www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 12. November 2015

An Efficient Cloud Security System Using Verifiable Decryption Process

S.Saphna Kumari
Department of Computer Science and Engineering
K.Ramakrishnan College of Technology, Samayapuram
Trichirappalli, India
smsaphna7@gmail.com

Abstract— **As internet applications are growing quickly and it have been prosperous in the era of cloud computing, people can process, store and share their data on the cloud. Cloud shares its infrastructure between several organizations and it is managed by a third-party. Attribute Based Encryption (ABE) is a public-key based encryption techniques which allows users to encrypt data based on user attributes. Encrypted data stored in the cloud was assigned with an access control by using access polices and attributes associated with private keys and ciphertexts. Access controls to data operate on the assumption that data servers can be trusted to keep data confidential and enforce access control policies correctly. In existing standard ABE schemes, the decryption require many pairing operations and are expensive and the complexity of the access policy is proportional to the number of attributes. To overcome this problem an ABE system with outsourced decryption was introduced. This scheme provides no guarantee on the correctness of the transformation done by the cloud server. To provide correctness of the cloud transformation, this project uses the security model of ABE with verifiable outsourced decryption by providing the verification at the time of output decryption.**

Keywords—Attribute Based Encryption(ABE), outsourced decryption, cloud security

I. INTRODUCTION

While the storage of corporate data on remote servers is not a new development, current expansion of cloud computing justifies a more careful look at its actual consequences involving privacy and confidentiality issues. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. The overhead of using cloud storage should be minimized as much as possible, such that user does not need to perform too many operations to use the data.

To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent cloud storage server to audit the outsourced data when needed [2]. As more sensitive data is shared and stored by third-party across many sites on the internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level. The drawbacks of the standard ABE schemes are their relatively large cipher text size and high decryption cost and also it requires many number of pairing operations in decryption. These pairing operations are usually more expensive than exponentiation. To overcome this problem green et.al suggested to outsourced decryption in attribute based encryption. This scheme provides no guarantee on the correctness of the transformation done by the cloud server. There are two schemes that are associated with the Attribute Based Encryption with verifiable decryption is: 1) Cipher-Text Policy Attribute Based Encryption (CP-ABE). 2) Key Policy Attribute Based Encryption (KP-ABE).

Attribute Based Encryption with Verifiable Outsourced Decryption is a public key based encryption technique, in which the encrypted content that is known as cipher-text is associated with the access policy and the attributes of the user [1]. Attribute Based Encryption with Verifiable Outsourced Decryption is a challenging application that serves as public key based encryption that allows the user for the encryption and the decryption of the file/ data based on their own attributes. This application also provides the user's data in terms of security saying no malicious cloud will be able to learn about the encrypted file and also provides fully security against the key being compromised by the cryptanalyst.

II.VERIFIABLE OUTSOURCED DECRYPTION

Aiming at eliminating the most overhead computation at both attribute authority and user sides, it propose an outsourced ABE scheme not only supporting outsourced decryption but also enabling delegating key generation. In this construction, they

introduce a trivial policy controlled by a default attribute and use an AND gate connecting the trivial policy and user's policy [4]. During key-issuing, attribute authority can outsource computation through delegating the task of generating partial private key for user's policy to a Key Generation Service Provider (KGSP) to reduce local overhead. Moreover, the outsourced decryption is realized by utilizing the idea of key blinding. More precisely, user can send the blinded private key to a Decryption Service Provider (DSP) to perform partial decryption and do the complete decryption at local. Following our technique, constant efficiency is achieved at both attribute authority and user sides.

In addition, they observe that when experiencing commercial cloud computing services, the CSPs may be selfish in order to save its computation or bandwidth, which may cause results returned incorrectly. In order to deal with this problem, they consider to realize checkability on results returned from both KGSP and DSP, and provide a security and functionality enhanced construction, which is provable secure under the recent formulized Refereed Delegation of Computation (RDoC) model. Out technique is to make a secret sharing on the outsourcing key for KGSP and let k parallel KGSPs utilize their individual share to generate partial private keys.

III.SYSTEM DESIGN

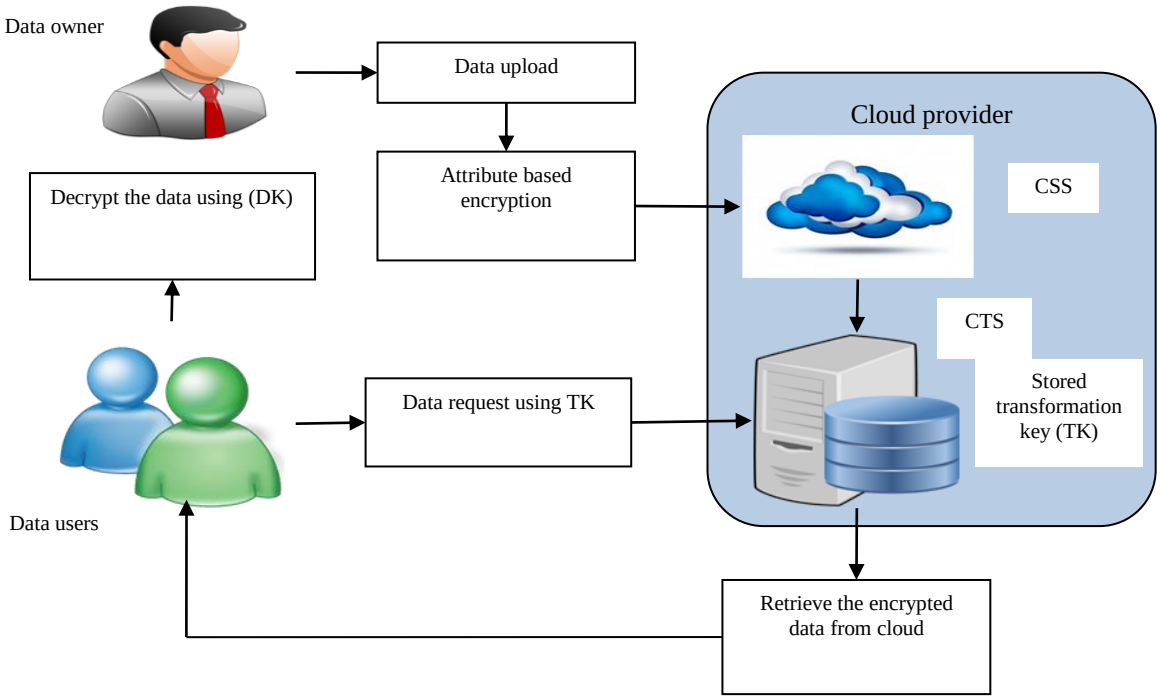

Figure 1.1 SYSTEM ARCHITECTURE

In a KP-ABE scheme, every cipher text is associated with a set of attributes and every user's private key is associated with an access policy on attributes. A user is able to decrypt a cipher text only if the set of attributes associated with cipher text satisfies the access policy associated with the user's private key. In a KP-ABE scheme, the roles of an attribute set and an access policy are swapped from what they described for CP-ABE [3]. One of the main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource-limited devices due to pairing operations and the number of pairing operations required to decrypt a cipher text grows with the complexity of the access policy. Attribute Based Encryption with Verifiable Outsourced Decryption is a public key based encryption technique, in which the encrypted content that is known as cipher-text is associated with the access policy and the attributes of the user.

International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 12. November 2015

IV. COMPONENTS

A. *Cloud Entities*

Cloud computing is computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. Clouds can be classified as public, private or hybrid. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. The system model consists of three types of entities: the cloud server (server), the data owners (owners) and the data consumers (users).

- Cloud server is responsible for store the data in cloud storage. It contains two sub servers such as Ciphertext transformation server (CTS), Cloud storage server (CSS)
- Data owner is the owner of storage system. They are stored data in cloud and also download the data from cloud without any authorization
- Cloud users are access the data from cloud using the attribute and use data based on access control mechanism.

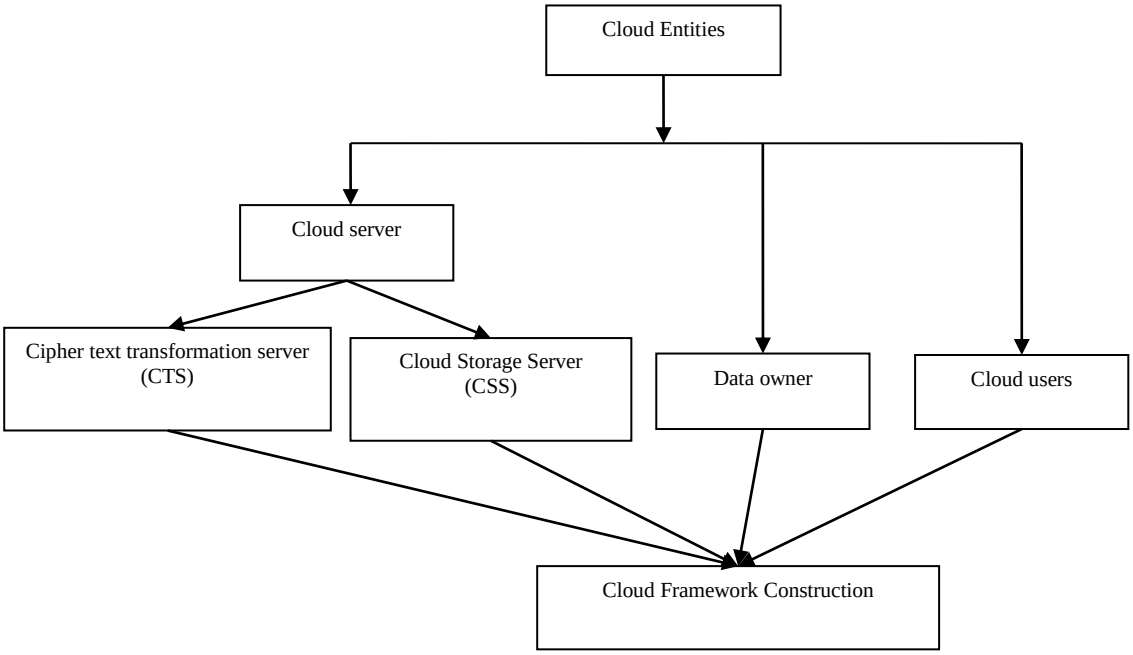

Figure 1.2 Cloud entities

B. *Key generation and key distribution*

The owner generates the public key and the secret key based on the user attributes and the access control assigned with the them. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It monitors and records all the attempts which are made to access a system. Access Control may also identify the users attempting to access a system are authorized or not. Various access control models are in use, including Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. These access control methods are effective in unchangeable distributed system, where there are only a set of Users with a known set of services. The cloud server is responsible for the distribution of secret key and public key for each legal user in the system.

The cloud server split into two servers such as Cloud Storage Server (CSS), Ciphertext Transformation Server. However, the cloud server is not involved in any attribute management and the creation of secret keys that is associated with attributes. The owner divides the secret key into transformation key (denoted by TK) and El Gamal-type secret key (denoted by DK). DK is kept secret in user side. TK is transferred from user to CTS server.

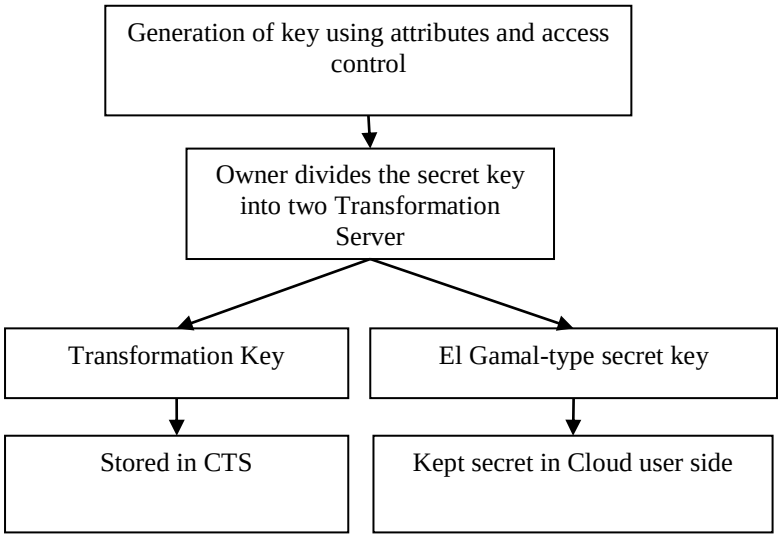

Figure 1.3 Key generation and distribution

C. Security model

The cloud server stores the owners' data and provides data access service to users. It generates the decryption token of a cipher text for the user by using the secret keys of the user issued by the CTS. User Revocation starts with the intuition of the user revocation operation as follows. Whenever there is a user to be revoked, the data owner first determines a minimal set of attributes without which the leaving user's access structure will never be satisfied. Next, they updates these attributes by redefining their corresponding system master key components [5]. The main issue with this intuitive scheme is that it would introduce a heavy computation overhead for the data owner to encrypt data files and might require the data owner to be always online to provide secret key update service for users, and in user side,the user may misuse the cipher text and may perform malicious access. To resolve this issue, they use verifiable outsourced decryption approach to improve security at the time of data decryption. It can be worked as Key Encapsulated Mechanism (KEM) setting approach where the ABE cipher text hides a symmetric session key. The formal definition of attribute-based KEM with outsourced decryption is exactly the same as that of ABE with outsourced decryption, except that the encryption algorithm of ABE is replaced by an encapsulation algorithm, which doesn't take a message as an input.

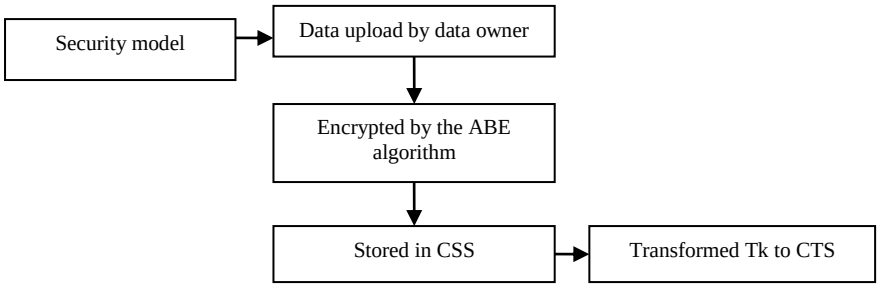

Figure 1.4 Security model

Data encryption as

- It divides the data into several data components as m=$m_1, \dots, m_n$
- It encrypts data components with different content Keys k=$k_1, \dots, k_n$ by using symmetric encryption methods.
- It then defines an access structure Mi for each content key k_i and encrypts it by running the encryption algorithm Encrypt [6].

D. Secure data sharing

Each user is assigned with CTS. Each user can freely get the cipher texts from the server in secure manner. To decrypt a cipher text, each user may submit their secret key TK issued by some CTS together and kept the key DK in user side and ask it together at the time of decryption token for some cipher text. Upon receiving the decryption token, the user can decrypt the cipher text by using its DK. Only when the user's attributes satisfy the access policy defined in the cipher text, the server can generate the correct decryption token. The secret keys and the global user's public key can be stored on the server; subsequently, the user Data owner not need to submit any secret keys if no secret keys are updated for the further decryption token generation. It aims to allow the users with eligible attributes to decrypt the entire data stored in the cloud server. However it cannot limit the users from accessing the data's which are not accessible to them. That is it cannot limit the data access control to the authorized users.

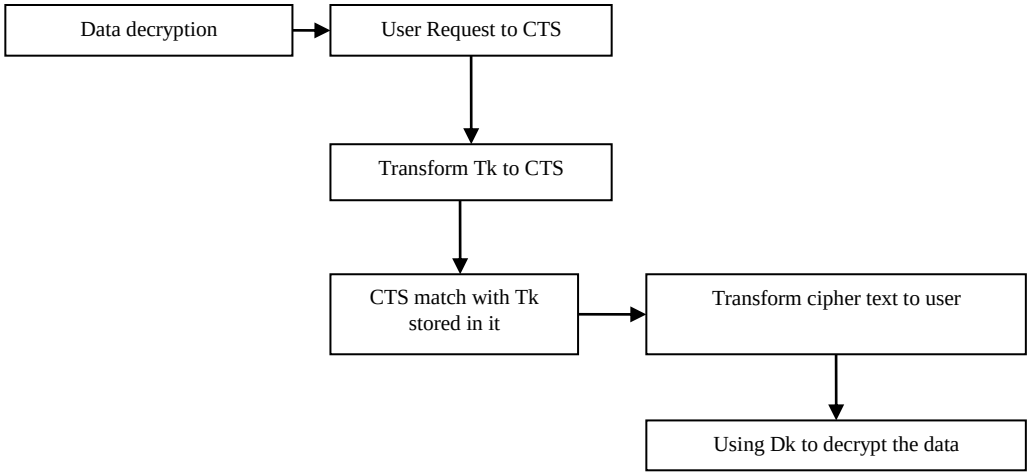

Figure 1.5 Secure data sharing

E. Evaluation Criteria

This module evaluates the performance of the system using the performance metrics such as storage overhead, communication cost and computation efficiency. The storage overhead is one of the most significant issues of the access control scheme in cloud storage systems. In their scheme, besides the storage of attributes, CTS also needs to store a public key and a secret key for each user in the system. Thus, the storage overhead on CTS in their scheme is also linear to the number of in the system. The communication cost of the normal access control is almost the same. The communication cost of attribute revocation is linear to the number of cipher texts which contain the revoked attribute. They compare the computation efficiency of both encryption and decryption in two criteria: the number of authorities and the number of attributes per authority.

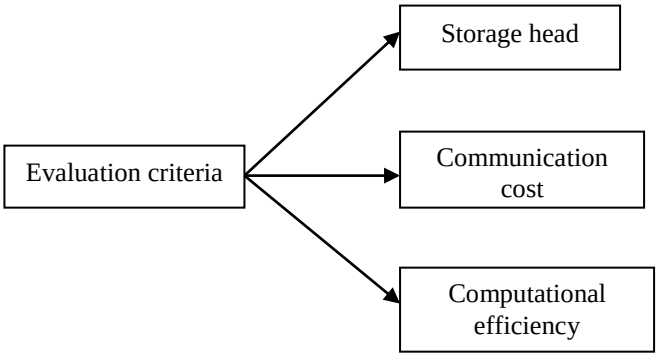

Figure 1.6 Evaliuation criteria

V. CONCLUSION

This paper proposes a novel framework of achieving grained access control for sharing personal data. Considering partially trustworthy cloud servers, it argues that to fully realize the concept, patients shall have complete control of their own privacy through encrypting their files to allow fine-grained access. The framework addresses the unique challenges brought by multiple data owners and users, in that greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. It utilizes ABE to encrypt the cloud data, so that user can allow access not only by personal users, but also various users from public Data owner mains with different professional roles, qualifications, and affiliations. We considered a new requirement of ABE with outsourced decryption: Verifiability. It is used to modify the original model of ABE with outsourced Decryption. This ABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .Our scheme does not rely on random oracles. A flexible access control for encrypted data stored in cloud is provided. It eliminates Decryption overhead for users according to attributes .This Data transformation is guaranteed to store in cloud. This secure attribute based cryptographic technique for robust data security that's being shared in the cloud.

Furthermore, enhance attribute scheme to multi authority attribute scheme to handle efficient and on demand user revocation, and prove its security. As future study, it will be interesting to enhance the fine grained access control in cloud computing with authorized CTS to verify the cloud server that stores and process the cloud records.

References

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.
[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.
[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.
[4] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Secur. Symp., 2011, p. 34.
[5] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[6] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 4, pp. 2201–2210, Aug. 2014. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6642027