클라우드 환경에서 데이터 접근 사용자의 프라이버시 보호를 위한 익명 CP-ABE 기법에 관한 연구+

황용운, 이임영
순천향대학교 컴퓨터학과
e-mail:[hwy0123, imylee]@sch.ac.kr

A Study on Anonymous CP-ABE Scheme for Privacy Protection of Data Access Users in Cloud Environments

Yong-Woon Hwang, Im-Yeong Lee
Dept of Computer Science Engineering, Soonchunhyang University

요 약

최근 클라우드에서 발생하는 보안위협을 해결하기 위한 다양한 보안 기술 중 속성기반 암호인 CP-ABE 방식의 접근제어 기법을 사용하여 사용자간의 데이터를 안전하게 공유한다. 현재까지 다양한 CP-ABE방식의 접근제어 기법이 연구되었지만, 이 중 보안위협에 취약한 방식들이 존재한다. 특히 제3자는 암호문에 지정된 접근구조를 통해 데이터에 접근하려는 사용자의 속성을 유추할 수 있고, 이로 인해 사용자의 프라이버시를 침해할 수 있다. 이에 사용자의 프라이버시를 보호할 수 있는 익명 CP-ABE 방식이 연구되고 있다. 하지만 기존에 연구된 익명 CP-ABE 방식 중 제대로 익명화가 적용되지 않은 방식과, 효율성이 부족한 방식들이 존재한다. 이에 복호화하는 사용자의 연산량은 증가된 암호문의 속성의 개수에 비례하기 때문에 비효율적이다. 본 논문에서는 데이터에 접근하는 사용자의 프라이버시를 보호하고, 사용자의 연산량의 효율을 높일 수 있는 익명 CP-ABE 방식을 제안한다.

1. 서론

최근 발달된 클라우드 컴퓨팅에는 다양한 보안위협이 존재한다. 특히 서비스 제공업체를 완전히 신뢰할 수 없으며, 악의적인 사용자로 인해 데이터가 유출되거나 손실 될 수 있다. 이에 다양한 보안기술 중 속성기반암호의 한 종류인 CP-ABE(Ciphertext-Policy Attribute Based Encryption)를 사용하여 클라우드 환경에서 데이터에 안전하게 접근하거나, 공유한다. 하지만 기존의 연구된 CP-ABE 방식들 중 다양한 보안위협에 취약한 방식들이 존재한다. 특히 암호문에 지정된 Access policy 부분을 통해 암호문에 접근하려는 사용자를 유추하여, 사용자의 프라이버시를 침해할 수 있다. 예를 들어 Access policy에 환자의 데이터 [Patient:LIS123], [질병명] 등이 포함되어 있고, 이 외에 환자와 관련된 속성이 포함되어 있다고 가정하자. 이를 통해 제 3자는 LIS123 환자가 질병을 앓고 있는 것을 유추할 수 있다. 이에 기존 CP-ABE 방식에서 암호문을 생성시 접근구조(Access policy)에 익명화를 주는 연구가 진행되고 있다[1][2]. 하지만 기존에 연구된 익명 CP-ABE 방식에서 Access policy에 대한 익명화가 적용되지 않은 방식들이 존재한다. 또한 암호문 생성시 Access policy에 지정된 속성의 개수가 증가함에 따라 암호문의 크기가 증가하기 때문에, 스토리지 공간을 낭비할 수 있으며, 이에 사용자가 암호문 복호화시 필요한 연산량은 증가할 것이다. 이에 연산량을 효율적으로 줄 일 수 있는 익명 CP-ABE 방식이 필요하다. 본 논문에서는 익명 CP-ABE 방식을 제안하여 클라우드 환경에서 저장된 데이터에 접근할 수 있는 사용자들의 프라이버시를 보호한다. 또한 암호문 생성시 일정크기의 암호문을 출력함으로써 스토리지의 공간을 효율적으로 사용하며, 사용자의 복호화하는 연산량을 감소시켜, 전체적으로 효율성을 높인다. 본 논문에서 제안하는 환경은 민감한 데이터를 관리하는 클라우드에 적용이 가능하다.

2. 관련연구

2.1 CP-ABE

CP-ABE 방식은 데이터 소유자가 암호문을 생성 할 때 자신의 데이터에 접근하려는 사용자의 속성 [Hospital A], [Doctor], [Nurse]을 가지고 접근구조를 생성하여 데이터를 암호화한다. 이후 수신자에게 암호문을 전송하고 수신자는 자신의 속성 집합 [Hospital A, Doctor]에 따라 암호문을 해독합니다[2].

+이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2016R1D1A1B03935917)

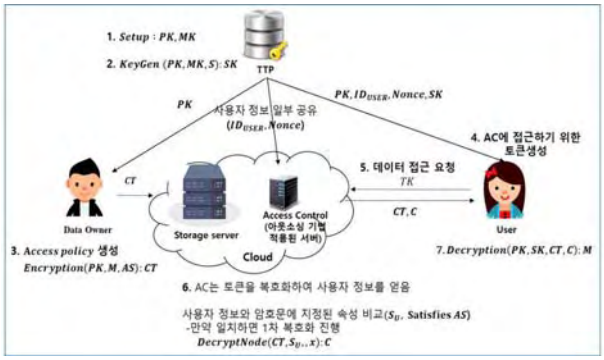

그림 1 제안방식 시나리오

3. 제안방식

본 제안방식은 클라우드 환경에서의 데이터에 접근하는 사용자의 프라이버시 보호를 위한 익명 CP-ABE방식을 제안한다.(그림 1). 제안방식은 초기단계, 데이터 암호화 단계, 사용자 데이터 접근 단계로 구성된다.

4.1 초기 단계

초기에 사용자는 TTP에 등록을 요청한다. 이후 사용자가 TTP에게 비밀키를 요청했을 때, TTP는 사용자의 속성을 가지고 비밀키를 생성한다. 비밀키 생성 후 TTP는 안전한 채널을 통해 데이터 소유자에게 PK 사용자에게 비밀키와 $PK, ID_{USER}, NONCE, SK$를 전송해준다.

- Setup단계 : 공개파라미터 PK, MK 생성
- $KeyGen(PK, MK, S) = SK$: 속성의 집합 S와 마스터키, PK를 통해 비밀키 SK를 생성

4.2 데이터 암호화 단계

데이터 소유자는 TTP로부터 받은 정보와 클라우드 환경 내에서 자신의 데이터에 접근 가능한 사용자의 속성을 기반으로 접근구조를 만든다. 이후 데이터를 암호화시 접근구조의 저장된 속성들의 멀티값을 조건에 맞게 계산하고 이를 통해 암호문 CT를 생성하여, 클라우드 스토리지에 저장한다. 기존 암호문 CT에는 접근구조(Access policy)가 포함되어 있기에 데이터에 접근하려는 사용자의 속성을 추측할 수 있다. 하지만 본 제안방식의 암호문에는 접근구조를 포함하지 않기 때문에, 데이터에 접근하는 사용자의 속성(프라이버시)를 보호할 수 있다.

- $Encrypt(PK, AS, m) = CT(C_0, C_1, C_2)$
  - AS는 접근구조로써 Access policy와 같이 표현됨

4.3 사용자 데이터 접근 단계

사용자가 TTP로부터 전송받은 정보를 통해 TK를 생성하여 클라우드 스토리지에 접근한다. AC에서 사용자가 접근하려는 암호문에 지정된 AS의 속성값과 사용자 속성을 연산하여 비교함으로써 1차 복호화를 진행한다. 이후 1차 복호화된 결과물과 암호문을 사용자에게 전송하고, 사용자는 비밀키 SK를 통해 암호문을 최종복호화하여 메시지 M을 획득한다.

- $Paritial\ decrypt(CT, S) = C$
- $Final\ decrypt(PK, C, SK, CT) = M$

4. 제안방식 분석

· 사용자 프라이버시 보호 : 본 제안방식은 다음과 같이 암호문 $CT(C_0, C_1, C_2)$에서 Access policy를 공개하지 않는다. Access policy가 비공개되어 있기 데이터 소유자 외에 아무도 알 수 없으며, 이는 데이터에 접근할 수 있는 사용자의 속성(프라이버시)를 보호할 수 있다.

· 연산의 효율성 : 본 제안방식은 암호문 생성시 지정된 속성의 수를 하나로 합쳐 고정된 크기의 암호문을 출력함으로써 스토리지의 공간을 최대한 활용할 수 있으며, 이로 인해 사용자가 복호화시 연산량을 줄일 수 있다. 또한 아웃소싱 기법이 지원된 AC Server에서 사용자의 복호화 연산량의 일부를 지원해준다. 이에 기존에 연구된 익명 CP-ABE 방식의 연산량과 비교해 사용자가 암호문을 복호화하는데 필요한 연산량은 감소되며, 연산의 효율성을 높일 수 있다.

5. 결론

클라우드 환경에서 저장된 데이터에 접근할 수 있는 사용자의 프라이버시 보호를 위해 본 논문에서는 연산의 효율성을 높인 익명 CP-ABE 방식을 제안하였다. 제안방식은 다양한 보안위협에 안전하며, 암호문 생성시 Access policy를 숨김으로써 데이터에 접근하는 사용자의 속성에 익명성을 제공한다. 그리고 클라우드 스토리지의 공간을 효율적으로 사용할 수 있으며, 사용자 측면에서 복호화 진행시 복호연산의 일부를 AC에서 아웃소싱 하여 연산함으로써 사용자에게 연산의 효율을 높일 수 있다.

향후 연구로는 현재 연구한 익명 CP-ABE 접근 기법을 기반으로 프로그래밍을 진행하여 세부적으로 연산량을 측정하고 비교할 것이며, Access policy의 일부만 숨길 수 있는 부분 익명성에 대한 연구가 필요할 것으로 사료된다.

참고문헌

[1] Zhang, Yinghui, et al. "Anonymous attribute-based encryption supporting efficient decryption test." Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM, pp. 511-518, 2013.

[2] Zhang, Leyou, Yilei Cui, and Yi Mu. "Improving Privacy-Preserving CP-ABE with Hidden Access Policy." International Conference on Cloud Computing and Security. Springer, Cham, pp. 596-605, 2018.