International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Cipher Text-Policy Attribute-Based Encryption

G. Swetha[1], **P. Sindhuja**[2], **P. SaiTeja**[2], **T. Thushara Devi**[2]

[1]Assistant Professor, Department of Information Technology in Teegala Krisha Reddy Engineering College, Telangana, India

[2]UG Scholar, Department of Information Technology in Teegala Krisha Reddy Engineering college, Telangana, India

ABSTRACT

This paper review on security of data stored in public cloud. This can be achieved by using encryption and decryption mechanism. The data owner can store the encrypted data within the cloud. Then the owner can issue the decryption keys to the authorized users. Based on this scheme data owners can easily share the data to intended users. Extensive number of users are trying to access data stored in the cloud simultaneously, it leads to new challenges mainly on confidentiality and integrity of data stored in cloud.

Keywords : Encrypted Data, Authorized Users.

I. INTRODUCTION

Cloud storage service has significant advantages on both convenient data sharing and cost reduction . Thus, more and more enterprises and individuals outsource their data to the cloud to be benefited from this service. However, this new paradigm of data storage poses new challenges on data confidentiality preservation . As cloud service separates the data from the cloud service client (individuals or entities), depriving their direct control over these data, the data owner cannot trust the cloud server to conduct secure data access control. Therefore, the secure access control problem has become a challenging issue in public cloud storage.

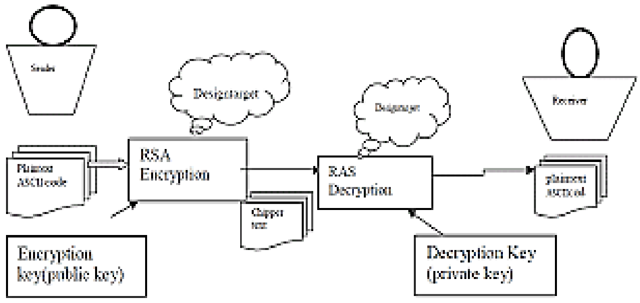

Figure 1: RSA algorithm and remote data cloud storage.

Support gradual access privilege releasing. To realize the function of timed releasing, it is necessary to introduce an effective scheme, which will not release the data access privilege to intended users until reaching pre-defined time points. A trivial solution is to let data owners manually release the time-sensitive data: The owner uploads the encrypted data under different policies at each releasing time such that the intended users cannot access the data until the corresponding time arrives. However, this solution forces the owner to repeatedly upload the different encryption versions of the same data, which puts unnecessary and heavy burden on the data owner.

We present how to design access structure for any potential timed release access policy, especially embedding multiple releasing time points for different intended users. To the best of our knowledge, we are the first to study the approach to design structures for general time-sensitive access requirements .Furthermore, a rigorous security proof is given to validate that the proposed scheme is secure and effective.

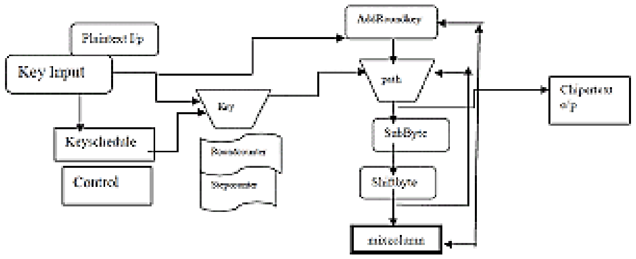

Figure 2: Data integrity and confidentially

II. OBJECTIVE

The main construction in Section V provides the basic algorithm and cryptography techniques to embed both time and attribute factors into access control for public cloud. However, it lacks a general method for data owners to make an efficient access structure for arbitrary access privilege construction with both time and attribute factors, especially, when a policy is embedded with multiple releasing time points, there exist many cases as described later in this section. These cases cannot be defined by a tree-based structure with existing mechanisms. In this section, we first list the potential sub-policies for time-sensitive data, and then gives an efficient and practical method to construct relevant access structures.

In the main construction of server is a time trapdoor should be attached to a node of the policy tree. Here we further give another scheme to support a time trapdoor without being attached to any node, which will be utilized to realize time-related sub-policies in the following subsections. From the perspective of the structure construction, such time trapdoor is a leaf node, which can be regarded as a special attribute. In this section, we use attached time trapdoor to indicate that it's attached to a certain internal node, and unattached time trapdoor to indicate that it is not attached to any node but acts as a special attribute.

III. IMPLEMENTATION

This paper aims at fine-grained access control for time sensitive data in cloud storage. One challenge is to simultaneously achieve both flexible timed release and fine granularity with lightweight overhead, which was not explored in existing works. In this paper, we proposed a scheme to achieve this goal. Our scheme seamlessly incorporates the concept of timed-release encryption to the architecture of cipher text policy attribute-based encryption. With a suit of proposed mechanisms, this scheme provides data owners with the capability to flexibly release the access privilege to different users at different time, according to a well-defined access policy over attributes and release time. We further studied access policy design for all potential access requirements of time sensitive, through suitable placement of time trapdoors. The analysis shows that our scheme can preserve the confidentiality of time-sensitive data, with a lightweight overhead on both CA and data owners. It thus well suits the practical large-scale access control system for cloud storage.

Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider.

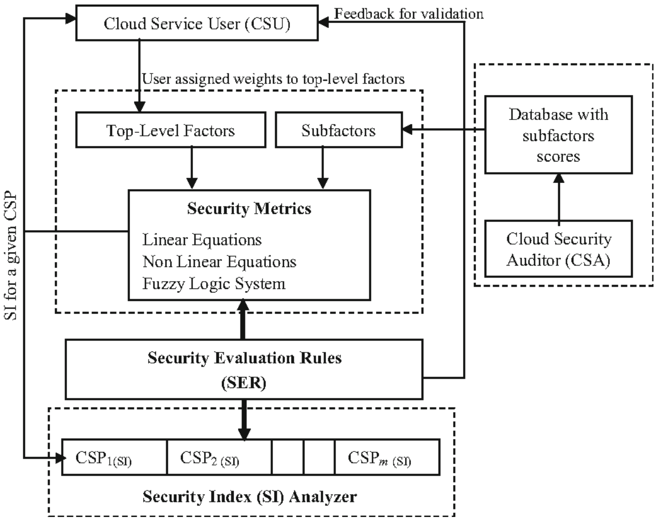

Figure 2 : Basic concept of cloud security.

Security Analysis We analyzes the security properties of data on some critical aspects as follows.

Fine-Grained and Timed-Release Access Control:

Our proposed TAFC provides data owners with the capability to define access policies according to flexible association of attributes and releasing times. With the access policy embedded in the cipher text, a user can decrypt the cipher text to access the data, only if his/her attribute set satisfies the policy, and the access time is later than the predefined releasing time. Security against Collusion Attack: In each user's attribute set-associated security key blinded based on a secure random number. This mechanism is implemented to resist the collusion attack: The adversary cannot combine different security keys to forge a new security key associated with a different attribute combination which comes from multiple attribute sets belong to different users. Therefore, the collusion will not bring more privileges to the adversary. Data Confidentiality:

The confidentiality property of can be analyzed from two aspects, the cryptography and the protocol as follows: As a cryptography algorithm to take into account, the adversary model can be described as the following security game.

1. Systematic review of security issues for cloud computing

We have carried out a systematic review of the existing literature regarding security in Cloud Computing, not only in order to summarize the existing vulnerabilities and threats concerning this topic but also to identify and analyze the current state and the most important security issues for Cloud Computing.

Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security. In SaaS, organizational data is often processed in plaintext and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored. Also, data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well. Also cloud providers can subcontract other services such as backup from third-party service providers, which may raise concerns. Moreover, most compliance standards do not envision compliance with regulations in a world of Cloud Computing. In the world of SaaS, the process of compliance is complex because data is located in the provider's datacenters, which may introduce regulatory compliance issues such as data privacy, segregation, and security, that must be enforced by the provider.

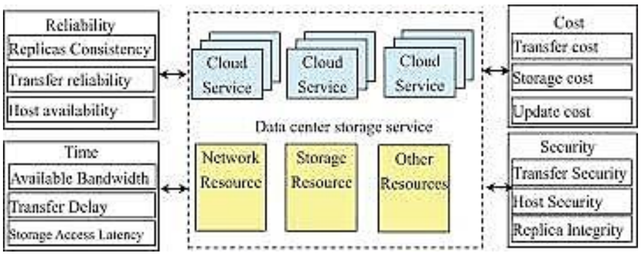

Figure 3. Storage of data at data centres.

We propose an efficient time and attribute factors combined access control scheme, named data segment, for time-sensitive data in public cloud. Our scheme possesses two important capabilities: It inherits the property of fine granularity from data stream .By introducing the trapdoor mechanism, it further retains the feature of timed release from cluster. Note that in, the introduced trapdoor mechanism is only related to the time factor, and only one corresponding secret needs to be published when exposing the related trapdoors. This makes our scheme highly efficient, which only brings about little overhead to the original data based scheme. So the data in cloud should have to be stored in an encrypted form. With the increase in the number of organizations using cloud technology for data operation, proper security and other potential vulnerable areas became a priority for organizations contracting with cloud providers. Cloud computing security processes the security control in cloud & provides customer data security, privacy & compliance with necessary regulations.

Data integrity means ensuring that data is identically maintained during any operation (such as transfer, storage, or retrieval). Put simply, data integrity is assurance that the data is consistent and correct. Ensuring the integrity of the data really means that it changes only in response to authorized transactions. This sounds good, but you must remember that a common standard to ensure data integrity does not yet exist.

Cloud security becomes effective only if the defensive implementation remain strong. There are many types of control for cloud security architecture, the categories are listed below: Detective Control: are meant to detect and react instantly & appropriately to any incident.Preventive Control: strengthen the system against any incident or attack by actually eliminating the vulnerabilities.Deterrent Control: are meant to reduce attack on cloud system; it reduces the threat level by giving a warning sign.Corrective Control: reduces the consequences of an incident by controlling/limiting the damage. Restoring system backup is an example of such type. Encryption protects data from being compromised. It helps in protecting data that is being transferred & stored in the cloud. Encryption helps in both protect unauthorized access along with prevention of data loss.

We should address how to design an efficient access structure for arbitrary access privilege construction with both time and attribute factors, especially when an access policy embeds multiple access privilege releasing time points. As an extension of the previous conference version, we give the potential sub-policies for time-sensitive data, and then present an efficient and practical method to construct relevant access structures.

Localized virtual machines and physical servers use the same operating systems as well as enterprise and web applications in a cloud server environment, increasing the threat of an attacker or malware exploiting vulnerabilities in these systems and applications remotely. Virtual machines are vulnerable as they move between the private cloud and the public cloud. A fully or partially shared cloud environment is expected to have a greater attack surface and therefore can be considered to be at greater risk than a dedicated resources environment.

IV. CONCLUSIONS

This paper aims to access control for time sensitive data in cloud storage. One challenge is to simultaneously achieve both flexible timed release and data with limited storage and infrastructure overhead. Our scheme seamlessly incorporates the concept of timed-release encryption to the architecture of cipher text policy attribute-based encryption.

V. REFERENCES

[1]. K.Yang, X.Jia, K.Ren, B.Zhang and R.Xie,"DAC-MACS: Effective data access control for multi authority cloud storage systems,"IEEE transactions on information Forensics & Security, vol. 7, 2012

[2]. Ming Li,Shucheng Yu,Yao Zheng,Kui Ren,Wenjing Lou, "Scalable and secure sharing of personal heath records in cloud computing using attribute based encryption,"IEEE transactions on parallel and distributed systems, vol 24, 2013

[3]. Elli Androulaki,Claudio Soriente,Luka malisa & Srdjan Capkun, "Enforcing location and time based access controlon cloud stored data,IEEE 34 th international conference on Distributed computing systems,2014.

[4]. Baishuang Hu, Qin Liu,Xuhui Liu,Tao Peng,Guojun Wang & Jie wu, ”DABKS:Dynamic attributebased Keyword search in cloud computing”,IEEE communication and information systems security symposium,2017

[5]. Quin Liu, Guojun Wang, & Jie wu,”Clock based proxy Re-encryption scheme in unreliable cloud,”IEEE 41st international conference on parallel processing workshops, 2012

[6]. Kan Yang, he Liu, Xiao Hua jia, “Time domain attribute based access control for cloud based video content sharing: A cryptographic approach, IEEE transaction on Multimedia, vol 18, 2016

[7]. Kui Ren, Cong Wang & Quian Wang, “Security Challenges for the Public Cloud, IEEE Computer Society, Jan2012

[8]. Cong Wang, Quian Wang & Kui Ren, ”Privacy preserving public auditing for data Storage Security in cloud Computing”,IEEE communication society,2010.

[9]. J.Bethencourt,A Sahai andb.Waters “cipher text Policy Attribute based encryption,” In proceeding of the 28thIEEE symposium on security and privacy,IEEE 2007.

[10]. R.L Rivest, A.Shamir and D.a Wagner,”Time lock puzzles and timed release Crypto,”Massachusets Institute of Technology, 1996

[11]. Gartner Inc: Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: . Accessed: 15-Jul-2011 http://www.gartner.com/it/page.jsp?id=1454221 Online. Available: . Accessed: 15-Jul-2011

[12]. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.Google Scholar

[13]. Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks (ICFN’10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.View ArticleGoogle Scholar

[14]. Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.. 2011. Available:

[15]. Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.Google Scholar