클라우드 환경에서 KP-ABSKE 기반의 데이터 접근기법에 관한 연구

황용운*, 이임영*, 서대희**
*순천향대학교 소프트웨어융합학과
**상명대학교 지능데이터융합학부
*hwy0123@sch.ac.kr, *imylee@sch.ac.kr, **daehseo@smu.ac.kr

A study on the data sharing system based on KP-ABSKE in the cloud environment

Yong Woon Hwang*, Im Yeong Lee*, Dae hee Seo**
*Department of Software Convergence, Soonchunhyang University
**Faculty of Artificial Intelligence and Data Engineering, Sangmyung University

요 약

최근 발달하고 있는 클라우드 환경에서도 데이터 위변조 및 유출 등 다양한 보안위협이 존재하기 때문에 클라우드 서버에 데이터를 암호화하여 저장하는 것이 중요하며, 사용자가 암호화된 데이터에 접근하기 위한 접근제어 기법이 중요하다. 다양한 보안기술 중 속성기반 암호의 한 종류인 KP-ABE와 검색가능 암호를 활용한 방식인 KP-ABSKE를 클라우드 환경에 사용하여 데이터 암복호화 및 접근제어를 수행하고 있다. 하지만 기존 KP-ABSKE 방식들은 암호문의 크기가 속성의 개수에 비례하여 커지기 때문에, 스토리지의 공간을 낭비할 수 있으며, 암호문을 탐색하는 과정에서 키워드의 개수에 따라 암호문 탐색의 연산량이 증가하기 때문에 비효율적이다. 이에 본 논문에서는 KP-ABSKE 기반의 데이터 공유 시스템 기법으로 앞서 요구된 문제를 해결하기 위해 고정크기 암호문 출력, 키워드 집계연산을 통한 탐색속도 효율성 증가를 목표로 안전한 데이터 접근제어 시스템을 제안하는 것이 목표이다.

Ⅰ. 서 론

최근 클라우드 컴퓨팅의 발달로 사람들은 클라우드를 활용하여, 데이터를 서버(스토리지)에 저장하거나 공유할 수 있다. 하지만 클라우드 환경에서도 서비스 제공업체를 완전히 신뢰할 수 없으며, 악의적인 사용자로 인해 데이터가 유출되거나 손실될 수 있는 등 다양한 보안위협이 존재한다. 이를 해결하기 위한 다양한 보안기술 중 속성기반 암호는 데이터 암복호화와 접근제어 두가지 기능 수행할 수 있는 암호 기술로써, 속성기반 암호의 한 종류인 KP-ABE(Key-Policy Attribute Based Encryption)를 활용한 데이터 접근제어 기법이 현재 많이 연구되고 있다[1]. 특히 클라우드에서 암호문을 탐색하는 과정인 검색가능 암호를 같이 활용한 KP-ABSKE(Key-Policy Attribute Based Searchable Keyword Encryption)를 다양한 클라우드 분야에서 사용되고 있다[2]. 하지만 기존에 연구된 KP-ABSKE 방식들은 데이터 소유자가 생성한 암호문의 크기가 암호문에 포함된 속성의 개수에 비례하여 커지기 때문에, 스토리지의 공간을 낭비할 수 있으며, 사용자의 복호화 연산량의 크기 때문에 컴퓨팅 성능에 부담이 있는 사용자에게는 비효율적이다. 또한 클라우드에서 암호문을 탐색하는 과정에서 탐색 횟수가 키워드 개수에 비례하기 때문에 비효율적이다. 이에 속성개수와 상관없이 고정적으로 출력되는 암호문과, 키워드 집계연산을 통해 암호문 탐색을 1번의 연산으로 탐색하는 것이 효율적이다[3].

본 논문은 KP-ABSKE 기반의 데이터 접근기법에 관한 연구로써, 기존의 KP-ABSKE에서 발생하는 문제점을 앞서 언급한 고정크기 암호문, 키워드 집계연산을 통한 암호문 탐색의 효율성 등의 요구사항을 제공하여 클라우드 환경에서 안전하고 효율적인 데이터 공유 시스템을 제안한다.

Ⅱ. 제안방식

본 장에서는 클라우드 환경에서 KP-ABSKE 기반의 데이터 접근기법에 관한 기법을 제안한다.

Step 1~2. AA에서 Setup 과정을 수행하여, 공개파라미터와 마스터키를 생성하여 데이터 소유자에게 공개파라미터를 전송한다. 이후 사용자가 비밀키를 요청하기 위해 자신의 속성으로 접근구조를 만들어 AA에게 보내고, AA는 사용자가 보내준 접근구조 AS에 대응되는 비밀키를 생성하여, 사용자에게 공개파라미터와 비밀키 SK를 전송해준다(그림 1의 1~2).

- $Setup(k) = PK, MK$
- $KeyGen(PK, MK, AS) = SK$

Step 3. 데이터 소유자는 사용자의 속성집합 $S = [a_1, a_2, \ldots a_n]$을 기반으로 데이터 암호화를 수행하는데, 아래의 수식 C_2과 같이 다수의 속성집합의 수식을 하나의 수식으로 연산하여 표현함으로써, 암호문의 크기를 고정적으로 출력한다. 그리고 각 암호문을 표시할 수 있는 키워드를 수집하여 연산을 통해 키워드 기반의 인덱스 값 I_W을 생성하고, 암호문과 함께 클라우드 서버에 전송하여 저장한다(그림 1의 3).

- $Encrypt(PK, M, S) = CT$
  - $CT = < S, C_0, C_1, C_2, C_3 >$, $I_W = < \widetilde{C_1}, \widetilde{C_2}, C_3 >$

Step 4. 사용자는 AA로부터 수신받은 비밀키를 가지고, 클라우드에 접근하기 위한 토큰을 생성한다. 토큰에는 사용자의 속성값들과 암호문을 표시할 수 있는 키워드들의 집계연산된 값이 포함되어 있으며, 사용자는 클라우드 서버에 토큰을 보내, 암호문을 요청한다(그림 1의 4).

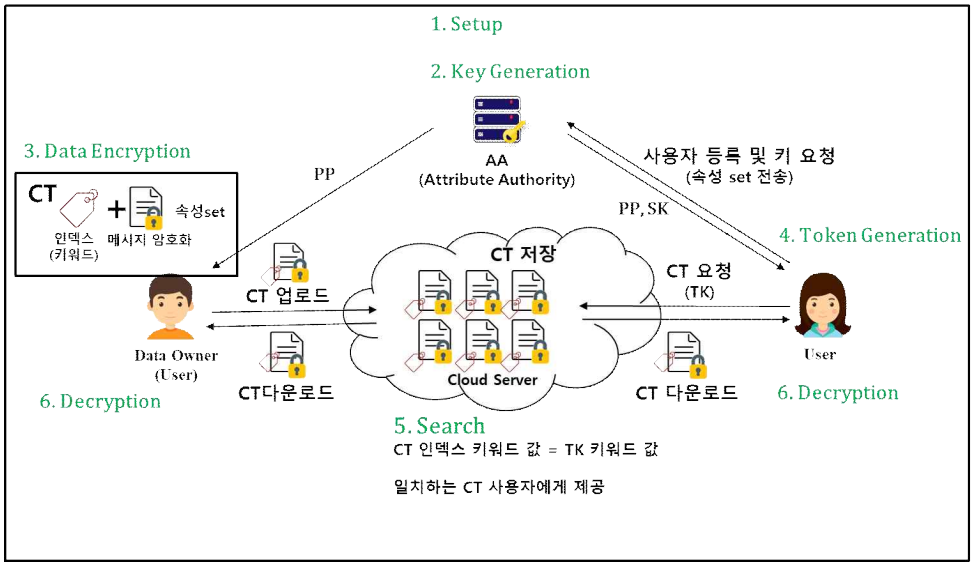

그림 1. KP-ABSKE 전체 시나리오

• $Trapdoor(SK, W) = T_W = e(\prod_{i=1}^{n} H_1(x_i)^{\beta}, g^W)$

Step 5. 클라우드 서버는 사용자로부터 수신받은 토큰을 가지고, 사용자가 요청한 암호문을 집계된 키워드를 통해 탐색하여, 사용자에게 전송해 준다(그림 1의 5).

• $Search(I_W, T_W) : e(\widetilde{C_2}, T_W) = e(C_3, \widetilde{C_1})$

Step 6. 사용자는 자신의 접근구조와 암호문에 포함된 속성값과 비교하여 속성값이 일치(만족)하면 비밀키 SK를 통해 복호화를 수행한다. 올바르게 복호화가 진행되면 사용자는 메시지 M을 획득할 수 있다(그림 1의 6).

• $Decrypt1(CT, AS, x) = C$

• $Decrypt2(PK, SK, CT, C) = M$

- $M = C_0 / (e(C_1, D_i) \cdot C^s)$

Ⅲ. 제안방식 분석

• 공유 데이터 무결성 및 기밀성 제공: 본 제안방식은 데이터를 KP-ABSKE를 활용하여 암호화하고 저장 및 공유하기 때문에 데이터에 대한 기밀성과 무결성이 제공된다. 데이터는 속성으로 암호화되어 있기 때문에, 이를 복호화하려는 사용자 중 암호문에 포함된 속성을 내포한 접근구조를 가진 정당한 사용자 외에 복호화 할 수 없다.

• Search efficiency: 클라우드에 저장된 수많은 암호화 데이터 중 사용자가 원하는 데이터를 탐색할 시 모든 데이터가 암호화되어 있기 때문에 탐색하기 어렵다. 이에 암호문을 복호화하여 사용자가 원하는 데이터를 확인하여야 하며, 이는 비효율적이다. 본 제안방식은 데이터가 암호화된 상태에서 사용자가 원하는 데이터를 탐색할 수 있는 연구인 검색가능 암호 기술이 적용되어 있다. 다중키워드 사용시 키워드 집계연산을 수행하기 때문에 탐색속도가 키워드 개수에 비례하지 않으며, 이는 기존의 KP-ABSKE과 비교하여 탐색속도가 빠르다.

• 클라우드 스토리지 공간 낭비: 기존의 연구된 KP-ABE 방식들의 암호문의 크기는 속성의 수에 비례하여 선형적으로 증가하고, 이에 따라 암호문이 저장된 클라우드 스토리지 공간은 비효율적이다. 본 제안방식은 암호문을 다수의 속성값을 하나의 수식으로 연산함으로써, 속성개수에 상관없이 암호문의 크기가 고정적으로 출력함으로써, 기존의 암호문이 저장시 낭비된 스토리지를 효율적으로 사용 가능하다.

Ⅳ. 결론

본 논문에서는 클라우드 환경에서 KP-ABSKE 기반의 데이터 접근기법을 제안하였다. 제안방식은 속성기반암호의 한 종류인 KP-ABE 방식과 검색가능암호를 활용하여, 데이터 소유자가 업로드한 데이터에 대한 기밀성 및 무결성을 제공할 수 있다. 또한, 암호문에 포함된 속성을 가진 사용자만이 암호문을 풀 수 있는 권한이 있기 때문에, 정당한 사용자만이 암호문에 접근하여 데이터 복호화할 수 있다. 그리고 기존의 KP-ABE에서 발생되는 암호문 크기가 속성의 개수에 비례하여 커지는 문제는 고정크기 암호문 출력으로, 다중키워드 개수에 따라, 클라우드 서버에서 암호문을 탐색하는 횟수가 증가하는 문제점들은 키워드 집계연산을 통해 해결하였다.

향후 연구로는 클라우드에 저장된 데이터를 사용자가 복호화하여 획득하였을 때, 획득한 데이터가 데이터 소유자가 업로드한 데이터인지 확인할 수 있는 사인크립션이나, 서명에 대한 연구가 필요할 것으로 사료된다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음 (2021-0-01516)

참 고 문 헌

[1] 박광용, 송유진. "속성기반 암호기술." 정보보호학회지, 제20호 2권, pp. 85-92, 2010.

[2] Yin, H., Xiong, Y., Zhang, J., Ou, L., Liao, S., Qin, Z. "A key-policy searchable attribute-based encryption scheme for efficient keyword search and fine-grained access control over encrypted data." Electronics, 8(3), 265, 2019.

[3] Wang, H., Dong, X., & Cao, Z. "Multi-value-independent ciphertext-policy attribute based encryption with fast keyword search." IEEE Transactions on Services Computing, 2017.