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

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1069 – 1074

RESEARCH ARTICLE

Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control

S Divya Bharathy
Department of Computer Science Engineering
RMK Engineering College
Chennai
divya101091@gmail.com

T Ramesh
Department of Computer Science Engineering
RMK Engineering College
Chennai
trh.cse@rmkec.ac.in

Abstract—we propose a privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme supports secure and efficient dynamic operation on data blocks, including: data update, creation, modification and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. We also provide options for file recovery. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against replay attacks. User revocation and access control policies highly contributes to avoid abuse of cloud services and shared technology issues.

Keywords—Access Control, Authentication, Cloud storage, access policy, attributes

I. INTRODUCTION

Cloud Computing is the emerging technology where we can get platform as a service, software as a service and infrastructure as a service. When it comes to storage as a service, data privacy and data utilization are the primary issues to be dealt with. To handle the transaction of files to and from the cloud server, the files are encrypted before being outsourced to the commercial public cloud.

The topic of cloud computing is gaining a lot of attention from both academic and industrial worlds. The main idea is to make applications available on flexible execution environments primarily located in the internet. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).

Recent researches pointed out the top most nine issues in cloud which threatens the security. From security point of view the following are the threatening issues in cloud.

1. Data Breaches

In which the sensitive data falls into the hands of their competitors.

2. Data Loss

Data loss due to accidental deletion by the cloud service provider, or worse, a physical catastrophe such as fire or earthquake, could lead to the permanent loss consumers' data unless the provider takes adequate measures to backup data.

3. Account Hijacking

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites.

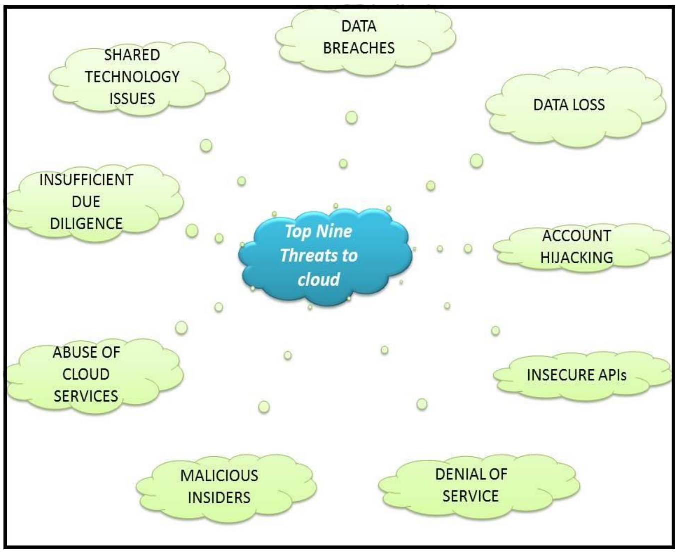

Fig 1 Top Security threats to cloud

4. Insecure APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs.

5. Denial of Service

Simply put, denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker (or attackers, as is the case in distributed denial-of-service (DDoS) attacks) causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding.

6. Malicious Insiders

The risk of malicious insiders has been debated in the security industry. While the level of threat is left to debate, the fact that the insider threat is a real adversary is not.

7.Abuse of Cloud Services

One of cloud computing's greatest benefits is that it allows even small organizations access to vast amounts of computing power. However, not everyone wants to use this power for good. It might take an attacker years to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes.

8.Insufficient Due Diligence

Cloud computing has brought with it a gold rush of sorts, with many organizations rushing into the promise of cost reductions, operational efficiencies and improved security. While these can be realistic goals for organizations that have the resources to adopt cloud technologies properly, too many enterprises jump into the cloud without understanding the full scope of the undertaking. Without a complete understanding of the CSP environment, applications or services being pushed to the cloud, and operational responsibilities such as incident response, encryption, and security monitoring, organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks.

9.Shared Technology Issues

Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms, and applications. Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models. A defensive in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud.

The storage holds pertinent data and information on function on how they will be implemented. Optimization on storage is based on how the storage facility protected from different attacks and availability of back-up. Cloud computing is always about consistency and availability of service which will naturally require the storage to be available all the time. Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement.

Cloud servers are prone to Byzantine failure, where a storage server can fail in arbitrary ways. The cloud is also prone to data modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it can modify data files as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption.

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking).Access control is also gaining importance in online social networking where users (members) store their personal information, pictures, videos and share them with selected groups of users or communities they belong to. It is not just enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed. However, the user should be able to prove to the other users that he/she is a valid user who stored the information without revealing the identity.

Existing work on access control in cloud are centralized in nature. Even if some decentralized approaches were proposed does not support authentication. Earlier work provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where single key distribution center (KDC) distributes secret keys and attributes to all users.

II. ARCHITECTURES

A. EXISTING ARCHITECTURE

The pictorial overview of the existing architecture is depicted in Fig. 1.Existing access control architecture in cloud are centralized in nature. Centralization lacks reliability. For example in this project if we use single centralized KDC, if that fails then the whole system will shut down. If The scheme uses a symmetric key approach and does not support authentication. Earlier work provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of large number of users that are supported in a cloud environment. We, therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attribute to users. It is also quite natural for clouds to have may KDCs in different locations in the world.

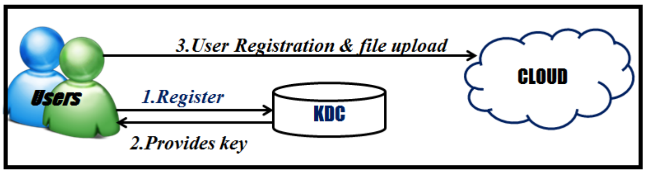

Fig. 1 Single KDC architecture

B. PROPOSED ARCHITECTURE

The Single KDC architecture with no anonymous authentication makes it more complicated and it also increases the storage overhead at the single KDC.

The pictorial overview of the decentralized KDC is depicted in Fig. 2.The proposed decentralized architecture, also authenticate users, who want to remain anonymous while accessing the cloud. We proposed a distributed access control mechanism in clouds. In the preliminary version of this paper, we extend the previous work with added features which enables to authenticate the validity of the message without revealing the identity of user who has stored information in the cloud.

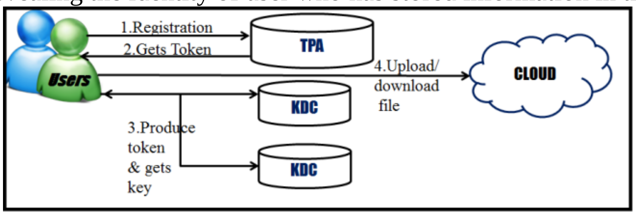

Fig. 2 Decentralized KDC architecture

In this paper, we also address user revocation. We use attribute based signature scheme to achieve authenticity and privacy. Our scheme is resistant to replay attacks, in which user can replace fresh data with stale data from previous write, even if it no longer has valid claim policy. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud. The proposed architecture consists of the following modules. The decentralized Key Distribution Centre architecture here considers two KDCs.

The pictorial representation of the overall flow of the proposed architecture is depicted in Fig. 2a. The user who is the file owner has a collection of files stores the files in cloud server in the form of encrypted files and with indexing. The cloud authenticates the user even without knowing the original identity of the user; rather two step authentications takes place with the help of the Trusted Party Authenticator (TPA) and Key Distribution Centre (KDC).

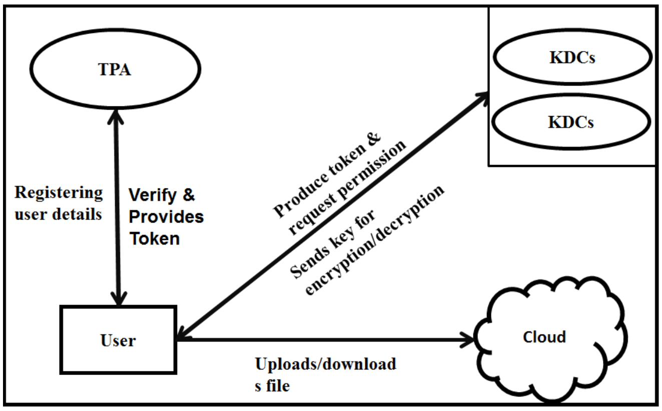

Fig. 2a. Overall architecture flow diagram

1) Service Request to TPA: The user registers with the original identity and enrolls with the Third Party Authenticator(TPA).The user sends request to the Third Party Authenticator(TPA) for registration.

2) TPA Policy Creation: The TPA along with token provides the rules and regulation to be followed by Creator, Reader and Writer.

3) User File Upload: The file creator after getting proper authentication encrypts the file and uploads his files in the cloud.

4) KDC Key Generation: The Key Distribution Centers which are decentralized generate different keys to different types of users after getting tokens from users.

5) Key Revocation: Whenever there is misbehavior detected upon a user his key is revoked and that particular user can neither use or re-enter the cloud environment.

6) Cloud Admin: Cloud admin has the list of Key Distribution Centres(KDCs) and Third Party Authenticator(TPA). The cloud admin sets the norms to be followed by TPA and KDC. It monitors the key generation policies and informs abnormal behaviours.

C. COMPARISON OF OUR SCHEME WITH EXISTING ACCESS CONTROL SCHEMES

Schemes	Centralized/ Decentralized	Privacy preserving authentication	User Revocation	Attribute hiding	File Recovery
Secure and efficient access to outsourced data	Centralized	No authentication	No	No	No
Effective Data Access Control for Multi-authority attribute-based encryption	Decentralized	Not privacy preserving	Yes	No	No
Realizing fine grained and flexible access control to outsourced data with attribute based cryptosystems	Centralized	Not privacy preserving	No	No	No
BASE PAPER SCHEME	Decentralized	Anonymous authentication	NO	YES	NO
PROPOSED SCHEME	Decentralized	Anonymous authentication	YES	YES	YES

Fig. 3 Comparison with other access control schemes

III. PERFORMANCE ANALYSIS

A. Time based Performance

The performance of this paper was analysed under various sizes of files. First the time performance is been analysed. Then the encryption/decryption operation time is been analysed. It takes random time duration for CRUD (Create,Read,Upload,Download) operations for any size of file.

File Size	Upload Speed(Sec)	Download Speed(Sec)
10 bytes	16	0
1 kb	18	2
10 kb	20	3
100 kb	23	7
1 mb	24	7
10 mb	27	9

Table1: Time performance for transaction on cloud

IV. CONCLUSIONS AND FUTUTRE WORK

We have presented a privacy preserving access control technique which is decentralized. The cloud authenticates the user by verifying the credential's even without knowing the original identity of the user. We also address user revocation and our scheme prevents replay attacks. Key distribution is done in a decentralized way. The individual user's access policy is been concealed and known only to each particular user. This project can overcome the top threats in clouds which are identified recently. The threats that can be overcome are data loss, insecure APIs, Denial of Service, abuse of cloud services, shared technology issues. The proposed work also addresses file recovery options.

Multi-party based access control scheme can be implemented in future. So that we can reduce the number of user revocation.

References

[1] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds,"*IEEE Transactions on Parallel and Distributed Systems*, pp. 1045-9219, 2013.
[2] S. Ruj, M. Stojmenovic and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds”, *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 556–563, 2012.
[3] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing”, *IEEE T. Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.
[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy keyword search over encrypted data in cloud computing,” in *IEEE INFOCOM.* , pp. 441–445, 2010.
[5] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in *Financial Cryptography Workshops*, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.
[6] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-based authentication for cloud computing,” in *CloudCom*, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.
[7] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.
[8] A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-based cloud computing,” in *TRUST*, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010.
[9] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, “Trustcloud: A framework for accountability and trust in cloud computing,” HP Technical Report HPL-2011-38. Available at http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.
[10] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” in *ACM ASIACCS*, pp. 282–292, 2010.
[11] D. F. Ferraiolo and D. R. Kuhn, “Role-based access controls,” in *15th National Computer Security Conference*, 1992.
[12] A B Lewko and B Waters, “Decentralizing attribute based encryption”, springer 2011.

