NPP: A NEW PRIVACY-AWARE PUBLIC AUDITING SCHEME FOR CLOUD DATA SHARING WITH GROUP USERS

A.Hannah[1], B.Gobinathan[2]
[1]Computer Science and Engineering, Indira Institute of Engineering and Technology, Chennai, India
[2]Associate Professor & Head of the Department, Computer Science and Engineering, Indira Institute of Engineering and Technology, Chennai, India

ABSTRACT

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation is inefficient due to the large size of shared data in the cloud. In this research, we propose Panda, a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In addition, Hash based Signature Verification approach is used to monitor the traceability of group members which helps to identify the user misbehaves about the shared data.

INTRODUCTION

OVERVIEW OF THE PROJECT

CLOUD Computing has been envisioned as the next-generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc. While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, 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, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time. Secondly, there do exist various motivations for CSP to behave unfaithfully towards the cloud users regarding the status of their outsourced data. For examples, CSP might reclaim storage for monetary reasons by discarding data that has not been or is rarely accessed, or even hide data loss incidents so as to maintain a reputation. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale data storage, it does not immediately offer any guarantee on data integrity and availability.

SCOPE

The main scope of this project is to provide the public audit and identify traceability of shared data.

AIM

The main aim of this project is to provide Data integrity, Traceability using a novel public auditing mechanism for Shared Data in the Cloud with efficient user revocation.

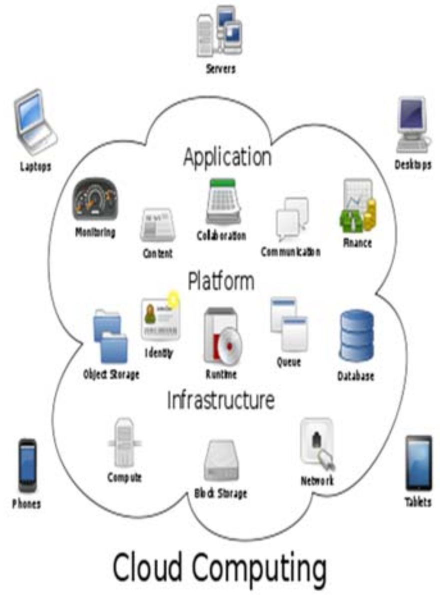
OBJECTIVE

The objectives of the projects are to

1. Provide efficient user revocation
2. Provide Traceability
3. Provide public audit-ability
4. Identity Privacy

DOMAIN INTRODUCTION

The project comes under "Cloud computing" Area



Cloud computing is the delivery of computing and storage capacity as a service to a heterogeneous community of end-recipients. The name comes from the use of a cloud-shaped symbolas an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts services with a user's data, software and computation over a network. There are three types of cloud computing:

- Infrastructure as a Service (IaaS),
- Platform as a Service (PaaS), and
- Software as a Service (SaaS).

Using Infrastructure as a Service, users rent use of servers (as many as needed during the rental period) provided by one or more cloud providers. Using Platform as a Service, users rent use of servers and the system software to use in them. Using Software as a Service, users also rent application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run.

ISSUES IN EXISTING SYSTEM

- Traceability of shared data is very low.
- No clear idea about data freshness.

PROPOSED SYSTEM

- In Proposed system, Hash Based Signature verification is used to improve Traceability of shared data in the cloud. Here, hash values and prime numbers are used to generate the signature based verification key that should be unique for each block of the message.
- In proposed system, we propose Panda, a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key.

ADVANTAGES

- Traceability of shared data is high.
- Confident about data freshness.
- Attacker free.
- Computational time is very low.
- It improves Integrity of the data.

SYSTEM IMPLEMENTATION

Functional modules

- ➢ Group Generation
- ➢ File Generation
- ➢ Operations in Cloud
- ➢ Integrity Verification
- ➢ Traceability verification

Module explanation

Group Generation

In this module, at first the user sends request to data owner for authentication process, the request contains the user address. After receiving certification request, the data owner generates private key and sent it to the user. Finally, Data owner sends the public key of the group of user to the third party public verifier.

File Generation

In this module, Data owner encrypt the data before upload it into the cloud. Using Hash based Signature Verification data should be encrypted. Finally, data was uploaded in the public cloud for the access of respected group members.

Operations in Cloud

In this module, User can access the shared data using his/her own private key. At the time Cloud system executes the PANDA algorithm and it besides perform Hash Based Signature verification (HBSV) key. If any user relocated from group, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key.

Integrity Verification

In this module, third party public verifier performs auditing process for checking integrity of the shared data. Public cloud gives auditing proof to the public verifier and Hash based signature verification key.

Traceability Verification

In this module, Public verifier checks the integrity of shared data and verifier forward the result and the Hash Based Signature Verification key to the data owner. Data owner can check the traceability of shared data.

ALGORITHM USED

Secured Traceability Mechanism:

Step 1: Randomly picks a prime number p.

Step 2: Compute Hash value (H) for prime number p for each block.

Step 3: Store the hash value in public cloud with shared data.

Step 4: If user access the shared data the hash value should perform either addition or multiplication operation with partial private key during sign operation.

Step 5: Based on the user's access repeat step 4.

Step 6: Finally, the operations are forwarded to the data owner.

Step 7: Traceability computation involves reverse process of the hash value computation by using Subtraction or division operation.

Step 8: Repeat step 7 until finds the generated hash value.

Step 9: Decrypted result consists of particular count of user and generated hash value.

Step 10: Based on the partial private key of user, traceability of the user should be predicted.

CONCLUSION AND FUTURE WORK

CONCLUSION

Our proposed work is to improve the traceability and data integrity for shared Data in the Cloud with efficient user revocation. We are using homomorphic authenticable proxy signature (HAPS) convert the data into a block and it support block less verifiability. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key. Hash Based Signature Verification method is used to improve Traceability of shared data in the cloud. Proposed system establishes the correctness of shared data that should be audited by third party public verifier but traceability of data should be verified by the data owner only.

5.2 FUTURE ENHANCEMENT

By using complex polynomial construction in Hash Based Signature Verification method, we can improve the traceability of shared data in the public Cloud.

REFERENCE

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality of Service (IWQoS’09), pp. 1-9, 2009.

[2] 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.

[3] B. Wang, S.S. Chow, M. Li, and H. Li, “Storing Shared Data on the Cloud via Security-Mediator,” Proc. IEEE 33rd Int’l Conf. Distributed Computing Systems (ICDCS’13), pp. 124-133, 2013.

[4] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau, “Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds,” Proc. ACM Symp. Applied Computing (SAC’11), pp. 1550-1557, 2011.

[5] D. Cash, A. Kupcu, and D. Wichs, “Dynamic Proofs of Retrievability via Oblivious RAM,” Proc. 32nd Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT), pp. 279-295, 2013.

[6] Acar, T., M. Belenkiy, and A. Küpçü, Single password authentication. Computer Networks, 2013. 57(13): pp. 2597-2614

[7] Dinesha, H.A. and V.K. Agrawal. Multi-level authentication technique for accessing cloud services. International Conference on Computing, Communication and Applications (ICCCA), 2012

[8] Yassin, A., et al., Cloud Authentication Based on Anonymous One-Time Password, in Ubiquitous Information Technologies and Applications, 2013, Springer Netherlands. pp. 423-431

[9] Abdellaoui, A., Y.I. Khamlichi, and H. Chaoui, A Novel Strong Password Generator for Improving Cloud Authentication. Procedia Computer Science, 2016. 85: pp. 293-300

[10] Celesti, A., et al. Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication. in Advances in Future Internet (AFIN), 2010 Second International Conference on.