클라우드 스토리지 구조를 고려한 안전한 데이터 공유 방법에 대한 연구*

이선호, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[sunho431, imylee]@sch.ac.kr

A Study on Secure Data Sharing Method for Cloud Storage Structure

Sun-Ho Lee, Im-Yeong Lee
Dept. of Computer Software Engineering, Soonchunhyang University

요 약

디지털 정보량의 증가 추세에 맞추어 네트워크를 통해 자신의 데이터를 원격 저장소에 저장하고, 이를 다양한 디바이스를 통해 언제 어디서나 접근할 수 있는 클라우드스토리지 서비스가 등장하게 되었다. 이는 기존에 데이터를 휴대하기 위해 사용되던 이동식 저장매체와 달리 저장용량의 크기 제한이 없고, 저장매체를 소지해야 하는 문제점이 없어 많은 사용자로부터 사용되고 있다. 이러한 클라우드 스토리지에 여러 사용자의 데이터가 저장됨에 따라 클라우드 스토리지의 신뢰성 문제가 이슈화 되고 있다. 비윤리적인 관리자 및 공격자로부터 클라우드에 저장된 데이터를 안전하게 보호하기 위해 다양한 암호 기술을 클라우드 스토리지에 적용하려는 연구가 진행되고 있다. 하지만 기존의 검색가능 암호 기술은 사용자가 저장하고자 하는 데이터를 직접 업로드하고, 해당 자료를 필요에 따라 공유 하고, 공유대상이 변화되는 클라우드 스토리지 환경에서 비효율성을 가지고 있어 실제 서비스에 적용하기 힘든 단점을 가지고 있다. 따라서 본 논문에서는 클라우드 컴퓨팅 환경을 고려하여 검색 가능한 암호화 색인 생성 및 이를 재암호화해 다른 사용자와 안전하게 공유할 수 있는 색인 관리 기법을 제안한다.

1. 서론

데이터를 휴대할 수 있도록 하는 이동식 저장매체의 발전되었다. 이러한 이동식 저장매체는 높은 휴대성으로 인해 분실 및 도난의 위험이 높으며, 이로 인하여 저장되어 있던 개인 정보가 유출되는 문제가 이슈화 되고 있다. 네트워크의 발달로 빠른 데이터 통신이 가능해짐에 따라 자신의 데이터를 원격 저장소에 저장하고 언제 어디서나 다양한 디바이스를 통해 자신의 데이터에 접근할 수 있는 클라우드 컴퓨팅 서비스가 등장하게 되었으며, 최근 다양한 업체에서 경쟁적으로 고용량의 클라우드 스토리지를 무료로 제공하고 있다. 따라서 현재 클라우드 스토리지 서비스를 이용하는 사용자가 급증하고 있으며, 수많은 사용자들의 데이터가 클라우드 스토리지에 저장되고 있다. 실제로 Research Institute의 조사에 따르면 69%의 미국인이 클라우드 컴퓨팅을 사용하고 있다고 조사되었다. 이렇게 여러 사용자의 주요 자료가 클라우드에 저장됨에 따라 big brother problem이 우려되며, 공격자 및 비윤리적인 관리자로 인한 자료 유출 문제가 발생할 수 있는 가능성을 가지고 있다. 이러한 문제점을 해결하기 위해서 데이터를 암호화 하는 방법이 있지만 이는 데이터 접근을 어렵게 하는 문제점을 가지고 있다. 따라서 데이터의 색인을 서버에 암호화하고, 공격자 및 비윤리적인 관리자로부터 데이터 정보를 노출하지 않고 색인을 검색할 수 있는 검색 가능한 암호시스템(searchable encryption system)이 등장하게 되었다[1-8].

하지만 이 방식은 사용자간 데이터 공유가 빈번하게 일어나는 클라우드 환경에 적용키 어렵다. 이어서 클라우드 스토리지에서 안전한 데이터 공유를 위해 암호화된 색인을 복호화 과정 없이 공유하고자 하는 대상이 검색할 수 있도록 재암호화 해주는 검색가능한재암호시스템(searchable re-encryption system)이 등장했다[9]. 하지만 기존의 방식은 데이터를 공유 받은 사용자가 공유 받은 데이터를 또 다른 사용자와 공유하는 과정을 고려하지 않았으며, 클라우드 스토리지의 구조를 고려하지 않아 색인 및 데이터의 암호화를 분할하지 않고 일괄 처리 하고 있다. 하지만 실제 클라우드 스토리지는 색인 및 데이터 정보를 저장하는 마스터 서버와 데이터를 저장하는 서버가 분리되어 있어 해당 방식을 적용키 어렵다. 따라서 본 논문에서는 클라우드 스토리지 구조를 고려하여 안전하게 클라우드 사용자의 데이터를 공유할 수 있는 색인 관리 기법을 제안하고자 한다.

2. 요구사항

검색가능 암호 시스템은 아래와 같은 요구사항을 만족해야한다.

- 기밀성: 원격 데이터 서버와 클라이언트 단말기 간의

* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2010-0022607)

통신 데이터는 정당한 개체만이 확인할 수 있어야 한다.

- 검색 속도: 제한적 시스템 자원을 가지는 클라이언트에서도 클라우드-스토리지 시스템에 저장된 문서에서 검색하고자 하는 워드를 포함하는 문서를 빠르게 검색할 수 있어야 한다.
- 통신량: 클라이언트와 서버간의 에너지 효율 및 네트워크 자원의 효율성을 위하여 통신량이 적어야 한다.
- 연산 효율성: 색인의 생성 및 검색을 수행하기 위한 연산의 효율성이 제공되어야 한다. 또한 데이터를 다른 사용자와 안전하게 공유하기 위한 연산의 효율성이 제공되어야 한다.
- 사용자간 공유 효율성: 원격 데이터 서버에 저장된 암호화 데이터를 신뢰 할 수 없는 서버로부터 안전하고 효율적으로 공유 대상자에게 공유할 수 있어야 한다. 클라우드 서비스 제공자는 사용자가 공유를 원하는 데이터만 안전하게 공유 할 수 있도록 해야 한다.

3. 제안방식

앞서 정의된 요구사항을 만족하기 위해 본 논문에서 다음과 같은 방식을 제안한다.

3.1 시스템 계수

먼저 제안방식은 다음과 같은 시스템 계수를 사용한다.

- p: 소수
- G: p를 법으로 하는 덧셈군
- g: G의 생성자
- e: 겹선형 사상, $G \times G \rightarrow G_T$
- sk_*: *의 개인키
- pk_*: *의 공개키
- m: 평문 데이터
- c: 암호화 데이터
- w_*: m의 *번째 키워드
- n: m의 키워드 개수
- di: 데이터 식별자
- $H_1()$: 해시함수, $\{0,1\}^* \rightarrow G$
- $H_2()$: 해시함수, $\{0,1\}^* \rightarrow G$
- $H_3()$: 해시함수, $G_T \rightarrow \{0,1\}^*$
- T_*: 키워드 *을 검색하는 트랩도어
- $rk_{a \rightarrow b}$: a의 암호문을 b의 암호문으로 변경하는 재암호화 키

3.2 프로토콜

- Key Generation phase

클라우드 스토리지 이용자는 안전하게 생성된 키 쌍을 전송받는다.

$x \in Z_q$ 선택

$sk = x$ 설정

$pk = g^x$ 설정

- Encryption phase

사용자는 검색 및 재암호화가 가능한 암호문을 다음과 같이 생성

$di = H(m)$

$A = pk^{di}$

$B = e(g,g)^{sk_a \cdot di}$

$c_i = H_2(e(g, H_1(w_i))^{di})$

$C = \{C_1, C_2, ..., C_n\}$

$D = e(g, H_2(pk))^{di} \cdot m$

$E_a = (A, B, C, D)$

- ReKey Generation phase

데이터의 소유주가 자신의 데이터를 다른 사용자에게 공유하고자 할 때, 재암호화를 위한키를 생성한다. 사용자 a가 사용자b에게 데이터를 공유하고자 할 경우 a의 개인키와 b의 공개키로 재암호화키를 다음과 같이 생성

$A' = pk_b^{di}$

$rk_{a \rightarrow b} = (A', pk_b^{-sk_a})$

- ReEnc phase

클라우드 스토리지 서비스 서버는 사용자로부터 입력된 재암호화키와 재암호화하려는 목표 암호문 그리고 공개키를 가지고 재암호화를 다음과 같이 수행

$B' = e(A, rk_{a \rightarrow b})$

$E_b = (A', B', C, D)$

- Trapdoor Generation phase

데이터를 검색할 사용자는 검색하고자 하는 키워드와 자신의 개인키로 트랩도어를 생성한다.

$T_w = H_1(w)^{-sk_b}$

- Test phase

사용자는 데이터가 자신이 찾고자하는 키워드를 가지고 있는지 확인하기 위하여, 자신의 공개키와 트랩도어, 암호문을 입력 받아 다음과 같이 테스트를 수행한다.

$c_i = ? H_2(e(A', T_w))$

- Decryption phase

색인을 검색한 정당한 사용자는 자신의 비밀키 그리고 암호화 색인을 가지고 데이터 암호화 키를 획득하고, 데이터

암호화키로 데이터를 다음과 같이 복호화 한다.

$m = D/e(A', H_2(pk_a))^{-sk_b}$

4. 제안방식 분석

제안방식은 아래와 같은 요구사항을 만족한다.

- 기밀성: 제안 방식은 페어링을 이용하여 악의적인 제3자가 클라이언트와 서버 간의 통신을 도청한다고 해도 통신 내용을 유추하기 어렵다.
- 검색 속도: 한 번의 페어링연산과 해시 연산만으로 문서에 키워드가 포함되는지 확인할 수 있어 빠른 검색 속도를 제공한다.
- 통신량: 키워드 검색 및 재암호화를 위해 한 라운드의 통신과정만이 필요해 통신량의 효율성을 제공한다.
- 연산 효율성: 경량화된 페어링 연산을 기반으로 색인을 생성 및 검색하며, 재암호화 과정을 수행하여 연산의 효율성을 제공한다.
- 사용자간 공유 효율성: 재암호화를 이용해 신뢰 할 수 없는 원격 데이터 서버에 암호화 저장된 데이터를 안전하고 효율적으로 공유할 수 있도록 하였다. 제안 방식은 기존 방식과 다르게 공유 대상자를 사전에 지정할 필요가 없으며, 공유 대상자를 지정하기 위해 별도의 장치가 필요치 않다, 마지막으로 공유 받은 데이터를 다른 사용자에게 공유할 때 별도의 과정이 필요 없다.

5. 결론

클라우드 스토리지 서비스의 등장으로 많은 사용자들이 해당 서비스를 통해 데이터를 저장 및 접근할 수 있게 되었다. 이러한 저장소에 저장되는 데이터의 안전성을 보장 받고자 최근 클라우드 스토리지에 검색 가능한 암호 기술을 적용하고자 하는 연구가 시작되고 있다. 하지만 기존의 연구된 대부분의 검색 가능한 암호의 경우 주로 이메일 환경을 고려하고 있어 데이터를 공유할 대상을 사전에 정하고, 공유대상을 추가하는데 비효율적인 문제를 가지고 있다. 클라우드 스토리지 환경에서는 사용자 자신이 사용할 데이터를 직접 올리고, 이를 필요에 따라 원하는 사용자와 안전하게 공유하는 유형으로 사용되며, 색인과 같은 데이터 정보와 데이터가 분리되어 있어 기존방식을 클라우드 스토리지 환경에 적용키 어렵다. 따라서 우리는 이러한 클라우드 스토리지 환경을 고려하여 보안 요구사항을 설정하였으며, 프록시 재암호화와 검색 가능한 재암호화 기능을 동시에 제공하는 방식을 제안하였다. 제안 방식은 기존 연구에 대비하여 동일한 연산량적 효율성으로 자유로운 공유 기능을 제공한다. 클라우드 스토리지에서의 데이터를 유연하고 쉽게 검색하기 위해서는 다수의 키워드를 이용한 검색이 중요한 이슈가 될 것으로 사료된다. 따라서 차후에는 가변길이의 다중 키워드로 구성되어 있는 색인을 암호화 하고, 또 이를 유연하게 검색할 수 있는 재암호화 시스템에 대한 연구가 필요하다.

참고문헌

[1] D.Boneh, G.Crescenzo, R.Ostrovsky and G.Persiano, “Public Key Encryption with Keyword Search,” Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May, 2004.

[2] D.Boneh and B.Waters, Conjunctive, “Subset and Range Queries on Encrypted Data,” Proceedings of the 4th Theory of Cryptography Conference, Amsterdam, Netherlands, Febraury, 2007.

[3] Y.H.Hwang and P.J.Lee, “Public key encryption with conjunctive keyword search and its extension to a multi-user system,” Proceeding of First International Conference on Pairing-Based Cryptography, Tokyo, Japan, July, 2007.

[4] F.Bao, R.H.Deng, X.Ding, and Y.Yang, “Private Query on Encrypted Data in Multi-User Settings,” Proceeding of the 4th international conference on Information security practice and experience, Sydney, Australia, April, 2008.

[5] Kamara, S.and Lauter.K., “Cryptographic cloud-storage,” Proceedings of Workshops on Financial Cryptography and Data Security, Canary Islands, Spain, January, 2010.

[6] Ion, M., Russello, G.and Crispo, B., “Enforcing Multi-user Access Policies to Encrypted Cloud Databases,” International Symposium on Policies for Distributed Systems and Networks, Trento, Italy, June, 2011.

[7] B.Zhang, and F.Zhang, “An efficient public key encryption with conjunctive-subset keywords search,” Journal of Network and Computer Applications.vol.34, no.1, 2011.

[8] Y.Yang, “Towards Multi-user Private Keyword Search for Cloud Computing,” Proceeding of International Conference on Cloud Computing, Singapore, Singapore, July, 2011.

[9] Chen, X., Li, Y., “Efficient Proxy Re-encryption with Private Keyword Searching in Untrusted Storage,” I.J.Computer Network and Information Security.vol.3, no.2, 2011.