IDENTITY BASED ENCRYPTION AND OUTSOURCED REVOCATION IN CLOUD COMPUTING

Sheik Bajilal, Miss G.Keerthana, Sri.V.Bhaskara Murthy,
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

ABSTRACT

The notion of database outsourcing enables the admin to delegate the database management to a cloud service provider (CSP) that provides various database service to different users. Recently plenty of research work has been done on primitive of outsourced database. However, it seems that no existing solution can perfectly support the properties of both correctness and completeness for the query results, especially in the case when the dishonest CSP intentionally returns an empty set for the query request of the user. In this case, we propose a new Identity based encryption scheme for outsourced revocation, which can simultaneously achieve the correctness and completeness of search results even if the dishonest CSP purposely returns an empty set. Further more , we can prove that our construction can achieve the desired security properties even in the encrypted outsourced database.

I. INTRODUCTION

Cloud computing enables convenient and on-demand network access to a centralized pool of configurable computing resources. It has plenty of benefits for real- world applications such as on-demand self-service, ubiquitous network access, location independent re- source pooling, rapid resource elasticity, usage-based pricing, outsourcing, etc. In the outsourcing computation paradigm, the resource-constraint clients can outsource the expensive computing and storage into the cloud service provider (CSP). In the outsourced database (ODB) model, the data owner delegates the database management to the CSP, in order to reduce the heavy database maintenance cost. In addition, the data owner performs the database encryption operations and uploads the encrypted database with the corresponding indices to the CSP. The CSP is responsible for providing all necessary resources and services (e.g. software, hardware and network) to users. The users can issue various query requests to the CSP and receive the corresponding results from CSP. One security challenge is the secrecy of outsourced data: the CSP should not learn anything about what it is actually stored. another security challenge is the verifiability of results.The verifiability consists of the following two security issues [29]: (i) Correctness: the result has not been tampered with; (ii) Completeness: the result should include all valid tuples that satisfy the computation conditions.

1.1 Our Contributions

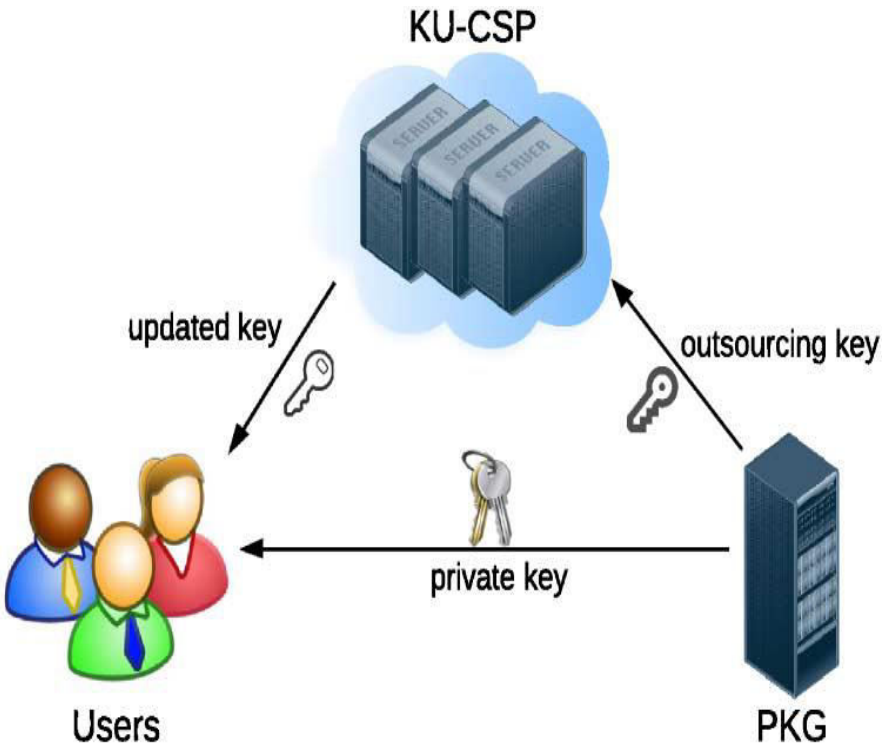
Our main contributions are three folds:

• We propose a new verifiable auditing scheme for ODB, which can simultaneously achieve the correctness and completeness of search results even if the CSP intentionally returns an empty set. Besides, the proposed scheme supports com- mon database operations such as selection and projection.

• We prove that the proposed scheme is secure in the semi-honest-but-curious server model. Our solution is also effective even in the encrypted outsourced database which ensures the confidentiality of the sensitive data.

• The proposed scheme can be extended for the dynamic database by incorporating the idea of verifiable database with updates (VDB) [6].1 That is, the data owner can update the tuples of out- sourced database at any time while the misbehav- ior of server to cheat the users will be detected with an overwhelming probability.

II. SYSTEM ARCHITECTURE



III. EXISTING SYSTEM

Cloud computing provides a scalable environment for growing amounts of data and processes that work on various applications and services by means of on-demand self-services. Especially, the outsourced storage in clouds has become a new profit growth point by providing a comparably low-cost, scalable, location-independent platform for managing clients' data. The cloud storage service (CSS) relieves the burden for storage management and maintenance. However, if such an important service is vulnerable to attacks or failures, it would bring irretrievable losses to the clients because their data or archives are stored in an uncertain storage pool outside the enterprises.

Dis advantages:

These security risks come from the following reasons:

1. The cloud infrastructures are much more powerful and reliable than personal computing devices, but they are still susceptible to internal threats (e.g., via virtual machine) and external threats that can damage data integrity.

2. The data change may not be timely known by the cloud users; Even if these disputes may result from the users own improper operations.

IV. PROPOSED SYSTEM:

We proposed a dynamic audit service for integrity verification of un trusted and outsourced storages. Constructed on interactive proof system (IPS) with the zero knowledge property, our audit service can provide public audit ability without downloading raw data and protect privacy of the data. Also, our audit system can support dynamic data operations and timely anomaly detection with the help of several effective techniques, such as random sampling, and index-hash table (IHT). We also propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof-of-concept prototype is also implemented to evaluate the feasibility of our proposed approaches. Our experimental results not only validate the effectiveness of our approaches, but also show that our system does not create any significant computation cost and require less extra storage for integrity verification.

Advantages:

- To verify the outsourced database located in CSP
- To audit the encrypted outsourced database

V. IMPLEMENTATION

1.Admin **:**

In this module admin login first, then only access the request from the CSP. In this we have two operations.

1.1 Upload files
1.2 Edit Users

2.Cloud service Provider :

In this module CSP login first , then CSP generate the key for the user request and key will sent to the mail. And CSP is the interface between the admin and user. In this we have three operations.

2.1 User Request
2.2 View Files
2.3 Remove Files

3.User:

In this module a user have to register first and then login.User can choose the file and send request to the CSP, and user can receive the key from the CSP then download the files. In this we have two operations.

3.1 View Files

3.2 Download files

VI. CONCLUSION

In this paper, we investigate the integrity auditing of outsourced database in cloud computing. Our main contribution is to propose a new identity based encryption scheme of outsourced database which can achieve the verifiability of search result even if the result is an empty set. Besides, our scheme supports common database operations such as selection and projection. Furthermore, our construction can be easily extended to the scenario of dynamic database by incorporating the notion of revocation database with updates. We also prove that our scheme can achieve the desired security goals and provide detailed simulation tests.

REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology – CRYPTO'98. Springer, 1998.

[2] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247–259.

[3] F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficient certificate validation and revocation," in Public Key Cryptography PKC 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375–388.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology – CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213–229.

[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS '08. New York, NY, USA: ACM, 2008, pp. 417–426.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557–557.

[7] R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation," Cryptology ePrint Archive, Report 2011/518, 2011.

[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC '97. New York, NY, USA: ACM, 1997, pp. 506–516.

[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proceedings of the Second international conference on Theory of Cryptography, ser. TCC'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 264–282.

[10] R. Canetti, B. Riva, and G. Rothblum, “Two protocols for delegation of computation,” in Information Theoretic Security, ser. Lecture Notes in Computer Science, A. Smith, Ed. Springer Berlin / Heidelberg, 2012, vol. 7412, pp. 37–61.