Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

Arpitha.K [1],Aawini.T [2] ,Divya J. [3] , Kalyani P [4] , Prof. Sudhakar Avareddy [5]
[1,2,3,4] Department of CSE , BITM Bellary, Karnataka.
[5] Department of ISE , BITM Bellary, Karnataka

[1] arpithakalva1@gmail.com ,[2]ashwinitv9@gmail.com , [3]divyachowdary45@gmail.com
[4]polamkalyanireddy@gmail.com

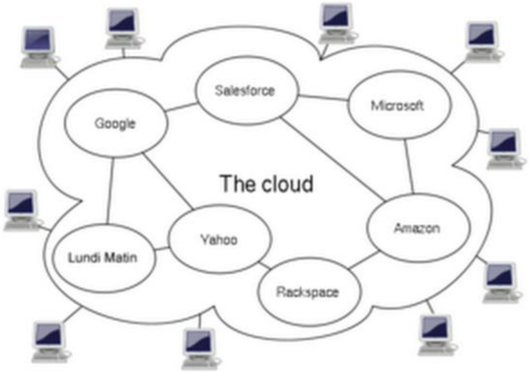
Abstract: Cloud computing provides an economical and efficient solution for sharing data among the cloud users with low maintenance. There is still a challenging issue, due to the frequent change of the membership for sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud. Here, a secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud has been proposed. Any cloud user can anonymously share data with others by providing group signature and dynamic broadcast encryption techniques. Meanwhile, the storage overhead and encryption computation cost of the scheme are independent with the number of revoked users.

Keywords: Mona, Cloud Computing.

1. INTRODUCTION TO CLOUD COMPUTING

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud is used as a metaphor for "the Internet" so the phrase cloud computing means "a type of Internet-based computing," where different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet.

2. General Architecture of cloud computing



The Cloud Architecture shows that there are many number of cloud service providers (like Google, Microsoft, Amazon, Yahoo and so on....)which makes the cloud users to access the required data from different locations.

3. Characteristics of Cloud Computing

i)Application Programming Interface: (API) enables machines to access the software to interact with cloud software in the same way the traditional interface (e.g., computer desktop) do the interaction between human and computers.

ii) Cost: As the infrastructure is provided by a third party the organizations does not need to be purchased for one-time or infrequent intensive computing tasks which claim that computing cost reduce as a result public-cloud delivery model converts capital expenditure to operational expenditure.

iii)Device and location independence: Cloud users can connect from anywhere to the cloud server. It enables the users to access systems using a web browser independent of their location via the internet.

iv)Virtualization: Technology allows sharing of servers and storage devices and increased utilization. Applications can be easily migrated from one physical server to another.

v)Multitenancy: Enables sharing of resources and costs across a many users.

Reliability: Cloud computing improves reliability with the use of multiple redundant sites, which makes it is more suitable for business continuity and disaster recovery.

vi)Maintenance: Cloud computing applications are easier to maintain, because they do not need to be installed on each user's computer and can be accessed from different places.

vii)Broad network access: Cloud servers are available over the network and can be accessed through standard mechanisms (e.g., mobile phones, tablets, laptops, and workstation.

viii)Security: Due to centralization of data. Security is often as good as or better than other traditional systems. However, the complexity of security is greatly increased when data is distributed over wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users.

ix)Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

4.Components of Cloud Computing

a)CLIENT: A client is a computer hardware and software which relies o the cloud for application delivery or which is specifically designed for delivery of cloud services.

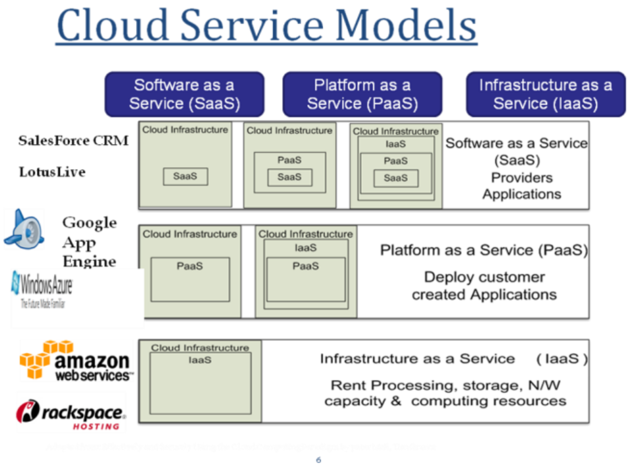
b)SERVICES: A cloud service is a software system design to support interoperable machine to machine inter-action over a network which may be accessed by other cloud computing components software or end users directly.

c)APPICATIONS: A cloud application influences the cloud model of software architecture often eliminating the need to install and run the application on the customers own computer. Thus reduces software maintenance.

d)STORAGE: Cloud storage is the delivery of data storage as a service.

5. Services of Cloud Computing:

- SaaS (Software as a Service)
  Where customers use software that is run on the providers infrastructure.
- Paas(Platform as a Service)
  Where a customer leverages the provider's resources to run custom applications.
- Iaas(Infrastructure as a Service)
  Where a customer makes use of a service provider's computing, storage or networking infrastructure.


Cloud Service Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
SalesForce CRM
LotusLive
Cloud Infrastructure
SaaS
PaaS
IaaS
Software as a Service (SaaS) Providers Applications
Google App Engine
WindowsAzure
Platform as a Service (PaaS)
Deploy customer created Applications
amazon webservices
rackspace HOSTING
Infrastructure as a Service (IaaS)
Rent Processing, storage, N/W capacity & computing resources
6

6. Applications of Cloud Computing

1. Clients would be able to access their applications and data from anywhere at any time they could access the cloud computing system using any computer linked to the Internet.
2. It could bring hardware costs down. Cloud computing systems would reduce the need for advanced hardware on the client side.
3. Cloud computing systems give these organizations company-wide access to computer applications. The companies don't have to buy a set of software or software licenses for every employee. Instead, the company could pay a metered fee to a cloud computing company.

4. Servers and digital storage devices take up space. Some companies rent physical space to store servers and databases because they don't have it available on site. Cloud computing gives these companies the option of storing data on someone else's hardware, removing the need for physical space on the front end. Corporations might save money on IT support.
5. If the cloud computing system's back end is a grid computing system, then the client could take advantage of the entire network's processing power. Often, scientists and researchers work with calculations so complex that it would take years for individual computers to complete them. On a grid computing system, the client could send the calculation to the cloud for processing. The cloud system would tap into the processing power of all available computers on the back end,

significantly speeding up the calculation.

7. Merits and Demerits of cloud Computing

Merits:

i) Lower computer costs:

You do not need a high-powered and high-priced computer to run cloud computing web-based applications. Since applications run in the cloud, not on the desktop PC, your desktop PC does not need the processing power or hard disk space demanded by traditional desktop software. When you are using web-based applications, your PC can be less expensive, with a smaller hard disk, less memory, more efficient processor.

ii) Improved performance:

With few large programs hogging your computer's memory, you will see better performance from your PC. Computers in a cloud computing system boot and run faster because they have fewer programs and processes loaded into memory.

iii) Reduced software costs:

Instead of purchasing expensive software applications, you can get most of soft wares from cloud service providers that you need to run your application for free.

iv) Instant software updates:

Most cloud computing applications today, such as the Google Docs suite better than paying for Instant software updates. When the application is web-based, updates happen automatically available when you log into the cloud without needing to pay for or download an upgrade.

v) Unlimited storage capacity:

Cloud computing offers unlimited virtual storage. Your computer's current 1 Tbyte hard drive is small compared to the hundreds of Pbytes available in the cloud.

vi) Increased data reliability:

Unlike desktop computing, in which if a hard disk crashes and destroy all your valuable data, a computer crashing in the cloud should not affect the storage of your data. if your personal computer crashes, all your data is still out there in the cloud and it is still accessible. So cloud computing is a data-safe computing platform!.

Demerits:

i) Requires a constant Internet connection:

Cloud computing is impossible if you cannot connect to the Internet. Since you use the Internet to connect to both your applications and documents, if you do not have an Internet connection you cannot access anything, sometimes even your own documents.

ii) Does not work well with low-speed connections:

With a low-speed Internet connection, it is unable to connect to the cloud server to access the data since Web-based applications require a lot of bandwidth to download the data.

iii) Features might be limited:

Today many web-based applications are not as full-featured as their desktop-based applications. For example, you can do a lot more with Microsoft PowerPoint than with Google Presentation's web-based offering.

iv) Stored data might not be secure:

Cloud computing, allows the users to store all your data on the cloud. But sometimes the data cannot be confidential since we cannot trust cloud service providers.

v) Stored data can be lost:

The data stored in the cloud is obviously safe, even though the data is replicated across multiple machines. But there is a chance that your data goes missing; you have no physical or local backup.

8. MONA:

To achieve secure data sharing for dynamic groups in the cloud, we combine the group signature and dynamic broadcast encryption techniques. Specifically, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users which protects the confidentiality from the revoked users in the dynamic broadcast encryption scheme.

8.1 Introduction to Mona

Cloud computing [1] is recognized as an alternative to traditional information technology [2] due to its intrinsic resource-sharing and low-maintenance characteristics. 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 datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Specifically, the cloud servers managed by cloud providers are not fully trusted by usersWhile the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [3]. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

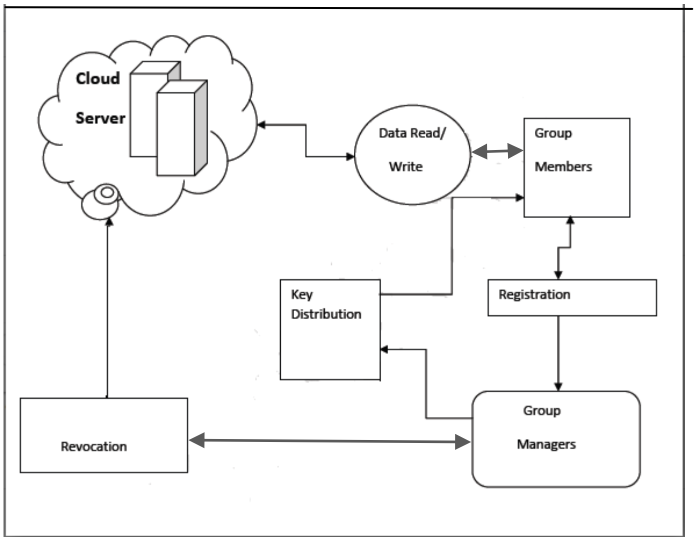
First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner [4], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management. Several security schemes for data sharing on untrusted servers have been proposed[5]. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute [6] based on the cipher text-policy attribute-based encryption technique scheme, which allows any member in a group to share data with others. To solve the challenges presented above, we propose Mona, a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include:

1. We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.

2. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users.

3. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can berevealed by the group manager when disputes occur.

Mona Architecture:



Architecture:

The architecture model consists of three main different entities: The Cloud Server, Group Manager (admin) and a large number of Group Members.

1. Cloud Server: Cloud is operated by cloud service providers and provides priced abundant storage services.

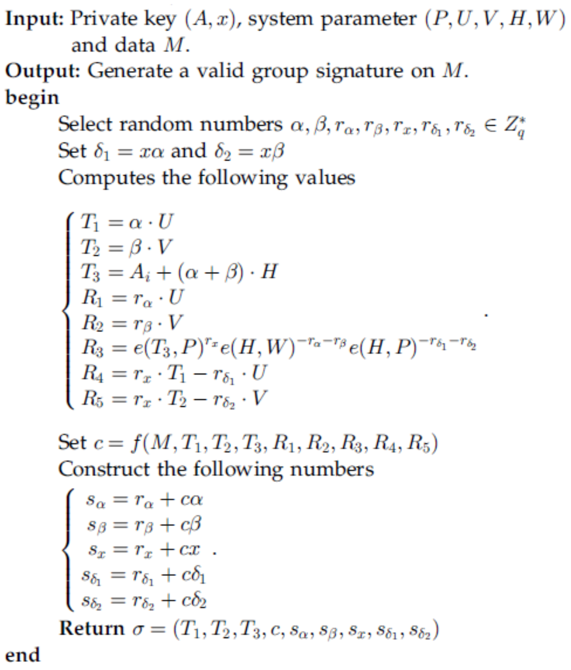
2. Group Manager: Group Manager takes the charge of system parameters like user registration, user revocation, secret key generation.

3. Group Members: Group members are the set of registered users that will store their private data into the cloud server and can download it and share the data with others in the group.

9. Algorithms used

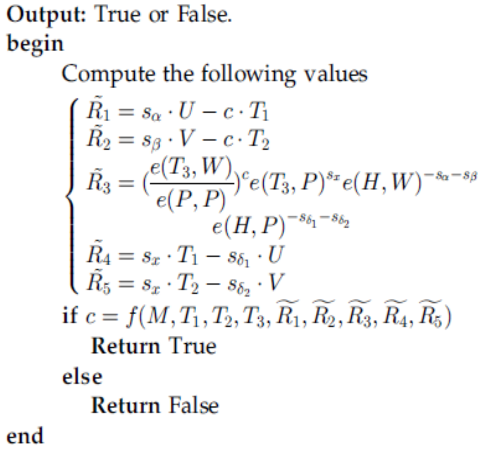
- Signature Generation
- Signature Verification
- Revocation Verification

Signature Generation



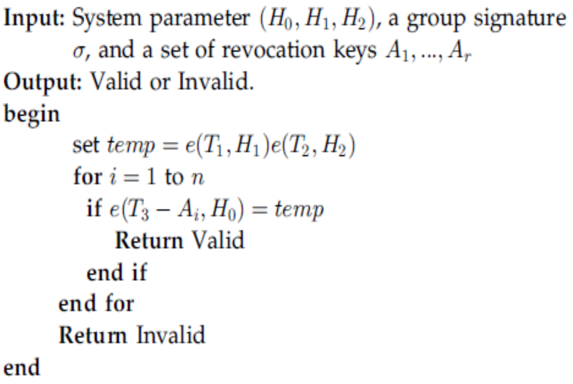
```
Input: Private key $(A, x)$, system parameter $(P, U, V, H, W)$
    and data $M$.
Output: Generate a valid group signature on $M$.
begin
    Select random numbers $\alpha, \beta, r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \in Z_q^*$
    Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$
    Computes the following values
    $\begin{cases} T_1 = \alpha \cdot U \\ T_2 = \beta \cdot V \\ T_3 = A_i + (\alpha + \beta) \cdot H \\ R_1 = r_\alpha \cdot U \\ R_2 = r_\beta \cdot V \\ R_3 = e(T_3, P)^{r_x} e(H, W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}} \\ R_4 = r_x \cdot T_1 - r_{\delta_1} \cdot U \\ R_5 = r_x \cdot T_2 - r_{\delta_2} \cdot V \end{cases}$
    Set $c = f(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$
    Construct the following numbers
    $\begin{cases} s_\alpha = r_\alpha + c\alpha \\ s_\beta = r_\beta + c\beta \\ s_x = r_x + cx \ . \\ s_{\delta_1} = r_{\delta_1} + c\delta_1 \\ s_{\delta_2} = r_{\delta_2} + c\delta_2 \end{cases}$
    Return $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
end
```

Signature Verification:



```
Output: True or False.
begin
    Compute the following values
    $\begin{cases} \tilde{R_1} = s_\alpha \cdot U - c \cdot T_1 \\ \tilde{R_2} = s_\beta \cdot V - c \cdot T_2 \\ \tilde{R_3} = (\frac{e(T_3, W)}{e(P, P)})^c e(T_3, P)^{s_x} e(H, W)^{-s_\alpha - s_\beta} \\ \qquad e(H, P)^{-s_{\delta_1} - s_{\delta_2}} \\ \tilde{R_4} = s_x \cdot T_1 - s_{\delta_1} \cdot U \\ \tilde{R_5} = s_x \cdot T_2 - s_{\delta_2} \cdot V \end{cases}$
    if $c = f(M, T_1, T_2, T_3, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}, \widetilde{R_4}, \widetilde{R_5})$
        Return True
    else
        Return False
end
```

Revocation Verification:



```
Input: System parameter $(H_0, H_1, H_2)$, a group signature
       $\sigma$, and a set of revocation keys $A_1, ..., A_r$
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
```

10. Simulation

To Study the performance we simulate MONA by using C programming language which provides a competitive security level with 1,024-bit RSA. The simulation consists of three components. Client side, Manager side as well as cloud side.

Client Computation Cost: The computation cost in MONA increases with the number of revoked users, as clients require to perform signature generation and signature verification algorithms to compute the parameters and check whether the data owner is a revoked user or not.

Cloud Computation Cost: To evaluate the performance of the cloud in Mona, we test its computation cost to respond various client operation requests including file generation, file access, and file deletion. Assuming the sizes of requested files are 100 and 10 MB. It can be seen that the computation cost of the cloud is deemed acceptable, even when the number of revoked users is large. This is because the cloud only involves group signature and revocation verifications to ensure the validity of the requestor for all operations. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations.

11. CONCLUSION

In this paper, a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud has been designed. In this scheme any user in the group can upload and download the files which enables to share data among dynamic groups(Multi-Owner data sharing) without revealing the real identity of the user and security is also provided while downloading the file by a method called key generation. This scheme also supports the efficient user revocation and new user joining. Any new user can directly decrypt the files stored in the cloud before their participation, Moreover, the storage overhead and the encryption computation cost are efficient which also guarantees efficiency of the scheme.

12. References

1. 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.
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. 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. 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.
6. www.wikipedia.com