Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.136 – 143

MULTI-ACCESS OF PREVILEGED DATA IN CLOUD BY AUTHENTICATION PROTOCOL

Cherukuri Anusha[1], Challari Bindu Bhargavi[2], Iruku Venkata Sai Sirisha[3], Kusumanchi Bhargavi[4]
[1]Asst. Professor, CSE, INTERNATIONAL SCHOOL OF TECHNOLOGY AND SCIENCES (FOR WOMEN), EAST GONAGUDEM, RAJANAGARM Rajahmundry, A.P, India
[2]Student B.Tech CSE, INTERNATIONAL SCHOOL OF TECHNOLOGY AND SCIENCES (FOR WOMEN), EAST GONAGUDEM, RAJANAGARM Rajahmundry, A.P, India
[3]Student B.Tech CSE, INTERNATIONAL SCHOOL OF TECHNOLOGY AND SCIENCES (FOR WOMEN), EAST GONAGUDEM, RAJANAGARM Rajahmundry, A.P, India
[4]Student B.Tech CSE, INTERNATIONAL SCHOOL OF TECHNOLOGY AND SCIENCES (FOR WOMEN), EAST GONAGUDEM, RAJANAGARM Rajahmundry, A.P, India
[1] Cherukuri.anusha22@gmail.com; [2] Bindubhargavi25.ch@gmail.com;
[3] Sai.sirisha.519@gmail.com; [4] Bhargavi.kusumanchi95@gmail.com

Abstract- ***Cloud is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand cloud server. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. privacy issue during a user access challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, we propose a multi-access privileged data authentication protocol (MAPDAP) to address above privacy issue for cloud storage. In the MAPDAP, 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. It indicates that the proposed protocol realizing privacy preserving data access authority sharing, is attractive for multi-user collaborative cloud applications.***

Index Terms— Cloud, authentication protocol, privileged, shared authority

---*---

1. INTRODUCTION

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[1]. Recent studies have been worked to promote the cloud computing evolve towards the internet of services [2], [3]. 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 remote user can 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 this 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. In cloud environment security protocol follow some requirements1) 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. 2) Data anonymity: any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel. 3) 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. 4) Forward security: any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

Researchers 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 [4], [5], data possession protocols [6], [7], data public auditing protocols [8]–[10].

In this paper, we address the privacy issue to propose a multi access privileged data authentication protocol (MAPDAP) to address above privacy issue for cloud storage. In the MAPDAP for cloud data storage, which realizes authentication and authorization without compromising a user's private information. The main contributions are follows. 1) Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing,

2) 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.

3) 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.

The remainder of the paper is organized as follows. Section 2 introduces related works. Section 3 introduces the system model, and Section 4 presents the proposed authentication protocol. Section 5 mention conclusion.

2. RELATED WORK

Dunning *et al.* [11] proposed an anonymous ID assignment based data sharing algorithm (AIDA) for multiparty oriented cloud and distributed computing systems. In the AIDA, an integer data sharing algorithm is designed on top of secure sum data mining operation, and adopts a variable and unbounded number of iterations for anonymous assignment. Specifically, Newton's identities and Sturm's theorem are used for the data mining, a distributed solution of certain polynomials over finite fields enhances the algorithm scalability, and Markov chain representations are used to determine statistics on the required number of iterations.

Liu *et al.* [12] proposed a multi-owner data sharing secure scheme (Mona) for dynamic groups in the cloud [3] applications. The Mona aims to realize that a user can securely share its data with other users via the un trusted cloud server, and can efficiently support dynamic group interaction.

Grzonkowsk*et al.* [13] proposed a zero-knowledge proof (ZKP) based authentication scheme for sharing cloud services. Based on the social home networks, a user centric approach is applied to enable the sharing of personalized content and sophisticated network-based services via TCP/IP infrastructures, in which a trusted third party is introduced for decentralized interactions, the cloud resources, and the data owners' real identities can only be revealed by the group manager for dispute arbitration. It indicates the storage overhead and encryption computation cost are independent with the amount of the users.

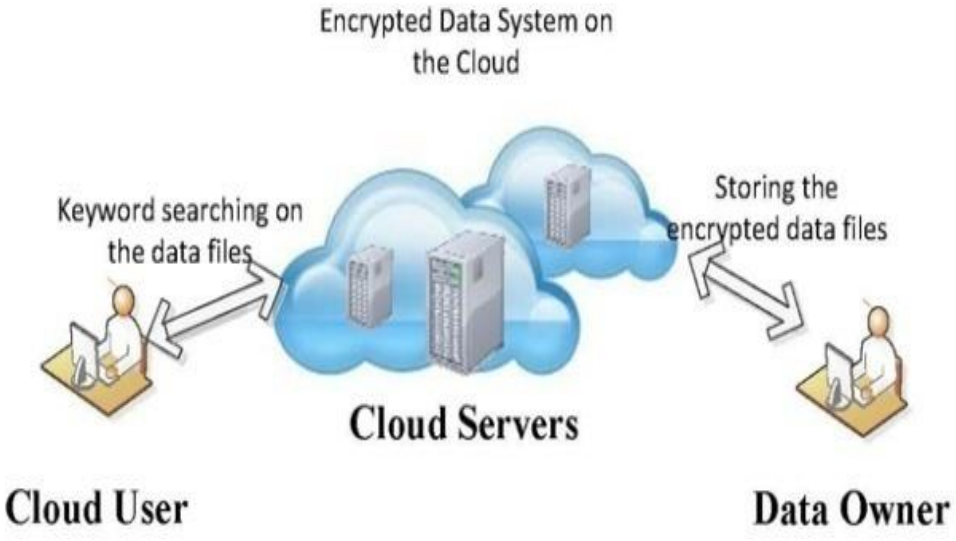

Fig 1 : The Cloud Storage System Model

The above mentioned works, various security issues are addressed. However, a user's subtle access request related privacy problem caused by data accessing and data sharing has not been studied yet in the literature. Here, we identify a new privacy challenge, and propose a protocol not only focusing on authentication to realize the valid data accessing, but also considering authorization to provide the privileged access authority sharing.

3. SYSTEM MODEL

Fig. 1 illustrates 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, flat forms, 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 (e.g., supply chain management), and the users could have different affiliation attributes from different interest groups.

4. MULTI-ACCESS PRIVILEGED DATA AUTHENTICATION PROTOCOL

The cloud storage system includes a cloud server *S*, and users *{Ux}* ($x = \{1; :::;m\}$, $m \in$ N). The corresponding *Ua* and *Ub* are two users, which have independent access authorities on their own data fields. It means that a user has an access permission for particular data fields stored by *S*, and the user cannot exceed its authority access to obtain other users' data fields. Here, we consider *S* and *{Ua, Ub}* to present the protocol phases for data access control and access authority sharing with enhanced privacy considerations. The main notations are introduced.

TABLE 1
Notations

Notation	Description
S, *Ux*	The cloud server, and a user (i.e., cloud data owner).
PIDUx *Ux*'s	pseudorandom identifier(pseudonym).
TUx TUy's	identity token that is assigned by S.
sidSx, *sidUx*	The pseudorandom session identifier of *S*, *Ux*.

I,J,K,rUx	The randomly generated numbers R *Uy*, *Ux*
RUy *RUx*	The access request pointer that represents *Ux*'s access desire on *Uy*'s data fields.
DUx, *_DUx* *Ux*'s	own authorized data fields, and *Ux*'s temp authorized data fields.
AUx , *LUx* , *PUx*	The data attribute access list, re-structure data access list, and data access policy.
fmpk=mskg	The pair wise master public/ privacy keys.
fpk=skg	The pairwise public/privacy keys.
*k*U*x* , *kUx*	The aggregated keys, and the re-encryption keys.
Vℓ	The locally computed value *V* according to the same algorithm.
CSx , *CUx*	The ciphertexts.
FSx (*x; PUx*)	The defined polynomial owned by S.
FUx (*x;LUx*)	The defined polynomial owned by *Ux*.

{Ua, Ub} respectively generate the session identifiers *{sidUa , sidUb }*, extract the identity tokens *{*T_{Ua} , T_{Ub}*}*, and transmits *{*sid_{Ua}|| T_{Ua} , sid_{Ub}// T_{Ub} *}* to *S* as an access query to initiate a new session. Accordingly, we take the interactions of *Ua* and *S* as an example to introduce the following authentication phase. Upon receiving *Ua*'s challenge, *S* first generates a session identifier *sidSa* , and establishes the master public key *mpk* = (*gi, h, hi*,BG, *e*(*g, h*),*H*) and master privacy key *msk* = (I*; g*). *S* randomly chooses $I \in Zq$, and computes $gi = g\alpha i$ and $h^i = h^{\alpha i-1}$ ($i = \{1....n\} \in Z^*$). *S* randomly chooses v$\in \{0, 1\}^*$, and extracts *Ua*'s access authority policy P_{Ua} = [*pij*]$n\times m$ (*pij* $\in \{0,1\}$), and *Ua* are assigned with the access authority on its own data fields *DUa* within *PUa* 's permission. *S* further defines a polynomial *FSa* (*x*, P_{Ua}) according to P_{Ua} and L_{Ua} .

```
function FSa (x,P_Ua )
{
        for( i= 1,i< n, i++)
{
        for(j=1,j<m, j++)
        x=(x + i*j*H(L_Ua )) **pij
}}}
```


4.1 {Ua, Ub}'s DATA ACCESS CONTROL

U_a first extracts it data attribute access list $A_{Ua} = [a_{ij}]$ ($a_{ij} \in \{0; 1\}$, $a_{ij} \leq p_{ij}$) to restructure an access list $L_{Ua} = [l_{ij}]_{n \times m}$ for $l_{ij} = p_{ij} - a_{ij}$. U_a also defines a polynomial $F_{Ua}(x, L_{Ua})$ according to L_{Ua} and T_{Ua}

```
function FSa (x,P_Ua )
{
        for( i= 1,i< n, i++)
{
        for(j=1,j<m, m++)
        x=(x + i*j*H(L_Ua )) **pij
}}}
```

4.2. {Ua, Ub}'s ACCESS REQUEST MATCHING AND DATA ACCESS AUTHORITY SHARING

When receiving the ciphertexts $\{C_{Ua}, C_{Ub}\}$ within an allowable time interval, and *S* extracts $\{PID_{Ua}, PID_{Ub}\}$ to derive the access requests $\{RU_{ba}, RU_{ab}\}$.

$RU_{ba} = H(sidSa \,||\, PID_{Ua}) + MUa0$
$RU_{ab} = H(sidSa \,||\, PID_{Ub}) + MUb0$

S checks the above mentioned requests with memory request functions MUa0, MUb0 of both Ua and Ub *d*esires to access each other's authorized data, and to share its authorized data fields each other. *S* extracts the keys values and re-encrypted the memory functions MU'a0 ,MU'b0 give the chance to read the data in cloud systems.

5. CONCLUSION

Data accessing has become a challenging issue in cloud storage systems. Some techniques have been proposed to achieve the secure data access control in a multi authority cloud storage system. MAPDAP must be designed with sufficient resistance. MAPDAP issues are mainly related to the security policies provided to the users accessing the uploaded data, and the technique must specify their own defined security In this work, we have finds a new privacy challenge during data accessing in the cloud computing to achieve privileged access authority sharing. Authentication is established to guarantee data confidentiality and data integrity.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2009.
[2] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," *IEEE Communications Magazine*, vol. 50, no. 9, pp, 24-25, 2012.
[3] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services," *IEEE Internet Computing*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, 2012.

[4] 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.
[5] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," *Computer*, vol. 45, no. 7, pp. 73-78, 2012.
[6] 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.
[7] 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.
[8] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, 2012.
[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847-859, 2011.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," *IEEE Transactions on Knowledge and Data Engineering*, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.
[15] 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.
[16] 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.

AUTHORS

Cherukuri Anusha is currently working as Assistant Professor in ISTS Engineering college in Computer Science department. She focuses on security and privacy issues in Cloud computing environment. Her research interests include authentication protocol design, and security formal modeling and analysis.

Challari Bindu Bhargavi is currently studying Btech(CSE) third year in ISTS Engineering college. Her research interests are cloud computing and Networking.

Iruku Venkata Sai Sirisha is currently studying Btech(CSE) third year in ISTS Engineering college. Her research interests are cloud computing and Networking.

Kusumanchi Bhargavi is currently studying Btech(CSE) third year in ISTS Engineering college. Her research interests are cloud computing and Mobile technologies.

