ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

Controlled Access Permissions Based on Cloud Server

Priyanga.M [1], Baskar.K [2]

P.G. Student, Department of Computer Engineering, PGP college of Engineering and Technology, Namakkal, India[1]

Assistant Professor, Department of Computer Engineering, PGP College of Engineering and Technology, Namakkal, India[2]

ABSTRACT: Cloud computing is a promising information technology architecture for both enterprises and individuals. It launches an attractive data storage and interactive paradigm with obvious advantages, including on-demand self-services, ubiquitous network access, and location independent resource pooling. Recent studies have been worked to promote the cloud computing evolve towards the internet of services. Subsequently, security and privacy issues are becoming key concerns with the increasing popularity of cloud services. Conventional security approaches mainly focus on the strong authentication to realize that a user can remotely access its own data in on-demand mode. Along with the diversity of the application requirements, users may want to access and share each other's authorized data fields to achieve productive benefits, which brings new security and privacy challenges for the cloud storage. In the cloud storage, a user remotely stores its data via online infrastructures, platforms, or software for cloud services, which are operated in the distributed, parallel, and cooperative modes. During cloud data accessing, the user autonomously interacts with the cloud server without external interferences, and is assigned with the full and independent authority on its own data fields. It is necessary to guarantee that the users' outsourced data cannot be unauthorized accessed by other users, and is of critical importance to ensure the private information during the users' data access challenges. In this paper, we address the aforementioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. The main contributions are Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.Apply cipher text-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

KEYWORDS: Proxy re-encryption, Ubiquitous network operations, Data anonymity.

I. INTRODUCTION

In the cloud storage based supply chain management, there are various interest groups (e.g., supplier, carrier, and retailer) in the system. Each group owns its users which are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. There into, a supplier purposely may want to access a carrier's data fields, but it is not sure whether the carrier will allow its access request. If the carrier refuses its request, the supplier's access desire will be revealed along with nothing obtained towards the desired data fields. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It is unreasonable to thoroughly disclose the supplier's private information without any privacy considerations. It illustrates three revised cases to address above imperceptible privacy issue.

• *Case 1:* The carrier also wants to access the supplier's data fields, and the cloud server should inform each other and transmit the shared access authority to the both users;

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

• *Case 2:* The carrier has no interest on other users' data fields, therefore its authorized data fields should be properly protected, meanwhile the supplier's access request will also be concealed;
Case 3: The carrier may want to access the retailer's data fields, but it is not certain whether the retailer will accept its request or not. The retailer's authorized data fields should not be public if the retailer has no interests in the carrier's data fields, and the carrier's request is also privately hidden.
Towards above three cases, security protection and privacy preservation are both considered without revealing sensitive access desire related information.

II. RELATED CONTENT

In the cloud environments, a reasonable security protocol should achieve the following requirements.

A. Authentication

A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.

B. Data anonymity

Any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.

C. User privacy

Any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.

D. Forward security

Any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages. Researches have been worked to strengthen security protection and privacy preservation in cloud applications, and there are various cryptographic algorithms to address potential security and privacy problems, including security architectures, data possession protocols data public auditing protocols , secure data storage and data sharing protocols, access control mechanisms , privacy preserving protocols and key management. However, most previous researches focus on the authentication to realize that only a legal user can access its authorized data, which ignores the case that different users may want to access and share each other's authorized data fields to achieve productive benefits. When a user challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this work, we aim to address a user's sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation.

III. FUTURE IDEAS

In this paper, we address the aforementioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information.
The main contributions are as follows.

A. Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.

B. Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

C. Apply cipher text-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

IV. EXISTING SYSTEM

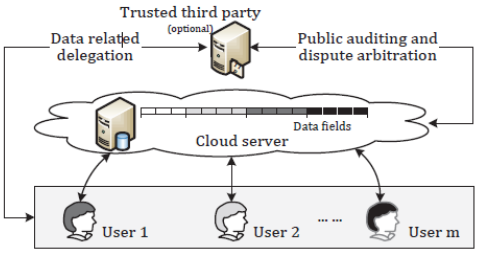

Fig.1. The cloud storage system model.

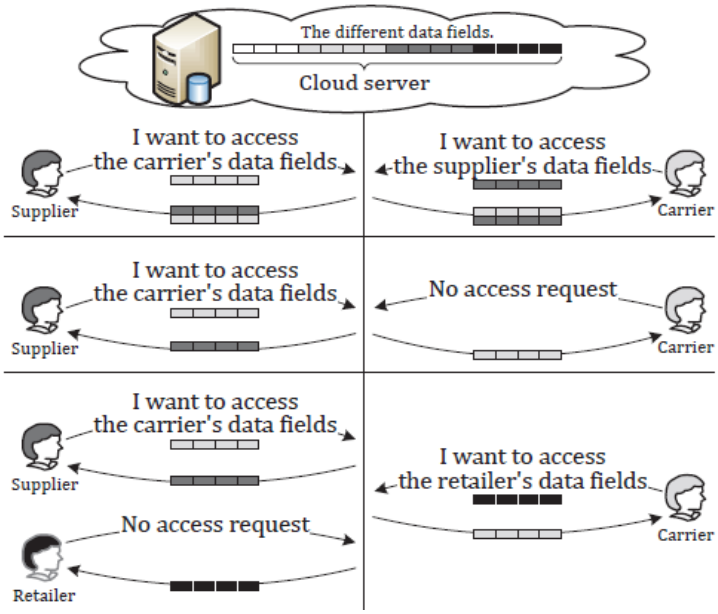

Fig. 1. Three possible cases during data accessing and data sharing in cloud applications

A system model for the cloud storage architecture, which includes three main network entities: users (*Ux*), a cloud server (*S*), and a trusted third party.

User: an individual or group entity, which owns its data stored in the cloud for online data storage and computing. Different users may be affiliated with a common organization, and are assigned with independent authorities on certain data fields.

Cloud server: an entity, which is managed by a particular cloud service provider or cloud application operator to provide data storage and computing services. The cloud server is regarded as an entity with unrestricted storage and computational resources.

Trusted third party: an optional and neutral entity, which has advanced capabilities on behalf of the users, to perform data public auditing and dispute arbitration. In the cloud storage, a user remotely stores its data via online infrastructures, platforms, or software for cloud services, which are operated in the distributed, parallel, and cooperative modes. During cloud data accessing, the user autonomously interacts with the cloud server without external interferences, and is assigned with the full and independent authority on its own data fields. It is necessary to guarantee that the users' outsourced data cannot be unauthorized accessed by other users, and is of critical importance to ensure the private information during the users' data access challenges. In some scenarios, there are multiple users in a system

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

(e.g., supply chain management), and the users could have different affiliation attributes from different interest groups. One of the users may want to access other associate users' data fields to achieve bi-directional data sharing, but it cares about two aspects: whether the aimed user would like to share its data fields, and how cannot expose its access request if the aimed user declines or ignores its challenge. In the paper, we pay more attention on the process of data access control and access authority sharing other than the specific file oriented cloud data transmission and management.

V.PROJECT DESCRIPTION

A. Authentication

A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user. The cipher text-policy attribute based access control and bilinear pairings are introduced for identification between *Uθ* and *S*, and only the legal user can derive the ciphertexts. Additionally, *Uθ* checks the re-computed ciphertexts according to the proxy re-encryption, which realizes flexible data sharing instead of publishing the interactive users' secret keys.

B. Data Anonymity

Any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel the pseudonym *PIDU_* are hidden by the hash function so that other entities cannot derives the real values by inverse operations. Meanwhile, *U~θ*'s temp authorized fields *_D U~_* is encrypted by *k__* for anonymous data transmission. Hence, an adversary cannot recognize the data, even if the adversary intercepts the transmitted data, it will not decode the full-fledged cryptographic algorithms.

C. User Privacy

Any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing The access request pointer (e.g., *RUxU_*) is wrapped along with *H*(*sidS_ ∥PIDU_*) for privately informing *S* about *Uθ*'s access desires. Only if both users are interested in each other's data fields, *S* will establish the re-encryption key *kU_* to realize authority sharing between *Ua*and *Ub*. Otherwise, *S* will temporarily reserve the desired access requests for a certain period of time, and cannot accurately determine which user is actively interested in the other user's data fields.

D. Forward Security

Any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages. The dual session identifiers *{sidS_ ,sidU_ }* and pseudorandom numbers are introduced as session variation operators to ensure the communications dynamic. An adversary regards the prior session as random even if *{S, Uθ}* get corrupted, or the adversary obtains the PRNG algorithm. The current security compromises cannot correlate with the prior interrogations.

E. Attribute based access control

Attribute based access control defines a new access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes(user attributes, resource attributes, environment attribute etc.). Attribute values can be set-valued or atomic-valued. Set-valued attributes contain more than one atomic values. Examples are role, project. Atomic-valued attributes contains only one atomic value. Examples are clearance, sensitivity. Attributes can be compared to static values or to one another thus enabling relation-based access control.

*Ua*first extracts it data attribute access list $AUa = [aij]$ $(aij \in \{0; 1\}, aij \leq pij)$
to re-structure an access list
$LUa = [lij]n \times m$for $lij = pij - aij$. *Ua*
also defines a polynomial

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

FUa(*x*;*LUa*)
according to *LUa*and *TUa*.
FUa(*x*;*LUa*) = *n*Π,*mi*=1,*j*=1 (*x* + *ijH*(*TUa*))*lij*(mod *q*).
It turns out that *FUa*(*x*;*LUa*) satisfies the equation.
FUa(*x*;*LUa*) = *n*Π,*mi*=1,*j*=1 (*x* + *ijH*(*TUa*))*pij*−*aij*=*FSa*(*x*; *PUa*)=*FSa*(*x*;*AUa*):
Afterwards, *Ua*randomly chooses _ ∈*Zq*, and the decryption key *kAUa*for *AUa*can be obtained.
kAUa= (*g*(*β*+1)/*FSa*(*α*,*AUa*); *hβ*−1)
*Ua*further computes a set of values {*NUa*1, *NUa*2, *NUa*3}. Here, *fSai*is used to represent *xi*'s coefficient in *FSa*(*x*; *PUa*), and *fUai*is used to represent *xi*'s coefficient in *FUa*(*x*;*LUa*).
*NUa*1 = *e*(*MSa*21; Π*ni*=1 (*hi*)*fUaihfUa*0); *NUa*2 = *e*(Π*ni*=1 (*MSa*2*i*)*fUai* ; *hβ*−1);
*NUa*3 = *e*(*g*(*β*+1)/*FSa*(*α*,*AUa*);*MSa*1):
It turns out that *e*(*g*; *h*)*MSa*0 satisfies the equation.
*NUa*1 =*e*(*gαiMSa*0 ; Π*ni*=1 (*hi*)*fUaihfUa*0) =*e*(*g*; *h*)*αMSa*0 Σ*ni*=1(*αi*−1*fUai*+*fUa*0) =*e*(*g*; *h*)*MSa*0*FUa* (*α*,*LUa*);
*NUa*2 =*e*(Π*ni*=1 *gαiMSa*0*fUai* ; *hβ*−1) =*e*(*g*; *h*)*MSa*0(Σ*ni*=1 *αifUai*+*fUa*0−*fUa*0)(*β*−1) =*e*(*g*; *h*)*MSa*0*βFUa*(*α*,*LUa*)−*MSa*0*fUa*0 ;
*NUa*3 =*e*(*g*(*β*+1)/*FSa*(*α*,*AUa*); *hfSa*0*MSa*0 Π*ni*=1
(*hi*)*fSaiMSa*0) =*e*(*g*; *h*)(*β*+1)/*FSa*(*α*,*AUa*)*FSa*(*α*,*PUa*)*MSa*0 = *e*(*g*; *h*)*MSa*0*βFUa*(*α*,*LUa*)+*MSa*0*FUa* (*α*,*LUa*);
(*NUa*1*NUa*2=*NUa*3) −1/*fUa*0 =(*e*(*g*; *h*) −*MSa*0*fUa*0) −1/*fUa*0 =*e*(*g*; *h*)*MSa*0 :
Ua locally re-computes {*_ℓ*, *Mℓ Sa*0 }, derives its own authorized data fields *DUa*, and checks whether the ciphertext *CSa*is encrypted by *Mℓ Sa*0. If it holds, *Ua*will be a legal user that can properly decrypt the ciphertext *CSa*; otherwise, the protocol will terminate.
_ℓ = *MSa*3 ⊕*H*(*e*(*g*; *h*)*MSa*0);
*Mℓ Sa*0 = *H*(*PUa*∥*TUa*∥*_ℓ*);
DUa= *MSa*4 ⊕*H*(*sidUa*∥*_ℓ*):
Ua further extracts its pseudonym *PIDUa*, a session sensitive access request *RUb*
Ua, and the public key *pkUa*. Here, *Rub Ua*is introduced to let *S*know its data access
desire. It turns out that *Rub Ua*makes *S* know the facts: 1) *Ua*wants to access *Ub*'s temp authorized data fields *_D Ub*; 2) *Ra* will also agree to share its temp authorized data fields *_D Ua*with *Ub*in the case that *Ub*grants its request. Afterwards, *Ua*randomly chooses *rUa*
∈*Z*∗*q* , computes a set of values {*MUa*0, *MUa*1, *MUa*2, *MUa*3} to establish a ciphertext *CUa*, and transmits *CUa*to *S* for further access request matching.
*MUa*0 = *H*(*sidSa*∥*PIDUa*) ⊕*Rub Ua* ;
*MUa*1 = *gpkUarUa* ;
*MUa*2 = *e*(*g*; *h*)*rUa* ;
*MUa*3 = *hrUa* :
Similarly, *Ub*performs the corresponding operations, including that *Ub*extracts *AUb*, and determines {*LUb*, *FUb*(*x*;*LUb*), *fUbi*}. *Ub*further randomly chooses *_′* ∈*Zq*, and computes the values {*NUb*1, *NUb*2, *NUb*3, *_′ℓ*, *Mℓ Ub*}to derive its own data fields *DUb*. *Ub*also extracts its pseudonym *PIDUb*and an access request *RUaUb*to establish a ciphertext *CUb*with the elements {*MUb*0;*MUb*1;*MUb*2;*MUb*3}.

F. Proxy Re-Encryption

In the SAPA, *S* acts as a semi-trusted proxy to realize {*Ua*, *Ub*}'s access authority sharing. During the proxy re-encryption, {*Ua*, *Ub*} respectively establish ciphertexts {*MUa*1, *MUb*1} by their public keys {*pkUa*,*pkUb*}, and *S* generates the corresponding re-encryption keys {*kUa*, *kUb*} for {*Ua*, *Ub*}. Based on the re-encryption keys, the ciphertexts {*MUa*1, *MUb*1} are re-encrypted into {*M′ Ua*1, *M′ Ub*1 }, and {*Ua*, *Ub*} can decrypt the re-structured ciphertexts {*M′ Ub*1, *M′ Ua*1 } by their own private key {*skUa*, *skUb*} without revealing any sensitive information. Till now, {*Ua*, *Ub*} have realized the access authority sharing in the case that both *Ua*and *Ub*have the access desires on each other's data fields. Meanwhile, there may be other typical cases when *Ua*has an interest in *Ub*'s data fields with a challenged access request *Rub Ua*. 1) In the case that *Ub*has no interest in *Ua*'s data fields, it turns out that *Ub*'s access request *Rub Ub*and *Rub Ua*satisfy that *F*(*Rub Ua*(*Rub Ub*)*T*) = *F*(1). For *Ua*, *S* will extract a dummy data fields

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

*Dnull*as a response. *Ub*will be informed that a certain user is interested in its data fields, but cannot determine *Ua*'sdetailed identity for privacy considerations. 2) In the case that *Ub*has an interest in *Uc*'s data fields rather than *Ua*'s data fields, but *Uc*has no interest in *Ub*'s data fields. It turns out that the challenged access requests *Rub Ua*,*RUcUb*, and *R U~bUc*satisfy that *F*(*Rub Ua*(*RUcUb*
)*T*) = *F*(*RUcUb*(*R U~bUc*)*T*) = *F*(1), in which *U~b*indicates that the user is not *Ub*. *Dnull*will be transmitted to *{Ua, Ub, Uc}* without data sharing.

VI.CONCLUSION

In this paper, we propose a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security); 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol realizing computing to achieve privacy-preserving access authority sharing. Authentication is established privacy-preserving data access authority sharing is attractive for multi-user collaborative cloud applications.In this work, we have identified a new privacy challenge during data accessing in the cloud to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2009.
[2] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE Internet Computing*, vol. 14, no. 5, pp. 14-22, 2010.
[3] C. Wang, K. Ren, W. Lou, J, Lou,"Toward Publicly Auditable Secure Cloud Data Storage Services," *IEEE Network*, vol. 24, no. 4, pp. 19-24, 2010.
[4 S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 3, pp. 1424-1432, 2011.
[5 A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," *IEEE Communications Magazine*, vol. 50, no. 9, pp, 24-25, 2012.
[6 J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," *Computer*, vol. 45, no. 7, pp. 73-78, 2012.
[7 Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no, 12, pp. 2231-2244, 2012.
[8 H. Wang, "Proxy Provable Data Possession in Public Clouds," *IEEE Transactions on Services Computing*, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.
[9 X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.
[10 C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220-232, 2012.
[11 S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 556-568, 2012.
[12 L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 402-413, 2013.