색인 구조를 고려한 안전한 검색가능암호기술에 관한 연구1)

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

A Study on Secure Searchable Encryption Considering Index Stucture

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

요 약

네트워크 및 컴퓨팅 기술의 발달로 데이터를 위탁 저장하고 이를 언제어디서든 다양한 단말로 처리할 수 있는 클라우드 스토리지 서비스가 활성화되고 있다. 하지만, 위탁 저장된 민감한 정보가 암호화 없이 저장된다면 서버에 저장된 데이터를 데이터 소유주의 동의 없이 공격자 및 비윤리적인 서버관리자가 열람할 수 있어 저장된 데이터의 암호화 및 이를 검색하는 검색 가능한 암호시스템(Searchable Encryption System)이 등장하게 되었다. 기존의 검색가능 암호 시스템은 같은 키워드를 검색하기위해 생성된 트랩도어가 동일한 형태를 가지게 되어 공격자가 검색 쿼리를 통해 사용자가 어떤 데이터를 저장하고 검색하는지 학습이 가능하다. 본 논문은 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 SaaS(Storage as a Service)는 용량 확장의 제한 없이 사용한 용량만큼 과금이 되는 장점으로 널리 사용되고 있다. 이러한 위탁 저장소에 저장되는 민감한 정보들을 안전하게 저장하고 이를 복호화 과정 없이 검색하기 위해 검색 가능한 암호시스템이 등장하게 되었다[1-4].

위와같은 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 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 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.

1) 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2013R1A1A2012940)

3.1 시스템계수

본 제안방식에서 사용되는 시스템 계수는 다음과 같다.

계수	설명	계수	설명
p	소수	G	p를 법으로 하는 덧셈군
G_T	p를 법으로 하는 곱셈군	g	G의 생성자
e	겹선형 사상, $G\times G\rightarrow G_T$	k	데이터 암/복호화를 위한 대칭키
$E_k()$	키 k로 대칭키 암호화	$D_k()$	키 k로 대칭키 복호화
sk_*	*의 개인키	pk_*	*의 공개키
w_*	데이터의 *번째 키워드	W	키워드 집합
n	데이터가 가지는 키워드 개수	$H()$	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 가능한 암호화 색인 및 데이터를 다음과 같이 생성한다.

$hk = H(k)$

$A = pk_a^{hk}$

$b_i = H_2(w_i)^{sk_a}$

$B = \{b_1, b_2, ..., b_n\}$

$C = e(g, H_2(pk_a))^{hk} \cdot k$

$D = EC_k(m)$

$E_a = (A, B, C, D)$ 암호화 색인으로 출력

3.3 데이터 검색

TrapdoorGeneration: 데이터를 검색할 사용자는 검색하고자 하는 키워드와 자신의 개인키로 트랩도어를 생성한다.

$X = pk_s^r \quad (r \in Z_p^*)$

$Y = H_2(w)^{sk_a \cdot r}$

$T_w = X \| Y$

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

$e(pk_s, b_i) = ? e(X, Y)$

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

$k = C / e(A, H_2(pk_a))^{-sk_a}$

이를 가지고 암호화 된 데이터를 복호화 한다.

$m = DC_k(D)$

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 제안방식은 기존방식과 달리 매번 바뀌는 트랩도어 생성을 위해 기존방식보다 연산량이 소폭 증가되었다.

5. 결론

본 연구를 통해 우리는 위탁 저장소의 색인 구조를 고려하여 보안 요구사항을 설정하고 이를 만족하는 안전한 데이터 저장 및 검색 기법을 제안하였다. 제안 방식은 기존 연구와 달리 중복 키워드의 병합이 가능해 색인을 유지하기 위한 용량의 효율성을 제공한다. 또, 기존의 검색 가능 암호 시스템은 키워드에 해당하는 데이터를 검색하기 위해 저장된 데이터 전부와 비교 연산을 수행하지만, 제안방식은 키워드 색인 기반의 기존 검색 알고리즘을 적용할 수 있어 빠른 검색속도를 제공한다. 추후 좀 더 유연한 검색을 위해 다중 키워드 검색을 지원하는 기법에 대한 연구가 필요하다.

참고문헌

[1] Song, D.X., Wagner, D., and Perrig, A. Practical Techniques for Searching on Encrypted Data. In Symposium on Security and Privacy. California, USA (2000)

[2] Goh, E.J. Secure Indexes. ePrint Crpytography Archive, (2004)

[3] Curtmola, R., Garay, J., Kamara, S., and Ostrovsky, R. Searchable Symmetric Encryption Improved Definitions and Efficient Constructions. In Proceedings of the 13th ACM Conference on Computer and Communications Security. Virginia, USA (2006)

[4] Boneh, D., Crescenzo, G., Ostrovsky, R., and Persiano, G. Public Key Encryption with Keyword Search. In Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken, Switzerland (2004)