 12.5 | 11.6 | 12 | 7.8 |
| 500 | 35 | 40.5 | 33.8 | 32.3 |
| 1000 | 80.5 | 85.6 | 77.4 | 50.8 |
| 1500 | 95.1 | 122.2 | 82.1 | 51.9 |

Table 2 shows that turnaround time for upload and download the file. In general, the time to upload and download the data increased with the increase in the file size This table reveal that the proposed method outperforms the existing method appropriate to the absence of heavy computations and memory overhead.

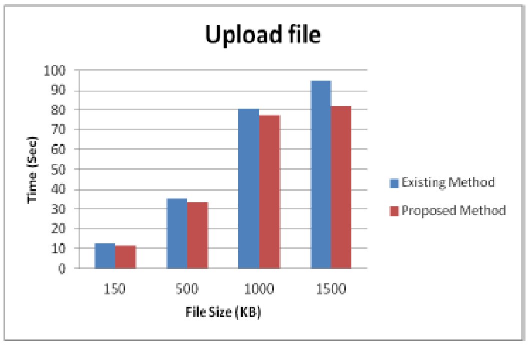

**Figure 2:** Performance of File Upload

In Figure 2 shows the result for upload time. X axis represents the file size Y axis represents the time. In existing system method 1.5mb was uploaded in 95.1s, where as in proposed system method it takes 82.1s to upload a 1.5mb file. This graph clearly shows that as compare to the existing system the performance of proposed system is higher.

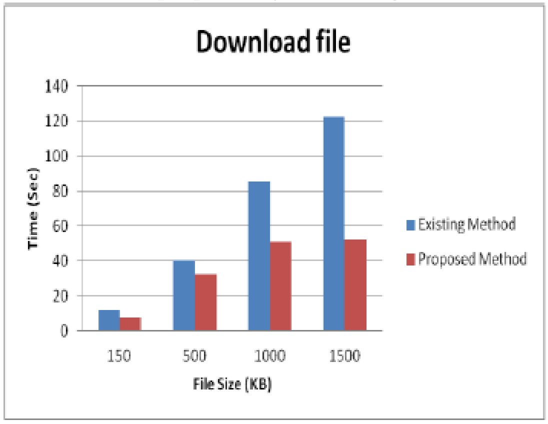

**Figure 3:** Performance of File Download.

In Figure 3 shows the result for download time. X axis represents the file size Y axis represents the time. In existing system method 1.5mb was downloaded in 122.2s, where as in proposed system method it takes 51.9s to upload a 1.5mb file. This graph clearly shows that as compare to the existing system the performance of proposed system is higher.

## V. CONCLUSION

This document implements an Identity-Based Ring Signature which ensures the secure use of a recognizable ring signature for large quantities of cloud data sharing. The signature ring is group-oriented, privacy-based signature. It is a digital signature of this kind. This method offers the end user privacy and credibility. The ring signature based on identity eliminates the cycle of official document authentication, which in traditional public key architecture is a question of bottleneck. The proposed system supports multiple users to share shared details between the participants and each participant will engage in the complexities of the data.

## VI. REFERENCES

[1]. Zhu, Z., & Jiang, R. (2016). “A secure anti-collusion data sharing scheme for dynamic groups in the cloud”. *IEEE Transactions on parallel and distributed systems*.

[2]. S. Vasundra (2016) “Efficient & Secure Privacy Preserving Public Auditing Scheme for Cloud Storage”, ISSN- 2278-1323, Vol 5, Issue 9.

[3]. Camenisch, J., & Michels, M. (1998, October). A group signature scheme with improved efficiency. In *Asiacrypt* (Vol. 98, pp. 160-174).

[4]. Chow, S. S., Yiu, S. M., & Hui, L. C. (2005, June). Efficient identity based ring signature. In *International Conference on Applied Cryptography and Network Security* (pp. 499-512). Springer, Berlin, Heidelberg.

[5]. Zhu, Z., Jiang, Z., & Jiang, R. (2013, December). The attack on mona: Secure multi-owner data sharing for dynamic groups in the cloud. In *Information Science and Cloud Computing*

[6]. *Companion (ISCC-C), 2013 International Conference on* (pp. 213-218). IEEE.

[7]. Liu, X., Zhang, Y., Wang, B., & Yan, J. (2013). Mona: Secure multi-owner data sharing for dynamic groups in the cloud. *ieee transactions on parallel and distributed systems*, *24*(6).

[8]. Zhou, L., Varadharajan, V., & Hitchens, M. (2013). Achieving secure role-based access control on encrypted data in cloud storage. *IEEE transactions on information forensics and security*, *8*(12).

[9]. Zou, X., Dai, Y. S., & Bertino, E. (2008, April). A practical and flexible key management mechanism for trusted collaborative computing. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE* (pp. 538-546). IEEE.

[10]. Nabeel, M., Shang, N., & Bertino, E. (2013). Privacy preserving policy-based content sharing in public clouds. *IEEE Transactions on Knowledge and Data Engineering*, *25*(11), 2602-2614.

[11]. Herranz, J., & Sáez, G. New identity-based ring signature schemes. In *ICICS* (Vol. 4, pp. 27-39).