일회용 트랩도어를 이용한 검색 가능한 암호 시스템에 관한 연구

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

A Study on Searchable Encryption System using One-Time Trapdoor

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

요 약

네트워크 및 컴퓨팅 기술의 발달로 데이터를 위탁 저장하고 이를 언제어디서든 다양한 단말로 처리할 수 있는 클라우드컴퓨팅서비스가 활성화되고 있다. 특히 클라우드컴퓨팅 서비스 중 DaaS가 널리 사용되고 있다. 하지만, 위탁 저장된 데이터베이스에 신체 정보라던가 개인의 민감한 정보가 암호화 없이 저장된다면 서버에 저장된 데이터를 데이터 소유주의 동의 없이 공격자 및 비윤리적인 서버관리자가 열람할 수 있다는 보안 문제점이 있어 위탁 저장된 데이터베이스의 암호화가 필요하다. 하지만 기존에 사용되고 있는 암호화 알고리즘으로 암호화된 데이터를 안전하게 검색하기 위해선 암호화 데이터를 전부 데이터 소유자의 단말기에 내려 받고 전부 복호화해서 검색해야 하기에 데이터를 위탁 저장하는 의미가 퇴색된다. 이와 같은 문제를 해결하기위해 검색 가능한 암호시스템(Searchable Encryption System)이 등장하게 되었다. 하지만 기존의 검색가능 암호 시스템은 같은 키워드를 검색하기위해 생성된 트랩도어가 동일한 형태를 가지게 된다. 수많은 검색 쿼리들이 위탁저장소에 전송되며, 저장소의 관리자는 쿼리를 통해 키워드를 유추하고, 쿼리를 통해 사용자가 어떤 데이터를 저장하고 검색하는지 학습이 가능하기 때문이다. 따라서 본 논문은 동일한 사용자가 같은 키워드를 검색하더라도 매번 다른 트랩도어가 생성되도록 하여 비윤리적인 서버관리자가 검색 쿼리를 통해 검색 내용 및 데이터를 유추할 수 없도록 하는 일회용 트랩도어를 이용한 검색가능 암호 시스템을 제안한다.

1. 서론

네트워크 및 컴퓨팅 기술의 발달로 기업 및 개인은 직접 서버를 관리해야하는 부담 및 운용비용을 줄이기 위해 데이터를 위탁 저장하고 이를 언제어디서든 다양한 단말로 처리할 수 있는 클라우드컴퓨팅서비스가 활성화되고 있다. 특히 클라우드컴퓨팅 서비스 중 DaaS(Database as a Service)는 용량 확장의 제한 없이 사용한 용량만큼 과금이 되는 장점으로 널리 사용되고 있다. 실제로 Research Institute의 조사에 따르면 69%의 미국인이 클라우드 컴퓨팅을 사용하고 있다고 조사되었다. 하지만, 위탁 저장된 데이터베이스에 신체 정보라던가 개인의 민감한 정보가 암호화 없이 저장된다면 서버에 저장된 데이터를 데이터 소유주의 동의 없이 공격자 및 비윤리적인 서버관리자가 열람할 수 있다는 보안 문제점이 있다. 따라서 위탁 저장된 데이터베이스의 암호화가 필요하지만 기존에 사용되고 있는 암호화 알고리즘으로 암호화된 데이터를 안전하게 검색하기 위해선 암호화 데이터를 전부 데이터 소유자의 단말기에 내려 받고 전부 복호화해서 검색해야 하기에 데이터를 위탁 저장하는 의미가 퇴색된다. 이와 같은 문제를 해결하기위해 검색 가능한 암호시스템(Searchable Encryption System)이 등장하게 되었다[1-8]. 이는 준동형 암호의 특징을 이용해 암호화된 데이터를 복호화 없이 검색할 수 있는 암호 기법으로 최근 많은 연구가 진행되고 있다.

검색 가능한 암호 시스템의 이용과정은 다음과 같다. 데이터 소유자는 먼저 위탁 저장하고자 하는 데이터를 암호화하여 클라우드와 같은 제3의 위탁저장소에 저장한다. 그 후 자신이 저장한 자료 중 특정 키워드를 가지는 데이터를 검색하기 위해 키워드를 암호화하여 트랩도어를 생성한다. 생성된 트랩도어는 서버로 전송되며, 서버는 트랩도어를 가지고 암호화된 데이터를 검색하게 된다. 검색 과정을 통해 서버는 키워드의 정보 및 데이터의 정보를 알 수 없으며 단지 데이터가 키워드에 해당되는지의 여부만 알 수 있게 된다. 이 과정을 통해 서버는 키워드에 해당되는 암호화된 데이터들을 사용자에게 알려주게 된다. 이 검색가능 암호시스템이 트랩도어로 암호화된 데이터를 찾는다고 완전한 안전성을 가진다고 가정하기엔 문제점이 있다. 기존의 검색가능 암호 시스템은 같은 키워드를 검색하기위해 생성된 트랩도어가 동일한 형태를 가지게 된다. 수많은 검색 쿼리들이 위탁저장소에 전송되며, 저장소의 관

리자는 쿼리를 통해 키워드를 유추하고, 쿼리를 통해 사용자가 어떤 데이터를 저장하고 검색하는지 학습이 가능하기 때문이다.

따라서 본 논문은 동일한 사용자가 같은 키워드를 검색하더라도 매번 다른 트랩도어가 생성되도록 하여 비윤리적인 서버관리자가 검색 쿼리를 통해 검색 내용 및 데이터를 유추할 수 없도록 하는 일회용 트랩도어(One-Time Trapdoor)를 이용한 검색가능 암호 시스템을 제안한다.

2. 요구사항

위탁 저장소 환경에서 안전하게 데이터를 저장 및 검색하려면 다음과 같은 요구사항을 만족해야 한다.

- 기밀성: 원격 저장소와 클라이언트 단말기 간의 통신 데이터는 정당한 개체만이 확인할 수 있어야 한다. 데이터 검색을 위해 생성되는 트랩도어는 같은 키워드를 검색하더라도 매번 다른 형태로 생성되어야 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.

3. 제안방식

본 장에선 위탁 저장소의 구조적 특성을 고려하여 일회용 트랩도어를 이용한 검색 가능한 암호 시스템을 제안한다. 데이터 저장, 검색 시나리오별로 어떠한 단계가 진행되는지 서술한다.

3.1 시스템계수

본 제안방식에서 사용되는 시스템 계수는 다음과 같다.

- p: 소수
- G: p를 법으로 하는 덧셈군
- G_T: p를 법으로 하는 곱셈군
- g: G의 생성자
- e: 겹선형 사상, $G\times G\rightarrow G_T$
- sk_*: $*$의 개인키
- pk_*: $*$의 공개키
- $EC_k()$: 키 k로 대칭키 암호화
- $DC_k()$: 키 k로 대칭키 복호화
- k: 데이터 암/복호화를 위한 대칭키
- w_*: 데이터의 $*$번째 키워드
- W: 키워드 집합
- n: 데이터가 가지는 키워드 개수
- pd: 평문 데이터
- ed: 암호화 데이터
- di: 데이터 식별자
- $H()$: 해시함수
- $H_1()$: 해시함수, $\{0,1\}^*\rightarrow G$
- $H_2()$: 해시함수, $G_T\rightarrow\{0,1\}^*$
- T_*: 키워드 $*$을 검색하는 트랩도어

3.2 데이터 저장

Key generation

클라우드 스토리 서비스를 이용하는 사용자 a 그리고 서비스 제공자 s는 자신들의 키 쌍을 다음과 같이 소지한다.

$$sk_a = a, pk_a = g^a$$

$$sk_s = s, pk_s = g^s$$

Index and data encryption

사용자는 검색 및 재암호화가 가능한 암호화 색인 및 데이터를 다음과 같이 생성한다.

$$di = H(k)$$

$$A = pk_a^{di}$$

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

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

$$C = \{c_1, c_2, ..., c_n\}$$

$$D = e(g, H_2(pk_a))^{di} \cdot k$$

$E_a = (A, B, C, D)$ 암호화 색인으로 출력

$ed = EC_k(pd)$ 암호화 데이터로 출력

3.3 데이터 검색

TrapdoorGeneration

데이터를 검색할 사용자는 검색하고자 하는 키워드와 자신의 개인키로 트랩도어를 생성한다.

$$r \in Z_p^*$$

$$X = H_1(w)^{-sk_a \cdot r}$$

$$Y = pk_s^{-r}$$

$$T_w = X \parallel Y$$

Test

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

$$e(c_i, pk_s) = ?\, e(H_2(e(A,X)), Y)$$

$$= e\left(H_2\left(e\left(pk_a^{di}, H_1(w)^{-sk_a \cdot r}\right)\right), pk_s^{-r}\right)$$

$$= e\left(H_2\left(e\left(g^{sk_a \cdot di}, H_1(w)^{-sk_a \cdot r}\right)\right), pk_s^{-r}\right)$$

$$= e\left(H_2\left(e\left(g, H_1(w)^{di}\right)\right), pk_s\right)$$

Dec

데이터 소유자는 자신의 비밀키 sk 그리고 복호화 하고자 하는 데이터의 암호화 키를 다음과 같이 추출 한다.

$$k = D/e(A, H_2(pk_a))^{-sk_a}$$
$$= D/e(pk_a^{di}, H_2(pk_a)^{-sk_a})$$
$$= D/e(g^{sk_a \cdot di}, H_2(pk_a)^{-sk_a})$$
$$= D/e(g, H_2(pk_a))^{di}$$
$$= e(g, H_2(pk_a))^{di} \cdot k/e(g, H_2(pk_a))^{di}$$

이를 가지고 암호화 된 데이터를 복호화 한다.

$$pd = DC_k(ed)$$

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. 또한 임의 값을 이용하여 같은 키워드를 검색하는 트랩도어를 생성하더라도 매번 다른 형태의 트랩도어가 생성되어 비윤리적인 서버관리자가 검색쿼리를 통해 검색하는 키워드 및 데이터의 내용을 학습하기 어렵다.
- 통신량: 키워드 검색 및 재암호화를 위해 한 라운드의 통신과정만이 필요해 통신량의 효율성을 제공한다.
- 연산 효율성: 경량화된 페어링 연산을 기반으로 색인을 생성 및 검색 과정을 수행하여 연산의 효율성을 제공한다.

5. 결론

본 연구를 통해 우리는 위탁 저장소 환경을 고려하여 보안 요구사항을 설정하고 이를 만족하는 안전한 데이터 저장 및 검색 기법을 제안하였다. 제안 방식은 기존 연구에 대비하여 동일한 연산량적 효율성으로 안전한 검색 기능을 제공한다. 위탁 저장소에서의 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 Encryp-tion 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 En-crypted Data,” Proceedings of the 4th Theory of Cryptography Confer-ence, Amsterdam, Netherlands, Febraury, 2007.

[3] Y.H.Hwang and P.J.Lee, “Public key encryption with conjunctive key-word 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 confer-ence on Information security practice and experience, Sydney, Austral-ia, April, 2008.

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

[6] M.Ion, G.Russello, and B. Crispo, “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 con-junctive-subset keywords search,” Journal of Network and Computer Ap-plications. vol.34, no.1, 2011.

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