www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 3 March 2014 Page No. 4069-4072

Providing Data Sharing For Multiple Users In Cloud

Mushra[1], Akhila Thejaswi R[2]

[1]Department of Computer Science and Engineering, Sahyadri College of Engineering and Management
Mangalore-575007

[2]Department of Information Science and Engineering, Sahyadri College of Engineering and Management
Mangalore-575007

[1] IV Semester M.Tech (Computer Science and Engineering)

[2] Assistant Professor, ISE, Sahyadri College of Engineering and Management

Emails: [1]mshrb07@gmail.com, [2]akhila.cs@sahyadri.edu.in

Abstract— **With the character of low maintenance, cloud computing provides a cheap and economical resolution for sharing cluster resource among cloud users. Sadly, sharing information an exceedingly in a multi-owner manner whereas protective information and identity privacy from an untrusted cloud continues to be a difficult issue, because of the frequent modification of the membership.**

During this paper, we tend to propose a secure multi-owner data sharing theme, named Mona, for dynamic teams within the cloud. By investing cluster signature and dynamic broadcast encryption techniques, any cloud user will anonymously share information with others. Meanwhile, the storage overhead and cryptography computation price of our theme area unit freelance with the quantity of revoked users. Additionally, I tend to analyze the protection of our theme with rigorous proofs, and demonstrate the potency of us theme in experiments.

Key words—Cloud computing, data sharing, privacy-preserving, access control, dynamic groups

I. Introduction

Based on intrinsic resource sharing and low-maintenance characteristics, cloud computing is referred as traditional information technology[1]. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful data centers.

One of the most basic services offered by cloud suppliers is information storage. Allow us to take into account a sensible information application. A corporation permits its staffs within the same cluster or department to store and share files within the cloud. By utilizing the cloud, the staffs may be utterly discharged from the difficult native information storage and maintenance.

However, it conjointly poses a major risk to the confidentiality of these keep files. Specifically, the cloud servers managed by cloud suppliers don't seem to be totally sure by users whereas the information files keep within the cloud is also sensitive and confidential, like business plans. To preserve information privacy, a basic resolution is to cipher information files, and so transfer the encrypted information into the cloud [2]. sadly, coming up with Associate in Nursing economical and secure information sharing theme for teams within the cloud isn't a simple task because of the subsequent difficult problems.

First, identity privacy is one amongst the foremost vital issues for the wide preparation of cloud computing. While not the guarantee of identity privacy, users could also be unwilling to hitch in cloud computing systems as a result of their real identities can be simply disclosed to cloud suppliers and attackers. On the opposite hand, unconditional identity privacy could incur the abuse of privacy. For instance, a misbehaved employees will deceive others within the company by sharing false files while not being traceable. Therefore, traceability, that allows the cluster manager (e.g., a corporation manager) to reveal the important identity of a user, is additionally extremely fascinating.

Second, is that the multiple-owner ,it's like extremely counselled member in a very cluster ought to be able to totally relish the info storing and sharing services provided by the cloud. Compared with the single-owner manner [3], wherever solely the cluster manager will store and modify information within the cloud, the multiple-owner manner is a lot of versatile in sensible applications. a lot of concretely, every user within the cluster is to not solely read information, however additionally modify his/her a part of information within the entire file shared by the corporate.

At last, teams square measure unremarkably dynamic in follow, e.g., new employee's participation and current worker revocation during a company. The changes of membership create secure knowledge sharing extraordinarily troublesome. On one hand, the anonymous system challenges new granted users to be told the content of information files hold on before their participation, as a result of its not possible for brand new granted users to contact with anonymous knowledge homeowners, and acquire the corresponding decoding keys. On the opposite hand, Associate in nursing economical membership revocation mechanism while not change the key keys of the remaining users is additionally desired to reduce the quality of key management. Many security schemes for knowledge sharing on untrusted servers are planned [4], [5], [6]. In these approaches, knowledge homeowners store the encrypted knowledge files in untrusted storage and distribute the corresponding decoding keys solely to approved users. Thus, unauthorized users also as storage servers cannot learn the content of the information files as a result of they need no information of the decoding keys.

However, the complexities of user participation and revocation in these schemes area unit linearly increasing the amount of information house owners and therefore the number of revoked users, severally. By setting a gaggle with one attribute, Lu et al. [7] planned a secure beginning theme supported the cipher text-policy attribute-based secret writing technique [8], that permits any member in a very cluster to share knowledge with others. However, the difficulty of user revocation isn't addressed in their theme. Yu et al. [3] conferred a scalable and fine-grained knowledge access management theme in cloud computing supported the key policy attribute-based encryption (KP-ABE) technique [9].

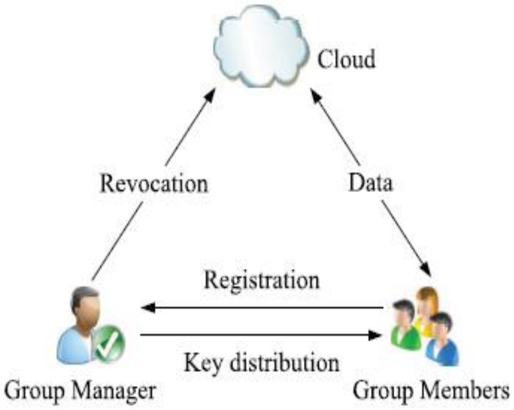
II. PROPOSED SYSTEM

1. we have a tendency to propose a secure multi-owner knowledge sharing theme. It implies that any user within the cluster will firmly share knowledge with others by the untrusted cloud.
2. Our planned theme is in a position to support dynamic teams expeditiously. Specifically, new granted users will directly decipher knowledge files uploaded before their participation while not contacting with knowledge house owners. User revocation is simply achieved through a completely unique revocation list while not change the key keys of the remaining users. The dimensions and computation overhead of cryptography area unit constant and freelance with the quantity of revoked users.
3. We offer secure and privacy-preserving access management to users, that guarantees any member in an exceedingly cluster to anonymously utilize the cloud resource. Moreover, the important identities of information house owners are discovered by the cluster manager once disputes occur.
4. We offer rigorous security analysis, and perform in depth simulations to demonstrate the potency of our theme in terms of storage and computation overhead.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ Any user within the cluster will store and share information files with others by the cloud.
- ✓ The coding complexness and size of cipher texts square measure freelance with the quantity of revoked users within the system.
- ✓ User revocation is achieved while not change the personal keys of the remaining users.
- ✓ A new user will directly decipher the files hold on within the cloud before his participation.

III. SYSTEM ARCHITECTURE



Cloud is operated by CSPs and provides priced teeming storage services. However, the cloud isn't totally trustworthy by users since the CSPs area unit terribly doubtless to be outside of the cloud users' trustworthy domain. Almost like [3], [7], we tend to assume that the cloud server is honest however curious. That is, the cloud server won't maliciously delete or modify user information because of the protection of knowledge auditing schemes [17], [18], however can try and learn the content of the hold on information and therefore the identities of cloud users.

Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the important identity of a dispute information owner. Within the given example, the cluster manager is acted by the administrator of the corporate. Therefore, we tend to assume that the cluster manager is totally trustworthy by the opposite parties.

Group member's area unit a group of registered users that may store their personal information into the cloud server and share them with others within the cluster. In our example, the staffs play the role of cluster members. Note that, the cluster membership is dynamically modified, because of the employee's resignation and new worker participation within the company.

IV. MODULES

1. Registration

2. Login

3. File Upload

4. Chart Creation

5. File Download

6. User deletion

Modules Description

1. Registration:
In this module associate degree User has got to register 1st, then solely he/she has got to access the information base.

2. Login:
During this module, any of the on top of mentioned person need to login, they ought to login by giving their email and arcanum.

3. File Upload:
During this module Manager (Owner) uploads the file(along with meta data) into info, with the assistance of this data and its contents, the tip user has got to transfer the file. The uploaded file was in encrypted kind; solely registered user will decode it. Even CSP will solely read the encrypted file kind.

4. Chart Creation:
User will read the chart that is dynamically created by calculative the dimensions of the file.

5. File Download:
The Registered users will transfer the file and might do updates. The changed files are uploaded into cloud server by the user.

6. User Deletion:
Manager (admin) will reject the user, therefore as that rejected user doesn't login and access the info.

V. ALGORITHMS USED

1. Signature Generation
2. Signature Verification
3. Revocation Verification

Algorithms Description:

1. Signature Generation**:**

```
Input: Private key(A,x), System parameter (P,U,V,H,W)   and data M.
Output: Generate a valid group signature on M.
Begin
    Select random numbers
    Set $\delta 1 = x\alpha$ and $\delta 2 = x\beta$
Computes the following values
    $T1 = \alpha .U$
    $T2 = \beta .V$
    $T3 = A_{i\,+}(\alpha+\beta).H$
    $R1 = \gamma_{\alpha\,.}U$
    $R2 = \gamma_{\beta\,.}V$
    $R3 = e(T_{3,}P)^{\gamma}{}_{x}\,e(H,W)^{-\gamma}{}_{\alpha}{}^{-\gamma}{}_{\beta}\,e(H,P)^{-\gamma\delta}{}_{1}{}^{-\gamma\delta}{}_{2}$
    $R4 = \gamma_{x\,.}T1- \gamma\delta_1.U$
    $R5 = \gamma_{x\,.}T2- \gamma\delta_2.V$
  Set $c = f(M,T_{1,}\ T_{2,}\ T_{3,}\ R_{1,}\ R_{2,}\ R_{3,}\ R_{4,}\ R_5)$
  Construct the following numbers
        $s_{\alpha} = \gamma_{\alpha\,+}\ c\alpha$
        $s_{\beta} = \gamma_{\beta\,+}\ c\beta$
        $s_{x} = \gamma_{x\,+}\ cx$
        $s_{\delta 1} = \gamma_{\delta 1\,+}\ c\delta 1$
        $s_{\delta 2} = \gamma_{\delta 2\,+}\ c\delta 2$
  Return $\sigma = (T_{1,}\ T_{2,}\ T_{3,}c,s_{\alpha,},s_{\beta,},s_{x,}\ s_{\delta 1,}\ s_{\delta 2})$
  end
```

2. Signature Verification:

```
Input : System Parameter (P,U,V,H,W),M and a Signature
$\sigma = (T_{1,}\ T_{2,}\ T_{3,}c,s_{\alpha,},s_{\beta,},s_{x,}\ s_{\delta 1,}\ s_{\delta 2})$
Output : True or False.
Begin
        Compute the following values
          $R_1 = s_{\alpha\,.}\ U - c.T_1$
          $R_2 = s_{\beta\,.}\ V - c.T_2$
          $R_3 = (e(T_3,W)/e(P,P))^c\ e(T_3,P)^{s}{}_{x}\ e(H,W)^{-s}{}_{\alpha}{}^{-s}{}_{\beta}$
          $R_4 = s_x\ .T_1 - s_{\delta 1}\ .U$
          $R_2 = s_x\ .T_2 - s_{\delta 2}\ .V$
        if $c = f(M,T_{1,}\ T_{2,}\ T_{3,}R_{1,}\ R_{2,}\ R_{3,}\ R_{4,}\ R_5)$
          Return True
    Else
          Return False
  End
```

,

3. Revocation Verification:

```
Input: System Parameter ($H_{0,}\ H_{1,}\ H_2$),a group signature $\sigma$,
       And asset of revocation keys $A_{1,\ldots\ldots}A_r$
Output : Valid or Invalid
Begin
     Set temp = $e(T_{1,}\ H_1)\ e(T_{2,}\ H_2)$
     for I = 1 to n
       if $e(T_{3\,-}\ A_{i,}H_0)$ = temp
          Return Valid
         End if
       End for
       Return Invalid
end
```

VII. CONCLUSION

In this paper, we design a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud” , pp.1182 – 1191.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, “A View of Cloud Computing,” Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] 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.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing Remote Untrusted Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] 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 Security Symp. (NDSS), pp. 29-43, 2005.