

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2014-0050477 (43) 공개일자 2014년04월29일
(51) 국제특허분류(Int. Cl.) <i>G06F 17/30</i> (2006.01) <i>G06F 21/60</i> (2013.01) (21) 출원번호 10-2012-0116947 (22) 출원일자 2012년10월19일 심사청구일자 2012년10월19일	(71) 출원인 경희대학교 산학협력단 경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스 내 (서천동, 경희대학교) 송실대학교산학협력단 서울특별시 동작구 상도로 369 (상도동) (72) 발명자 이승룡 경기 성남시 분당구 구미로144번길 25, 102동 102호 (구미동, 삼환빌라) 페레즈 지산 경기 용인시 기흥구 덕영대로 1732, 전자정보대학 351호 (서천동, 경희대학교) 박영택 서울 서초구 서초중앙로 206, D동 601호 (반포동, 삼호가든맨션) (74) 대리인 특허법인 신지	

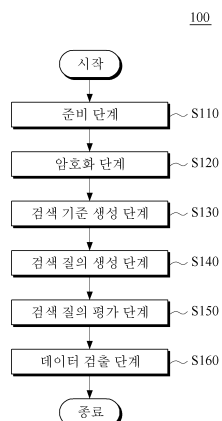
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 **검색 가능한 암호화 방법 및 암호화된 데이터 검색방법**

(57) 요약

본 발명은 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법으로서, 서버에 저장할 데이터로부터 추출된 키워드들과 각 키워드의 빈도의 목록으로 구성된 인덱스를 생성하고, 암호화 및 복호화용 키들을 생성하는 준비 단계와, 암호화용 키를 이용하여 데이터, 인덱스 내부의 키워드 및 인덱스 내부의 키워드 빈도를 각각 암호화하여 서버에 저장하는 암호화 단계와, 서버로부터 암호화된 데이터를 검색하기 위한 검색 키워드를 포함하는 검색 기준을 생성하고, 생성된 검색 기준을 프록시 재-암호화 방법(proxy re-encryption)으로 암호화하는 검색 기준 생성 단계와 암호화된 검색 기준에 기초하여 검색 질의 생성하고, 생성된 검색 질의를 준동형 암호화 방법으로(homomorphic encryption) 암호화하여 서버로 전송하는 검색 질의 생성 단계와 서버에서 암호화된 검색 질의에 대한 평가를 암호화 상태에서 수행하여 검색 질의 평가 결과를 도출하는 검색 질의 평가 단계와 검색 질의 평가 결과에 기초하여 원하는 데이터를 검출하는 데이터 검출 단계를 포함한다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	1415123336
부처명	지식경제부
연구사업명	대학 IT 연구센터 육성지원
연구과제명	동서신의학 u-라이프케어연구센터
기 여 율	40/100
주관기관	경희대학교 산학협력단
연구기간	2012.01.01 ~ 2012.12.31이 발명을 지원한 국가연구개발사업
과제고유번호	2011-0030823
부처명	교육과학기술부
연구사업명	선도연구센터지원사업
연구과제명	디지털로그휴먼미디어 감성인지 기술연구개발
기 여 율	30/100
주관기관	경희대학교 산학협력단
연구기간	2012.09.01 ~ 2013.08.31이 발명을 지원한 국가연구개발사업
과제고유번호	10035348
부처명	지식경제부
연구사업명	SW컴퓨팅산업원천기술개발사업
연구과제명	모바일 플랫폼 기반 계획 및 학습 인지 모델 프레임워크 기술 개발
기 여 율	30/100
주관기관	숭실대학교 산학협력단
연구기간	2012.03.01 ~ 2013.02.28

특허청구의 범위

청구항 1

서버에 저장할 데이터로부터 추출된 키워드들과 각 키워드의 빈도(frequency)의 목록으로 구성된 인덱스를 생성하고, 암호화 및 복호화용 키들을 생성하는, 준비 단계;

상기 암호화용 키를 이용하여 데이터, 인덱스 내부의 키워드 및 인덱스 내부의 키워드 빈도를 각각 암호화하여 서버에 저장하는, 암호화 단계;

서버로부터 암호화된 데이터를 검색하기 위한 검색 키워드를 포함하는 검색 기준을 생성하고, 상기 생성된 검색 기준을 프록시 재-암호화 방법(proxy re-encryption)으로 암호화하는, 검색 기준 생성 단계;

상기 암호화된 검색 기준에 기초하여 검색 질의 생성하고, 상기 생성된 검색 질의를 준동형 암호화 방법으로(homomorphic encryption) 암호화하여 서버로 전송하는, 검색 질의 생성 단계;

서버에서 상기 암호화된 검색 질의에 대한 평가를 암호화 상태에서 수행하여 평가 값을 도출하는, 검색 질의 평가 단계; 및

상기 평가 값에 기초하여 서버로부터 데이터를 검출하는, 데이터 검출 단계를 포함하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

청구항 2

제 1항에 있어서,

상기 암호화 단계는

데이터 암호화용 비밀 키를 이용하여 대칭키 암호화 방법으로 상기 데이터를 암호화하고, 키워드 암호화용 데이터 소유자 키를 이용하여 프록시 재-암호화 방법으로 상기 인덱스 내부의 키워드를 암호화하고, 키워드 빈도 암호화용 비밀 키를 이용하여 대칭키 암호화 방법으로 상기 인덱스 내부의 키워드 빈도를 암호화하여, 서버로 전송하는 것을 특징으로 하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

청구항 3

제 1항에 있어서,

상기 암호화 단계에서 상기 데이터와 상기 인덱스 내부의 키워드가 각각 분리되어 암호화되고 저장되는 것을 특징으로 하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

청구항 4

제 2항에 있어서,

상기 준비 단계는 상기 검색 기준 암호화용 사용자 키를 생성하고, 상기 사용자 키 암호화용 사용자 공공 키 및 상기 사용자 키 복호화용 사용자 개인 키를 생성하는 것을 특징으로 하고,

상기 암호화 단계는 상기 사용자 공공 키를 이용하여 비대칭키 암호화 방법으로 상기 사용자 키를 암호화하여 서버에 저장하는 것을 더 포함하는 것을 특징으로 하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

청구항 5

제 4항에 있어서,

상기 서버로부터 암호화된 사용자 키를 내려 받아 상기 사용자 개인 키를 이용하여 복호화하는 단계를 더 포함하고,

상기 검색 기준 생성 단계는 상기 복호화된 사용자 키를 이용하여 프록시 재-암호화 방법으로 상기 생성된 검색 질의를 암호화하는 것을 특징으로 하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

청구항 6

제 1항에 있어서,

상기 검색 질의 생성 단계는 중개자 단말에서 상기 검색 질의의 생성을 수행하는 것을 특징으로 하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

청구항 7

제 5항에 있어서,

상기 준비 단계는 데이터 소유자 키를 이용하여 암호화된 키워드를 변환하고 재 암호화하여 암호화된 키워드 암호문을 생성하는데 이용되는 변환 키를 생성하는 것을 특징으로 하고,

상기 검색 질의 평가 단계는,

상기 암호화된 키워드를 상기 변환 키를 이용하여 프록시 재-암호화 방법으로 재 암호화하여 키워드 암호문을 생성하는 제 1단계와, 상기 키워드 암호문과 상기 암호화된 검색 질의를 암호화된 상태에서 비교하여 상기 검색 질의에 대한 평가를 수행함으로써 암호화된 평가 값을 도출하는 제 2 단계를 포함하는 것을 특징으로 하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

청구항 8

제 7항에 있어서,

상기 암호화된 평가 값을 가진 상기 암호화된 검색 질의를 구성하는 검색 키워드가 상기 키워드 암호문을 구성하는 저장 키워드들에 포함되는지 여부에 대한 암호화된 정보인 것을 특징으로 하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

청구항 9

제 7항에 있어서,

상기 검색 질의 평가 단계는

준동형 암호화 방법을 이용하여 암호화된 상태에서 검색 질의에 대한 평가를 수행하므로 서버에 검색 정보에 대한 노출이 없는 것을 특징으로 하는, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법.

명세서

기술분야

[0001] 본 발명은 데이터 암호화 방법 및 암호화된 데이터의 검색방법에 관한 것이다. 보다 상세하게는, 검색 가능한 데이터 암호화 방법과 검색 정보의 노출 없이 외부 서버에 저장된 암호화된 데이터로부터 원하는 데이터를 검색하는 방법에 관한 것이다.

배경기술

[0002] 최근 클라우드 스토리지와 같은 외부 저장 공간에 저장된 데이터에 대한 보안 문제가 이슈가 되고 있다. 외부 저장 공간에 저장된 데이터를 보호하기 위해 접근 제어나 키 관리 기술들이 주로 사용되는데, 이는 외부 침입자를 막기에 유효한 방법이지만 외부 저장 공간의 운영자가 저장되어 있는 데이터를 악의적으로 사용하는 것을 근본적으로 방지하지 못한다. 이렇게 신뢰할 수 없는 외부 저장 공간의 운영자로부터 데이터를 안전하게 보호하기 위하여 데이터를 암호화하여 저장하는 방법을 이용할 수 있다. 그러나 이러한 방법은 일반적인 데이터 검색 방법으로는 사용자가 원하는 데이터에 대한 검색이 불가능하다는 문제점을 갖는다. 따라서 검색 가능한 암호화 방법 및 암호화된 데이터에 대한 검색 방법을 고려할 필요가 있다.

[0003] 2000년 Song XD와 다수에 의해 제시된 내용에는 검색 가능한 대칭 키 암호방식(Symmetric Key Cryptography,

SKC)이 기재되어 있는데, 이 방식은 트랩도어들을 이용함으로써 암호화된 데이터로부터 특정 키워드에 대한 검색을 가능하게 한다. 2004년 Boneh 외 다수에 의해 제시된 내용에는 검색 가능한 공개 키 암호방식(Public Key Cryptography, PKC)이 기재되어 있는데, 이 방식 역시 암호화된 데이터에 대한 검색을 위하여 트랩도어를 이용한다. 이러한 SKC와 PKC는 트랩도어들의 수에 의해 사용자가 이용할 수 있는 검색 질의의 수가 제한된다는 문제점을 갖는다. 나아가 트랩도어를 이용한 검색 방법은 외부 저장공간에 저장된 데이터에 대한 수정을 가할 때마다 트랩도어를 업데이트하고 재분배할 필요가 있다는 문제점을 갖는다.

[0004] 그래서 2011년 Kmara S와 다수에 의해 제시된 내용에는 검색 인증(Search Authentication, SA)을 갖는 대칭 검색가능 암호방식(Symmetric Searchable Encryption, SSE)이 기재되어 있는데, 이 방식은 암호화된 데이터를 검색하기 위하여 반전 인덱스(inverted index)를 이용한다. 그러나, 이 방식은 개인 스토리지 시스템에 한정되어 여러 사용자들이 암호화된 데이터를 검색하는 것을 허용하지 않는다는 문제점을 갖는다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 프록시 재-암호화 방법 및 준동형 암호화 방법으로 암호화된 검색 질의에 기초하여 암호화 상태에서 검색 질의를 수행하므로 검색 정보의 노출 없이 외부 서버에서 원하는 데이터를 검색하는 방법을 제공한다.

[0006] 또한, 본 발명은 사용자가 검색 질의의 수의 제한 없이 암호화된 데이터를 검색하는 방법을 제공한다.

[0007] 또한, 본 발명은 암호화된 데이터에 대한 검색을 승인 받은 다수의 사용자가 암호화된 데이터를 검색하는 방법을 제공한다.

과제의 해결 수단

[0008] 일 실시예에 따른 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법은 서버에 저장할 데이터로부터 추출된 키워드들과 각 키워드의 빈도의 목록으로 구성된 인덱스를 생성하고, 암호화 및 복호화용 키들을 생성하는 준비 단계와, 암호화용 키를 이용하여 데이터, 인덱스 내부의 키워드 및 인덱스 내부의 키워드 빈도를 각각 암호화하여 서버에 저장하는 암호화 단계와, 서버로부터 암호화된 데이터를 검색하기 위하여 검색 키워드를 포함하는 검색 기준을 생성하고 생성된 검색 기준을 암호화하는 검색 기준 생성 단계와, 암호화된 검색 기준에 기초하여 검색 질의 생성하고 생성된 검색 질의를 암호화하여 서버로 전송하는 검색 질의 생성 단계와 서버에서 암호화된 검색 질의에 대한 평가를 수행하여 검색 질의 평가 결과를 도출하는 검색 질의 평가 단계와, 검색 질의 평가 결과에 기초하여 원하는 데이터를 검출하는 데이터 검출 단계를 포함한다.

[0009] 하나의 보충적이거나 대안적인 실시예에서, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법에서 암호화 단계는 데이터 암호화용 비밀 키를 이용하여 대칭키 암호화 방법으로 데이터를 암호화하고, 키워드 암호화용 데이터 소유자 키를 이용하여 프록시 재-암호화 방법으로 인덱스 내부의 키워드를 암호화하고, 키워드 빈도 암호화용 비밀 키를 이용하여 대칭키 암호화 방법으로 인덱스 내부의 키워드 빈도를 암호화하는 것을 특징으로 한다.

[0010] 다른 보충적이거나 대안적인 실시예에서, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법에서 암호화 단계는 데이터와 인덱스 내부의 키워드가 각각 분리되어 암호화되고 저장되기 때문에 데이터의 내용을 나타내는 적합한 키워드를 선택하기 위하여 데이터의 변화 없이 인덱스 내부의 키워드들을 변경할 수 있는 것을 특징으로 한다.

[0011] 다른 보충적이거나 대안적인 실시예에서, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법에서 준비 단계는 검색 기준 암호화용 사용자 키를 생성하고, 사용자 키 암호화용 사용자 공공 키 및 사용자 키 복호화용 사용자 개인 키를 생성하는 것을 특징으로 하고, 암호화 단계는 사용자 공공 키를 이용하여 비대칭키 암호화 방법으로 사용자 키를 암호화하여 서버에 저장하는 것을 더 포함하고, 키워드 빈도 암호화용 비밀 키를 이용하여 준동형 암호화 방법으로 생성된 검색 질의를 암호화하여 서버로 전송하는 것을 특징으로 한다.

[0012] 다른 보충적이거나 대안적인 실시예에서, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법에서 준비 단계는 서버에 저장된 데이터 소유자 키를 이용하여 암호화된 키워드를 변환하여 재 암호화하는데 이용되는 변환 키를 생성하는 것을 특징으로 한다.

- [0013] 다른 보충적이거나 대안적인 실시예에서, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법에서 검색 질의 평가 단계는 변환 키를 이용하여 프록시 재-암호화 방법으로 암호화된 키워드를 재 암호화하고, 재 암호화된 키워드와 암호화된 검색 질의를 비교하여 암호화된 검색 질의에 대한 평가를 수행함으로써 암호화된 평가 값을 계산하는 것을 특징으로 하고, 암호화된 평가 값은 암호화된 검색 질의를 구성하는 검색 키워드가 재 암호화된 키워드를 구성하는 저장 키워드들에 포함되는 지에 대한 암호화된 정보 값을 의미하는 것을 특징으로 한다.
- [0014] 다른 보충적이거나 대안적인 실시예에서, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법에서 검색 질의 평가 단계는 준동형 암호화 방법을 이용하여 암호화된 상태에서 검색 질의에 대한 평가를 수행하므로 서버에 검색 정보에 대한 노출이 없는 것을 특징으로 한다.
- [0015] 다른 보충적이거나 대안적인 실시예에서, 검색 가능한 암호화 방법 및 암호화된 데이터 검색 방법에서 데이터 검출 단계는 준동형 암호화 방법으로 암호화된 평가 값을 복호화하고, 복호화된 평가 값에 기초하여 암호화된 키워드를 복호화하고 암호화된 키워드 빈도를 복호화하여 원하는 데이터를 검출하는 것을 특징으로 한다.

발명의 효과

- [0016] 본 발명은 프록시 재-암호화 방법과 준동형 암호화 방법으로 암호화된 검색 질의에 기초하여 암호화 상태에서 검색 질의를 수행하므로 외부 서버에서 데이터를 검색하는 과정에서 외부 서버 등에 검색 정보 등의 노출을 막을 수 있어 데이터의 기밀성이 보장된다.
- [0017] 또한, 본 발명은 트랩도어를 이용하는 대신에 고유의 검색 질의를 정의해서 데이터를 검색하는 방법이므로 사용자가 검색 질의의 수의 제한 없이 암호화된 데이터를 검색할 수 있다.
- [0018] 또한, 본 발명은 데이터 소유자에 의해 제공된 사용자키를 승인된 사용자에게 발급함으로써 검색을 승인 받은 다수의 사용자가 암호화된 데이터를 검색할 수 있다.

도면의 간단한 설명

- [0019] 도 1은 본 발명의 일 실시예에 따른 검색 가능한 암호화 방법 및 암호화된 데이터의 검색 방법에 대한 순서도이다.
- 도 2는 본 발명의 일 실시예에 따른 검색 가능한 암호화 방법의 순서도이다.
- 도 3은 본 발명의 일 실시예에 따른 암호화된 데이터의 검색 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0020] 도 1은 본 발명의 일 실시예에 따른 검색 가능한 암호화 방법 및 암호화된 데이터의 검색 방법에 대한 순서도이다.
- [0021] 도 1을 참조하면 검색 가능한 암호화 방법 및 암호화된 데이터의 검색 방법은 준비단계(S110), 암호화 단계(S120), 검색 기준 생성 단계(S130), 검색 질의 생성 단계(S140), 검색 질의 평가 단계(S150), 데이터 검출 단계(S160)를 포함한다.
- [0022] 준비단계(S110)를 설명하면, 이는 데이터 소유자 단말(10)에서 수행되나, 이에 한정되지 않는다. 여기서 우선 데이터 소유자 단말(10)은 인덱싱 알고리즘을 이용함으로써, 인덱스 $\mathcal{I}$ 를 생성한다. $\mathcal{I}$ 는 키워드와 각 키워드 빈도의 목록을 포함한다.
- [0023] 향후 검색 질의들은 이 키워드들에 기초하여 평가될 수 있다. 그리고, $\mathcal{I}$ 가 생성되면, 데이터 소유자 단말(10)은 데이터 소유자 키(ω_o), 사용자 키(ω_u) 및 변환 키($\omega_o \rightarrow u$)를 생성함으로써, 프록시 재-암호화 방법을 초기화한다.
- [0024] 다음으로, 암호화 단계(S120)를 설명하면, 이는 데이터 소유자 단말(10)에서 수행되나, 이에 한정되지 않는다.

데이터 소유자 단말(10)은 일반적인 부호화 함수를 사용하여, 인덱스 내부의 키워드들을 $\mathcal{I}_{kw_0 \dots}$ 를 부호화한다.

[0025] 그리고, 데이터 소유주 키 ω_o 를 이용하여 부호화된 키워드들 $\hat{\mathcal{I}}_{kw_0 \dots n}^{\omega_o}$ 을 프록시 재-암호화 알고리즘(proxy re-encryption)으로 암호화한다.

[0026] 여기서, 외부 서버가 중개자의 비밀키로 암호화된 키워드 빈도로부터, 암호화된 키워드들에 대한 어느 정보도 알아낼 수 없게 할 수 있다. 그리고, 데이터 소유자 단말(10)은 외부 서버에 저장된 암호화된 데이터에 대한 검색 능력을 승인 받기를 원하는 사용자의 공공 키를 가지고 사용자 키를 암호화한다.

[0027] 일단, 데이터 소유자 단말(10)이 $\mathcal{I}_{kw_0 \dots n}$, $\mathcal{I}_{fo \dots n}$ 및 ω_u 를 확보하면 암호화하여, 암호화된 데이터와 함께, 암호화된 키워드 $\hat{\mathcal{I}}_{kw_0 \dots n}^{\omega_o}$, 암호화된 키워드 빈도 $\mathcal{I}_{fo \dots n}^{sk}$ 및 암호화된 사용자 키 $\omega_u^{k_{pub}}$ 를 외부 서버에 저장한다.

[0028] 그리고, 이러한 암호화 단계(S120)는 데이터와 인덱스 내부의 키워드가 각각 분리되어 암호화하고 저장하므로, 데이터의 내용을 나타내는 적합한 키워드를 선택하기 위하여 상기 데이터의 변화 없이 인덱스 내부의 키워드들을 변경할 수 있다.

[0029] 다음으로, 검색 기준 생성 단계(S130)를 설명하면, 우선 사용자 단말(50)은 외부 서버로부터 암호화된 사용자 키를 내려 받고, 사용자 개인키를 이용하여 복호화한다.

[0030] 여기서, 사용자 키를 비대칭 암호화 방식으로 암호화하여 승인된 사용자에게 발급하는 것은 인덱스 내부의 키워드를 각 승인된 사용자에게 분리하여 암호화할 필요 없이 다수의 사용자가 암호화된 데이터에 대하여 검색하는 것을 가능하게 한다. 그리고, 키워드들의 목록 $(kw_0 \dots kw_l)$ 으로 구성된, 즉 검색 키워드로 구성된 검색

기준 $(\mathcal{C}_{kw_0 \dots l})$ 을 정의하고, $\mathcal{C}_{kw_0 \dots l}$ 을 일반적인 부호화 함수를 사용하여 부호화한다.

[0031] 그리고, 외부 서버나 중개자 단말(30)로부터 키워드들의 기밀성을 보장하기 위하여, 사용자 키를 이용하여 $\hat{\mathcal{C}}_{kw_0 \dots l}$ 을 프록시 재-암호화 방법에 의해 암호화한다.

[0032] 그리고, 암호화된 검색 기준을 중개자 단말(30)에 보낸다.

[0033] 다음으로, 검색 질의 생성 단계(S140)를 설명하면, 검색 질의 생성 단계는 중개자 단말에서 수행될 수 있으나, 이에 한정되지 않는다. 여기서, 중개자 단말(30)은 $\hat{\mathcal{C}}_{kw_0 \dots l}^{\omega_u}$ 를 수신하여, 이에 기초하여 검색질의를 생성한다. 검색 질의는 다항식 $P(x)$ 으로 모델링 될 수 있다. 다항식 $P(x)$ 은 수학식 1과 같이 묘사된다.

수학식 1

$$P(x \in \hat{\mathcal{C}}_{kw_0 \dots l}^{\omega_u}) = \sum_{i=0}^l \alpha_i x^i = 0$$

[0035] 일단, $P(x)$ 가 $\hat{\mathcal{C}}_{kw_0 \dots l}^{\omega_u}$ 에 기초하여 정의되면, 중개자 단말(30)은 중개자 준동형 공공 키 σ_{pk} , 준동형 비밀 키 σ_{sk} 를 생성함으로써, 준동형 암호화 방법(homomorphic encryption)을 초기화한다. 준동형 암호화 방법

을 이용함으로써, 암호화된 상태에서 키워드 검색을 통한 원하는 데이터를 검색하는 것이 가능할 수 있다.

[0036] 그리고, 중개자 단말(30)은 σ_{sk} 를 사용하여 준동형 암호화 알고리즘을 으로 $P(x)$ 의 계수 $(\alpha_{0...l})$ 를 암호화한다.

[0037] 그리고, 암호화된 검색질의 $\alpha_{0...l}^{\sigma_{sk}}$ 및 σ_{sk} 은 외부 서버로 전송된다. 여기서, 암호화된 계수들 $\alpha_{0...l}^{\sigma_{sk}}$ 은 암호화된 역 인덱스(암호화된 키워드) $\hat{I}_{kw0...n}^{\omega_o}$ 에 대한 검색 질의를 평가하기 위하여 사용된다.

[0038] 다음으로, 검색 질의 평가 단계(S150)를 설명하면, 중개자 단말(30)에 의하여 외부 전송된 암호화된 검색 질의 $\alpha_{0...l}^{\sigma_{sk}}$ 는 암호화된 키워드 $\hat{I}_{kw0...n}^{\omega_o}$ 에 대응하여 평가된다. $\alpha_{0...l}^{\sigma_{sk}}$ 를 수신하면, 외부 서버는 데이터 소유자에 의하여 제공된 각각의 사용자 변환 키 $(\omega_o \rightarrow u)$ 를 가지고 암호화된 키워드를 $\hat{I}_{kw0...n}^{\omega_o}$ 를, 키워드 암호화문으로 변환한다.

[0039] 암호화된 키워드가 키워드 암호화문으로 변환되면, 중개자 단말(30)은 $P(y)$ 의 계수로 $\alpha_{0...l}^{\sigma_{sk}}$ 의 각 원소를 사용함으로써, 다항식 $P(y)$ 을 정의한다. 그리고, $r.P(y)$ 를 평가함으로써, 암호화된 평가 값 Δy_i 을 계산한다 $\Delta y_i = r.P(y_i)$. 여기서, $y_i \in \hat{I}_{kw0...n}^{\omega_u}$ 이고, r 은 랜덤 숫자이다. 외부 서버가 수학식 2를 평가해내면, 중개자 단말(30)에 숨겨진 키워드 주파수를 갖는 평가 값의 목록을 포함하는 질의 평가 결과에 대하여 전송 한다.

수학식 2

$$P(y_{0...n} \in \hat{I}_{kw0...n}^{\omega_u}) = \Delta y_{0...n}$$

[0041] 다음으로, 데이터 검출 단계(S160)를 설명하면, 중개자 단말(30)은 중개자 준동형 비밀 키를 이용하여, 암호화된 평가 값을 복호화한다.

[0042] 여기서, ψ_i 는 0 또는 랜덤 숫자가 될 수 있다. 검색 질의가 암호화된 검색 기준 과 동일한 루트를 가지는 수학적 식 3과 같은 다항식으로서 모델링되기 때문에, 외부 서버에서의 질의 평가는 0 또는 0이 아닌 값이 될 수 있다.

수학식 3

$$P(x \in \hat{C}_{kw0...l}^{\omega_u}) = \sum_{i=0}^l \alpha_i x^i$$

[0044] 0은 암호화된 검색 질의를 구성하는 검색 키워드가 키워드 암호문을 구성하는 저장 키워드에 포함되는 것을 의미하는 값이고, 0이 아닌 값은 암호화된 검색 질의를 구성하는 검색 키워드가 키워드 암호문을 구성하는 저장 키워드에 포함되지 않는 것을 의미하는 값이다. 검색 키워드가 저장 키워드에 포함되지 않는 경우, 사용자에게 의하여 생성된 검색 기준은 무의미한 것이 된다. 그러나, 질의 평가 결과가 0이라면, 사용자의 검색 기준은 유효한 기준이되고, 이런 경우 중개자 단말(30)은 중개자 비밀 키를 사용함으로써, 대응되는 주파수 인덱스를 해독

한다.

- [0045] 그리고, 중개자 단말(30)은, 질의 평가 결과를 정렬하고, 사용자 단말(50)에 응답을 준다. 사용자 단말(50)이 중개자 단말(30)의 응답을 수신함에 따라, 사용자 단말(50)은 각 사용자 키를 이용하여 검색 기준을 해독한다.
- [0046] 복호화를 통해, 사용자 단말(50)은 암호화된 키워드와 매칭되는 키워드를 알게 된다. 여기서, k 는 $\hat{C}_{kw_0 \dots l}^{\omega u}$ 와 $\hat{I}_{kw_0 \dots n}^{\omega u}$ 사이의 동일한 숫자 항이다. 결국, 사용자 단말(50)은 인덱스 내부를 구성하는 키워드 및 키워드 빈도에 대한 정보를 획득하여, 외부 서버로부터 원하는 데이터를 검출 할 수 있다.
- [0047] 도 2는 본 발명의 일 실시예에 따른 검색 가능한 암호화 방법의 순서도이다.
- [0048] 데이터 소유자 단말(10)이 서버에 저장하고자 하는 데이터로부터 추출된 키워드와 이에 대응하는 키워드 빈도의 목록으로 구성된 인덱스를 생성한다(S201).
- [0049] 그리고, 데이터 암호화용 비밀키, 데이터 소유자 키, 사용자 키 및 변환 키를 생성한다(S202).
- [0050] 다음으로, 중개자 단말(30)이 중개자 비밀키, 중개자 준동형 비밀 키를 생성한다(S203).
- [0051] 다음으로, 사용자 단말(50)이 사용자 공공 키, 사용자 개인 키를 생성한다(S204).
- [0052] 다음으로, 데이터 소유자 단말(10)이 중개자 단말(30)에 키워드 빈도를 전송한다(S205).
- [0053] 다음으로, 사용자 단말(50)이 데이터 소유자 단말(10)에 사용자 공공키를 전송한다(S206).
- [0054] 다음으로, 데이터 소유자 단말(10)이 데이터 암호화용 비밀키를 이용하여 데이터를 대칭 암호화 방식으로 암호화한다(S207).
- [0055] 그리고, 키워드를 부호화하고, 데이터 소유자 키를 이용하여 부호화된 키워드를 프록시 재-암호화방식으로 암호화한다(S208).
- [0056] 그리고, 사용자 공공 키를 이용하여 사용자 키를 비대칭암호화 방식으로 암호화한다(S209).
- [0057] 다음으로, 중개자 단말(30)이 키워드 주파수 암호화용 제1 중개자 비밀 키를 이용하여 키워드 주파수를 대칭 암호화 방식으로 암호화한다(S210).
- [0058] 그리고, 중개자 단말(30)이 데이터 소유자 단말(10)에 암호화된 키워드 빈도를 전송한다(S211).
- [0059] 다음으로, 데이터 소유자 단말(10)이 암호화된 데이터, 암호화된 키워드와 키워드의 빈도로 구성된 인덱스, 암호화된 사용자 키를 외부 서버(70)에 저장한다(S212).
- [0060] 도 3은 본 발명의 일 실시예에 따른 암호화된 데이터의 검색 방법의 순서도이다.
- [0061] 사용자 단말(50)이 외부 서버(70)에 저장된 암호화된 사용자 키를 다운로드 한다(S301).
- [0062] 그리고, 사용자 개인 키를 이용하여 암호화된 사용자 키를 비대칭 복호화 방식으로 복호화한다(S302).
- [0063] 그리고, 암호화된 데이터의 검색을 위한 키워드를 포함하는 검색 기준을 생성하고, 부호화 함수를 사용하여 검색 기준을 부호화하고, 사용자 키를 이용하여 부호화된 검색 기준을 프록시 재-암호화 방식으로 암호화한다(S303).
- [0064] 그리고, 중개자 단말(30)에 암호화된 검색기준을 전송한다(S304).
- [0065] 다음으로, 중개자 단말(30)이 암호화된 검색 기준에 기초하여 검색 질의를 생성하고, 중개자 준동형 비밀키를 이용하여 생성된 검색질의를 준동형 암호화 방식으로 암호화한다(S305).
- [0066] 그리고, 외부 서버(70)에 암호화된 검색질의를 전송한다(S306).
- [0067] 다음으로, 외부 서버(70)가 사용자 키를 이용하여 암호화된 키워드를 프록시 재-암호화 방식으로 재암호화한다(S307).
- [0068] 그리고, 암호화된 검색질의를 암호화 상태에서 수행한다(S308).

- [0069] 그리고, 중개자 단말(30)에 암호화된 질의 수행 결과를 전송한다(S309).
- [0070] 다음으로, 중개자 단말(30)은 암호화된 질의 수행 결과를 복호화한다(S310).
- [0071] 그리고, 사용자 단말(50)에 질의 수행 결과를 전송한다(S311).
- [0072] 다음으로, 사용자 단말(50)은 암호화된 검색기준을 복호화한다(S311).
- [0073] 그리고, 암호화된 검색기준을 복호화한다(S312).
- [0074] 그리고, 사용자가 원하는 데이터를 검출한다(S313)

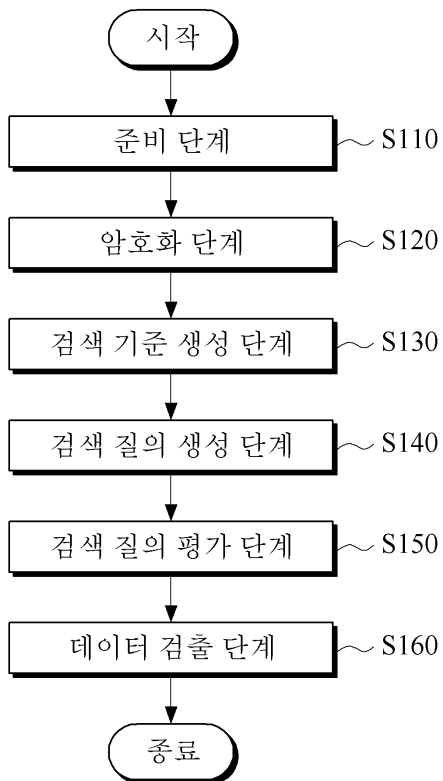
부호의 설명

- [0075] 10 : 데이터 소유자 단말
- 30 : 중개자 단말
- 50 : 사용자 단말
- 70 : 외부 서버

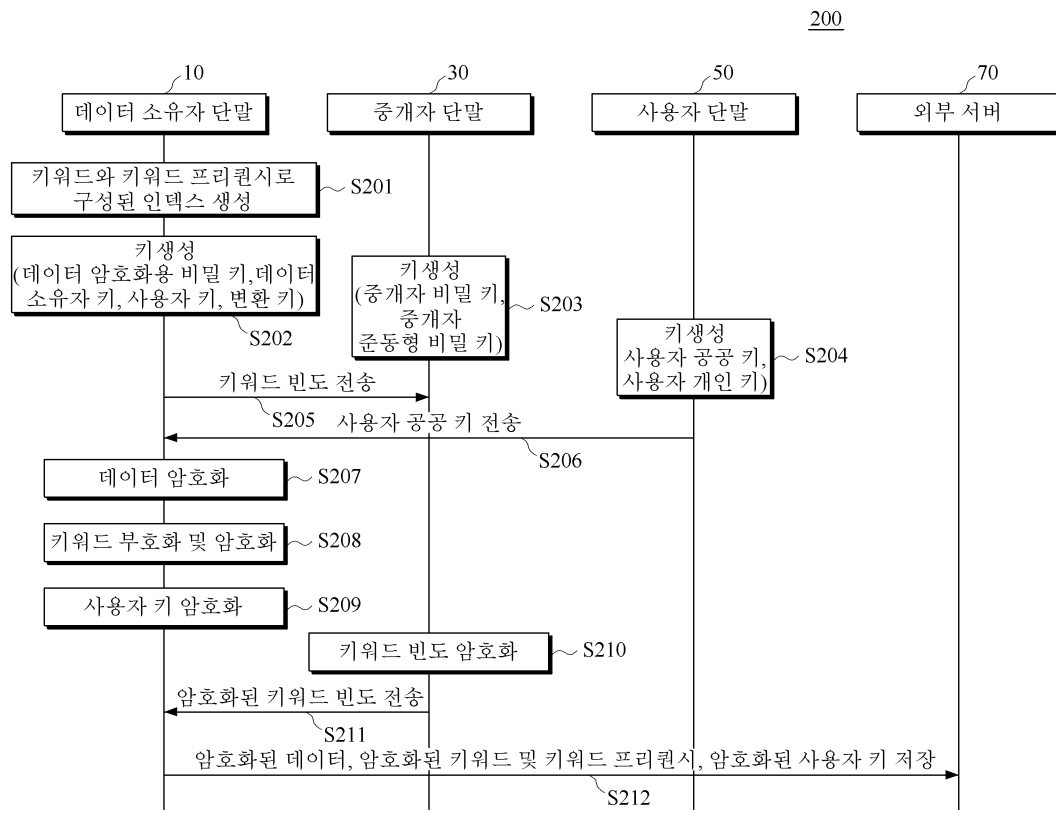
도면

도면1

100



도면2



도면3

