Secure Data Access Control Scheme Using Type-Based Re-encryption in Cloud Environment

Namje Park

Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju-do, 690-781, Korea
namjepark@jejunu.ac.kr

Abstract. Cloud computing service provider cannot be totally trusted due to data security reasons, risk of data security and violation of privacy factors should be considered. Especially, guaranteeing data confidentiality is required. To solve these problems, S.C. Yu etc. proposed scheme which guarantees data confidentiality and fine-grained access control. However, data confidentiality can be violated by collusion attack of revoked user and cloud server. To solve this problem, we guaranteed data confidentiality by storing and dividing data file into header and body. In addition, the method of selective delegation regarding the whole or partial message according to delegator's reliability towards delegate using type-based re-encryption was specified.

1 Introduction

Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. Especially, cloud computing is used in internet business for data storage service. Cloud computing has five kinds of characteristics (Multitenancy, Massive scalability, Elasticity, Pay-as-you-go, Self-provisioning resources). Enterprise utilizes these characteristics to increase revenue [7].

However, in spite of these useful characteristics, cloud computing should consider several issues to use your existing business environment [1]. In particular, medical data that relate to certain person must be protected to ensure data confidentiality. Thus, we focus on confidentiality. We propose secure protocol model for cloud computing environments in this paper. Also, we suggest specific models to process medical data. On the other hand, protocol model in cloud computing environments must be guaranteed to fine-grained access control as well as data confidentiality. For example, access control should be differentiated by user's attribute such as positions (doctor, nurse, etc). In addition, it must be able to revoke decryption right for data access. Thus, user revocation would require re-encryption of data files accessible to the leaving user.

To ensure these requirements, [6] proposed system model using Key Policy-Attribute Based Encryption (KP-ABE) and Proxy Re-Encryption (PRE). Formally, [6] ensure data confidentiality using KP-ABE and data owner delegate computation overload to proxy using PRE. Also, [6] introduce user revocation on system model. But, proposed scheme is vulnerable to collusion attack of revoked user and cloud server.

R. Katarzyniak et al. (Eds.): Semantic Methods, SCI 381, pp. 319–327.
springerlink.com

And there is no selective delegation for level of trust. To resolve these challenges, we divide data files stored on the cloud servers into header, body in [6]. Decryption rights such as head (encrypted key using KP-ABE) and body (encrypted message using symmetric encryption) is concentrated to cloud servers in [6]. For this reason, cloud server is the most powerful. This paper begins to point that cloud servers can't be trusted. So we create the trusted authority named privilege manager to manage header. And body is stored on the cloud servers like existing way. Thus, we will split the power that concentrated to cloud servers. Also we introduce data access privilege management model using Type-based Proxy Re-encryption's concept in mobile cloud environments. Finally, we show scenario about privacy preserving data sharing in health cloud environments and analyze security against collusion attack.

2 Related Work

2.1 Bilinear Mapping

Let G and G_T be two cyclic multiplicative groups with the same prime order q. A bilinear pairing is a map $e: G \times G \rightarrow G_T$ with the following properties:

- Bilinearity: $\forall g_1, g_2 \in G, \forall a, b \in Z_q^*$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
- Non-degeneracy: There exist $g_1, g_2 \in G$ such that $e(g_1, g_2) \neq 1$.
- Computability: There exists an effcient algorithm to compute $e(g_1, g_2)$ for $\forall g_1, g_2 \in G$.

2.2 Attribute Based Encryption

Attribute Based Encryption is classified as CP-ABE (Cipher-text Policy-Attribute Based Encryption) [3] and KP-ABE (Key Policy-Attribute Based Encryption) [8]. In this paper, we should take advantage of KP-ABE. Data are encrypted by set of attributes and user secret key are associated with access structure in KP-ABE. In access structure, internal nodes are threshold gates and leaf nodes are associated with attributes which is used to encrypt data. Thus, if encrypted data's attribute satisfy user secret key's access structure, user is able to decrypt a cipher-text. Formally, KP-ABE is used to encryption and decryption for Data Encryption Key (DEK) in proposed scheme.

2.3 Proxy Re-encryption

Proxy Re-Encryption is cryptographic scheme in which proxy is able to convert cipher-text encrypted under Alice's public key into cipher-text that can be decrypted by Bob's secret key. But, proxy is semi-trusted server so that proxy server should not be seen original plaintext in PRE. Formally, user should update header's secret key component using [5] in proposed scheme.

2.4 Existing Study for Cloud Computing

[6] forecasted that existing business environment will move to cloud computing environment, and proposed a system model which can guarantee data confidentiality. The