클라우드 환경에서 속성 재암호 기반의 데이터 공유 기법1)

김수현, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[kimsh, imylee]@sch.ac.kr

Data Sharing Scheme based on Attribute Re-Encryption in Cloud Computing

Su-Hyun Kim, Im-Yeong Lee
Department of Computer Software Engineering Soonchunhyang University

약

클라우드 컴퓨팅 환경에서는 사용자의 데이터를 수많은 분산서버를 이용하여 데이터를 암호화하여 저장한다. 이러한 클라우드 스토리지에 사용자의 수많은 데이터가 저장됨에 따라 클라우드 스토리지의 신뢰성에 문제가 발생하고 있다. 비신뢰적인 관리자 및 공격자로부터 클라우드 서버에 저장된 사용자의 데이터를 안전하게 저장하기 위한 다양한 암호 기술들이 계속해서 연구되고 있다. 하지만 기존의 데이터 암호 기술들은 클라우드 스토리지 상에서 여러 사용자 간의 데이터 공유 서비스에 적용하기 힘든 단점을 가지고 있다. 따라서 본 논문에서는 비신뢰적인 클라우드 스토리지를 고려하여 속성기반 암호로 암호화된 키를 재암호화하여 다른 사용자와 안전하고 효율적으로 공유할 수 있는 데이터 공유 기법을 제안한다.

1. 서론

비신뢰적인 관리자 및 공격자로부터 클라우드 서버에 저장된 사용자의 데이터를 안전하게 저장하기 위한 다양한 암호 기술들이 계속해서 연구되고 있다. 하지만 기존의 데이터 암호 기술들은 클라우드 스토리지 상에서 여러 사용자 간의 데이터 공유 서비스에 적용하기 힘든 단점을 가지고 있다. 이러한 문제점들을 해결하기 위해 가장 기본적인 방법으로 저장된 데이터에 대한 암호화를 통해 관리할 수 있다. 하지만 기존의 단순한 암호화 방식은 클라우드 환경에 저장된 데이터의 접근 관리에 따른 문제점이 발생한다. 즉, 사용자들은 클라우드 서버에 저장된 데이터에 다수의 사용자가 접근하기를 원하거나, 사용자의 등급별 접근제어 등 다양한 기능을 요구하게 된다. 하지만 기존의 공개키 암호나 대칭키 암호기법으로는 키 관리의 문제점과 접근제어와 같은 요구사항을 충족시켜 줄 수 없다.

따라서 본 논문에서는 비신뢰적인 클라우드 스토리지를 고려하여 속성기반 암호로 암호화된 키를 재암호화하여 다른 사용자와 안전하고 효율적으로 공유할 수 있는 데이터 공유기법을 제안한다.

1) 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음. (IITP-2015-H8501-15-1008)

2. 제안방식

2.1 시스템 모델

본 제안방식에서는 사용자 속성의 폐기과정이 필요 없는 데이터 공유 기법을 제안하였다. 공유 받고자 하는 사용자 B의 속성 공개키를 기반으로 사용자A가 자신의 속성으로 암호화된 데이터를 복호화할 수 있는 암호키를 재암호화 하여 사용자 B에게 전달해 주는 기법이다. 따라서 본 제안방식에서는 불필요한 과정을 줄임으로써 효율성을 제공하고, 보다 안전하게 데이터를 공유할 수 있다.

(1) Setup

보안 파라미터 k를 입력하여 그 값에 대응하는 공개키 PK와 마스터키 MK를 출력한다.

1) $G = [p, G, G_T, g \in G, e] \leftarrow \geq n(1^k)$

랜덤값 $w \in Z_p^*$를 생성한다.

2)속성 $i, (1 \leq i \leq n)$에 대응하는 랜덤한 $a_i, \widehat{a_i}, a_i^* \in Z_p^*$를 선택한다.

3) $Y = e(g,g)^w$와

$A_i = g^{a_i}, \widehat{A_i} = g^{\widehat{a_i}}, A_i^* = g^{a_i^*}$를 계산한다.

4) PK는 $< Y, p, G, G_T, g, e(A_i, \widehat{A_i}, A_i^*)_{1 \leq i \leq n} >$이고,

MK는 $< w,(a_i,\hat{a_i},a_i^*)_{1 \le i \le n} >$이다.

(2) KeyGen
마스터키 MK와 속성 집합 L을 입력하여 접근구조에 대응하는 비밀키 SKL을 출력하는 알고리즘이다.
1)속성집합 $L=[L_1,L_2,....,L_n]$을 입력하여 비밀키를 생성한다.

2)$s_i \in Z_p^*$를 랜덤하게 선택하고 $s=\sum_{i=1}^{n} s_i, D_0=g^{w-s}$를 계산한다.

3)만약에 $L_i=1$ 이면, $[D_i,D_i^*]=[g^{\frac{s_i}{\hat{a_i}}},g^{\frac{s_i}{a_i^*}}]$를 계산하고,

$L_i=0$이면, $[D_i,D_i^*]=[g^{\frac{s_i}{\hat{a_i}}},g^{\frac{s_i}{a_i^*}}]$를 계산한다.
4) 비밀키는 $SK_L =< D_0,(D_i,D_i^*)_{1 \le i \le n} >$이다.

(3) Encrypt
공개키 PK와 접근구조 W와 평문 M을 입력하여 그 평문에 대응하는 암호문 CT를 출력하는 알고리즘이다.
1)접근 구조 $W=[W_1, W_2,..., W_n]$와 평문 M을 암호화 한다.
2) 랜덤 값 $r \in Z_p^*$과 $\tilde{C}=MY^T, C_0=g^r$를 계산한다.
3)다음을 만족하는 $C_i : W_i=1, C_i=A_i^r, W_i=0$ $C_i=\widehat{A_i^r}, W_i=*, C_i=A_i^{*r}$'를 계산한다.
4) 암호문은 $CT=< \tilde{C}, C_0,(C_i)_{1 \le i \le n} >$이다.
5) $di=H(CT)$
$A=pk^{di}$
$B=e(g,g)^{SK_{La}} \cdot di$
$C=e(g,H(pk))^{di} \cdot m$
$E_a=(A,B,C)$

6) E_a를 클라우드 스토리지에 저장한다.

(4) ReKey Generation
사용자 A는 데이터를 공유하고자 하는 사용자 B의 속성 공개키를 이용하여 데이터를 복호화 할 수 있는 암호키를 재암호화하여 전달해준다.
1)$A'=pk_b^{di}$
$rk_{a\to b}=(A',pk_b^{-sk_{La}})$
$B'=e(A,rk_{a\to b})$
$E_b=(A',B',C)$

4. 제안방식 분석

제안 방식은 데이터 공유 과정에서 페어링을 이용하여 악의적인 제3자가 클라이언트와 서버 간의 통신을 도청한다고 해도 통신 내용을 유추하기 어렵다. 또한, 사용자 A의 암호키를 재암호화하는 과정에서 재암호화키 $rk_{a\to b}=(A',pk_b^{-sk_{La}})$는 데이터 공유 시 일회성을 제공하는 키로써, 공유 받는 대상인 사용자 B는 지속적으로 사용이 불가능하다. 따라서, 후방향 안전성 또한 제공이 된다.

5. 결론 및 향후 연구 방향

본 논문에서는 비신뢰적인 클라우드 스토리지를 고려하여 속성기반 암호로 암호화된 키를 재암호화하여 다른 사용자와 안전하고 효율적으로 공유할 수 있는 데이터 공유기법을 제안하였다. 이처럼 클라우드 환경에서 세밀한 사용자 접근제어와 데이터 공유를 가능하게 함으로써, 클라우드 서버에 저장되는 민감한 정보들을 보다 안전하게 관리할 수 있다. 제안 프로토콜은 기밀성이 높은 데이터, 사용자의 개인정보를 포함하는 다양한 대용량 데이터를 안전하고 효율적으로 공유하는 구조로서 클라우드 컴퓨팅 환경에서 보다 효율적으로 사용될 것으로 기대한다.

참고문헌

[1] A. Sahai and B. Waters, "Fuzzy identity- based encryption," Proc. of Eurocrypt'05, LNCS 3494, pp. 457-473, 2005.

[2] Shamir, Adi. "Identity-based cryptosystems and signature schemes." Advances in cryptology. Springer Berlin Heidelberg, 1985.

[3] D. Hubbard and M. Sutton, "Top threats to cloud computing," in Cloud Security Al liance,Mar.2010.

[4] Ming, et al. "An efficient attribute based encryption scheme with revocation for outsourced data sharing control.", IEEE, 2011.