



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2016년01월18일

(11) 등록번호 10-1586439

(24) 등록일자 2016년01월12일

(51) 국제특허분류(Int. Cl.)

H04L 9/30 (2006.01) H04L 9/32 (2006.01)

(21) 출원번호 10-2014-0114172

(22) 출원일자 2014년08월29일

심사청구일자 2014년08월29일

(56) 선행기술조사문헌

Jiawei Yuan 외 1인, Communications and Network security (CNS), 2013 IEEE Conference, "Secure and Constant Cost Public Cloud Storage Auditing with Deduplication" (2013.10.16. 공개)

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

정익래

서울특별시 광진구 긴고랑로4길 53, 203호(중곡1동, 호동아파트)

김동민

서울특별시 동대문구 약령시로 154, 1동 505호(청량리동, 미주아파트)

(74) 대리인

심경식, 홍성욱

전체 청구항 수 : 총 13 항

심사관 : 문형섭

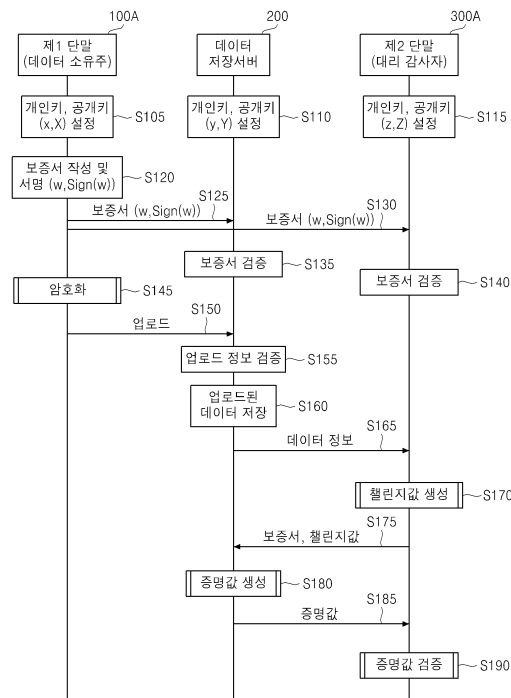
(54) 발명의 명칭 프라이버시를 보장하는 사용자 데이터의 무결성 검증 방법 및 그 장치

### (57) 요약

프라이버시를 보장하는 사용자 데이터의 무결성 검증 방법이 개시된다. 본 발명의 프라이버시를 보장하는 사용자 데이터의 무결성 검증 방법은 프라이버시가 보장된 사용자 데이터 무결성 검증에 필요한 파라미터들을 생성하는 단계; 상기 제1 단말이 상기 파라미터 생성 단계에서 생성된 파라미터 및 암호학적으로 안전한 해쉬 함수에 기초

(뒷면에 계속)

대 표 도 - 도2



하여 업로드할 데이터 파일을 암호화한 후 데이터 저장 서버에 업로드 하는 데이터 아웃소싱 단계; 상기 데이터 저장 서버가 상기 파라미터 생성 단계에서 생성된 파라미터에 기초하여 업로드된 데이터의 정당성을 검증하는 단계; 상기 제2 단말이 상기 업로드된 데이터 파일 일부에 대한 챌린지(challenge)값을 생성하는 단계; 상기 데이터 저장 서버가 상기 제2 단말로부터 상기 챌린지 값을 수신하고, 상기 파라미터 생성 단계에서 생성된 파라미터 및 상기 챌린지 값에 기초하여 증명값을 생성하는 단계; 및 상기 제2 단말이 상기 증명값(proof)과 공개키들을 이용하여 상기 증명값(proof)의 정당성을 검증하는 단계를 포함한다.

이 발명을 지원한 국가연구개발사업

|          |                                      |
|----------|--------------------------------------|
| 과제고유번호   | 2013068200                           |
| 부처명      | 미래창조과학부                              |
| 연구관리전문기관 | 한국연구재단                               |
| 연구사업명    | (이공)중견연구자지원_핵심연구                     |
| 연구과제명    | 실용적인 래티스 기반 익명성 보장 및 연산 가능한 서명 기술 연구 |
| 기 여 율    | 1/1                                  |
| 주관기관     | 고려대학교 산학협력단                          |
| 연구기간     | 2013.12.01 ~ 2014.11.30              |

---

## 명세서

### 청구범위

#### 청구항 1

데이터 파일을 생성하는 제1 단말, 상기 데이터 파일을 저장하는 인터넷 상의 데이터 저장 서버, 상기 데이터 저장 서버에 저장된 데이터 파일의 무결성을 감사하는 제2 단말 간의 상호 관계에 의거하여 사용자 데이터의 무결성을 검증하는 사용자 데이터 무결성 검증 방법에 있어서,

프라이머시가 보장된 사용자 데이터 무결성 검증에 필요한 파라미터들을 생성하고, 상기 제1 단말이 상기 제2 단말에 대한 보증서 및 서명 쌍을 생성하여 상기 데이터 저장 서버 및 상기 제2 단말에 전송하는 단계;

상기 제1 단말이 상기 파라미터 생성 단계에서 생성된 파라미터 및 암호학적으로 안전한 해쉬 함수에 기초하여 업로드할 데이터 파일을 암호화한 후 데이터 저장 서버에 업로드 하는 데이터 아웃소싱 단계;

상기 데이터 저장 서버가 상기 파라미터 생성 단계에서 생성된 파라미터에 기초하여 업로드된 데이터의 정당성을 검증하는 단계;

상기 제2 단말이 상기 업로드된 데이터 파일 일부에 대한 챌린지(challenge)값을 생성하는 단계;

상기 데이터 저장 서버가 상기 제2 단말로부터 상기 챌린지 값과 상기 보증서 및 서명 쌍을 수신하고, 상기 수신한 보증서 및 서명 쌍, 상기 파라미터 생성 단계에서 생성된 파라미터 및 상기 챌린지 값에 기초하여 증명값을 생성하는 단계; 및

상기 제2 단말이 상기 증명값(proof)과 공개키들을 이용하여 상기 증명값(proof)의 정당성을 검증하는 단계를 포함하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

#### 청구항 2

제1항에 있어서, 상기 파라미터 생성 단계는

상기 제1 단말, 상기 데이터 저장 서버, 상기 제2 단말이 각각 자신의 개인키와 공개키를 생성하는 단계;

상기 제1 단말이 상기 제2 단말에 대한 보증서를 작성한 후 상기 제1 단말의 개인키로 서명하는 단계;

상기 보증서 및 서명 쌍을 상기 데이터 저장서버 및 상기 제2 단말에게 전송하는 단계; 및

상기 제1 단말이 공개파라미터를 생성하는 단계를 포함하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

#### 청구항 3

제2항에 있어서, 상기 파라미터 생성 단계는

상기 제1 단말로부터 상기 보증서 및 서명 쌍을 수신한 상기 데이터 저장 서버 및 상기 제2 단말 각각이 해당 서명 값이 상기 보증서에 대해 정당한지를 확인하는 단계; 및

상기 확인 결과 상기 서명 값이 상기 보증서에 대해 정당하지 않은 경우 상기 제1 단말에게 상기 보증서 및 서명 쌍을 재요청하는 단계를 더 포함하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

#### 청구항 4

제2항에 있어서, 상기 업로드 데이터 정당성 검증 단계는

상기 파라미터 생성 단계에서 생성된 상기 데이터 저장 서버의 개인키(y), 상기 제1 단말 및 상기 제2 단말 각

각의 공개키(X, Z) 및 상기 제1 단말이 생성한 공개파라미터(u)에 기초하여 상기 업로드 데이터의 정당성을 검증하되,

하기의 수학적식1 및 수학적식2에 의거하여 제1 및 제2 변수를 생성하고,

하기의 수학적식3이 성립하는지를 확인하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

(수학적식1)

$$t = H(e(X, Z)^y, w)$$

이 때, X는 상기 제1 단말의 공개키, Z는 상기 제2 단말의 공개키, y는 상기 데이터 저장서버의 개인키, w는 상기 제1 단말에서 생성한 보증서이다.

(수학적식2)

$$W_i = \Omega_i(i)$$

이 때, t는 (수학적식 1)에 의해 생성된 제1 변수이다.

(수학적식3)

$$e(T_{m_i}, g) = e(h(W_i) \cdot u^{m_i}, X)$$

이 때,  $T_{m_i}$ 은 데이터 업로드시 전송된 태그, u는 상기 제1 단말이 생성한 공개 파라미터,  $m_i$ 는 i번째 데이터 블록, X는 상기 제1 단말의 공개키이다.

## 청구항 5

제2항에 있어서, 상기 쉘린지값 생성 단계는

상기 업로드된 데이터 중 선택된 블록의 개수(c)와 제1 및 제2 난수( $k_1$ ,  $k_2$ )를 포함하는 쉘린지값을 생성하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

## 청구항 6

제5항에 있어서, 상기 증명값 생성 단계는

정수 집합의 원소인 제3 난수(r)를 생성하고, 상기 제3 난수(r)에 기초하여 제1 증명값(R)을 생성하는 단계;

제1 및 제2 난수( $k_1$ ,  $k_2$ )를 각각 의사난수함수( $\pi$ ) 및 의사난수치환(f)에 적용하여 제3 변수( $a_j$ )를 생성하고, 상기 제3 변수( $a_j$ ) 및 메시지 블록 개수( $m_i$ )에 기초하여 제2 증명값(T)을 생성하는 단계;

상기 제3 변수( $a_j$ ), 메시지 블록 개수( $m_i$ ) 및 상기 제1 증명값(R)에 기초하여 제3 증명값(m)을 생성하는 단계;

상기 데이터 저장 서버의 개인키(y)와, 상기 제1 및 제2 단말의 공개키(X, Z)에 기초하여 제4 증명값( $S_m$ )을 생성하는 단계; 및

상기 제1 내지 제4 증명값을 상기 쉘린지값에 대한 증명값(proof) 값으로 결정하는 단계를 포함하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

## 청구항 7

제6항에 있어서, 상기 증명값 생성 단계는

상기 제2 단말로부터 상기 쉘린지 값 수신시 상기 제2 단말의 보증서 및 서명 쌍을 함께 수신하는 단계;

상기 제2 단말로부터 수신한 보증서 및 서명 쌍의 정당성을 검증하는 단계; 및

상기 제2 단말로부터 수신한 보증서 및 서명쌍이 정당한 경우 상기 제1 단말로부터 수신하여 기 저장된 보증서와 상기 제2 단말로부터 수신한 보증서를 비교하는 단계를 더 포함하고,

상기 제1 단말로부터 수신하여 기 저장된 보증서와 상기 제2 단말로부터 수신한 보증서가 같지 않은 경우 증명값 생성을 중단하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

## 청구항 8

제6항에 있어서, 상기 증명값 검증 단계는

상기 데이터 저장 서버의 비밀키(y) 및 상기 제1 및 제2 단말의 공개키(X, Z)에 기초하여 제3 증명값의 정당성을 판단하는 단계;

상기 제3 증명값이 정당한 경우 상기 제2 단말의 개인키를 이용하여 증명값 검증을 위한 제4 변수(t)를 생성하는 단계; 및

하기의 수학적식4에 의거하여 상기 증명값을 검증하는 단계를 포함하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

(수학적식 4)

$$e(T, G) = e\left(\prod_{i=1}^c h(\Omega_r(\pi_{k_1}(i)))^{f_{k_2}(i)} \cdot u^m \cdot R^{-h(R)}, X\right)$$

## 청구항 9

제1항에 있어서, 상기 데이터 아웃소싱 단계는

의사난수 함수로부터 모델링된 해쉬 함수에 기초하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 방법.

## 청구항 10

데이터 파일을 생성하는 제1 단말 및 데이터 파일을 저장하는 데이터 저장 서버와의 인터페이스를 제공하는 통신 인터페이스부;

프라이버시가 보장된 사용자 데이터 무결성 검증에 필요한 개인키 및 공개키(z, Z)를 설정하는 설정부;

상기 통신 인터페이스부를 통해 상기 제1 단말에서 생성한 보증서 및 서명 쌍을 전달받아 저장하는 제어부;

상기 데이터 저장 서버에 업로드된 데이터 파일에 대한 무결성 확인을 위해 상기 데이터 파일에 일부에 대한 쉼린지 값을 생성하여 상기 제어부에 저장된 보증서 및 서명 쌍과 함께 상기 데이터 저장 서버로 전송하는 쉼린지 값 생성부; 및

상기 데이터 저장 서버에서 생성된 증명값을 제공받아 그 증명값의 정당성을 검증하는 검증부를 포함하는 것을 특징으로 하는 사용자 데이터 무결성 검증 장치.

## 청구항 11

제10항에 있어서, 상기 제어부는

상기 제1 단말로부터 수신한 보증서 및 서명 쌍을 검증하여 해당 서명 값이 상기 보증서에 대해 정당한지를 확인하고 상기 서명 값이 상기 보증서에 대해 정당하지 않은 경우 상기 제1 단말에게 상기 보증서 및 서명 쌍을 재요청하는 것을 특징으로 하는 사용자 데이터 무결성 검증 장치.

## 청구항 12

제10항에 있어서, 상기 검증부는

상기 설정부에서 설정한 개인키(z)를 이용하여 증명값 검증을 위한 변수(t)를 생성하고, 하기의 수학적식4에 의거하여 상기 증명값을 검증하는 것을 특징으로 하는 사용자 데이터의 무결성 검증 장치.

(수학적식 4)

$$e(T, G) = e\left(\prod_{i=1}^c h(\Omega_i(\pi_{k_1}(i)))^{f_{k_1}(i)} \cdot u^m \cdot R^{-h(R), X}\right)$$

## 청구항 13

제12항에 있어서, 상기 검증부는

상기 데이터 저장 서버의 비밀키(y) 및 상기 제1 단말의 공개키(X)와, 상기 설정부에서 설정한 공개키(Z)에 기초하여 상기 증명값에 대한 1차 검증을 실시하고, 상기 1차 검증 결과가 정당하지 않은 경우 증명값 검증을 중단하는 것을 특징으로 하는 사용자 데이터 무결성 검증 장치.

## 발명의 설명

### 기술 분야

[0001] 본 발명은 프라이버시를 보장하는 사용자 데이터의 무결성 검증 방법 및 그 장치에 관한 것으로서, 특히, 클라우드 환경에서 데이터 소유주가 자신의 데이터를 서버에 업로드한 후, 대리인을 지정하여 서버나 다른 공격자의 악의적인 행동으로부터 자신의 데이터가 훼손되지 않고 저장되어 있는지를 확인하는 프라이버시를 보장하는 사용자 데이터의 무결성 검증 방법 및 그 장치에 관한 것이다.

### 배경 기술

[0002] 최근 사용자가 네트워크나 컴퓨터를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 정보통신 환경을 일컫는 유비쿼터스(Ubiquitous) 환경이 일반화되어 감에 따라 원격 컴퓨팅(remote computing)도 함께 확장되는 추세에 있으며, 이러한 원격 컴퓨팅 중 특히 클라우드 컴퓨팅(Cloud computing)이 미래의 컴퓨팅 환경을 주도할 새로운 패러다임으로 부각되고 있다.

[0003] 클라우드 컴퓨팅이란 정보가 인터넷 상의 서버에 영구적으로 저장되고, IT 기기 등(예컨대, 데스크 데스크톱, 태블릿 컴퓨터, 노트북, 넷북, 스마트폰 등)과 같은 클라이언트에는 일시적으로 보관되는 컴퓨터 환경을 뜻한다. 즉 이용자의 모든 정보를 인터넷 상의 서버에 저장하고, 이 정보를 각종 IT 기기를 통하여 언제 어디서든 이용할 수 있도록 한다는 개념이다.

[0004] 다시 말해, 클라우드 컴퓨팅 서비스는 구름(cloud)과 같이 무형의 형태로 존재하는 하드웨어나 소프트웨어 등의 컴퓨팅 자원을 자신이 필요한 만큼 빌려 쓰고 이에 대한 사용요금을 지급하는 방식의 컴퓨팅 서비스로, 서로 다른 물리적인 위치에 존재하는 컴퓨팅 자원을 가상화 기술로 통합해 제공하는 기술을 말한다.

[0005] 클라우드 컴퓨팅을 도입하면 기업 또는 개인은 컴퓨터 시스템을 유지, 보수 및 관리하기 위하여 들어가는 비용과 시간을 줄일 수 있으며, 서버의 구매, 설치, 업데이트 및 소프트웨어 구매를 위한 엄청난 비용과 시간 및 인력을 줄일 수 있다. 또한, 에너지 절감에도 기여할 수 있다. 한편, PC에 자료를 보관할 경우 하드디스크 장애 등으로 인하여 자료가 손실될 수도 있지만 클라우드 컴퓨팅 환경에서는 외부 서버에 자료들이 저장되기 때문에 안전하게 자료를 보관할 수 있고, 저장 공간의 제약도 극복할 수 있으며, 언제 어디서든 자신이 작업한 문서 등을 열람 및 수정할 수 있다.

[0006] 반면, 서버가 해킹을 당할 경우 개인정보가 유출될 수 있고, 서버 장애가 발생하면 자료 이용이 불가능하다는 단점이 있다. 따라서 클라우드 컴퓨팅이 미래의 컴퓨팅 환경에서의 지배적인 위치를 확보하기 위해 선택되어야

할 사항은 바로 사용자 데이터에 대한 무결성(integrity)이 보장되어야 한다.

[0007]

따라서 최근 클라우드 서버에 아웃소싱(outsourcing)한 데이터들의 무결성을 검사하는 기술들에 대한 연구가 활발하게 진행되고 있으나, 이러한 연구들은 대부분 아웃소싱한 데이터들에 대한 무결성 감사를 TPA(Third Party Auditor)라는 감사자가 아무런 비밀값 없이 누구나 수행할 수 있다. 그러므로 종래에는 데이터에 대한 프라이버시를 보장받을 수 없는 문제가 있었다. 이를 보완하기 위해 하기의 선행기술문헌 1에서는 데이터 소유주가 자신의 권한을 위임한 대리 감사자(Proxy auditor)만이 데이터 감사를 할 수 있는 기법을 제안하고 있다. 하지만 선행기술문헌 1에서 제안한 방법은 선행기술문헌 2에서 제시한 공격법에 의해 안전성 문제가 발생한다.

## 선행기술문헌

### 비특허문헌

[0008]

(비특허문헌 0001) 1. H. Wang, Proxy Provable Data Possession in Public Clouds, IEEE Transactions on Service Computing, 6(4), (2013), pp. 551-559.

(비특허문헌 0002) 2. Y. Yu, L. Niu, G. Yang, Y. Mu, W. Susil, On the security of auditing mechanisms for secure cloud storage, Future Generation Computer Systems, (2014), pp. 127-132.

## 발명의 내용

### 해결하려는 과제

[0009]

따라서 본 발명은 클라우드 컴퓨팅 환경에서 다양한 공격에 대하여 안전하고, 지정된 감사자만이 감사를 수행할 수 있도록 함으로써 프라이버시를 보장받을 수 있는 사용자 데이터 무결성 검증 방법 및 장치를 제공하고자 한다.

### 과제의 해결 수단

[0010]

상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 사용자 데이터의 무결성 검증 방법은 데이터 파일을 생성하는 제1 단말, 상기 데이터 파일을 저장하는 인터넷 상의 데이터 저장 서버, 상기 데이터 저장 서버에 저장된 데이터 파일의 무결성을 감사하는 제2 단말 간의 상호 관계에 의거하여 사용자 데이터의 무결성을 검증하는 사용자 데이터 무결성 검증 방법에 있어서, 프라이버시가 보장된 사용자 데이터 무결성 검증에 필요한 파라미터들을 생성하는 단계; 상기 제1 단말이 상기 파라미터 생성 단계에서 생성된 파라미터 및 암호학적으로 안전한 해쉬 함수에 기초하여 업로드할 데이터 파일을 암호화한 후 데이터 저장 서버에 업로드 하는 데이터 아웃소싱 단계; 상기 데이터 저장 서버가 상기 파라미터 생성 단계에서 생성된 파라미터에 기초하여 업로드된 데이터의 정당성을 검증하는 단계; 상기 제2 단말이 상기 업로드된 데이터 파일 일부에 대한 챌린지(challenge)값을 생성하는 단계; 상기 데이터 저장 서버가 상기 제2 단말로부터 상기 챌린지 값을 수신하고, 상기 파라미터 생성 단계에서 생성된 파라미터 및 상기 챌린지 값에 기초하여 증명값을 생성하는 단계; 및 상기 제2 단말이 상기 증명값(proof)과 공개키들을 이용하여 상기 증명값(proof)의 정당성을 검증하는 단계를 포함한다.

[0011]

바람직하게는, 상기 파라미터 생성 단계는 상기 제1 단말, 상기 데이터 저장 서버, 상기 제2 단말이 각각 자신의 개인키와 공개키를 생성하는 단계; 상기 제1 단말이 상기 제2 단말에 대한 보증서를 작성한 후 상기 제1 단말의 개인키로 서명하는 단계; 상기 보증서 및 서명 쌍을 상기 데이터 저장서버 및 상기 제2 단말에게 전송하는 단계; 및 상기 제1 단말이 공개파라미터를 생성하는 단계를 포함할 수 있다.

[0012]

바람직하게는, 상기 파라미터 생성 단계는 상기 제1 단말로부터 상기 보증서 및 서명 쌍을 수신한 상기 데이터 저장 서버 및 상기 제2 단말 각각이 해당 서명 값이 상기 보증서에 대해 정당한지를 확인하는 단계; 및 상기 확인 결과 상기 서명 값이 상기 보증서에 대해 정당한지 않은 경우 상기 제1 단말에게 상기 보증서 및 서명 쌍을 재요청하는 단계를 더 포함할 수 있다.

[0013]

바람직하게는, 상기 업로드 데이터 정당성 검증 단계는 상기 파라미터 생성 단계에서 생성된 상기 데이터 저장 서버의 개인키( $y$ ), 상기 제1 단말 및 상기 제2 단말 각각의 공개키( $X$ ,  $Z$ ) 및 상기 제1 단말이 생성한 공개파라미터( $u$ )에 기초하여 상기 업로드 데이터의 정당성을 검증하되, 하기의 수학식1 및 수학식2에 의거하여 제1 및 제2 변수를 생성하고, 하기의 수학식3이 성립하는지를 확인할 수 있다.

- [0014] (수학식1)
- [0015]  $t = H(e(X, Z)^y, w)$
- [0016] 이 때, X는 상기 제1 단말의 공개키, Z는 상기 제2 단말의 공개키, y는 상기 데이터 저장서버의 개인키, w는 상기 제1 단말에서 생성한 보증서이다.
- [0017] (수학식2)
- [0018]  $W_i = \Omega_i(i)$
- [0019] 이 때, t는 (수학식 1)에 의해 생성된 제1 변수이다.
- [0020] (수학식3)
- [0021]  $e(T_{m_i}, g) = e(h(W_i) \cdot u^{m_i}, X)$
- [0022] 이 때,  $T_{m_i}$ 은 데이터 업로드시 전송된 태그, u는 상기 제1 단말이 생성한 공개 파라미터,  $m_i$ 는 i번째 데이터 블록, X는 상기 제1 단말의 공개키이다.
- [0023] 바람직하게는, 상기 쉘린지값 생성 단계는 상기 업로드된 데이터 중 선택된 블록의 개수(c)와 제1 및 제2 난수( $k_1, k_2$ )를 포함하는 쉘린지값을 생성할 수 있다.
- [0024] 바람직하게는, 상기 증명값 생성 단계는 정수 집합의 원소인 제3 난수(r)를 생성하고, 상기 제3 난수(r)에 기초하여 제1 증명값(R)을 생성하는 단계; 제1 및 제2 난수( $k_1, k_2$ )를 각각 의사난수함수( $\pi$ ) 및 의사난수치환(f)에 적용하여 제3 변수( $a_j$ )를 생성하고, 상기 제3 변수( $a_j$ ) 및 메시지 블록 개수( $m_i$ )에 기초하여 제2 증명값(T)을 생성하는 단계; 상기 제3 변수( $a_j$ ), 메시지 블록 개수( $m_i$ ) 및 상기 제1 증명값(R)에 기초하여 제3 증명값(m)을 생성하는 단계; 상기 데이터 저장 서버의 개인키(y)와, 상기 제1 및 제2 단말의 공개키(X, Z)에 기초하여 제4 증명값( $S_m$ )을 생성하는 단계; 및 상기 제1 내지 제4 증명값을 상기 쉘린지값에 대한 증명값(proof) 값으로 결정하는 단계를 포함할 수 있다.
- [0025] 바람직하게는, 상기 증명값 생성 단계는 상기 제2 단말로부터 상기 쉘린지 값 수신시 상기 제2 단말의 보증서 및 서명 쌍을 함께 수신하는 단계; 상기 제2 단말로부터 수신한 보증서 및 서명 쌍의 정당성을 검증하는 단계; 및 상기 제2 단말로부터 수신한 보증서 및 서명쌍이 정당한 경우 상기 제1 단말로부터 수신하여 기 저장된 보증서와 상기 제2 단말로부터 수신한 보증서를 비교하는 단계를 더 포함하고, 상기 제1 단말로부터 수신하여 기 저장된 보증서와 상기 제2 단말로부터 수신한 보증서가 같지 않은 경우 증명값 생성을 중단할 수 있다.
- [0026] 바람직하게는, 상기 증명값 검증 단계는 상기 데이터 저장 서버의 비밀키(y) 및 상기 제1 및 제2 단말의 공개키(X, Z)에 기초하여 제3 증명값의 정당성을 판단하는 단계; 상기 제3 증명값이 정당한 경우 상기 제2 단말의 개인키를 이용하여 증명값 검증을 위한 제4 변수(t)를 생성하는 단계; 및 하기의 수학식4에 의거하여 상기 증명값을 검증하는 단계를 포함할 수 있다.
- [0027] (수학식 4)
- [0028] 
$$e(T, g) = e\left(\prod_{i=1}^c h(\Omega_i(\pi_{k_1}(i)))^{f_{k_2}(i)} \cdot u^m \cdot R^{-h(R)}, X\right)$$
- [0029] 한편, 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 사용자 데이터의 무결성 검증 장치는 데이터 파일을 생성하는 제1 단말 및 데이터 파일을 저장하는 데이터 저장 서버와의 인터페이스를 제공하는 통신 인터페이스부; 프라이버시가 보장된 사용자 데이터 무결성 검증에 필요한 개인키 및 공개키(z, Z)를 설정하는 설정부; 상기 통신 인터페이스부를 통해 상기 제1 단말에서 생성한 보증서 및 서명 쌍을 전달받아 저장하는 제어부; 상기 데이터 저장 서버에 업로드된 데이터 파일에 대한 무결성 확인을 위해 상기 데이터 파일에 일부에 대한 쉘린지 값을 생성하여 상기 제어부에 저장된 보증서 및 서명 쌍과 함께 상기 데이터 저장 서버로 전송하는 쉘린지값

생성부; 및 상기 데이터 저장 서버에서 생성된 증명값을 제공받아 그 증명값의 정당성을 검증하는 검증부를 포함한다.

[0030] 바람직하게는, 상기 제어부는 상기 제1 단말로부터 수신한 보증서 및 서명 쌍을 검증하여 해당 서명 값이 상기 보증서에 대해 정당한지를 확인하고 상기 서명 값이 상기 보증서에 대해 정당하지 않은 경우 상기 제1 단말에게 상기 보증서 및 서명 쌍을 재요청할 수 있다.

[0031] 바람직하게는, 상기 검증부는 상기 설정부에서 설정한 개인키( $z$ )를 이용하여 증명값 검증을 위한 변수( $t$ )를 생성하고, 상기의 수학식4에 의거하여 상기 증명값을 검증할 수 있다.

[0032] 바람직하게는, 상기 검증부는 상기 데이터 저장 서버의 비밀키( $y$ ) 및 상기 제1 단말의 공개키( $X$ )와, 상기 설정부에서 설정한 공개키( $Z$ )에 기초하여 상기 증명값에 대한 1차 검증을 실시하고, 상기 1차 검증 결과가 정당하지 않은 경우 증명값 검증을 중단할 수 있다.

### 발명의 효과

[0033] 본 발명은 곁선형 사상(bilinear maps) 기법과 BLS 짧은 서명(BLS short signature) 기법을 적용하여 사용자 데이터의 무결성을 검증하되, 지정된 감사자 만이 감사를 수행할 수 있도록 함으로써 다양한 공격에 대하여 데이터의 안전성을 보장하면서도, 데이터 프라이버시를 보장받을 수 있는 효과가 있다.

### 도면의 간단한 설명

[0034] 도 1은 본 발명의 사용자 데이터 무결성 검증 방법을 구현하기 위한 시스템 구성도를 도시한 도면이다.

도 2는 본 발명의 일 실시 예에 따른 사용자 데이터 무결성 검증 방법에 대한 시스템간 처리 절차도이다.

도 3은 도 2에 예시된 암호화 과정에 대한 개략적인 처리 흐름도이다.

도 4는 도 2에 예시된 쉼린지값 생성 과정에 대한 개략적인 처리 흐름도이다.

도 5는 도 2에 예시된 증명값 생성 과정에 대한 개략적인 처리 흐름도이다.

도 6은 도 2에 예시된 증명값 검증 과정에 대한 개략적인 처리 흐름도이다.

도 7은 본 발명의 일 실시 예에 따른 사용자 데이터 무결성 검증 장치에 대한 개략적인 블록도이다.

### 발명을 실시하기 위한 구체적인 내용

[0035] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0036] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0037] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0038] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0039] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이

속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0040] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다. 명세서 및 청구범위 전체에서, 어떤 부분이 어떤 구성 요소를 포함한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다.

[0041] 도 1은 본 발명의 사용자 데이터 무결성 검증 방법을 구현하기 위한 시스템 구성도를 도시한 도면이다. 도 1을 참조하면 본 발명의 일 실시 예에 따른 사용자 데이터 무결성 검증 방법은 통신망으로 연결된 데이터 소유주(100), 데이터 저장 서버(200) 및 데이터 소유주가 지정한 대리 감사자(300)가 서로 상호 작용을 함으로써 구현할 수 있다. 즉, 데이터 소유주(100)가 자신의 데이터를 데이터 저장 서버(200)에 업로드(S10)하면, 데이터 저장서버(200)는 그 데이터 파일을 저장(S20)한다. 한편, 데이터 소유주(100)가 대리 감사자(300)에 대하여 생성한 보증서를 대리 감사자(300)와 데이터 저장서버(200)가 공유(S30)하고, 데이터 소유주(100)의 감사 요청(S40)에 응답하여 대리 감사자(300)가 데이터 저장서버(200)에 저장된 데이터 파일에 대한 데이터 무결성 검증(S50)을 실시한다.

[0042] 이를 위해, 각 장치들은 서로 약속된 프로토콜에 의해 상호 작용을 하여야 하며, 본 발명은 의사난수 함수(pseudo-random function) 및 의사난수 치환(pseudo-random permutation)과, 곱선형 사상(bilinear maps), BLS 짧은 서명(BLS short signature) 알고리즘이 적용되었다.

[0043] 도 2는 본 발명의 일 실시 예에 따른 사용자 데이터 무결성 검증 방법에 대한 시스템간 처리 절차도이다. 도 2의 예에서는 데이터 소유주의 단말을 제1 단말(100A), 데이터 소유주가 지정한 대리 감사자의 단말을 제2 단말(300A)이라 칭하고 데이터 저장 서버(200)와의 상호 처리 절차의 예를 설명하고 있다. 이 때,  $G_1$  그리고  $G_2$ 를 위수  $p$ 로 가지는 곱셈 순환군이라 하고,  $e: G_1 \times G_1 \rightarrow G_2$ 를 곱선형 사상이라 한다. 또한  $g$ 를  $G_1$ 의 생성자,  $H(\cdot): \{0,1\}^* \rightarrow Z_q^*$ 를 두 개의 입력을 가지는 암호학적으로 안전한 해시(hash) 함수,  $h(\cdot): Z_q^* \rightarrow G_1^*$ 를 또 다른 해시함수라고 하고,  $f: Z_q^* \times \{1,2,\dots,n\} \rightarrow Z_q^*$ ,  $\Omega: Z_q^* \times \{1,2,\dots,n\} \rightarrow Z_q^*$ 를 의사난수 함수,  $\pi: Z_q^* \times \{1,2,\dots,n\} \rightarrow \{1,2,\dots,n\}$ 를 의사난수 치환이라고 한다.

[0044] 먼저, 단계 S105 내지 S120에서, 제1 단말(100A), 데이터 저장서버(200) 및 제2 단말(300A)은 각각 프라이버시가 보장된 사용자 데이터 무결성 검증에 필요한 파라미터들을 생성한다. 즉, 단계 S105에서는, 제1 단말(100A)이 개인키 및 공개키( $x, X$ )를 설정한다. 이를 위해, 제1 단말(100A)은 난수  $x \leftarrow Z_q^*$ 를 생성하고,  $X \leftarrow g^x$ 를 계산한다. 단계 S110에서는, 데이터 저장서버(200)가 이와 동일한 방법으로 개인키 및 공개키( $y, Y$ )를 설정하고, 단계 S115에서는, 제2 단말(300A)이 이와 동일한 방법으로 개인키 및 공개키( $z, Z$ )를 설정한다. 한편, 단계 S120에서는, 제1 단말(100A)이 제2 단말(300A)에 대한 보증서( $w$ )를 작성한 후 제1 단말의 개인키로 서명(Sign( $w$ )))한다. 이 때, Sign은 안전한 전자 서명기법으로서, 공지된 다양한 서명 알고리즘을 적용할 수 있다. 그리고, 단계 S125 및 단계 S130에서, 제1 단말(100A)은 상기 보증서 및 서명 쌍( $w, \text{Sign}(w)$ )을 데이터 저장서버(200) 및 제2 단말(300A)에게 전송한다.

[0045] 한편, 단계 S135에서는, 데이터 저장 서버(200)가 제1 단말(100A)로부터 수신한 보증서 및 서명 쌍( $w, \text{Sign}(w)$ )에 대하여 정당한지를 확인하는 보증서 검증 과정을 수행하고, 단계 S140에서는, 제2 단말(300A)이 제1 단말(100A)로부터 수신한 보증서 및 서명 쌍( $w, \text{Sign}(w)$ )에 대하여 정당한지를 확인하는 보증서 검증 과정을 수행한다.

[0046] 상기 확인 결과 상기 서명 값이 해당 보증서에 대해 정당하지 않은 경우, 상기 데이터 저장서버(200) 및 제2 단말(300A)은 제1 단말(100A)에게 상기 보증서 및 서명 쌍을 재요청할 수 있다(미도시). 한편, 제1 단말(100A)은 공개파라미터( $u$ )를 생성한다(미도시).

[0047] 이와 같이 프라이버시가 보장된 사용자 데이터의 무결성 검증에 필요한 파라미터들을 생성한 후, 단계 S145에서, 제1 단말(100A)은 상기 생성된 파라미터 및 암호학적으로 안전한 해쉬 함수에 기초하여 업로드할 데이터 파일을 암호화한다. 이 때, 암호화를 위한 처리 과정의 예가 도 3에 예시되어 있다.

[0048] 도 3은 도 2에 예시된 암호화 과정(S145)에 대한 개략적인 처리 흐름도로서, 도 3을 참조하면, 먼저, 단계 S146

에서, 제1 단말(100A)은 업로드할 데이터 파일( $P=\{m_i\}$ )을 소정개로 분할한다. 그리고, 단계 S147에서는, 하기의 수학식1에 의해 태그( $T_{m_i}$ )를 생성한다.

### 수학식 1

$$t = H(e(Y, Z)^x, w), W_i = \Omega_i(i)$$

$$T_{m_i} = (h(W_i) \cdot u^{m_i})^x$$

이 때, Y는 데이터 저장서버(200)의 공개키, Z는 제2 단말(300A)의 공개키, x는 제1 단말(100A)의 개인키, w는 보증서, u는 제1 단말(100A)이 생성한 공개 파라미터,  $m_i$ 는 i번째 데이터 블록이다.

이와 같이 암호화 과정(S145)이 수행되면, 도 2의 단계 S150에서, 제1 단말(100A)은 생성된 태그( $T_{m_i}$ )와 메시지 블록( $m_i$ )들을 데이터 저장서버(200)로 업로드한다.

한편, 단계 S155에서, 데이터 저장서버(200)는 단계 S105 내지 S120에서 생성된 파라미터들에 기초하여 업로드된 데이터의 정당성을 검증한다. 이를 위해, 데이터 저장서버(200)는 데이터 저장 서버(200)의 개인키(y), 제1 단말(100A) 및 제2 단말(300A) 각각의 공개키(X, Z) 및 제1 단말(100A)이 생성한 공개파라미터(u)에 기초하여 상기 업로드 데이터의 정당성을 검증하되, 하기의 수학식2 및 수학식3에 의거하여 제1 및 제2 변수(t,  $W_i$ )를 생성하고, 하기의 수학식4가 성립하는지를 확인한다.

### 수학식 2

$$t = H(e(X, Z)^y, w)$$

이 때, X는 상기 제1 단말의 공개키, Z는 상기 제2 단말의 공개키, y는 상기 데이터 저장서버의 개인키, w는 상기 제1 단말에서 생성한 보증서이다.

### 수학식 3

$$W_i = \Omega_i(i)$$

이 때, t는 (수학식 1)에 의해 생성된 제1 변수이다.

### 수학식 4

$$e(T_{m_i}, g) = e(h(W_i) \cdot u^{m_i}, X)$$

이 때,  $T_{m_i}$ 은 데이터 업로드시 전송된 태그, u는 상기 제1 단말이 생성한 공개 파라미터,  $m_i$ 는 i번째 데이터 블록, X는 상기 제1 단말의 공개키이다.

단계 S155의 검증결과가 정당한 경우, 단계 S160에서는 데이터 저장서버(200)가 업로드된 데이터를 저장한다. 또한, 단계 S165에서, 데이터 저장서버(200)는 그 저장된 데이터에 대한 정보 일부를 제2 단말(300A)에게 제공한다. 이는 제2 단말(300A)이 그 데이터에 대한 챌린지(challenge)값을 생성하도록 하기 위함이다. 즉, 단계 S170에서, 제2 단말(300A)은 데이터 저장 서버(200)에 업로드된 데이터 파일에 대한 무결성 확인을 위해 상기 데이터 파일 일부에 대한 챌린지(challenge)값을 생성하고, 단계 S175에서, 그 챌린지(challenge) 값을 데이터 저장 서버(200)로 전송한다.

[0061] 도 4는 도 2에 예시된 쉘린지값 생성 과정(S170)에 대한 개략적인 처리 흐름도로서, 도 4를 참조하면, 단계 S171에서, 제2 단말(300A)은 데이터 저장 서버(200)에 업로드된 데이터 파일 전체 블록 중 일부를 선정한다. 예컨대, 데이터 파일 전체 블록 n개 중 임의로 c개의 블록만을 선정할 수 있다. 그리고, 그 선정된 c개의 블록들을 포함하는 임의의 부분집합(I)을 데이터 저장 서버(200)로부터 제공받는다. 이 때, 제2 단말(300A)은 데이터 저장 서버(200)에서 임의로 선택된 상기 데이터 파일 일부를 제공받거나, 제2 단말(300A)이 데이터 저장 서버(200)에게 요청하여 선택된 데이터 파일 일부를 제공받을 수 있다. 한편, 단계 S172에서, 제2 단말(300A)은 데이터 저장서버(200)로부터 제공받은 일부 블록에 대한 쉘린지 값을 생성한다. 상기 쉘린지값은 업로드된 데이터 중 선택된 블록의 개수(c)와 제1 및 제2 난수( $k_1, k_2$ )를 포함하는 것이 바람직하다.

[0062] 이와 같이 쉘린지 값이 생성되면, 도 2의 단계 S175에서, 제2 단말(300A)은 그 쉘린지값을 데이터 저장 서버(200)로 전송한다. 이 때, 제2 단말(300A)은 단계 S130에서 제1 단말(300A)로부터 제공받았던 보증서 및 서명쌍(w, Sign(w))을 함께 전송한다.

[0063] 그러면, 단계 S180에서, 데이터 저장 서버(200)는 단계 S105 내지 S120에서 생성된 파라미터들 및 상기 쉘린지 값에 기초하여 증명값(proof)을 생성한다.

[0064] 도 5는 도 2에 예시된 증명값 생성 과정(S180)에 대한 개략적인 처리 흐름도로서, 도 5를 참조하면, 단계 S181에서, 데이터 저장서버(200)는 제1 증명값(R)을 생성한다. 이를 위해, 데이터 저장서버(200)는 난수  $r \leftarrow Z_p^*$ 를 생성하고, 그 값에 의거하여 제1 증명값( $R = u^r$ )을 생성한다.

[0065] 단계 S182에서는 쉘린지값에 포함된 제1 및 제2 난수( $k_1, k_2$ )를 각각 의사난수함수( $\pi$ ) 및 의사난수치환(f)에 적용하여 제3 변수( $a_j$ )를 생성하고, 상기 제3 변수( $a_j$ ) 및 메시지 블록 개수( $m_i$ )에 기초하여 제2 증명값(T)을 생성한다. 이를 위해, 데이터 저장서버(200)는 하기의 수학적 식 5를 적용한다.

### 수학적 식 5

$$i_j = \pi_{k_1}(j), a_j = f_{k_2}(j), T = \prod_{j=1}^c T_{m_{i_j}}^{a_j}$$

[0067] 단계 S183에서는, 제3 변수( $a_j$ ), 메시지 블록 개수( $m_i$ ) 및 상기 제1 증명값(R)에 기초하여 제3 증명값(m)을 생성한다. 이를 위해, 데이터 저장서버(200)는 하기의 수학적 식 6을 적용한다.

### 수학적 식 6

$$\tilde{m} = \sum_{j=1}^c a_j m_{i_j}, m = \tilde{m} + h(R) \cdot r$$

[0069] 단계 S184에서는, 데이터 저장 서버(200)의 개인키(y)와, 상기 제1 및 제2 단말의 공개키(X,Z)에 기초하여 제4 증명값( $S_m$ )을 생성한다. 이를 위해, 데이터 저장서버(200)는 하기의 수학적 식 7을 적용한다.

### 수학적 식 7

$$S_m = h(m \| e(X, Z)^y)$$

[0071] 이와 같이 증명값(proof(T, m, R,  $S_m$ ))을 생성한 데이터 저장 서버(200)는 도 2의 단계 S185에서, 이를 제2 단말(300A)에게 전송한다.

[0072] 도 2의 단계 S190에서, 제2 단말(300A)은 상기 증명값(proof(T, m, R,  $S_m$ ))과 공개키들을 이용하여 상기 증명값

(proof(T, m, R, S<sub>m</sub>))의 정당성을 검증한다.

[0073] 도 6은 도 2에 예시된 증명값 검증 과정(S190)에 대한 개략적인 처리 흐름도로서, 도 6을 참조하면, 단계 S191에서, 제2 단말(300A)는  $e(X, Z)^y$ 를 계산한 후, 제4 증명값(S<sub>m</sub>)을 통해 제3 증명값(m)의 변조 유무를 확인한다. 상기 확인 결과 제3 증명값(m)이 정당하다고 결정되면 제2 단말(300A)는 이후의 과정을 수행하지만, 그렇지 않은 경우 제2 단말(300A)는 증명값 검증 과정을 중단한다.

[0074] 단계 S192에서, 제2 단말(300A)는 제2 단말(300A)의 개인키를 이용하여 증명값 검증을 위한 제4 변수(t)를 생성한다. 이를 위해 제2 단말(300A)는 하기의 수학식 8을 적용한다.

### 수학식 8

[0075] 
$$t = H(e(X, Y)^z, w)$$

[0076] 한편, 단계 S193에서, 제2 단말(300A)는 수학식 9에 의거하여 상기 증명값을 검증한다.

### 수학식 9

[0077] 
$$e(T, g) = e\left(\prod_{i=1}^c h(\mathcal{Q}_t(\pi_{k_1}(i)))^{f_{k_2}(i)} \cdot u^m \cdot R^{-h(R)}, X\right)$$

[0078] 이 때, 상기 수학식 9가 성립하기 위한 검증 단계는 다음과 같다.

[0079] 
$$\begin{aligned} e(T, g) &= e\left(\prod_{j=1}^c T_{m_i}^{a_i}, g\right) \\ &= e\left(\prod_{j=1}^c \left[h(W_{i_j})^{a_i}\right]^z \cdot u^{x \sum_{i=1}^c a_i m_i}, g\right) \\ &= e\left(\prod_{j=1}^c \left[h(W_{i_j})^{a_i}\right] \cdot u^{x \sum_{i=1}^c a_i m_i}, X\right) \\ &= e\left(\prod_{j=1}^c h(\mathcal{Q}_t(i_j))^{f_{k_2}(i)} \cdot u^{m-h(R) \cdot r}, X\right) \\ &= e\left(\prod_{j=1}^c h(\mathcal{Q}_t(i_j))^{f_{k_2}(i)} \cdot u^m \cdot u^{-h(R) \cdot r}, X\right) \\ &= e\left(\prod_{j=1}^c h(\mathcal{Q}_t(\pi_{k_1}(j)))^{f_{k_2}(j)} \cdot u^m \cdot R^{-h(R)}, X\right) \end{aligned}$$

[0080] 이와 같이 수학식 9 성립되면 상기 증명값(proof(T, m, R, S<sub>m</sub>))이 정당한 것이고, 해당 데이터의 무결성이 보장된 것으로 간주한다.

[0081] 도 7은 본 발명의 일 실시 예에 따른 사용자 데이터 무결성 검증 장치에 대한 개략적인 블록도이다. 도 7을 참조하면, 본 발명의 일 실시 예에 따른 사용자 데이터 무결성 검증 장치(300A)는 사용자 인터페이스부(I/F)(310), 제어부(320), 개인키 및 공개키 설정부(330), 챌린지값 생성부(340), 검증부(350) 및 통신 인터페이스부(I/F)(360)를 포함한다.

[0082] 통신 인터페이스부(I/F)(360)는 데이터 파일을 생성하는 제1 단말(도 1의 '100') 및 통신 데이터 파일을 저장하는 데이터 저장 서버(도 1의 '200')와의 인터페이스를 제공한다.

[0083] 사용자 인터페이스부(I/F)(310)는 사용자와의 인터페이스를 제공한다. 예를 들어, 데이터 무결성 검증을 위한 데이터 선택 정보 등 사용자의 선택정보 및 조작신호를 입력받아 제어부(320)로 전달한다.

[0084] 제어부(320)는 미리 설정된 제어 프로그램에 의거하여 사용자 데이터 무결성 검증 장치의 동작을 제어한다. 예를 들어, 사용자 선택정보 또는 조작신호에 의거하여 챌린지값 생성부(340) 및 검증부(350)의 동작을 제어한다. 또한, 제어부(320)는 통신 인터페이스부를 통해 제1 단말(도 1의 '100')에서 생성한 보증서 및 서명 쌍(w,

Sign(w))을 전달받아 저장한다. 이 때, 제어부(320)는 제1 단말(도 1의 '100')로부터 수신한 보증서 및 서명 쌍(w, Sign(w))을 검증하여 해당 서명 값이 상기 보증서에 대해 정당한지를 먼저 확인하고 상기 서명 값이 상기 보증서에 대해 정당한 경우에만 이를 저장한다. 만약 상기 서명 값이 상기 보증서에 대해 정당하지 않은 경우 제어부(320)는 제1 단말(도 1의 '100')에게 상기 보증서 및 서명 쌍을 재요청하여 다시 제공받는다.

[0085]

개인키 및 공개키 설정부(330)는 프라이버시가 보장된 사용자 데이터 무결성 검증에 필요한 개인키 및 공개키( $z$ ,  $Z$ )를 설정한다. 이를 위해, 개인키 및 공개키 설정부(330)는 난수  $z \leftarrow Z_q^*$ 를 생성하고,  $Z \leftarrow g^z$ 를 계산한다.

[0086]

챌린지값 생성부(340)는 클라우드 컴퓨팅 환경에서, 클라우드 서버 역할을 하는 데이터 저장 서버(도 1의 '200')에 업로드된 데이터 파일에 대한 무결성 확인을 위해 상기 데이터 파일에 일부에 대한 챌린지 값을 생성한다. 또한, 통신 인터페이스부(I/F)(360)를 통해 그 챌린지값과 상기 제어부(320)에 저장된 보증서 및 서명 쌍(w, Sign(w))을 데이터 저장서버(도 1의 '200')로 전송한다. 이를 위해, 챌린지값 생성부(340)는, 통신 인터페이스부(I/F)(360)를 통해, 데이터 저장 서버(도 1의 '200')로부터 데이터 파일 전체 블록(n) 중 임의로 선택한 몇 개(c)의 블록들을 포함하는 임의의 부분집합(I)을 제공받고, 상기 부분집합(I)에 대하여 챌린지 값을 생성한다.

[0087]

검증부(350)는 데이터 저장 서버(도 1의 200)에서 생성된 증명값(proof(T, m, R,  $S_m$ ))을 제공받아 그 증명값의 정당성을 검증한다. 이를 위해, 검증부(240)는 개인키 및 공개키 설정부(330)에서 설정한 개인키( $z$ )를 이용하여 증명값 검증을 위한 변수(t)를 생성하고, 도 6을 참조한 설명에서 언급한 수학식9에 의거하여 상기 증명값을 검증하는 것이 바람직하다.

[0088]

또한, 검증부(350)는 데이터 저장 서버(도 1의 200)의 비밀키(y) 및 제1 단말(도 1의 '100')의 공개키(X)와, 개인키 및 공개키 설정부(330)에서 설정한 공개키(Z)에 기초하여 상기 증명값에 대한 1차 검증을 실시하고, 상기 1차 검증 결과가 정당하지 않은 경우 증명값 검증을 중단할 수 있다. 즉, 검증부(350)는 도 6을 참조한 설명에서 언급한 바와 같이 제4 증명값( $S_m$ )에 기초하여 제3 증명값(m)의 변조 여부를 판단하고, 상기 제3 증명값(m)이 정당하다고 판단된 경우에 이후의 과정을 수행한다.

[0089]

한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0090]

상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등)를 포함한다.

[0091]

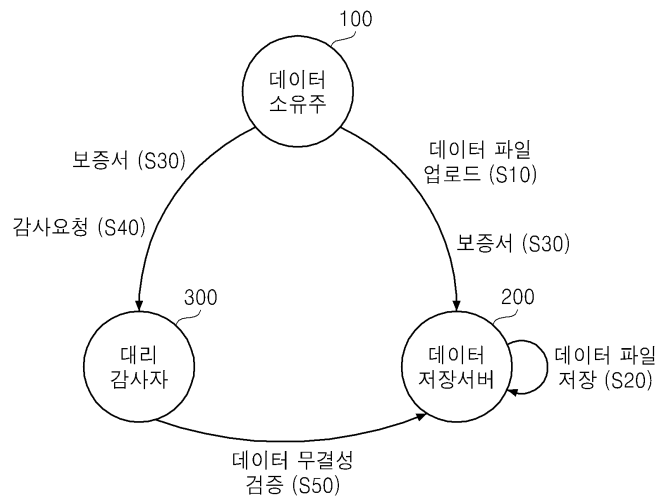
이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다.

[0092]

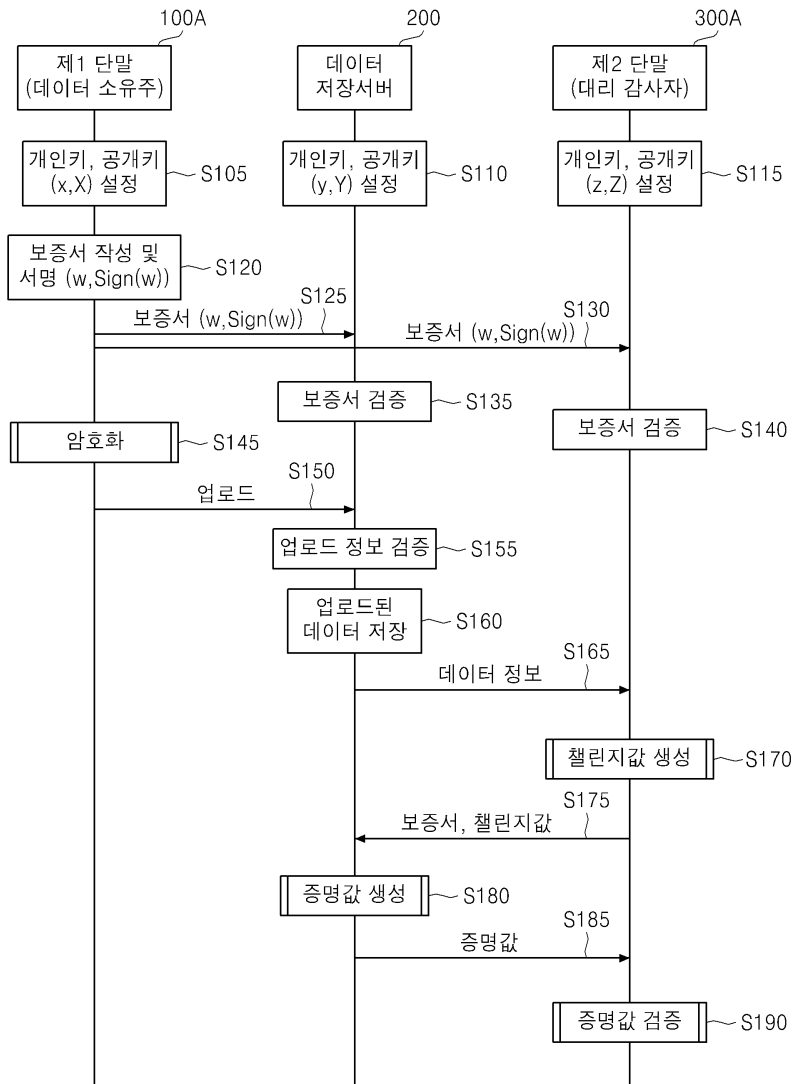
본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

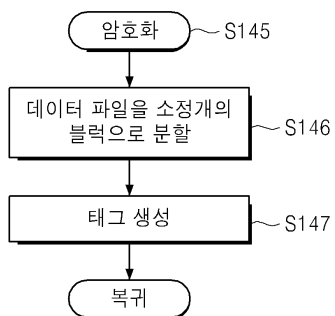
도면1



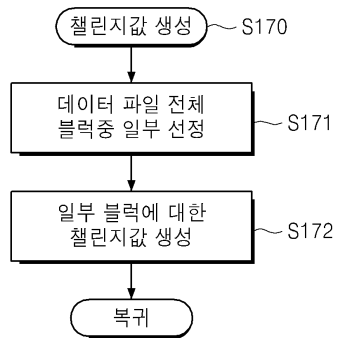
도면2



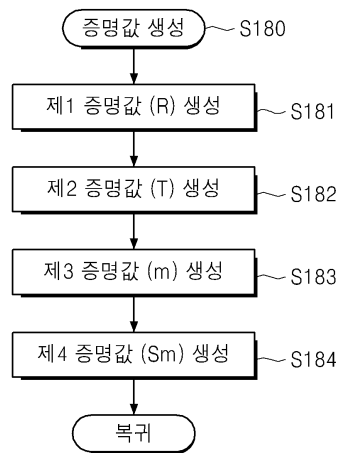
도면3



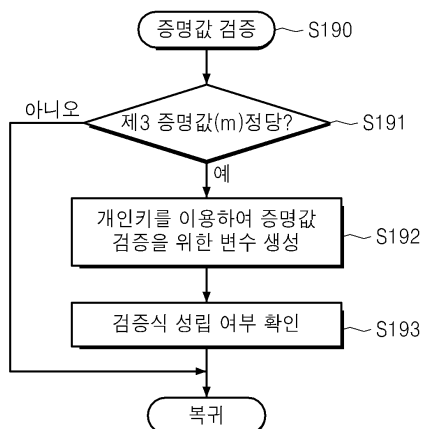
도면4



도면5



도면6



도면7

