ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

A Review on Privacy Preserving Data Access Control Mechanism in Hybrid Clouds

D. Vishwaksen Reddy

Final year Btech in CSE dept, KMIT, Narayanaguda , Hyderabad, India

ABSTRACT: Cloud computing is the widely used approach of computing utility, whereas users can store their data remotely and don't have any possession of their data. Once users have uploaded their data on the cloud they are not ware about their location and not responsible for maintenance of data. By outsourcing physically large and sensitive data on the outside location increases the threat of privacy and integrity of data. We should focus not only on enhancing the cloud but also on building tools, technologies and processes that will make it easier for developers and architects to plug in applications to the cloud securely and easily. Cloud computing is a very challenging and potentially formidable task. In this paper, new adaptive scheme is proposed for privacy preservation of data on cloud. Extensive security and performance analysis shows that proposed schemes are provable and highly efficient.

KEYWORDS: Cloud computing, Access control, Privacy, Integrity.

I. INTRODUCTION

Cloud Computing has been envisioned as the next generation information technology architecture for enterprises. It has a number of advantages like : On demand self-service, ubiquitous network access, location independent resource pooling, rapid resources elasticity. Cloud computing has changed the way of business and usage of information technology. Cloud computing can be deployed into three different models: 1) Public model 2) Private model 3) Hybrid model Private model:- It deals with managing , buying and organizing your own infrastructure. Hosting is done for specific types of clients , infrastructure required for hosting could be on – premises or third part y location. Security concerns are addressed through Virtual private network s or firewall. On premises approach is the better one for deploying private cloud .private models is the most secured and reliable model with limited access and network Public model: True cloud implementation is public cloud, where services and infrastructure are accessible to variety of clients. Services can be provided to different users either free of cost or pay per bases. Google is a example of cloud computing. Best model for today's business. Instead of spending a lot on the capital, resources, man power and software we can purchase all of the service on rent ad can pay according to their usability. Hybrid d Model:-

This model provides the advantages of both private and public cloud. This model is used for handling cloud bursting , which refers to a scenario where existing private cloud infrastructure is not able to handle load spikes and requires a fallback option to support the load. So cloud migrates the load between public and private hosting without any inconvenience to users.

II. PRIVACY PRESERVATION

In real time environment. Thousand of clientcan are accessing the data at thesame time. So cloud service provider should provide astrong user verification mechanism , which is highly secured and reduces the computational overhead of cryptographic computation In the cncern of, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, but still having a large range of possibility of internal and external attacks that threaten the integrity of data.[3]-[7].it's also the possibility that CSP behaves unfaithfully towards the client repository

DOI: 10.15680/IJIRCCE.2017. 0508050

which is outsourced .some unwanted data and rarely used data can be removed or leaked to external entities for financial benefits[8]-[10] in short we can predict that the outsourced data on the cloud is not offereing any guarnteeon

data integrity and availability , and if the problem is not addressed , may impede the deployment of cloud architecture Simply downloading of data everytime and checking the integrity of the data by applying integrity algorithm and then again saving the data on the cloud is very time consuming p and not feasible and practical approach. Overhead of using cloud services could be minimized. For easier management, cloud Server must inly be responsible for verification of the request from single party/ entity. That will reduce the burden over the cloud and increases the throughput. Introduction of third part or one more entity that can provides the assurance of the integrity of data and provides data .It eliminates the burden of users to periodically checking integrity of data. Auditing results provided by TPA help the cloud service provider to increase the efficiency and usability of cloud resources. With this techniques dependencies of business industries increased and revenue of CSP and companies also increased. Specifically, our contribution can be summarized as the following three aspects:

1) We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e.,our scheme enables an external auditor to audit user's outsourced data in the cloud without learning the data content.

2) To the best of our knowledge, our scheme is the first to support scalable and efficient public auditing in the Cloud Computing. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.

3) We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

III. RELATED WORK

Privacy-preserving cloud computing solutions have been developed from theoretical recommendations to concrete cryptographic proposals. There are many works which deal with general security issues in cloud computing but only few works deal also with user privacy.

In hybrid clouds explore the cost of common cryptographic primitives (AES, MD5, SHA-1, RSA, DSA, and ECDSA) and their viability for cloud security purposes. The authors deal with the encryption of cloud storage but do not mention privacy-preserving access to a cloud storage.

The work employs a pairing based signature scheme BLS to make the privacy-preserving security audit of cloud storage data by the Third Party Auditor (TPA). The solution uses batch verification to reduce communication overhead from cloud server and computation cost on TPA side. Further, the paper introduces the verification protocols that can accommodate dynamic data files. The paper explores the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud Computing in a privacy-preserving way. These solutions and provide privacy-preserving public audit but do not offer the anonymous access of users to cloud services.

In hybrid clouds establishes requirements for a secure and anonymous communication system that uses a cloud architecture (Tor and Freenet). Nevertheless, the author does not outline any cryptographic solution. Another non-cryptographic solution ensuring user privacy in cloud scenarios is presented. Here we propose a client-based privacy manager which reduces the risk of the leakage of user private information. we use a non-cryptographic approach to obtain the benefits of the public cloud storage without exposing the content of files. The approach is based on redundancy techniques including an information dispersal algorithm (IDA).

1. A basic part in privacy enhancing cloud services

Group signature schemes are used in many privacy enhancing cryptographic protections that are applied in cloud services the main purpose is to allow members of a group sign messages on behalf of the group. Every group member can sign a message by own group member secret key *gsk[i]* that is usually issued by a group manager. A verifier checks the validity of the signature with a group public key *gpk*. The verifier is able to verify that the signer is indeed the member of the group while the signer's identity is not released. The identities of the members are traceable only in certain circumstances, e.g. breaking the rules.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

Revocation can be done by the group manager or a revocation manager who owns group manager's secret key *gmsk*. The group signature schemes usually employ the following entities:

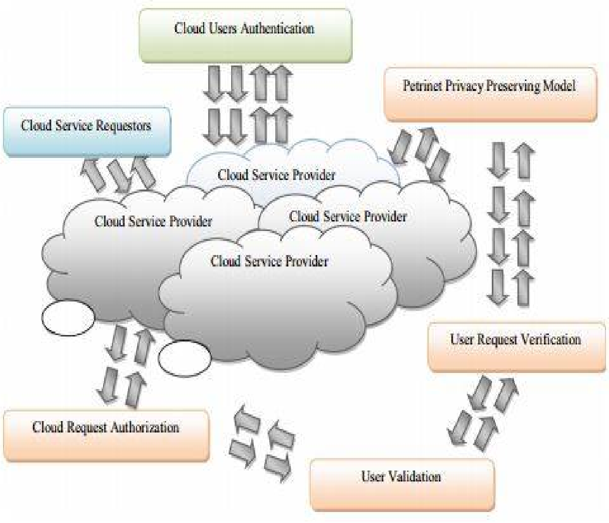
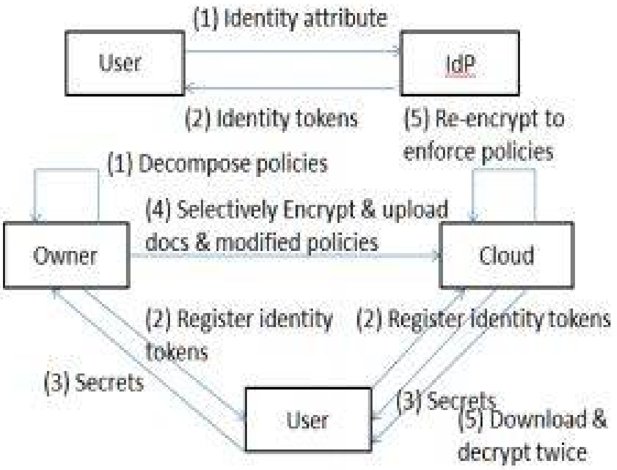


Fig 3.1 Privacy preserving work flow in cloud

Group manager – this entity adds group members into a group, and generates and issues the secret keys of group members.
Revocation manager – this entity disclosures the identity of dishonest members.
User – a group member who owns the group member secret key *gsk[i]*. The user can sign a message on behalf of the group.
Verifier – this entity verifies the validity of the signature by using the group public key *gpk*.

IV. PROPOSED SYSTEM


(1) Identity attribute
User
IdP
(2) Identity tokens
(5) Re-encrypt to enforce policies
(1) Decompose policies
(4) Selectively Encrypt & upload docs & modified policies
Owner
Cloud
(2) Register identity tokens
(2) Register identity tokens
(3) Secrets
(3) Secrets
(5) Download & decrypt twice
User

We now give a general idea of our solution to the problem of delegated access control to outsourced data in the cloud.

DOI: 10.15680/IJIRCCE.2017. 0508050

The first module identity token issuance comprises of two tasks. In the first task, the user login with user-id and password and the server will generate key for two step authentication based on their identity attribute and mail to user. The second module encrypts the data and uploads on the cloud. Data owners are in blame of encrypting the data before uploading them on the cloud that is fine grained encryption and re-encrypting the data that is coarse grained encryption whenever user credentials change.

The third module identity token registration where users register to owner to get token and register the identity token in order to obtain secrets to decrypt the data that they are approved right to use. Users register only those identity tokens related to the owner's sub ACPs and register the left over identity tokens with the Cloud in a privacy preserving method. The users download encrypted data from the Cloud and decrypt the data using the derived keys. Users decrypt double to first remove the encryption layer added by the cloud and then by the owner. As access control is imposed through encryption, users can decrypt only those data for which they have compelling secrets.

The fourth module encryption evolution management, over time user credentials may change. Further, previously encrypted data may go through numerous updates. In such situations, data previously encrypted must be re-encrypted with a new key. As the Cloud performs the access control enforcing encryption, it simply re encrypts the pretentious data without the involvement of the Owner. Policy decomposition: In the single layer encryption approach, the Owner obtains a high communication and computation overhead since it has to manage all the authorizations when user dynamics change. To increase the performance, if the access control related encryption is somehow delegated to the Cloud, the Owner can be freed from the responsibility of managing authorizations through re-encryption. The Cloud is not trusted for the confidentiality of the outsourced data. So the Owner has to initially encrypt the data and upload the encrypted data to the cloud.

Therefore, in order for the Cloud to allow enforcing authorization policies through encryption and avoiding re-encryption by the Owner, the data may have to be encrypted again to have two encryption layers. Using the policy decomposition, the Owner decomposes each ACP into two sub ACPs. The Owner carries out the minimum number of attributes to assure confidentiality of data from the Cloud. The policy decomposition produces two sets of sub ACPs, for the owner and other for the cloud. Privacy Preserving Attribute Based Group Key Management: BGKM (Broadcast Group Key Management) scheme is special type of Group Key Management scheme where private communication channels are not used and rekey operation is performed in single broadcasting. In BGKM scheme private keys are not given to the users. Instead users are given a secret. Secret is combined with public information. From that actual private keys are obtained. This scheme require a private communication only once for initial secret sharing. In such scheme, change of public information does not affect secrets of existing users. The subsequent rekeying operations are performed using one broadcast message.

V. CONCLUSION

Along these lines our method depends on two layers of encryption that objective such prerequisite. In the proposed approach, the information proprietor plays out a coarse-grained encryption, while the cloud plays out a fine-grained encryption on the proprietor scrambled information. A test is to deteriorate get to control approaches (ACPs) with the end goal that the two layer encryption can be made.

We likewise use a productive gathering key administration plot that backings informative ACPs. Our framework guarantees the secrecy of the information and jam the security of client's information from the cloud while appointing the vast majority of the entrance control implementation to the cloud

REFERENCES

[1] Mohamed Nabeel, Elisa Bertino Fellow, Privacy preserving delegated access control in public clouds, IEEE.

[2] M. Nabeel and E. Bertino, Privacy preserving delegated access control in the storage as a service model, in IEEE International Conference on Information Reuse and Integration (IRI), 2012.

[3] M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, Towards privacy preserving access control in the cloud, in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Works haring, ser. Collaborate Com '11, 2011, pp. 172–180.

DOI: 10.15680/IJIRCCE.2017. 0508050

[4] M. Nabeel, N. Shang, and E. Bertino, Privacy preserving policy based content sharing in public clouds, IEEE Transactions on Knowledge and Data Engineering, 2012.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in CCS ’06: Proceedings of the 13th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2006, pp. 89–98.

[6] X. Liang, Z. Cao, H. Lin, and J. Shao, Attribute based proxy re-encryption with delegating capabilities, in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS ’09. New York, NY, USA: ACM, 2009, pp. 276–286.

[7] M. Nabeel and E. Bertino, Attribute based group key management, IEEE Transactions on Dependable and Secure Computing, 2012

[8] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images, World Academy of Science, Engineering and Technology International Journal of Computer, Information Science and Engineering Vol:1 No:2, 2007

[9] N. Shang, M. Nabeel, F. Paci, and E. Bertino, A privacy preserving approach to policy-based content dissemination,” in ICDE ’10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

BIOGRAPHY

D. Vishwaksen Reddy is a B.Tech student in the Computer Science and Engineering Department, Keshav Memorial Institute of Technology, Narayanaguda, Hyderabad, Telangana. His research interests are Cloud Computing, Information Retrival Systems, Data mining etc.