

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2014-0033573 (43) 공개일자 2014년03월19일
(51) 국제특허분류(Int. Cl.) G06F 21/30 (2013.01) G06F 15/16 (2006.01)	(71) 출원인 경희대학교 산학협력단 경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스 내 (서천동, 경희대학교)	
(21) 출원번호 10-2012-0097344		
(22) 출원일자 2012년09월03일	(72) 발명자	
심사청구일자 2012년09월03일	이승룡 경기 성남시 분당구 구미로144번길 25, 102동 102호 (구미동, 삼환빌라)	
	폐베즈 지산 경기 용인시 기흥구 덕영대로 1732, 전자정보대학 351호 (서천동, 경희대학교)	
	(74) 대리인 특허법인 신지	

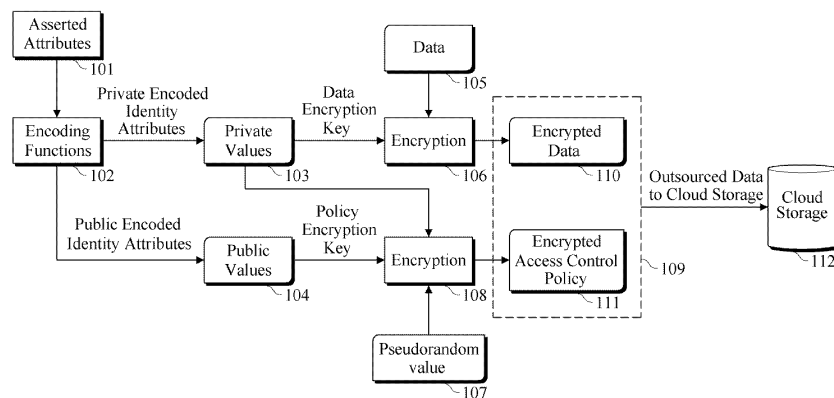
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 퍼블릭 클라우드 스토리지 서비스를 위한 데이터 위임 및 액세스 방법

(57) 요약

타깃 사용자를 위하여 클라우드 스토리지에 데이터를 위임하고 또한 위임된 데이터에 액세스하는 방법이 개시된다. 일 실시예에 따른 데이터의 위임 방법은 권한 엔티티(authority)와 접촉하여 상기 타깃 사용자의 아이덴티티 속성들을 확인하는 초기화 단계, 확인된 아이덴티티 속성들을 퍼블릭 인코딩 함수와 프라이빗 인코딩 함수로 인코딩하는 정책 모델링 단계, 랜덤 마스크와 프라이빗 인코딩 함수로 인코딩된 프라이빗 속성값들을 이용하여 생성된 마스터 키로 데이터를 암호화하는 데이터 은닉 단계, 퍼블릭 속성값들과 퍼블릭 인코딩 함수로 인코딩된 프라이빗 속성값들을 암호화하는 정책 은닉 단계, 및 암호화된 프라이빗 속성값, 암호화된 퍼블릭 속성값, 및 암호화된 데이터와 함께 은닉된 랜덤 마스크와 마스터 키를 클라우드 스토리지에 전달하는 위임 단계를 포함한다.

대표도



이 발명을 지원한 국가연구개발사업

과제고유번호 2011-0030823

부처명 교육과학기술부

연구사업명 선도연구센터지원사업

연구과제명 디지로그휴먼미디어 감성인지 기술연구개발

기 여 율 1/1

주관기관 경희대학교산학협력단

연구기간 2012.09.01 ~ 2013.08.31

특허청구의 범위

청구항 1

타깃 사용자를 위하여 클라우드 스토리지에 데이터를 위임하는 방법에 있어서,

권한 엔티티(authority)와 접촉하여 상기 타깃 사용자의 아이덴티티 속성들을 확인하는 초기화 단계;

확인된 상기 아이덴티티 속성들을 퍼블릭 인코딩 함수와 프라이빗 인코딩 함수로 인코딩하는 정책 모델링 단계;

랜덤 마스크와 상기 프라이빗 인코딩 함수로 인코딩된 프라이빗 속성값들을 이용하여 생성된 마스터 키로 상기 데이터를 암호화하는 데이터 은닉 단계;

상기 퍼블릭 속성값들과 상기 퍼블릭 인코딩 함수로 인코딩된 프라이빗 속성값들을 암호화하는 정책 은닉 단계; 및

상기 암호화된 프라이빗 속성값, 상기 암호화된 퍼블릭 속성값, 및 상기 암호화된 데이터와 함께 은닉된 상기 랜덤 마스크와 상기 마스터 키를 상기 클라우드 스토리지에 전달하는 위임 단계를 포함하는 퍼블릭 클라우드 스토리지 서비스를 위한 데이터 위임 방법.

청구항 2

제1항에 있어서,

상기 마스터 키는 상기 데이터 은닉 단계에서 상기 인코딩된 프라이빗 속성값들을 시드로 사용하여 생성된 가상 랜덤 함수로 초기화하여 구하는 것을 특징으로 하는 퍼블릭 클라우드 스토리지 서비스를 위한 데이터 위임 방법.

청구항 3

제1항에 있어서,

상기 퍼블릭 속성값들은 랜덤 대칭 인코딩 키를 사용하여 암호화하고,

상기 프라이빗 속성값들은 대칭 인코딩 키를 암호화하되, 상기 대칭 인코딩 키는 상기 프라이빗 속성값들 각각에 대하여 대응되는 퍼블릭 속성값과 상기 랜덤 마스크를 사용하여 가상 랜덤 함수를 초기화하여 구하는 것을 특징으로 하는 퍼블릭 클라우드 스토리지 서비스를 위한 데이터 위임 방법.

청구항 4

제1항의 데이터 위임 방법에 따라서 위임된 데이터에 액세스하기 위한 방법에 있어서,

상기 타깃 사용자가 상기 퍼블릭 속성값들을 획득하고 또한 상기 데이터에 대한 액세스 요청을 모델링하여 암호화된 데이터 액세스 요청을 전달하는 속성 준비 단계;

상기 암호화된 퍼블릭 속성값들과 상기 퍼블릭 인코딩 함수로 인코딩된 암호화된 프라이빗 속성값들을 이용하여 데이터 액세스 제어 정책을 검증하는 정책 검증 단계; 및

상기 정책 검증 단계의 검증 결과를 이용하여 위임된 상기 데이터를 복호화하는 단계를 포함하는 퍼블릭 클라우드 스토리지 서비스를 위한 데이터 액세스 방법.

청구항 5

제4항에 있어서, 상기 속성 준비 단계에서는

상기 클라우드 스토리지로부터 상기 은닉된 랜덤 마스크와 은닉된 적법성 키를 획득하는 단계;

프라이빗 키를 사용하여 상기 은닉된 랜덤 마스크와 은닉된 적법성 키를 복호화하여 상기 랜덤 마스크와 상기 적법성 키를 얻는 단계; 및

아이덴티티 속성들에 대하여 상기 퍼블릭 속성값들을 계산하는 단계를 포함하는 것을 특징으로 하는 퍼블릭 클

라우드 스토리지 서비스를 위한 데이터 액세스 방법.

명세서

기술분야

[0001] 본 발명은 퍼블릭 클라우드 스토리지 서비스(public cloud storage service)에 관한 것으로, 보다 구체적으로 데이터를 위임하고 또한 위임된 데이터에 액세스를 하기 위한 퍼블릭 클라우드 스토리지 서비스에서의 액세스 제어 정책(access control policy)을 활성화하는 방법과 관련된다.

배경기술

[0002] 퍼블릭 클라우드 스토리지 서비스에서 정당한 권한을 갖는 데이터 액세스를 보장하기 위하여, 액세스 제어 정책 프레임워크가 사용되고 있다. 액세스 제어 정책 프레임워크라는 개념은 사용자의 액세스 파라미터가 데이터 소유자에 의하여 규정된 액세스 제어 정책에 부합하는지를 보장하는 것과 관련된다. 이러한 액세스 제어 정책은 일반적으로 신뢰성있는 엔티티(trustable entity)에 의하여 검증(evaluation)되는 것을 전제로 하고 있다.

[0003] 퍼블릭 클라우드 스토리지 서비스에서 액세스 제어 정책 프레임워크를 사용하는 것과 관련하여 여러 가지 알고리즘들이 제안되었다. 그 중의 하나는 비특허문헌 1이다. 비특허문헌 1에서, Weichao Wang 등은 대규모의 대용량 데이터를 위한 클라우드 기반 데이터 공유 시스템(cloud based data sharing system)을 제안하고 있다.

정교한 액세스 제어를 달성하기 위하여, 데이터는 복수의 데이터 블록들 $D_1, D_2, \dots, D_n$ 로 나누어지는데 각 데이터 블록은 고유의 블록 부호화키(distinctive block encryption key)로 부호화된다. 이들 부호화키들은 이진 트리(binary tree)에서 부모 노드(parent node), 즉 비-잎 노드(non-leaf node)로부터 유효한 블록 부호화키를 유추하는 가능성을 가지고 데이터 소유자에 의하여 관리된다. 데이터 소유자는 직접 모든 합법적인 사용자에게 비밀 값(secret value)과 함께 보안 토큰(security token)을 발행한다. 보안 토큰은 적법한 사용자에게 의하여 개시되는 요청을 보장하기 위하여 스토리지 제공자에 의하여 사용된다. 데이터 소유자는 직접 사용자의 액세스 권한(access privileges)을 평가한 후에 적절한 비밀 값을 공개한다.

[0004] 비특허문헌 2에는 정책 기반 보장 파일 삭제(policy-based assured file deletion)에 기초한 보안 오브레이 클라우드 시스템(secure overlay cloud storage system)인 FADE가 개시되어 있다. 기밀성이 보장되고 또한 권한 있는 데이터 액세스를 보장하기 위하여, 아웃소싱되는 데이터(outsourced data)를 은닉하기 위하여 데이터 암호화 키(data encryption key)가 사용되고, 데이터 암호화 키를 암호화하기 위하여 제어 키(control key)가 사용된다. 은닉된 아웃소싱된 데이터와 데이터 암호화 키는 클라우드 스토리지로 내보내지는 반면, 제어 키는 키 관리자에 의하여 관리된다. 이 키 관리자에 의하여 정책이 유지되고 검증된다. 이에 의하면, 정책이 변경될 때마다, 적절한 제어 키는 삭제되어서 아웃소싱된 데이터에 대한 액세스가 제한되는 한계가 있다.

[0005] 비특허문헌 3에는 아마존 S3에 기반한 스토리지 서비스인 트러스트스토어(TrustStore)가 개시되어 있다. 트러스트스토어에서는 스토리지 가입자들이 데이터 기밀성과 무결성이 고려된 상황에서 스토리지 서비스 제공자(Storage Service Provider, SSP)에게 그들의 비밀 데이터를 아웃소싱할 수 있다. 트러스트스토어에서는 키 관리 서비스 제공자(Key Management Service Provider, KMSP)를 사용하여 복호화 키를 생성하여 배포하는 것에 추가하여, 이 KMSP가 또한 사용자 인증의 책임을 맡는다. 트러스트스토어에서는 데이터를 두 부분, 즉 데이터 조각들(data-fragments)과 메타데이터 오브젝트(meta-data object)로 분리한다. 데이터 조각들은 데이터를 같은 크기로 분할한 것으로서, 각각 서로 구별되는 부호화 키를 사용하여 부호화된다. 그리고 메타데이터 오브젝트는 부호화 키와 데이터 조각들에 대한 정보를 담고 있다. 데이터 조각들은 스토리지 제공자들에게 아웃소싱되며, 메타데이터는 KMSP에 저장된다.

[0006] 비특허문헌 4에는 암호 클라우드 스토리지(Cryptographic Cloud Storage)가 개시되어 있다. 암호 클라우드 스토리지는 3개의 주요 구성요소, 즉 데이터 프로세서(Data Processor, DP), 데이터 인증기(Data Verifier, DV), 및 신임장 생성기(Credential Generator, CG)로 구성되어 있다. DP는 아웃소싱된 데이터를 부호화하고, DV는 클라우드 스토리지에서 데이터 무결성을 인증하며, CG는 데이터 소유자가 아웃소싱된 데이터를 공유하기를 원하는 사용자들을 위하여 복호화 키를 생성한다. 복호화 키는 액세스 제어 정책과 사용자의 액세스 권한에 따라서 생성된다. 이러한 암호 클라우드 스토리지를 이용하면, 복호화 키를 ABE(Attributes Based Encryption)를 이용

하여 암호화함으로써 정교한 액세스 제어를 달성할 수 있다(비특허문헌 5 참조).

[0007] 그러나 전문적인 비특허문헌들에 개시되어 있는 액세스 제어 정책들은 모두 스토리지 서비스 제공자 및/또는 인증 관리자가 신뢰할만한 엔티티인 것을 전제로 하고 있다. 하지만, 현실적으로 스토리지 서비스 제공자 및/또는 인증 관리자가 100% 신뢰하기 어려운 측면이 있을 뿐만 아니라 또한 아웃소싱된 데이터에 대한 불법적인 접근을 기술적으로 완벽하게 차단하기는 어려운 측면이 있기 때문에, 스토리지 시스템 전체가 비신뢰 시스템일 수도 있다. 이러한 상황에서, 전문적인 비특허문헌들에 개시되어 있는 액세스 제어 정책들은 보안성과 기밀성을 완벽하게 달성하기에 한계가 있다.

선행기술문헌

비특허문헌

- [0008] (비특허문헌 0001) 1. Wang, W., Li, Z., Owens, R., Bhargava, B.: Secure and efficient access to outsourced data. In: Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW '09, pp. 55-66. ACM, New York, NY, USA (2009).
- (비특허문헌 0002) 2. Tang, Y., Lee, P.P.C., Lui, J.C.S., Perlman, R.: Fade: Secure overlay cloud storage with file assured deletion. In: SecureComm, pp. 380-397 (2010).
- (비특허문헌 0003) 3. Yao, J., Chen, S., Nepal, S., Levy, D., Zic, J.: Truststore: Making amazon s3 trustworthy with services composition. In: Cluster, Cloud and Grid Computing (CCGrid), 2010 10th IEEE/ACM International Conference on, pp. 600 -605 (2010).
- (비특허문헌 0004) 4. Kamara, S., Lauter, K.: Cryptographic cloud storage. In: Proceedings of the 14th international conference on Financial cryptography and data security, FC'10, pp. 136-149. Springer-Verlag, Berlin, Heidelberg (2010).
- (비특허문헌 0005) 5. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on Computer and communications security, CCS '06, pp. 89-98. ACM, New York, NY, USA (2006).

발명의 내용

해결하려는 과제

- [0009] 액세스 제어 정책은 권한을 부여 받은 사용자(authorized user)만이 리소스에 액세스할 수 있도록 하는 것이다. 데이터 공유 시스템에서는 이러한 액세스 제어 정책이 다수의 사용자들 사이에서 공유되는 데이터에 대한 액세스를 지배하고 관리한다. 통상적으로 액세스 제어 정책을 검증하기 위하여, 액세스 파라미터(access parameters)가 이 정책에 부합하는지를 체크할 수 있는 신뢰할만한 엔티티(trusted entity)가 요구된다. 이 경우에는 액세스 제어 정책을 검증하기 위하여 정책 검증자(policy evaluator)는 액세스 제어 정책과 함께 권한을 부여 받은 사용자의 액세스 파라미터를 알게 되는 것이 허용된다.
- [0010] 퍼블릭 클라우드 스토리지 서비스에서, 스토리지 제공자는 신뢰할만한 엔티티(trustable entity)로 간주되지 않을 수가 있다. 이 경우에, 만일 스토리지 제공자가 액세스 제어 정책을 검증하는 동안에 아웃소싱되는 데이터나 정보에 대한 비밀 정보를 알게 된다면, 아웃소싱되는 데이터의 비밀유지(privacy)는 잘 되지 않을 수가 있다. 이러한 문제를 해결하기 위하여, 본 발명에서는 암호화된 액세스 제어 정책 프레임워크가 제안된다.
- [0011] 본 발명이 해결하고자 하는 하나의 과제는 비록 퍼블릭 클라우드 스토리지 서비스의 제공자가 신뢰할 수 없는 엔티티(untrusted entity)라고 하더라도 아웃소싱되는 데이터나 정보의 기밀성을 유지할 수 있는 퍼블릭 클라우드 스토리지 서비스를 위한 데이터 위임 방법 및 위임된 데이터에 대한 액세스 방법을 제공하는 것이다.

과제의 해결 수단

- [0012] 상기한 과제를 해결하기 위한 본 발명의 일 실시예에 따른 퍼블릭 클라우드 스토리지 서비스를 위한 데이터 위임 방법은 타깃 사용자를 위하여 클라우드 스토리지에 데이터를 위임하는 방법으로서, 권한 엔티티(authority)와 접촉하여 상기 타깃 사용자의 아이덴티티 속성들을 확인하는 초기화 단계, 확인된 상기 아이덴티티 속성들을 퍼블릭 인코딩 함수와 프라이빗 인코딩 함수로 인코딩하는 정책 모델링 단계, 랜덤 마스크와 상기 프라이빗 인코딩 함수로 인코딩된 프라이빗 속성값들을 이용하여 생성된 마스터 키로 상기 데이터를 암호화하는 데이터 은닉 단계, 상기 퍼블릭 속성값들과 상기 퍼블릭 인코딩 함수로 인코딩된 프라이빗 속성값들을 암호화하는 정책 은닉 단계, 및 상기 암호화된 프라이빗 속성값, 상기 암호화된 퍼블릭 속성값, 및 상기 암호화된 데이터와 함께 은닉된 상기 랜덤 마스크와 상기 마스터 키를 상기 클라우드 스토리지에 전달하는 위임 단계를 포함한다.
- [0013] 상기 실시예의 일 측면에 의하면, 상기 마스터 키는 상기 데이터 은닉 단계에서 상기 인코딩된 프라이빗 속성값들을 시드로 사용하여 생성된 가상 랜덤 함수로 초기화하여 구할 수 있다.
- [0014] 상기 실시예의 다른 측면에 의하면, 상기 퍼블릭 속성값들은 랜덤 대칭 인코딩 키를 사용하여 암호화하고, 상기 프라이빗 속성값들은 대칭 인코딩 키를 암호화하되, 상기 대칭 인코딩 키는 상기 프라이빗 속성값들 각각에 대하여 대응되는 퍼블릭 속성값과 상기 랜덤 마스크를 사용하여 가상 랜덤 함수를 초기화할 수 있다.
- [0015] 상기한 과제를 해결하기 위한 본 발명의 일 실시예에 따른 퍼블릭 클라우드 스토리지 서비스를 위한 위임된 데이터에 대한 액세스 방법은 전술한 데이터 위임 방법에 따라서 위임된 데이터에 액세스하기 위한 방법으로서, 상기 타깃 사용자가 상기 퍼블릭 속성값들을 획득하고 또한 상기 데이터에 대한 액세스 요청을 모델링하여 암호화된 데이터 액세스 요청을 전달하는 속성 준비 단계, 상기 암호화된 퍼블릭 속성값들과 상기 퍼블릭 인코딩 함수로 인코딩된 암호화된 프라이빗 속성값들을 이용하여 데이터 액세스 제어 정책을 검증하는 정책 검증 단계, 및 상기 정책 검증 단계의 검증 결과를 이용하여 위임된 상기 데이터를 복호화하는 단계를 포함한다.
- [0016] 상기 실시예의 일 측면에 의하면, 상기 속성 준비 단계는 상기 클라우드 스토리지로부터 상기 은닉된 랜덤 마스크와 은닉된 적법성 키를 획득하는 단계, 프라이빗 키를 사용하여 상기 은닉된 랜덤 마스크와 은닉된 적법성 키를 복호화하여 상기 랜덤 마스크와 상기 적법성 키를 얻는 단계, 및 아이덴티티 속성들에 대하여 상기 퍼블릭 속성값들을 계산하는 단계를 포함할 수 있다.

발명의 효과

- [0017] 본 발명에 따른 액세스 제어 정책의 구현 방법에 의하면, 정당한 권한이 있는 사용자는 아웃소싱되는 데이터에 대한 접속은 허용하지만, 스토리지 제공자는 액세스 제어 정책을 검증하는 과정에서 아웃소싱되는 데이터나 정보에 대하여 전혀 알 수가 없다. 따라서 본 발명에 의하면, 퍼블릭 클라우드 스토리지 서비스 등과 같이 서비스 제공자나 사용자들의 접속을 제어하는 인증 권한을 가진 엔티티가 완전히 신뢰할 수 없는 시스템이라고 하더라도, 아웃소싱되는 데이터의 비밀유지가 충분히 이루어질 수 있다.

도면의 간단한 설명

- [0018] 도 1은 본 발명의 일 실시예에 따른 액세스 제어 모델링 과정의 일례를 보여주는 블록 다이어그램이다.
- 도 2는 본 발명의 일 실시예에 따른 액세스 제어 모델링 과정의 일례를 보여 주는 흐름도이다.
- 도 3은 본 발명의 일 실시예에 따른 암호화된 액세스 제어 정책 검증 과정의 일례를 보여주는 블록 다이어그램이다.
- 도 4는 도 3의 액세스 제어 정책 검증 과정에 대응하는 흐름도의 일례이다.

발명을 실시하기 위한 구체적인 내용

- [0019] 이하, 첨부된 도면들을 참조하여 본 발명의 실시예를 상세하게 설명한다. 사용되는 용어들은 실시예에서의 기능을 고려하여 선택된 용어들로서, 그 용어의 의미는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 후술하는 실시예들에서 사용된 용어의 의미는, 본 명세서에 구체적으로 정의된 경우에는 그 정의에 따르며, 구체적인 정의가 없는 경우는 당업자들이 일반적으로 인식하는 의미로 해석되어야 할 것이다.

[0020] 도 1은 본 발명의 일 실시예에 따른 액세스 제어 모델링 과정의 일례를 보여주는 블록 다이어그램이다. 그리고 도 2는 도 1의 액세스 제어 모델링 과정에 대응하는 흐름도의 일례이다.

[0021] 도 1 및 도 2를 참조하면, 우선 타깃 사용자의 아이덴티티 정보(identity information)를 획득하기 위한 초기화 과정이 진행된다(도 1의 블록 101, 도 2의 단계 S11). 이를 위하여, 기밀이 유지되는 데이터를 타깃 사용자와 공유하기 위하여, 데이터 소유자는 권한 엔티티(authority)와 접촉하여 타깃 사용자의 아이덴티티 속성들(identity attributes, $att_{0...n}$)을 전달하고 이에 대한 확인을 요청한다. 데이터 소유자의 요청에 대한 응답으로, 권한 엔티티는 타깃 사용자의 아이덴티티 속성들이 아이덴티티 선택 기준(identity selection criteria)을 충족하는지 확인을 해준다. 이외에도, 권한 엔티티는 또한 타깃 사용자의 퍼블릭 키(k_{pub})를 데이터 소유자에게 제공할 수 있다.

[0022] 그리고 이러한 초기화 과정 이후에, 데이터 소유자가 퍼블릭 스토리지 서버로 데이터를 아웃소싱하는 절차가 진행된다(도 1의 블록 102 이후 및 도 2의 단계 S12 이후). 본 발명의 실시예에 의하면, 아웃소싱되는 데이터의 비밀유지가 이루어질 수 있도록, 후술하는 데이터 아웃소싱 절차는 네 개의 서로 연관된 단계들, 즉 정책 모델링(policy modeling) 단계, 데이터 은닉(data concealment) 단계, 정책 은닉(policy concealment) 단계, 및 위임(delegation) 단계를 포함하여 구성된다.

[0023] 먼저, 정책 모델링 단계에서는 두 개의 인코딩 함수, 즉 퍼블릭 인코딩 함수(public encoding function)와 프라이빗 인코딩 함수(private encoding function)를 사용하여, 확인된 아이덴티티 속성들을 인코딩한다(도 1의 블록 102, 103, 104 및 도 2의 단계 S12). 이것은 데이터 소유자가 인코딩 함수들을 사용하여 확인된 아이덴티티 속성들을 인코딩함으로써, 이러한 것들을 소유하고 있다는 것이 사용자의 적법성과 진정성(legitimacy and authenticity)을 보장할 수 있도록 활용하기 위한 것이다. 본 단계에서는 각각의 확인된 아이덴티티 속성(att_i)에 대하여, 데이터 소유자는 두 개의 인코딩 함수(encoding function)를 사용하여 수학적 1과 같은 두 개의 값, 즉 퍼블릭 인코딩된 아이덴티티 속성값(public encoded identity attribute value, l_i , 이하, '퍼블릭 속성값(public values)'이라 한다) 및 프라이빗 인코딩된 아이덴티티 속성값(private encoded identity attribute value, $\hat{l}_i$, 이하, '프라이빗 속성값(private values)'이라 한다)을 계산한다. 도 1에서 블록 103과 블록 104는 각각 블록 102의 결과로 생성되는 프라이빗 속성값과 퍼블릭 속성값을 가리킨다.

수학적 1

$$l_i: H_1(att_i)$$

$$\hat{l}_i: H_2(att_i)$$

[0024]

[0025] 여기서, H_1 은 퍼블릭 인코딩 함수이고, H_2 는 프라이빗 인코딩 함수이다.

[0026] 다음으로, 클라우드 스토리지(도 1의 블록 112)로 아웃소싱될 데이터에 대한 은닉 단계가 진행된다(도 1의 블록 103, 105, 106, 110 및 도 2의 단계 S13). 즉, 전술한 단계에서 생성된 프라이빗 속성값들(블록 103)을 이용하여 생성된 마스터 키(master key)로 아웃소싱될 데이터를 부호화한다. 보다 구체적으로, 먼저 정책 모델링 단계에서 생성된 프라이빗 속성값들($\hat{l}_{0...n}$, 블록 103)을 시드(seed)로 사용하여 가상 랜덤 함수(pseudo random function, ψ)를 생성한다. 그리고 생성된 가상 랜덤 함수는 마스터 암호화 키(k), 즉 데이터 암호화 키(data encryption key)를 초기화하는데, 아웃소싱될 데이터(블록 105)는 이 초기화를 통해 유도된 마스터 키(k)를 이용하여 암호화한다($\mathcal{F}^k$, 블록 106). 그리고 이와 같이 암호화된 데이터(encrypted data, 블록 110)가 클라우드 서버(블록 112)로 아웃소싱된다.

[0027] 계속해서, 프라이빗 속성값들과 퍼블릭 속성값들을 암호화하는 정책 은닉 단계가 수행된다(도 1의 블록 103, 104, 107, 108, 111 및 도 2의 단계 S14). 은닉 단계에서는 먼저, 정책 모델링 단계에서 생성된 프라이빗 속성

값들($\hat{l}_{0...n}$, 블록 103)을 은닉하기 위하여 랜덤 마스크($\tilde{r}$)를 생성한다. 그리고 각 프라이빗 속성값($\hat{l}_i$)에 대하여, 대응되는 퍼블릭 속성값(l_i)과 랜덤 마스크($\tilde{r}$)를 사용하여 가상 랜덤 함수(ψ)를 초기화한다(블록 107). 그 결과, 대칭 암호화 키(symmetric encryption key), 즉 위임 키(mandatory key : δ_i)가 생성된다. 이러한 과정은 다음의 수학적 식 2와 같이 표현될 수 있다. 그리고 각 프라이빗 속성값($\hat{l}_i$)은 각각의 대칭 암호화 키(δ_i)를 사용하여 암호화한다(블록 108). 암호화의 결과, 즉 암호화된 프라이빗 속성값들은 $\hat{l}_{0...n}^{\delta_{0...n}}$ 로 표시할 수 있다.

수학적 식 2

$$\psi(\hat{l}_i, \tilde{r}) \rightarrow \delta_i$$

그리고 데이터 소유자는 랜덤 대칭 암호화 키(random symmetric encryption key), 즉 적법성 키(legitimacy key, ω)를 생성하고, 이 랜덤 대칭 암호화 키(ω)를 이용하여 퍼블릭 속성값들($l_{0...n}$, 블록 104) 각각을 암호화한다(블록 108). 암호화의 결과, 즉 암호화된 퍼블릭 속성값들은 $l_{0...n}^{\omega}$ 로 표시할 수 있다.

마지막으로 암호화된 데이터를 포함한 정보들을 클라우드 스토리지에 저장하는 위임 단계가 수행된다(도 1의 블록 109 - 112 및 도 2의 단계 S15). 보다 구체적으로, 본 위임 단계에서 데이터 소유자는 암호화된 데이터(블록 110)는 물론 전술한 과정에서 은닉된 랜덤 마스크($\tilde{r}^{k_{pub}}$) 및 은닉된 적법성 키($\omega^{k_{pub}}$)와 함께 암호화된 값들, 즉 암호화된 퍼블릭 속성값들 $l_{0...n}^{\omega}$ 과 암호화된 프라이빗 속성값들 $\hat{l}_{0...n}^{\delta_{0...n}}$ (블록 111)을 클라우드 스토리지(112)로 아웃소싱함으로써 정책 검증 절차(policy evaluation process)를 위임한다.

도 3은 본 발명의 일 실시예에 따른 암호화된 액세스 제어 정책 검증 과정의 일례를 보여주는 블록 다이어그램이다. 그리고 도 4는 도 3의 액세스 제어 정책 검증 과정에 대응하는 흐름도의 일례이다. 본 실시예에 따른 액세스 제어 정책 검증 과정은 사용자가 클라우드 스토리지에 위임되어 있는 데이터에 대한 액세스, 즉 파일 액세스(file access)를 수행할 경우에 수행될 수 있지만, 여기에만 한정되는 것은 아니다.

만일 타깃 사용자가 요구되는 속성들의 집합(required set of attributes)을 소유하고 있다면, 이 타깃 사용자는 비밀값들을 알고 난 이후에 클라우드 서버와 위임된 프라이빗 매칭(delegated Private Matching, DPM) 프로토콜을 시작한다. 액세스 제어 정책을 검증하고 그리고 권한이 있는 타깃 사용자가 유효한 마스터 키를 유추하는 것을 도와줄 수 있도록, 파일 액세스 과정은 세 개의 연관된 단계들, 즉 속성 준비(attribute preparation) 단계, 정책 검증(policy evaluation) 단계, 및 위임된 값 복원(mandatory value recovery) 단계를 포함한다.

도 3 및 도 4를 참조하면, 클라우드 스토리지에 저장되어 있는 데이터에 접속하고자 하는 타깃 사용자는 퍼블릭 속성값들을 획득하는 속성 준비 단계를 수행한다(도 3의 블록 201 - 206 및 도 4의 단계 S21 및 단계 S22),

보다 구체적으로, 아웃소싱된 데이터에 액세스하기 위하여, 먼저 타깃 사용자는 클라우드 서버로부터 은닉된 랜덤 마스크($\tilde{r}^{k_{pub}}$)와 은닉된 적법성 키($\omega^{k_{pub}}$)를 획득한다. 그리고 프라이빗 키(k_{pri})를 사용하여, 타깃 사용자는 은닉된 랜덤 마스크($\tilde{r}^{k_{pub}}$)와 적법성 키($\omega^{k_{pub}}$)를 해독하여 랜덤 마스크($\tilde{r}$)와 적법성 키(ω)를 얻는다. 그 이후에, 각 아이덴티티 속성(att_i , 블록 201)에 대하여, 퍼블릭 속성값(l_i)이 상기 수학적 식 1에 의하여 계산된다(블록 202). 그리고 퍼블릭 속성값들($l_{0...n}$, 블록 203)이 랜덤 대칭 인코딩 키(ω)를 이용하여 은닉(인코딩)되며, 인코딩된 퍼블릭 속성값들이 전달된다(단계 S21).

다음으로 액세스 요청 모델링 과정(access request modeling)이 수행하여 암호화된 데이터 액세스 요청

(encrypted data access request)를 전달한다(단계 S22). 보다 구체적으로, 액세스 요청 모델링 과정(블록 204)에서는 루트 $l_{0...n}^{\omega}$ 를 갖는 다항식 $P(y)$ 가 계산될 수 있다. 그리고 타깃 사용자는 암호화 함수(encryption function)를 초기화하고, 비밀 키(secret key, σ_{sk})를 가지고 다항식 $P(y)$ 의 계수들($\alpha_{0...n}$)을 요청과 함께 암호화한다(블록 205 및 206). 그 다음으로, 퍼블릭 키(public key, σ_{pk})와 함께 암호화된 계수들($\alpha_{0...n}^{\sigma_{sk}}$)이 암호화된 데이터 액세스 요청(encrypted data access request)과 함께 클라우드 서버로 보내진다.

[0036] 그리고 암호화된 액세스 제어 정책을 이용하여 정책 검증 과정을 수행한다(도 3의 블록 207 및 208 및 도 4의 단계 S23). 보다 구체적으로, 인코딩된 계수들($\alpha_{0...n}^{\sigma_{sk}}$)을 수신하자마자, 클라우드 서버는 데이터 소유자에 의하여 제공된 은닉된 값들(블록 207), 즉 인코딩된 퍼블릭 속성값들($l_{0...n}^{\omega}$)에 대하여 인코딩된 계수들($\alpha_{0...n}^{\sigma_{sk}}$)을 갖는 다항식 $P(y)$ 을 검증한다(블록 208). 일단 다항식 $P(y)$ 가 검증이 되면, 클라우드 서버는 각 인코딩된 프라이빗 아이덴티티 속성 검증값($\tilde{l}_i^{\delta_i}$)에 대하여 정책 검증 결과(policy evaluation result)인 망각 값(oblivious value, Δ_i)을 $E_H(r.P(y) + \tilde{l}_i^{\delta_i})$ 와 같이 계산한다. 그리고 그 결과 값들인 망각 값들($\Delta_{0...n}$)이 사용자들에게 보내진다.

[0037] 다음으로 정책 검증의 결과값을 이용하여 위임된 값들을 복원하는 과정이 수행된다(도 3의 블록 209 및 도 4의 블록 S24). 보다 구체적으로, 클라우드 서버로부터 망각 값들($\Delta_{0...n}$)을 수신하자마자, 타깃 사용자는 비밀 키(σ_{sk})를 이용하여 $r.P(y) + \tilde{l}_i^{\delta_i}$ 을 복호화한다. 루트 $l_{0...n}^{\omega}$ 를 갖는 다항식 $P(y)$ 가 검증되었으므로, 복호화 함수는 은닉된 값(hidden values, 블록 209), 즉 암호화된 프라이빗 아이덴티티 속성 검증값($\tilde{l}_i^{\delta_i}$)을 얻을 수 있다. 그러나 사용자에게 의하여 생성된 은닉된 적법성 값들이 데이터 소유자가 클라우드 서버에 제공한 값들과 일치하지 않는 경우에는, 망각 값(Δ_i)을 복호화하면 임의의 숫자가 표시될 것이다.

[0038] 일단 사용자가 암호화된 프라이빗 아이덴티티 속성 검증값들($\tilde{l}_{0...n}^{\delta_{0...n}}$)을 가지게 되면, 사용자는 퍼블릭 속성값(l_i)과 랜덤 마스크($\tilde{r}$)를 이용하여 가상 랜덤 함수(ψ)를 초기화하는데, 이것은 위임 키(δ_i)를 생성한다. 이러한 과정은 수학식 3으로 표시될 수 있다.

수학식 3

$$\psi(l_i, \tilde{r}) \rightarrow \delta_i$$

[0039]

[0040] 그리고 이 위임 키(δ_i)를 이용하여 은닉된 값들을 복호화한다. 일단, 모든 값들이 얻어지면, 마스터 키가 유추된다. 마지막으로, 이 마스터 키를 사용하여 아웃소싱된 데이터에 액세스할 수 있다.

[0041] 이상의 설명은 본 발명의 실시예에 불과할 뿐, 이 실시예에 의하여 본 발명의 기술 사상이 한정되는 것으로 해석되어서는 안된다. 본 발명의 기술 사상은 특허청구범위에 기재된 발명에 의해서만 특정되어야 한다. 따라서 본 발명의 기술 사상을 벗어나지 않는 범위에서 전술한 실시예는 다양한 형태로 변형되어 구현될 수 있다는 것은 당업자에게 자명하다.

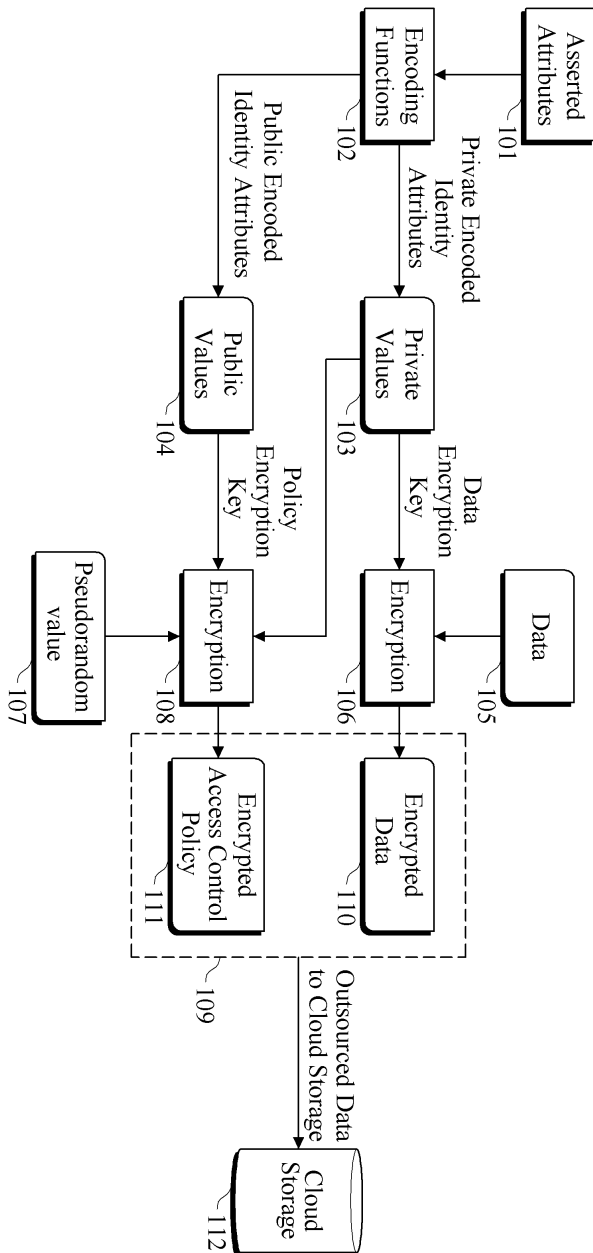
부호의 설명

[0042]

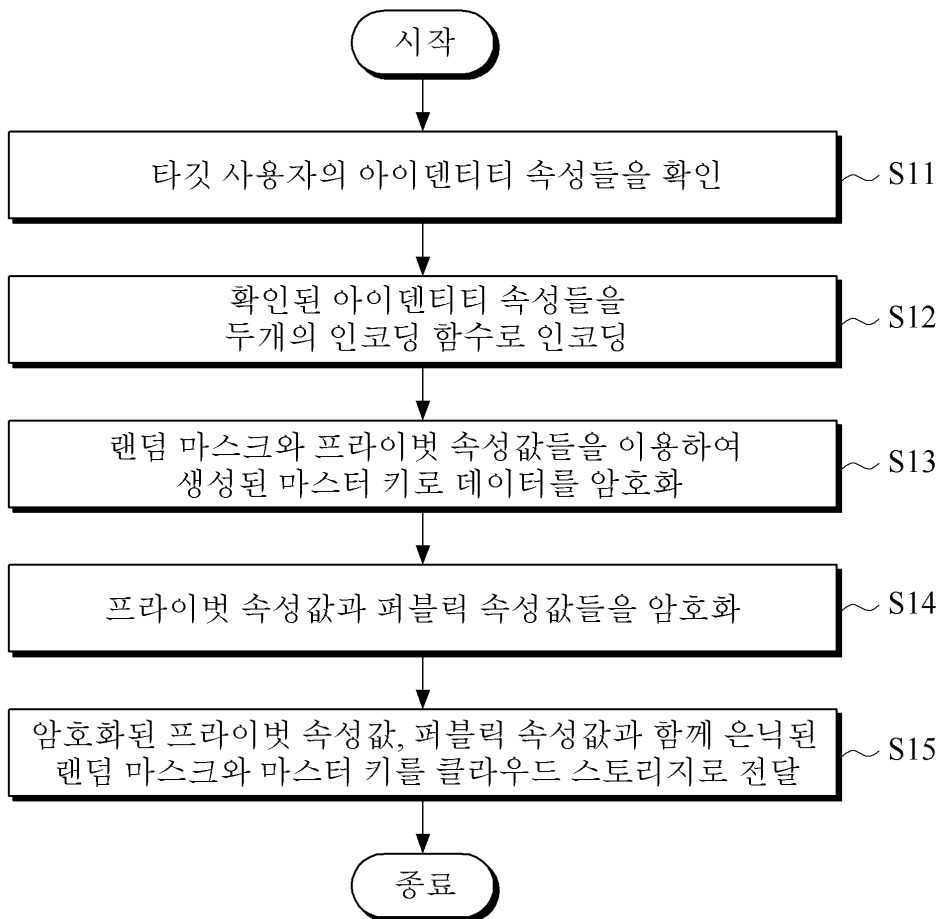
- 101 : 확인된 속성들(attributes)
- 102 : 인코딩 함수들(encoding functions)
- 103 : 프라이빗 값들(private values)
- 104 : 퍼블릭 값들(public values)
- 105 : 아웃소싱될 데이터(data)
- 106 및 107 : 암호화(encryption)
- 108 : 가상 랜덤 값(pseudo random value)
- 109 : 암호화된 데이터(encrypted data, 110) 및 암호화된 액세스 제어 정책(encrypted access control policy, 111)
- 112 : 클라우드 스토리지(cloud storage)
- 201 : 아이덴티티 속성들(identity attributes)
- 202 : 인코딩 함수(encoding function)
- 203 : 퍼블릭 값(public value)
- 204 : 액세스 요청 모델링(access request modeling)
- 205 : 암호화(encryption)
- 206 : 암호화된 요청(encrypted request)
- 207 : 암호화된 액세스 제어 정책(encrypted access control policy)
- 208 : 정책 검증(policy evaluation)
- 209 : 은닉된 값들(hidden values)

도면

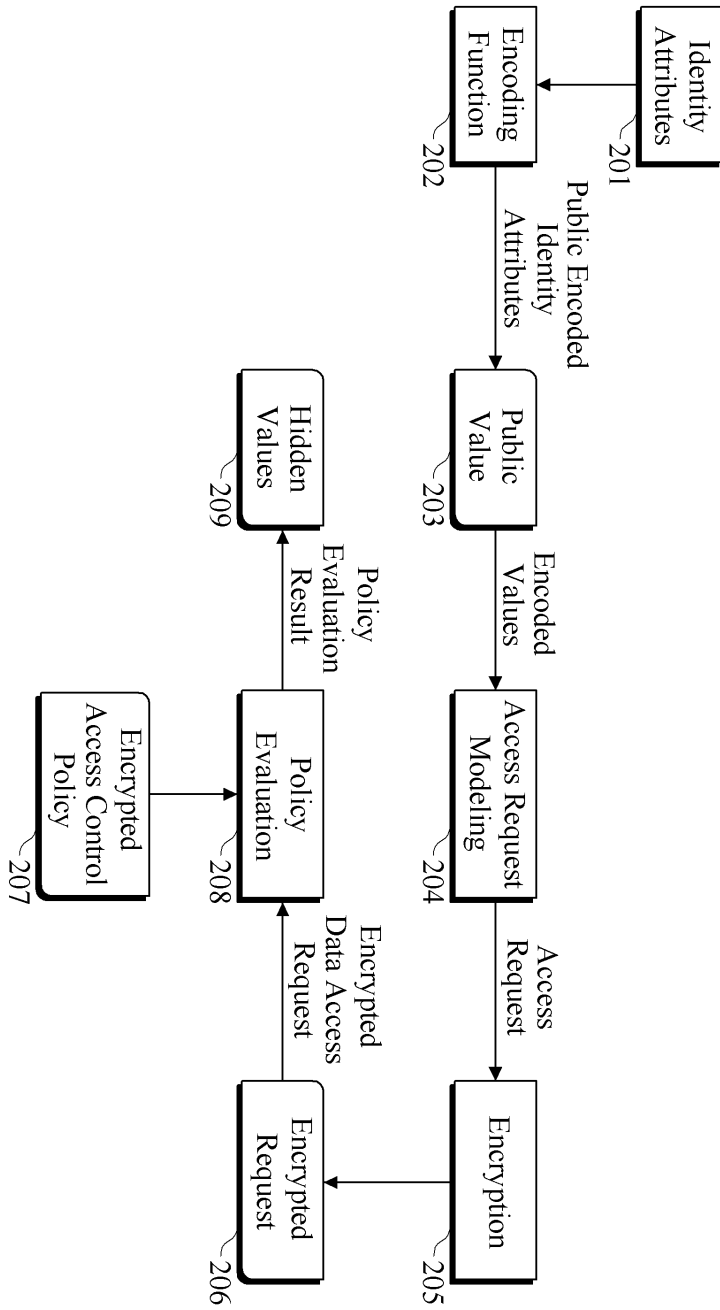
도면1



도면2



도면3



도면4

