

Hybrid Approach for Cloud Storage with Attribute based Encryption

Shivam Patole
M.Tech Scholar
VITM,Indore , India

Anwar Sarkeja
Assistant Professor
VITM, Indore , India

ABSTRACT

In cloud computing there is problem associated with whole life of cloud data. For storage three important aspects of data is Data confidentiality, Data integrity and availability. Data encryption is used for confidentiality. Now, after this encryption data is sent to storage. Now, after the user supplies its key than the data is opened. Thus to provide user based security control for cloud provider is the primary objective of this effort and can be achieved by Homomorphic encryption. Key management is another problem because the user is not expert to manage keys. The user has faced such problems. To develop a security architecture and implement client based confidentiality tool for storage in cloud computing and evaluate traditional security solutions and identify their remaining issues by which overall performance gets degraded. We will implement homomorphic encryption using improved KP-ABE system to achieve data confidentiality.

Keywords

Cloud, Cloud Security, Data privacy, ABE,KP-ABE, Cloud Storage

1. INTRODUCTION

Cloud Computing supports global and on-demand network accessibility to the resources (e.g. networks, servers, storage, applications and services). Public cloud and private cloud are the two major categories of cloud computing. A requirement for a localized, scalability, and flexible means to system access to cloud data exclusive of entirely trusting on the cloud service providers. Regarding security and safety of data which is confidential, this is the main issue of cloud. Thus to provide the security and kept the user's data confidential we have found a way to keep it secure. The method we are going to propose here will work on a simple approach. We are giving the idea of encryption, in which the user's data or message which the user wants to transfers on the network will be encrypted. Here the question arises how and which approach will be followed here for the encryption technique used here? The answer to this question is described as-

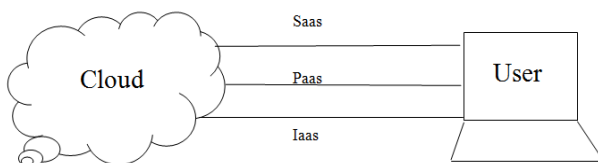


Figure 1.: Cloud Computing

Data encryption is the most operative in honor to avoiding sensitive or the very confidential data of the customer from an unauthorized access inappropriately, these functionality shortages the articulateness needed for more advanced information allocation. To deal with these budding needs,

Sahai and Waters initiated the notion of attribute-based encryption (ABE). Instead of encrypting to individual user, in ABE system, one can put in a right to use plan into the cipher text or decryption key.

2. RELATED WORK

ABE can be observed as a conservatory of the concept of identity-based encryption in which user identification is simplified to a set of illustrative characteristics instead of an only string denoting the user identity. When comparing with identity-based encryption i.e. ABE has important advantage as it achieves flexible one-to-many encryption in its place of one-to-one; it is proposed as a favorable device for concentrating the problem of confident and fine-grained data sharing and regionalized access control.

We offer a new KP-ABE formation with constant cipher text size by adopting and applying the knowledge of the identity-based broadcast encryption method. In our algorithm construction, the access policy can be expressed or defined as any intonation access structure. Temporarily, the cipher text size is independent of the number of cipher text features, and the number of bilinear pairing estimations is reduced to a constant. We prove that our scheme is semantically secure and locked in the selective-set model based on the general Diffie-Hellman exponent notion.

3. EXISTING SYSTEM

The encryption technique is been finalized and now this paper is going to present the results for vivid CP-ABE methodology with constant-size of the cipher texts. Here it will be very interesting to see if shorter private keys can be obtained without affecting the clarity or the dimension of cipher texts and to the construct adaptively and high secure such approach. The other more difficult and challenging problem we have faced to achieve related results in the communicative cipher text-policy location. , we had firstly studied the feasible and reliable with draw all operations in KP ABE scheme: single attribute withdrawal and unique identifier withdrawal. After that, based on unique identifier revocation procedure, we will suggested the KP-ABE-R scheme in which mischievous users can be efficiently and more collaboratively revoked.

Our motive going to present the cipher text policy based on the encryption scheme with complete efficient revocation with the help of using linear undisclosed allocation pattern and binary tree as the essential tools. We are going to that the allocating proficiency can be easily provided in the wished-for arrangement, but all the representatives are accompanying with their creative delegator's matchless identifier. The overview of our proposed paper has been diagrammatically presented with the help of two illustrative reorientations-

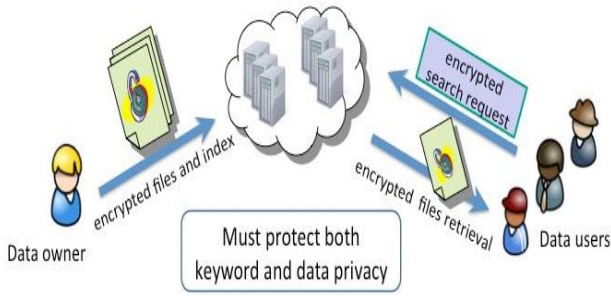


Figure 2: Encryption System

The figure 2 represented here shows that the data owner is encrypting his confidential files and index which he want to be secure from the outsiders, here the encryption technique is involved. Moreover, the data is encrypted if and only if the search request for the encryption is found. If the search request will not being found by any of the receiver then the key will not been send , hence it will be discarded. If their exists any of the search request on the server side the request, then the request will be successfully accepted and encrypted files will be retrieved by the data users. Here the search request will also be in an encrypted form.

Here the above figure has demonstrated how the encryption can be done and how the request of the search will be fulfilled. Here by it is very easy to understand the encryption system. Now with the second example we will discuss the ABE encryption technique. Here, In ABE encryption attributes are defined and it's more briefly discussed as-

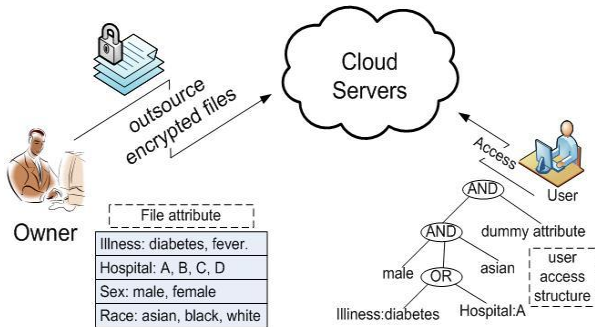


Figure 3: Attribute based Encryption

The figure 3 represents the encryption technique here, the user here provides his attributes for e.g. his illness which can be fever, diabetes etc., name of the hospital like A,B,C,D, his gender i.e. male or female, his race i.e. Asian, black or white.

4. PROPOSED SYSTEM

Cipher text-Policy Attribute-Based Encryption (KP-ABE) is a type of identity-based encryption, which uses one public key and the Master Private Key, used to make more restricted private keys. The KP-ABE is very expressive rules for which private keys can decrypt which cipher texts. Here in this algorithm Private keys have “attributes” or labels and the most important feature of this algorithm is Cipher text shaves its own decryption policies. Figure 4 describe about Cipher text policy Attribute-based encryption

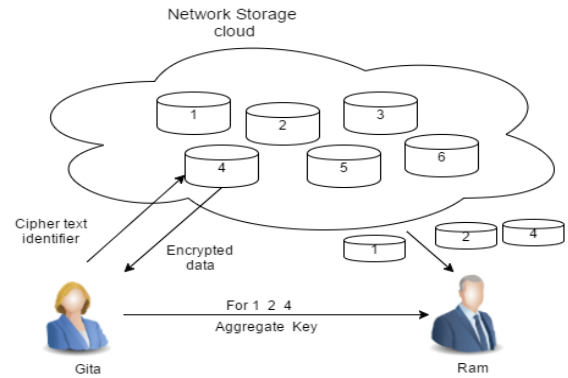


Figure 4: Cipher text-Policy Attribute-Based Encryption

Contrasting other Role-Based Access Control (RBAC) systems, KPABE acts not require a trusted authority, or any form of storage. The encryption the situation functions as the RBAC mechanism.

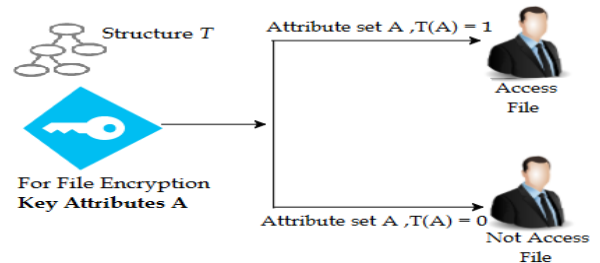


Figure 5: Role-Based Access Control

As shown in the above figure 5, KP-ABE reverses the role of encryption and key derivation. The encryption is associate with an access structure, which is constructed using the policy. KGS simply issues private keys for the attributes users have. If users (rather their attributes) satisfy the owner defined access structure, they can decrypt it. The second variant is closer to encryption found in open systems as the cipher text is associated the policy.

5. RESULT

Proposed system implemented on openshift cloud. Below steps describe how create public cloud on openshift cloud.

- Registration and verification
- Create Account
- Build Application with following configuration
 - JBoss Application Server
 - Web server
 - MY SQL SERVER
 - Database
 - PHPMyadmin
 - Database browser
- Install plugin in eclipse
- Mapping between eclipse and openshift
- Make Application on eclipse
- Deployed Application on cloud

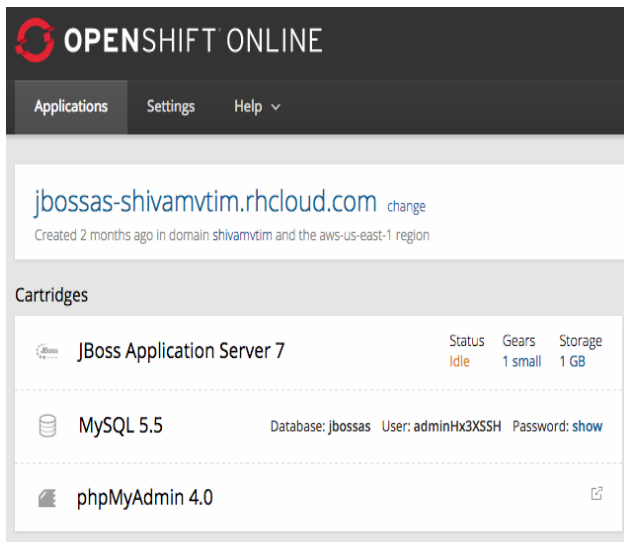


Figure 6: Dashboard of public cloud

Calculate encryption time and decryption time of uploaded file is show in below table.

Table1: encryption time and decryption time of uploaded file

| S.No | File Name | File Size | Encryption Time (ms) | Decryption Time (ms) |
|------|-----------|-----------|----------------------|----------------------|
| 1 | Cgg.txt | 538B | 19 | 12 |
| 2 | Db.sql | 58.4KB | 880 | 200 |
| 3 | Abc.txt | 14B | 12 | 6 |
| 4 | Hbhk.sql | 58.2KB | 860 | 180 |
| 5 | Build.xml | 5.5KB | 120 | 40 |

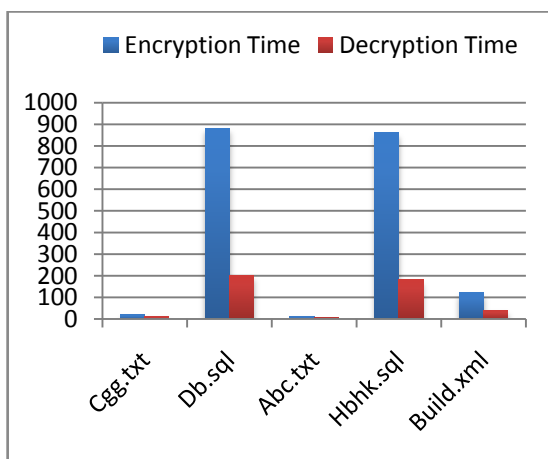


Figure 7: Encryption time and Decryption Time

6. CONCLUSION

The third party mechanism deals with continuous monitoring of user record. This monitoring along with improved throughput and efficiency is achieved. Out of these methods an enhanced secure scenarios is generated through our proposed KP-ABE. At the initial level of our research, we get the following benefits.

- Improved security solution with less operational overheads and retains reliability on novel encryptions
- Unauthorized access is blocked using improved key generation through user characteristics.

Continuous monitoring gives the user behavior measurements and analyzes the affection of such novel cryptosystem on other services

7. REFERENCES

- [1] Shucheng Yu , “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, in Proceedings of IEEE Infocomm, ISSN: 978-1-4244-5837-0/10, 2010.
- [2] Srijith “Towards Secure Cloud Bursting, Brokerage and Aggregation” 2010 Eighth IEEE European conference on web services
- [3] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE “Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE-2012
- [4] Cong Wang¹, Qian Wang¹, Kui Ren¹, and Wenjing Lou²,” Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, IEEE INFOCOM 2010, San Diego, CA, March 2010
- [5] Ms. Vaishnavi Moorthy¹, Dr. S. Sivasubramaniam²,” Implementing Remote Data Integrity Checking Protocol for Secured Storage Services with Data Dynamics and Public Verifiability In Cloud Computing, IOSR Journal of Engineering Mar. 2012, Vol. 2(3) pp: 496-500
- [6] C. Hota, S. Sanka, M. Rajarajan, S. Nair, "Capability-based Cryptographic Data Access Control in Cloud Computing", in International Journal of Advanced Networking and Applications, Volume 01, Issue 01, 2011.
- [7] Rosario Gennaro and Daniel Wichs, Fully Homomorphic Message Authenticators IBM Research, T.J. Watson, May 23, 2012
- [8] K. Kajendran, J. Jeyaseelan, J. Joshi, “An Approach for secures Data storage using Cloud Computing” In International Journal of Computer Trends and Technology- May to June Issue 2011
- [9] W. Luo, G. Bai, “Ensuring the Data Integrity In Cloud computing” In Proceedings of IEEE CCIS, 2011.
- [10] S. Sanka, C. Hota, and M. Rajarajan, “Secure data access in cloud computing,” in 2010 IEEE 4th International [13] <http://en.wikipedia.org/wiki>
- [11] H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.
- [12] Dianli GUO and Fengtong WEN, “A More Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment”, in Journal of Computational Information Systems, ISSN: 1553–9105, Vol. 9:No. 2, 2013, 407-413

- [13] Kristin Lauter, Michael Naehrig and Vinod Vaikuntanathan, “Can Homomorphic Encryption be Practical”, in ACM, 2008.
- [14] Craig Gentry, “Computing Arbitrary Functions of Encrypted Data”, in ACM by IBM T.J. Watson Research Center, 2008.
- [15] Bharath K. Samanthula, Gerry Howser, Yousef Elmehdwi, and Sanjay Madria, “An Efficient and Secure Data Sharing Framework using Homomorphic Encryption in the Cloud”, in Cloud 1st conference by ACM, ISSN: 978-1-4503, DOI: 1596-8/12/08, 2012.
- [16] Robert Griffin and Subhash Sankuratripati, “Key Management Interoperability Protocol Profile Version 1.1”, in OASIS Standards Organizations at <http://docs.oasis-open.org/kmip/profiles/v1.1/os/kmip-profiles-v1.1-os.doc>, 2013.
- [17] Web Article, “Amazon Web Services: Overview of Security Processes” by Amazon Services at <http://aws.amazon.com/security>, June 2013.
- [18] K. Raen, C. Wang, Q. Wang, “Security Challenges for the Public Cloud”, Published by IEEE Computer Society, Jan/Feb 2012.