원격 저장소 환경을 고려한 공개키 검색 가능 암호 시스템+

*이선호, **박성욱, ***이임영++
순천향대학교 컴퓨터소프트웨어학과
e-mail:[*sunho431, **swpark, ***imylee]@sch.ac.kr

Public-key Searchable Encryption System: Considering Remote Storage Environment

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

요 약

통신이 발달로 인터넷 망을 이용해 고용량의 데이터를 빠르게 주고받을 수 있게 되었으며, 이로 인하여 데이터를 원격 저장소에 저장하여 언제 어디서든 빠르게 접근할 수 있는 서비스가 발전하게 되었다. 하지만 데이터를 저장하는 서버의 보안 및 서버관리자의 신뢰 문재가 발생하게 되었고, 이를 해결하기위해 서버에 저장되는 데이터의 암호화 및 이를 검색할 수 있는 기술이 필요하게 되었다. 기존의 검색 가능 암호의 경우 이메일 서비스를 기반으로 구성이 되어 하나의 데이터에 많은 키워드를 저장하게 되는 원격 저장소 서비스에 적용하기 어렵다. 또한 필드 기반 검색기능을 제공해 검색이 유연하지 않고 결합 키워드 검색 시 연산의 효율성이 떨어지는 문제점이 존재한다. 따라서 본 논문은 블룸필터를 사용하여 대량의 키워드를 효율적으로 저장 및 검색 할 수 있으며 필드 프리한 결합키워드 검색을 지원하는 공개키 검색 가능 암호 시스템을 제안한다.

1. 서론

우리나라는 정보화 사업으로 인하여 세계최고 수준의 네트워크를 구성하였다. 사용자들은 이와 같이 빠른 네트워크를 통하여 자신의 주요 자료의 백업 및 언제 어디서든 자료에 접근할 수 있는 접근성을 보장 받기 위해 웹하드와 같은 원격 데이터 저장 서비스를 사용하게 되었다. 하지만 이와 같은 서비스를 제공하는 서버가 해커나 관리자에 인하여 개인 정보 및 주요정보가 노출되는 사건이 빈번하게 발생되었다. 이로 인하여 사용자는 신뢰할 수 없는 서버에 데이터 저장을 하는 부담해소하기 위해 데이터를 암호화 저장할 필요가 생겼으며 이와 함께 암호화된 데이터를 안전하게 검색할 수 있는 검색 가능한 암호 기술의 필요성이 대두 되었다. 하지만 기존의 검색 가능한 암호 시스템의 경우 이메일 환경을 기반으로 설계되어 필드에 제한적인 검색을 지원하고, 키워드 가지 수의 제한을 가지고 있다. 따라서 본 논문은 원격 저장소 환경을 고려하여 데이터에 대량의 키워드를 삽입 가능하고, 다중의 키워드로 필드에 제한 없이 검색 가능한 공개키 검색가능 암호 시스템을 제안한다.

Ⅱ. 요구사항

검색가능 암호 시스템은 아래와 같은 요구사항을 만족해야한다.

- 기밀성: 원격 데이터 서버와 클라이언트 단말기 간의 통신 데이터는 정당한 개체만이 확인할 수 있어야 한다.
- 검색 속도: 제한적 시스템 자원을 가지는 클라이언트에서도 원격 저장소 시스템에 저장된 문서에서 검색하고자 하는 워드를 포함하는 문서를 빠르게 검색할 수 있어야 한다.
- 저장 용량: 검색가능 암호 시스템에서 대용량 키워드를 저장하는 색인의 저장 공간 효율성을 제공해야한다.
- 통신량: 클라이언트와 서버간의 에너지 효율 및 네트워크 자원의 효율성을 위하여 통신량이 적어야 한다.
- 문서 검색 효율성: 한 번의 검색만으로 단일 키워드 검색이 아닌 유연한 결합 키워드 검색을 지원하는 효율성이 제공되어야 한다.

Ⅲ. 제안 방식

본 논문에서는 블룸필터를 사용하여 대량의 키워드 저장 및 다중 키워드 검색을 지원하는 공개키 기반 검색가능 암호시스템을 제안한다.

- 시스템 계수

G_1: 덧셈군
G_2: 곱셈군
i: 문서가 가지는 키워드의 개수
j: 검색하고자 하는 키워드의 개수
l: 블룸필터 생성용 해시함수 개수

+ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2010-0022607)
++ 교신저자: imylee@sch.ac.kr

n: 블룸필터의 길이
m: 검색 쿼리용 블룸필터의 체크비트 개수
p: 큰 소수
g: G_1생성자
h_*: 블룸필터 생성을 위한 *번째 해시함수
$H_1[]$: G_1의 원소를 반환하는 해시함수
f_*: $H_1[*]$의 결과
w_*: *번째 키워드
I_*: 블룸필터의 인덱스번호
sk: 개인키
pk: 공개키
BF: 키워드로 생성된 블룸필터 값
W: 문서에 해당하는 키워드들의 집합
SW: 검색할 키워드들의 집합
x, r_1, r_2: Z_p^*상의 임의 값

- $KeyGen(1^k)$

Step 1. 큰 소수 p를 법으로 하는 잉여계에서 임의의 원소 x를 선택하여 개인키로 지정한다.

$x = Z_p^*$

$sk : x$

Step 2. 생성자 g에 개인키x승을 하여 공개키를 생성한다.

$y = g^x \bmod p$

$pk : y, g, p$

- $BuildIndex(pk, W)$

Step 1. 문서에 해당하는 키워드들에 블룸필터 생성을 위한 해시함수들을 적용하여 해시함수의 값에 해당하는 인덱스를 1로 치환하여 블룸필터 를 생성한다.

$W = [w_1, w_2, ..., w_i]$

$BF = \{h_1[w_1], h_2[w_1], ..., h_l[w_1]\}, ..., \{h_1[w_i], h_2[w_i], ..., h_l[w_i]\}$

Step 2. 페어링을 암호를 이용하여 블룸필터 값을 암호화한다.

$I = (y^{r_1}, f_1^{r_1}, f_2^{r_1}, ..., f_n^{r_1})$

- $GenTrapdoor(sk, SW)$

Step 1. 다중 키워드 검색을 위한 블룸필터를 생성 뒤 블룸필터에서 1의 값을 가지는 인덱스로 쿼리문Q를 생성한다.

$BF = \{h_1[w_1], h_2[w_1], ..., h_l[w_1]\}, ..., \{h_1[w_j], h_2[w_j], ..., h_l[w_j]\}$

$Q = I_1, I_2, ..., I_m$

Step 2. 쿼리문과 개인키를 이용하여 검색을 위한 트랩도어를 생성한다.

$T = (g^{r_2}, (f_{I_1}, ..., f_{I_m})^{r_2/x}, I_1, ..., I_m)$

- $Test(pk, I, T)$

Step 1. 공개키와 문서의 키워드 집합으로 생성된 인덱스, 검색 쿼리로 생성된 트랩도어로 문서가 키워드를 포함하는지 테스트한다.

$$e(g^{r_2}, \prod_{i=1}^{m} f_i^{r_1}) = ?$$
$$e(y^{r_1}, f_1^{r_2/x}) \times e(y^{r_1}, f_m^{r_2/x}) \times ... \times e(y^{r_1}, f_m^{r_2/x})$$

Ⅳ. 제안 방식 분석

- 기밀성: 제안 방식은 페어링을 이용하여 악의적인 제3자가 클라이언트와 서버 간의 통신을 도청한다고 해도 통신 내용을 유추하기 어렵다.
- 검색 속도: 결합 키워드 검색 시 키워드의 개수만큼 검색 량이 증가하지 않아 빠른 검색속도를 제공한다.
- 저장 공간 효율성: 블룸필터를 사용하여 암축된 고정크기의 저장 공간을 차지하여 저장 공간의 효율성을 제공한다.
- 통신량 효율성: 단 한 번의 통신으로 다중 키워드 검색을 수행하는 통신량 효율성을 제공한다.
- 문서 검색 효율성: 필드를 사용하지 않는 다중키워드 검색을 지원하여 검색의 효율성을 제공한다.

5. 결론

본 논문은 대용량 키워드 저장 및 필드 프리한 다중 키워드 검색을 지원 위해 블룸필터 및 겹선형 사상을 이용하여 한 번의 테스트 과정만으로 여러 키워드에 해당하는 문서를 검색할 수 있는 효율성을 제공하였다. 앞으로 다양한 단말기를 통한 일반사용자의 원격 서버의 데이터 저장이 증가할 것으로 보인다. 따라서 그룹 사용자 환경 등 다양한 환경 및 다양한 추가 기능을 제공하는 검색가능 암호 시스템의 지속적인 연구가 필요한 것으로 본다.

참고문헌

[1] 김선영, 서재우, 이필중, “검색 가능 암호 기술의 연구 동향,” 정보보호학회지, 19(2), pp. 63-73, 2009년 4월.

[2] E. J. Goh, “ecure Indexes,”Technical Report, 2003/216, IACR ePrint Crpytography Archive, 2003.

[3] R. Curtmola, j. Garay, S. Kamara, R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions", 13th ACM conference on Computer and communications security, pp.79-88, 2006.

[4] D. Boneh, G. D. Crescenzo, "Public-key Encryption with Keyword Search", Advances in Cryptology - EUROCRYPT 2004, pp.506-522, 2004.

[5] Y. H. Hwang, P. J. Lee "Public Key Encryption with Conjunctive Keyword Search and its Extension to a Multi-User System", Pairing-Based Cryptography - Pairing 2007, pp.2-22, 2007.