



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0104796
(43) 공개일자 2014년08월29일

(51) 국제특허분류(Int. Cl.)
G06F 21/64 (2013.01) G06F 21/31 (2013.01)
(21) 출원번호 10-2013-0018745
(22) 출원일자 2013년02월21일
심사청구일자 2013년02월21일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)
이원길
서울 성북구 안암로 145, 정보보호대학원 (안암동5가, 고려대학교)
(뒷면에 계속)
(74) 대리인
특허법인추현

전체 청구항 수 : 총 7 항

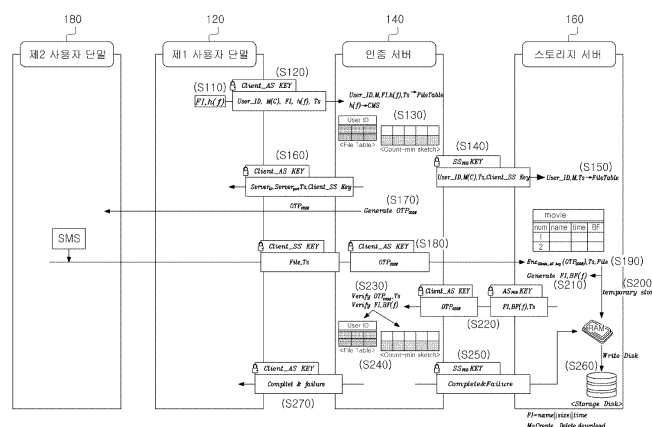
(54) 발명의 명칭 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법

(57) 요약

본 발명은 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법에 관한 것으로, 보다 구체적으로는 제1 사용자단말이 스토리지 서버에 업로드 하고자 하는 파일의 인덱스 정보와, 상기 파일의 해시값을 인증서버로 전송하는 단계; 상기 인증서버가 수신한 파일의 인덱스 정보를 테이블에 저장하고, 수신한 파일의 해시값을 다차원 배열 형태로 저장하는 단계; 상기 인증서버가 일회용 패스워드(One Time Password)를 생성하여, 제2 사용자단말로 전송하는 단계; 상기 인증서버가 상기 제1 사용자단말의 파일 업로드를 요청하는 요청메시지를 상기 스토리지 서버로 전송하는 단계; 상기 제2 사용자단말이 수신한 일회용 패스워드를 상기 제1 사용자단말로 전송하는 단계; 상기 제1 사용자단말이 수신한 일회용 패스워드 및 업로드하고자 하는 파일을 상기 스토리지 서버로 전송하는 단계; 상기 스토리지 서버가 수신한 파일을 임시 저장한 후, 상기 파일의 인덱스 정보와 해시값을 생성하여 상기 인증서버로 전송하는 단계; 상기 인증서버가 상기 스토리지 서버로부터 수신한 파일의 인덱스 정보와 해시값을 상기 제1 사용자단말로부터 수신한 파일의 인덱스 정보와 해시값을 상호 비교하여 정상 사용자 여부를 확인한 후, 상기 스토리지 서버 및 상기 제1 사용자단말로 사용자 인증완료를 나타내는 사용자인증 완료메시지를 전송하는 단계; 및 상기 스토리지 서버가 수신한 사용자인증 완료메시지에 응답하여 임시 저장중인 파일을 스토리지 디스크에 저장하는 단계;를 포함한다.

이러한 구성에 의해, 본 발명의 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 사용자단말로 발급된 일회용 패스워드의 확인을 통해 스토리지 서버에 허용되지 않는 사용자가 접속하거나, 정상 사용자가 스토리지 서버에 접속한 이력을 부인하는 것을 방지할 수 있는 효과가 있다. 이에 따라, 추후 발생하는 사용자에 의한 파일의 상태변경을 용이하게 확인할 수 있는 효과가 있다.

대표도



(72) 발명자

조관태

서울 노원구 동일로184길 13-6, 2층 (공릉동)

박진형

서울 성북구 안암로 145, 정보보호대학원 (안암동 5가, 고려대학교)

이 발명을 지원한 국가연구개발사업

과제고유번호 H2101-12-1001

부처명 지식경제부

연구사업명 지식정보 보안인력 양성

연구과제명 지식정보 보안인력 양성

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2013.01.01 ~ 2013.12.01

특허청구의 범위

청구항 1

제1 사용자단말이 스토리지 서버에 업로드 하고자 하는 파일의 인덱스 정보와, 상기 파일의 해시값을 인증서버로 전송하는 단계;

상기 인증서버가 수신한 파일의 인덱스 정보를 테이블에 저장하고, 수신한 파일의 해시값을 다차원 배열 형태로 저장하는 단계;

상기 인증서버가 일회용 패스워드(One Time Password)를 생성하여, 제2 사용자단말로 전송하는 단계;

상기 인증서버가 상기 제1 사용자단말의 파일 업로드를 요청하는 요청메시지를 상기 스토리지 서버로 전송하는 단계;

상기 제2 사용자단말이 수신한 일회용 패스워드를 상기 제1 사용자단말로 전송하는 단계;

상기 제1 사용자단말이 수신한 일회용 패스워드 및 업로드하고자 하는 파일을 상기 스토리지 서버로 전송하는 단계;

상기 스토리지 서버가 수신한 파일을 임시 저장한 후, 상기 업로드하고자 하는 파일의 인덱스 정보와 해시값을 생성하여 상기 인증서버로 전송하는 단계;

상기 인증서버가 상기 스토리지 서버로부터 수신한 파일의 인덱스 정보와 해시값을 상기 제1 사용자단말로부터 수신한 파일의 인덱스 정보와 해시값을 상호 비교하여 정상 사용자 여부를 확인한 후, 상기 스토리지 서버 및 상기 제1 사용자단말로 사용자 인증완료로 나타내는 사용자인증 완료메시지를 전송하는 단계; 및

상기 스토리지 서버가 수신한 사용자인증 완료메시지에 응답하여 임시 저장중인 파일을 스토리지 디스크에 저장하는 단계;

를 포함하는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법.

청구항 2

제1 사용자단말이 스토리지 서버로부터 다운로드하고자 하는 파일의 리스트를 수신하기 위한 파일 리스트 요청메시지를 인증서버로 전송하는 단계;

상기 인증서버가 수신한 파일리스트 요청메시지에 응답하여 상기 제1 사용자단말로 파일 리스트를 전송하는 단계;

상기 제1 사용자단말이 수신한 상기 파일 리스트로부터 다운로드하고자 하는 파일을 선택한 후, 선택한 파일리스트를 상기 인증서버로 전송하는 단계;

상기 인증서버가 상기 제1 사용자단말이 선택한 파일을 다운로드하기 위한 다운로드 요청 메시지를 상기 스토리지 서버로 전송하는 단계;

상기 스토리지 서버는 상기 제1 사용자단말이 선택한 파일을 상기 제1 사용자단말로 전송하는 단계;

상기 제1 사용자단말이 수신한 파일의 해시값을 생성하여 상기 인증서버로 전송하는 단계;

상기 인증서버가 상기 제1 사용자단말로부터 수신한 파일의 해시값을 카운트 민 스케치(Count Min Sketch) 방식에 의해 검증하고, 검증 완료메시지를 생성하여 상기 스토리지 서버 및 상기 제1 사용자단말로 전송하는 단계;

를 포함하는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법.

청구항 3

제1 사용자단말이 스토리지 서버에 저장된 파일 중 삭제하고자 하는 파일의 리스트를 수신하기 위한 삭제 파일

리스트 요청메시지를 인증서버로 전송하는 단계;

상기 인증서버가 수신한 삭제 파일 리스트 요청메시지에 응답하여 상기 제1 사용자단말로 삭제 파일 리스트를 전송하고, 일회용 패스워드(One Time Password)를 생성하여 제2 사용자단말로 전송하는 단계;

상기 제1 사용자단말이 수신한 삭제 파일 리스트로부터 삭제하고자 하는 삭제 대상 파일을 선택하고, 선택한 삭제 대상 파일 리스트 및 수신한 일회용 패스워드를 상기 인증서버로 전송하는 단계;

상기 인증서버가 수신한 일회용 패스워드와 자신이 생성한 일회용 패스워드와 비교하여 일회용 패스워드에 대한 검증을 수행하고, 상기 제1 사용자단말로부터 수신한 삭제 대상 파일 리스트 및 상기 삭제 대상 파일의 삭제를 요청하는 삭제 요청메시지를 스토리지 서버로 전송하는 단계;

상기 스토리지 서버가 삭제 대상 파일의 인덱스 정보와 해시값을 생성하여 상기 인증서버로 전송하고, 스토리지 디스크에 기저장된 삭제 대상 파일을 삭제하는 단계; 및

상기 인증서버가 삭제한 파일의 인덱스 정보를 테이블로부터 삭제하고, 상기 삭제한 파일의 해시값을 카운트 민 스케치(Count Min Sketch) 방식에 따라 저장된 다차원 배열로부터 삭제한 후, 삭제완료메시지를 생성하여 상기 제1 사용자단말로 전송하는 단계;

를 포함하는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법.

청구항 4

제1 사용자단말이 파일의 무결성 검증을 시작하는 검증메시지를 인증서버로 전송하는 단계;

상기 인증서버가 상기 제1 사용자단말로 무결성 검증을 수행하기 위한 파일 리스트를 전송하는 단계;

상기 제1 사용자단말이 수신한 파일 리스트 중 무결성 검증을 수행하고자 하는 파일을 선택한 후, 선택한 파일 리스트를 상기 인증서버로 전송하는 단계;

상기 인증서버가 수신한 파일 리스트의 파일 해시값을 수신하기 위한 해시값 요청메시지를 스토리지 서버로 전송하는 단계;

상기 스토리지 서버가 수신한 해시값 요청메시지에 응답하여 스토리지 디스크 내 해시값 전송을 요청한 파일을 검색한 후, 검색한 파일의 해시값을 생성하여 상기 인증서버로 전송하는 단계; 및

상기 인증서버가 수신한 파일의 해시값을 카운트 민 스케치(Count Min Sketch) 방식에 의해 무결성을 검증하고, 검증결과를 상기 제1 사용자단말로 전송하는 단계;

를 포함하는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법.

청구항 5

제1 사용자단말이 파일의 무결성 검증을 시작하는 검증메시지를 인증서버로 전송하는 단계;

상기 인증서버가 상기 제1 사용자단말로 디렉토리의 무결성 검증을 수행하기 위한 파일 리스트를 전송하는 단계;

상기 제1 사용자단말이 수신한 파일리스트로부터 무결성을 검증하고자 하는 디렉토리를 선택하여 상기 인증서버로 전송하는 단계;

상기 인증서버가 디렉토리별 카운트 민 스케치(Count Min Sketch) 방식에 따라 저장된 데이터 블록의 해시값을 요청하는 해시값 요청메시지를 스토리지 서버로 전송하는 단계;

상기 스토리지 서버가 수신한 해시값 요청메시지에 응답하여 디렉토리별 카운트 민 스케치 방식에 따라 저장된 데이터 블록의 해시값을 생성하여 상기 인증서버로 전송하는 단계;

상기 인증서버가 상기 스토리지 서버로부터 수신한 데이터 블록의 해시값을 머클 해시트리(Merkle Hash Tree) 연산방법에 적용하여 연산함으로써 디렉토리별 무결성을 검증하는 단계; 및

상기 인증서버가 상기 디렉토리의 무결성 검증결과를 상기 제1 사용자단말 및 상기 스토리지 서버로 전송하는 단계;

를 포함하는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법.

청구항 6

제1 사용자단말이 전체 파일의 무결성을 검증하기 위한 검증 시작메시지를 인증서버로 전송하는 단계;

상기 인증서버가 카운트 민 스케치(Count Min Sketch) 방식에 따라 다차원 배열형태로 기저장된 데이터 블록의 해시값 중 적어도 하나를 선택하여, 선택한 디렉토리별 카운트 민 스케치 방식에 따라 저장된 해시값 전송을 요청하는 해시값 요청메시지를 스토리지 서버로 전송하는 단계;

상기 스토리지 서버가 수신한 해시값 요청메시지에 응답하여 복수 개의 디렉토리별 카운트 민 스케치의 해시값을 생성하고, 생성한 해시값을 인증서버로 전송하는 단계;

상기 인증서버가 상기 스토리지 서버로부터 수신한 해시값과, 자신이 기저장하고 있는 해시값을 머클 해시 트리(Merkle Hash Tree) 연산방법을 이용하여 전체 파일에 대한 무결성 검증을 수행하는 단계;

상기 인증서버가 전체 파일에 대한 무결성 검증을 완료함에 따라 무결성 검증 완료메시지를 생성하여 상기 제1 사용자단말과 상기 스토리지 서버로 전송하는 단계;

를 포함하는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법.

청구항 7

제1항 내지 제6항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명세서

기술분야

[0001] 본 발명은 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법에 관한 것으로, 특히 사용자가 스토리지 서비스를 이용할 때, 스토리지 서버에 접속한 사용자의 부인 가능성을 방지하고, 스토리지 서비스 시 데이터의 무결성 여부를 검증할 수 있는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법에 관한 것이다.

배경기술

[0002] IT 기술이 다양한 분야에 적용되어 널리 사용됨에 따라, 사용되는 분야마다 대용량의 각종 데이터가 발생하게 되었다. 이처럼, 발생한 대용량의 데이터를 저장하기 위해, 최근 들어 스토리지 서비스를 많은 사용자들이 이용하고 있다.

[0003] 이러한 스토리지 서비스란, 네트워크 저장장치인 스토리지 서버에 사용자가 원하는 각종 데이터를 저장하여, 해당 사용자가 원하는 데이터를 다운로드하거나, 업로드 또는 삭제하는 등의 과정을 수행하는 서비스를 말한다.

[0004] 하지만 이처럼 스토리지 서비스의 이용 시, 스토리지 서버에 저장되어 있는 데이터에 대한 무결성 여부를 검증하기 어려웠다. 따라서, 스토리지 서비스를 제공하는 업체는 데이터의 무결성을 확보하기 위해, 데이터를 복제하여 분산 저장하는 방법을 이용하여 데이터의 무결성을 제공하고 있다.

[0005] 하지만 이러한 무결성 제공방법은 스토리지 서비스 제공자 측면에서 제공되는 사항일 뿐, 악의적인 의도를 갖는 공격자에 의해 데이터가 손상되는 경우에는 사용자에게 이러한 사항을 통보하지 않는다. 또한, 서비스 제공자는 사용자에게 스토리지 서비스의 신뢰성을 전달하기 위해, 계약상에 일정 수준의 데이터 무결성을 보장할 수 있다

고 제시하는데, 사용자가 이러한 항목을 악용하여 스토리지 서버 내 저장하지 않는 데이터를 저장했다고 주장하거나, 삭제한 데이터를 삭제하지 않았다는 주장함으로써, 서비스 제공자에게 거액의 손해 배상을 청구하는 등의 부작용이 존재한다는 문제점이 발생했다.

- [0006] 상술한 바와 같이, 본 발명의 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법을 살펴보면 다음과 같다.
- [0007] 선행기술 1은 한국공개특허공보 제2012-0097801호(2012.09.05)로서, 페이지의 물리적 저장 위치의 변경이 가능한 스토리지 시스템 및 상기 스토리지 시스템의 동작방법에 관한 것이다.
- [0008] 이러한 선행기술 1은 페이지들로서 복수의 메모리 셀들을 포함하는 메모리 셀 어레이; 호스트에 의해 인식되는 상기 페이지들의 논리적 주소들과 상기 페이지들의 물리적 주소들 사이의 관계를 정의하는 서로 다른 복수의 후보 변환 테이블들을 포함하는 변환부; 및 상기 호스트가 접근하고자 하는 대상 블록에 있는 대상 페이지의 주소를 생성하는 입/출력 컨트롤러;를 포함하고, 상기 변환부는 상기 복수의 후보 변환 테이블 중 어느 하나를 변환 테이블로 선택하고 선택된 상기 변환 테이블을 이용하여 상기 대상 페이지의 주소에 대응하는 상기 대상 페이지의 물리적 주소를 추출하고, 행(row) 디코더를 경유하여 상기 메모리 셀 어레이로 상기 대상 페이지의 물리적 주소를 제공함으로써, 플래시 메모리 시스템의 성능 및 안정성이 향상될 수 있다. 그리고 플래시 메모리 관리 소프트웨어의 구상에 있어 보다 많은 자유도가 제공될 수 있다.
- [0009] 또한, 선행기술 2는 한국공개특허공보 제2006-0068083호(2006.06.21)로서, 분산 저장장치 기반 침입 탐지 시스템 및 방법에 관한 것이다. 이러한 선행기술 2는 i) 파일을 저장하고, 상기 저장된 파일에 읽기/쓰기 동작을 수행하는 스토리지 노드 모듈, ii) 침입을 모니터링하고, 침입탐지시 손상된 데이터를 복구하는 관리 노드 모듈, iii) 침입 탐지 디렉토리를 설정하고, 침입 목록을 작성하는 설정 노드 모듈, 및 iv) 네트워크를 통하여 임의의 스토리지 노드 모듈에 저장되어 있는 파일에 대한 읽기/쓰기를 요청하는 클라이언트 노드 모듈을 포함하되,
- [0010] 상기 관리 노드 모듈은 상기 스토리지 노드 모듈이 파일 읽기/쓰기 동작을 요청받은 때에 보내온 파일 버전 정보를 분석하여 상기 스토리지 노드 상의 파일에 대한 침입을 탐지함으로써, 저장장치에 저장된 데이터의 자체적인 정보에 의하여 침입을 탐지하므로, 기존의 시스템 및 네트워크 침입 탐지 시스템이나 방화벽과 같은 일차적인 보안 기법에 자체적인 장애가 발생하여 침입을 탐지할 수 없는 경우에도 데이터에 대한 무결성 및 가용성을 제공할 수 있다.

발명의 내용

해결하려는 과제

- [0011] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 스토리지 서버에 파일을 업로드하거나, 삭제 시 일회용 패스워드를 발급받아 이를 확인함으로써, 사용자 부인방지를 제공할 수 있는 스토리지 서비스 이용에 따른 사용자의 부인 가능성 여부를 미연에 방지할 수 있는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법을 제공하고자 한다.
- [0012] 또한, 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 스토리지 서버에 저장되는 파일 내 데이터의 변조 유무를 판단함으로써, 데이터의 무결성 여부를 검증할 수 있는 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법을 제공하고자 한다.

과제의 해결 수단

- [0013] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 제1 사용자단말이 스토리지 서버에 업로드 하고자 하는 파일의 인덱스 정보와, 상기 파일의 해시값을 인증서버로 전송하는 단계; 상기 인증서버가 수신한 파일의 인덱스 정보를 테이블에 저장하고, 수신한 파일의 해시값을 다차원 배열 형태로 저장하는 단계; 상기 인증서버가 일회용 패스워드(One Time Password)를 생성하여, 제2 사용자단말로 전송하는 단계; 상기 인증서버가 상기 제1 사용자단말의 파일 업로드를 요청하는 요청메시지를 상기 스토리지 서버로 전송하는 단계; 상기 제2 사용자단말이 수신한 일회용 패스워드를 상기 제1 사용자단말로 전송하는 단계; 상기 제1 사용자단말이 수신한 일회용 패스워드 및 업로드하고자

하는 파일을 상기 스토리지 서버로 전송하는 단계; 상기 스토리지 서버가 수신한 파일을 임시 저장한 후, 상기 파일의 인덱스 정보와 해시값을 생성하여 상기 인증서버로 전송하는 단계; 상기 인증서버가 상기 스토리지 서버로부터 수신한 파일의 인덱스 정보와 해시값을 상기 제1 사용자단말로부터 수신한 파일의 인덱스 정보와 해시값을 상호 비교하여 정상 사용자 여부를 확인한 후, 상기 스토리지 서버 및 상기 제1 사용자단말로 사용자 인증완료 메시지를 보내는 사용자인증 완료메시지를 전송하는 단계; 및 상기 스토리지 서버가 수신한 사용자인증 완료메시지에 응답하여 임시 저장중인 파일을 스토리지 디스크에 저장하는 단계;를 포함한다.

[0014] 위와 같은 과제를 해결하기 위한 본 발명의 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 제1 사용자단말이 스토리지 서버로부터 다운로드하고자 하는 파일의 리스트를 수신하기 위한 파일 리스트 요청메시지를 인증서버로 전송하는 단계; 상기 인증서버가 수신한 파일리스트 요청메시지에 응답하여 상기 제1 사용자단말로 파일 리스트를 전송하는 단계; 상기 제1 사용자단말이 수신한 상기 파일 리스트로부터 다운로드하고자 하는 파일을 선택한 후, 선택한 파일리스트를 상기 인증서버로 전송하는 단계; 상기 인증서버가 상기 제1 사용자단말이 선택한 파일을 다운로드하기 위한 다운로드 요청 메시지를 상기 스토리지 서버로 전송하는 단계; 상기 스토리지 서버는 상기 제1 사용자단말이 선택한 파일을 상기 제1 사용자단말로 전송하는 단계; 상기 제1 사용자단말이 수신한 파일의 해시값을 생성하여 상기 인증서버로 전송하는 단계; 상기 인증서버가 상기 제1 사용자단말로부터 수신한 파일의 해시값을 카운트 민 스케치(Count Min Sketch) 방식에 의해 검증하고, 검증 완료메시지를 생성하여 상기 스토리지 서버 및 상기 제1 사용자단말로 전송하는 단계;를 포함한다.

[0015] 위와 같은 과제를 해결하기 위한 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 제1 사용자단말이 스토리지 서버에 저장된 파일 중 삭제하고자 하는 파일의 리스트를 수신하기 위한 삭제 파일 리스트 요청메시지를 인증서버로 전송하는 단계; 상기 인증서버가 수신한 삭제 파일 리스트 요청메시지에 응답하여 상기 제1 사용자단말로 삭제 파일 리스트를 전송하고, 일회용 패스워드(One Time Password)를 생성하여 제2 사용자단말로 전송하는 단계; 상기 제1 사용자단말이 수신한 삭제 파일 리스트로부터 삭제하고자 하는 삭제 대상 파일을 선택하고, 선택한 삭제 대상 파일 리스트 및 수신한 일회용 패스워드를 상기 인증서버로 전송하는 단계; 상기 인증서버가 수신한 일회용 패스워드와 자신이 생성한 일회용 패스워드와 비교하여 일회용 패스워드에 대한 검증을 수행하고, 상기 제1 사용자단말로부터 수신한 삭제 대상 파일 리스트 및 상기 삭제 대상 파일의 삭제를 요청하는 삭제 요청메시지를 스토리지 서버로 전송하는 단계; 상기 스토리지 서버가 삭제 대상 파일의 인덱스 정보와 해시값을 생성하여 상기 인증서버로 전송하고, 스토리지 디스크에 기저장된 삭제 대상 파일을 삭제하는 단계; 및 상기 인증서버가 삭제한 파일의 인덱스 정보를 테이블로부터 삭제하고, 상기 삭제한 파일의 해시값을 카운트 민 스케치(Count Min Sketch) 방식에 따라 저장된 다차원 배열로부터 삭제한 후, 삭제완료메시지를 생성하여 상기 제1 사용자단말로 전송하는 단계;를 포함한다.

[0016] 위와 같은 과제를 해결하기 위한 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 제1 사용자단말이 파일의 무결성 검증을 시작하는 검증메시지를 인증서버로 전송하는 단계; 상기 인증서버가 상기 제1 사용자단말로 무결성 검증을 수행하기 위한 파일 리스트를 전송하는 단계; 상기 제1 사용자단말이 수신한 파일 리스트 중 무결성 검증을 수행하고자 하는 파일을 선택한 후, 선택한 파일 리스트를 상기 인증서버로 전송하는 단계; 상기 인증서버가 수신한 파일 리스트의 파일 해시값을 수신하기 위한 해시값 요청메시지를 스토리지 서버로 전송하는 단계; 상기 스토리지 서버가 수신한 해시값 요청메시지에 응답하여 스토리지 디스크 내 해시값 전송을 요청한 파일을 검색한 후, 검색한 파일의 해시값을 생성하여 상기 인증서버로 전송하는 단계; 및 상기 인증서버가 수신한 파일의 해시값을 카운트 민 스케치(Count Min Sketch) 방식에 의해 무결성을 검증하고, 검증결과를 상기 제1 사용자단말로 전송하는 단계;를 포함한다.

[0017] 위와 같은 과제를 해결하기 위한 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 제1 사용자단말이 파일의 무결성 검증을 시작하는 검증메시지를 인증서버로 전송하는 단계; 상기 인증서버가 상기 제1 사용자단말로 디렉토리의 무결성 검증을 수행하기 위한 파일 리스트를 전송하는 단계; 상기 제1 사용자단말이 수신한 파일리스트로부터 무결성을 검증하고자 하는 디렉토리를 선택하여 상기 인증서버로 전송하는 단계; 상기 인증서버가 디렉토리별 카운트 민 스케치(Count Min Sketch) 방식에 따라 저장된 데이터 블록의 해시값을 요청하는 해시값 요청메시지를 스토리지 서버로 전송하는 단계; 상기 스토리지 서버가 수신한 해시값 요청메시지에 응답하여 디렉토리별 카운트 민 스케치 방식에 따라 저장된 데이터 블록의 해시값을 생성하여 상기 인증서버로 전송하는 단계; 상기 인증서버가 상기 스토리지 서버로부터 수신한 데이터 블록의 해시값을 머클 해시트리(Merkle Hash Tree) 연산방법에 적용하여 연산함으로써 디렉토리별 무결성을 검증하는 단계; 및 상기 인증서버가 상기 디렉토리의 무결성 검증결과를 상기 제1 사용자단말 및 상기

스토리지 서버로 전송하는 단계; 를 포함한다.

발명의 효과

- [0018] 본 발명의 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 사용자단말로 발급된 일회용 패스워드의 확인을 통해 스토리지 서버에 허용되지 않는 사용자가 접속하거나, 정상 사용자가 스토리지 서버에 접속한 이력을 부인하는 것을 방지할 수 있는 효과가 있다. 이에 따라, 사용자에게 의해 발생하는 파일의 상태변경을 용이하게 확인할 수 있는 효과가 있다.
- [0019] 또한 본 발명의 본 발명의 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 스토리지 서버에 저장되어 있는 데이터의 손실 및 변경유무를 확인함에 따라 데이터의 무결성을 용이하게 검증할 수 있는 효과가 있다.

도면의 간단한 설명

- [0020] 도 1은 본 발명의 일 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- 도 2는 스토리지 서버 디스크 파일 테이블을 나타낸 도면이다.
- 도 3은 인증서버의 메모리 해시트리구조를 나타낸 도면이다.
- 도 4는 본 발명의 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- 도 5는 카운트 민 스케치 방식을 나타낸 도면이다.
- 도 6은 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- 도 7은 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- 도 8은 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- 도 9는 머클 해시 트리 구조를 나타낸 도면이다.
- 도 10은 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0021] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.
- [0022] 먼저, 도 1을 참조하여 스토리지 서버에 파일을 업로드 하는 과정을 자세히 살펴보도록 한다.
- [0023] 도 1은 본 발명의 일 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- [0024] 도 1에 도시된 바와 같이, 먼저, 제1 사용자단말(120)이 스토리지 서버(160)에 업로드 하고자 하는 파일의 인덱스 정보 FI 와, 상기 파일 f 을 해시함수 h 를 이용해 해시하여 해시값 h(f)을 생성한다(S110). 이때, 상기 파일의 인덱스 정보 FI 는 파일의 이름과 크기 및 생성시간을 포함하는 메타데이터를 나타낸다.
- [0025] 이어서, 상기 제1 사용자단말(120)이 자신의 고유한 ID 정보 User_ID, 파일의 업로드를 위한 메시지 M(C), 생성한 파일의 인덱스 정보 FI, 해시값 h(f) 및 응답 공격을 방지하기 위한 타임스탬프값 Ts 을 인증서버(140)로 전

송하며, 자신과 상기 인증서버(140)간 대칭키인 Client_AS KEY 를 상기 인증서버(140)로 전송한다(S120).

- [0026] 이에 따라, 상기 인증서버(140)가 수신한 파일의 인덱스 정보 FI 를 파일 테이블 File Table 에 저장하고, 수신한 파일의 해시값 $h(f)$ 을 카운트 민 스케치(Count Min Sketch) 방식에 따라 형성된 다차원 배열 형태로 저장한다(S130).
- [0027] 도 2는 스토리지 서버 디스크 파일 테이블을 나타낸 도면이다.
- [0028] 도 2에 도시된 바와 같이, 상기 인증서버(140)가 수신한 파일의 인덱스 정보 FI 에 따라 파일의 종류별로 나누어 파일 테이블에 각각 저장할 수 있다.
- [0029] 예를 들면, 파일의 인덱스 정보 FI에 따라 영화에 관련된 파일의 이름, 생성시간 및 블룸필터(Bloom Filter)값을 각각 테이블 형태로 저장하고, 뿐만 아니라, 상기 파일의 이름, 생성시간, 블룸필터값을 문서, 음악, 사진 등의 종류별로 나누어 저장할 수 있다.
- [0030] 또한, 상기 파일의 해시값 $h(f)$ 은 카운트 민 스케치 방식에 따른 다차원 배열 형태로 저장되는데, 이러한 상기 카운트 민 스케치 방식이란 블룸필터(Bloom Filter) 자료구조를 응용하여 개발된 자료구조로서, 신규 데이터의 입력과 삭제가 가능할 뿐만 아니라 데이터 용량의 크기를 감소시킬 수 있다.
- [0031] 인증서버(140)가 이처럼, 다수의 사용자단말로부터 파일의 해시값을 수신함에 따라 수신한 파일의 해시값에 대하여 해시트리구조를 형성한다.
- [0032] 도 3은 인증서버의 메모리 해시트리구조를 나타낸 도면이다.
- [0033] 도 3에 도시된 바와 같이, 파일의 종류에 따라 파일의 해시값 또한 구분되어 형성된다. 예를 들어, 영화에 관련된 파일의 해시값을 다차원 배열형태로 저장하여 영화에 따른 카운트 민 스케치값 CMS(movie)을 생성하고, 이를 해시하여 $h(movie)$ 를 생성한다. 마찬가지로, 문서에 관련된 파일의 해시값을 다차원 배열형태로 저장하여 문서에 따른 카운트 민 스케치값 CMS(document)을 생성하고, 이를 해시하여 $h(document)$ 를 생성한다.
- [0034] 이후, 상기 영화에 대한 해시값 $h(movie)$ 과, 문서에 대한 해시값 $h(document)$ 간 XOR 연산을 수행한 후, 이를 다시 해시하여 영화와 문서간 해시값 $h(md)$ 을 획득할 수 있다.
- [0035] 이러한 방식으로, 영화와 문서간 해시값 $h(md)$ 뿐만 아니라 음악과 사진간 해시값 $h(mp)$ 를 획득할 수 있으며, 결과적으로, 상기 영화와 문서간 해시값 $h(md)$ 과, 음악과 사진간 해시값을 상호 XOR 연산하고, 이를 다시 해시하면 $h(h(md)||h(mp))$, 인증서버의 메모리 내 전체 루트해시값 Root(h) 을 획득할 수 있다.
- [0036] 이어서, 상기 인증서버(140)가 스토리지 서버(160)의 공개키 SS_{pub} KEY 와, 상기 제1 사용자단말(120)로부터 수신한 ID 정보 User_ID, 메시지 $M(C)$, 타임스탬프값 Ts 및 상기 제1 사용자단말(120)과 스토리지 서버(160)간 대칭키를 나타내는 Client_SS KEY를 스토리지 서버(160)로 전송한다(S140).
- [0037] 이에 따라, 상기 스토리지 서버(160)는 수신한 ID 정보 User_ID 와, 메시지 M, 타임스탬프값 Ts 를 내부의 파일 테이블 File Table 에 저장한다(S150).
- [0038] 또한, 상기 인증서버(140)가 상기 제1 사용자단말(120)과 인증서버(140)간 대칭키인 Client_AS KEY 와, 스토리지 서버(160)의 IP주소 $Server_{ip}$, 스토리지 서버(160)의 포트 $Server_{port}$, 제1 사용자단말(120)과 스토리지 서버(160)간 대칭키 Client_SS KEY 를 제1 사용자단말(120)로 전송한다(S160).
- [0039] 이후, 상기 인증서버(140)가 사용자 인증을 위한 일회용 패스워드 OTP_{code} 를 생성하고, 생성한 일회용 패스워드 OTP_{code} 를 제2 사용자단말(180)로 전송한다(S170). 이때, 상기 제2 사용자단말(180)은 상기 제1 사용자단말(120)을 사용하는 동일한 사용자가 항상 소지하며 휴대하는 휴대단말로서, 예를 들면, 스마트폰, 휴대폰, 태블릿 PC 등의 무선단말을 나타낼 수 있다.
- [0040] 이어서, 상기 인증서버(140)가 상기 제1 사용자단말(120)의 파일 업로드를 요청하는 요청메시지를 상기 스토리지 서버(160)로 전송한다.
- [0041] 이후, 상기 제2 사용자단말(180)이 수신한 일회용 패스워드 OTP_{code} 를 상기 제1 사용자단말(120)로 전송한다.
- [0042] 이에 따라, 상기 제1 사용자단말(120)이 제1 사용자단말(120)과 스토리지 서버(160)간 대칭키 Client_SS KEY, 업로드하고자 하는 파일 File, 상기 파일의 생성시간 Ts, 제1 사용자단말(120)과 인증서버(140)간 대칭키

Client_AS KEY 및 상기 일회용 패스워드 OTP_{CODE}를 상기 스토리지 서버(160)로 전송한다(S180).

- [0043] 상기 스토리지 서버(160)가 수신한 일회용 패스워드 OTP_{CODE}를 제1 사용자단말(120)과 인증서버(140)간 대칭키 Client_AS KEY 를 이용하여 암호화한다(S190).
- [0044] 상기 스토리지 서버(160)가 암호화된 일회용 패스워드 Enc_{client_AS KEY}(OTP_{CODE})와, 수신한 타임스탬프값 Ts, 업로드하고자 하는 파일 file 을 RAM 과 같은 내부의 메모리에 임시 저장한다(S200).
- [0045] 이어서, 상기 스토리지 서버(160)가 상기 업로드하고자 하는 파일의 인덱스 정보 FI 와 블룸필터값 BF(f)을 생성한다(S210).
- [0046] 상기 스토리지 서버(160)가 상기 제1 사용자단말(120)과 인증서버(140)간 대칭키 Client_AS KEY, 일회용 패스워드 OTP_{CODE}, 인증서버(140)의 공개키 AS_{PUB} KEY, 파일의 인덱스 정보 FI, 파일의 블룸필터값 BF(f), 타임스탬프값 Ts 을 상기 인증서버(140)로 전송한다(S220).
- [0047] 이에 따라, 상기 인증서버(140)가 상기 스토리지 서버(160)로부터 수신한 일회용 패스워드 OTP_{CODE} 를 자신이 생성한 일회용 패스워드 OTP_{CODE} 와 비교하고, 상기 스토리지 서버(160)로부터 수신한 타임스탬프값 Ts를 상기 제1 사용자단말(120)로부터 수신한 타임스탬프값 Ts와 비교(S230)하며, 이와 같이 비교된 일회용 패스워드 OTP_{CODE} 와 타임스탬프값 Ts 은 파일 테이블 File Table 에 저장한다(S240).
- [0048] 또한, 상기 인증서버(140)가 상기 스토리지 서버(160)로부터 수신한 파일의 인덱스 정보 FI 와 상기 제1 사용자단말(120)로부터 수신한 파일의 인덱스 정보 FI를 상호 비교하여 검증하고, 상기 스토리지 서버(160)로부터 수신한 블룸필터값 BF(f)과 상기 제1 사용자단말(120)로부터 수신한 해시값 h(f) 을 상호 비교하여 검증한다(S230).
- [0049] 상기 인증서버(140)가 상술한 바와 같이 검증이 완료된 파일의 인덱스 정보 FI 와 해시값 h(f)을 카운트 민 스케치 방법에 따라 다차원 배열 형태로 저장한다(S240).
- [0050] 이에 따라, 상기 인증서버(140)가 스토리지 서버(160)의 공개키 SS_{PUB} KEY 및 사용자 인증완료를 나타내는 사용자인증 완료메시지를 상기 스토리지 서버(160)로 전송한다(S250).
- [0051] 상기 스토리지 서버(160)가 수신한 사용자인증 완료메시지에 응답하여 내부임시 메모리에 저장중인 파일을 스토리지 디스크에 이동시켜 저장한다(S260).
- [0052] 또한, 상기 인증서버(140)가 상기 제1 사용자단말(120)과 인증서버(140)간 대칭키 Client_AS KEY 와, 사용자 인증완료를 나타내는 사용자인증 완료메시지를 상기 제1 사용자단말(120)로 전송한다(S270).
- [0053] 이하, 도 4를 참조하여, 스토리지 서버에 저장된 파일의 다운로드 과정에 대하여 자세히 살펴보도록 한다.
- [0054] 도 4는 본 발명의 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- [0055] 도 4에 도시된 바와 같이, 먼저, 제1 사용자단말(220)이 스토리지 서버(260)로부터 다운로드하기 위한 파일의 리스트를 수신하기 위해, 파일 리스트 요청메시지 M(down)를 인증서버(240)로 전송한다. 이때, 상기 제1 사용자단말(220)은 자신과 인증서버간 대칭키 Client_AS KEY 와, 사용자의 고유 ID정보 User_ID 를 함께 상기 인증서버(240)로 전송할 수 있다(S310).
- [0056] 이에 따라, 상기 인증서버(240)가 수신한 파일리스트 요청메시지 M(down)에 응답하여 상기 제1 사용자단말(220)과 인증서버(240)간 대칭키 Client_AS KEY 와, 파일 리스트 File Table 및 상기 제1 사용자단말(220)과 스토리지 서버(260)간 대칭키 Client_SS KEY를 상기 제1 사용자단말(220)로 전송한다(S320).
- [0057] 이후, 상기 제1 사용자단말(220)이 수신한 상기 파일 리스트 File Table 로부터 다운로드하고자 하는 파일을 선택한 후, 선택한 파일 리스트 File name 와, 자신의 IP 주소 User_IP 및 자신과 인증서버간 대칭키 Client_AS KEY 를 상기 인증서버(240)로 전송한다(S330).
- [0058] 이에 따라, 상기 인증서버(240)가 상기 제1 사용자단말(220)이 선택한 파일을 다운로드하기 위해, 스토리지 서버(260)의 공개키 SS_{pub}KEY 와, 상기 제1 사용자단말(220)의 고유 ID 정보 User_ID, IP 주소 Uer_IP, 다운로드하고자 하는 파일의 이름 Filename, 다운로드 요청 메시지 M(down) 및 제1 사용자단말(220)과 스토리지 서버(260)간 대칭키 Client_SS KEY를 상기 스토리지 서버(260)로 전송한다(S340).

0)간 대칭키 Client_SS KEY 를 상기 스토리지 서버(260)로 전송한다(S340).

- [0059] 이후, 상기 스토리지 서버(260)는 상기 제1 사용자단말(220)이 선택한 파일을 스토리지 디스크로부터 로딩하여, 로딩한 파일 file 과, 상기 제1 사용자단말(220)과 스토리지 서버(260)간 대칭키 Client_SS KEY 를 상기 제1 사용자단말(220)로 전송한다(S350). 상술한 바와 같이, 상기 제1 사용자단말(220)이 상기 스토리지 서버(260)로부터 파일의 다운로드를 완료하고, 다운로드한 파일에 대한 블룸필터값을 연산하여 파일의 해시값 $h(f)$ 을 생성한다(S360).
- [0060] 이어서, 상기 제1 사용자단말(220)이 자신과 인증서버간 대칭키 Client_AS KEY 와, 앞서 연산한 파일의 해시값 $BF(f)$ 을 상기 인증서버(240)로 전송한다(S370).
- [0061] 이후, 상기 인증서버(240)가 상기 제1 사용자단말(220)로부터 수신한 파일의 해시값 $BF(f)$ 을 카운트 민 스케치 (Count Min Sketch) 방식에 의해 검증한다(S380).
- [0062] 이하, 도 5를 참조하여, 카운트 민 스케치 방식에 대하여 보다 자세히 살펴보도록 한다.
- [0063] 도 5는 카운트 민 스케치 방식을 나타낸 도면이다.
- [0064] 상기 카운트 민 스케치(Count Min Sketch) 방식이란, 블룸필터(Bloom Filter) 자료구조를 응용하여 개발된 자료 구조 방식으로, 새로운 데이터의 입력과 삭제가 가능하며, 다차원 배열을 사용함으로써, 더욱 정확한 데이터의 검증을 수행할 수 있다.
- [0065] 예를 들어, 도 5에 도시된 바와 같이, 입력 데이터가 $h_1(a) = 3$ 인 경우에 다차원 배열 중 첫 번째 열의 세 번째 행에 데이터 '1'이 저장된다. 또한, 입력 데이터가 $h_2(a) = 4$ 인 경우에 다차원 배열 중 두 번째 열의 네 번째 행에 데이터 '1'이 저장됨에 따라 이를 비교함으로써, 데이터의 검증이 이루어진다.
- [0066] 이어서, 상기 인증서버(240)가 수신한 파일의 해시값 $BF(f)$ 에 대한 검증 완료메시지를 생성하여, 생성한 검증완료 메시지와, 상기 스토리지 서버(260)의 공개키 SSpub KEY를 상기 스토리지 서버(260)로 전송한다(S390).
- [0067] 또한, 상기 인증서버(240)가 상기 검증완료 메시지와, 상기 제1 사용자단말(220)과 인증서버(240)간 대칭키 Client_AS KEY를 상기 제1 사용자단말(220)로 전송한다(S400).
- [0068] 이하, 도 6을 참조하여 스토리지 서버 내 저장된 파일의 삭제과정에 대하여 자세히 살펴보도록 한다.
- [0069] 도 6은 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- [0070] 도 6에 도시된 바와 같이, 먼저, 제1 사용자단말(320)이 스토리지 서버(360)에 저장된 파일 중 삭제하고자 하는 파일의 리스트를 수신하기 위해, 상기 제1 사용자단말(320)과 인증서버(340)간 대칭키 Client_AS KEY와, 상기 제1 사용자단말(320)의 고유 ID 정보 User_ID 및 삭제 파일 리스트 요청메시지 M(delete)를 인증서버(340)로 전송한다(S410).
- [0071] 이에 따라, 상기 인증서버(340)가 수신한 삭제 파일 리스트 요청메시지 M(delete)에 응답하여 해당하는 파일을 로딩한 후, 상기 제1 사용자단말(320)과 인증서버(340)간 대칭키 Client_AS KEY와 파일 테이블 File Table을 상기 제1 사용자단말(320)로 삭제 파일 리스트를 전송한다(S420).
- [0072] 이어서, 상기 인증서버(340)가 일회용 패스워드 OTP_{CODE}(One Time Password)를 생성하여 제2 사용자단말(380)로 전송한다(S430).
- [0073] 이후, 상기 제2 사용자단말(380)이 상기 인증서버(340)로부터 수신한 일회용 패스워드 OTP_{CODE} 를 상기 제1 사용자단말(320)로 전송한다(S440).
- [0074] 이에 따라, 상기 제1 사용자단말(320)이 상기 제1 사용자단말(320)과 인증서버(340)간 대칭키 Client_AS KEY 와, 수신한 삭제 파일 리스트로부터 삭제하고자 하는 삭제 대상 파일을 선택하고, 선택한 삭제 대상 파일 리스트 Filename 및 상기 일회용 패스워드 OTP_{CODE}를 상기 인증서버(340)로 전송한다(S450).
- [0075] 이후, 상기 인증서버(340)가 수신한 일회용 패스워드 OTP_{CODE} 와 자신이 생성한 일회용 패스워드 OTP_{CODE} 를 상호 비교하여 일회용 패스워드에 대한 검증을 수행한다(S460).
- [0076] 이어서, 상기 인증서버(340)가 스토리지 서버(360)의 공개키 SS_{PUB} KEY와, 상기 제1 사용자단말(320)의 고유 ID

정보 User_ID, 삭제 파일 리스트 요청메시지 M(delete) 및 삭제하고자 하는 파일의 이름 Filename 을 상기 스토리지 서버(360)로 전송한다(S470).

- [0077] 이에 따라, 상기 스토리지 서버(360)가 스토리지 디스크로부터 삭제하고자 하는 파일의 블록필터값 BF(f)을 로딩한 후, 상기 블록필터값 BF(f)을 저장하는 파일 테이블 File Table 및 해당하는 파일 File을 삭제한다(S480).
- [0078] 이후, 상기 스토리지 서버(360)가 상기 인증서버(340)의 공개키 AS_{PUB} KEY와파일 인덱스 FI 및 상기 파일의 블록필터값 BF(f)을 상기 인증서버(340)로 전송한다(S490).
- [0079] 이에 따라, 상기 인증서버(340)는 수신한 파일의 인덱스 정보 FI를 파일 테이블 File Table로부터 삭제하고, 상기 삭제한 파일의 블록필터값 BF(f)을 카운트 민 스케치(Count Min Sketch) 방식에 따라 저장된 다차원 배열로부터 삭제한다(S500).
- [0080] 이후, 상기 인증서버(340)가 상기 제1 사용자단말(320)과 인증서버(340)간 대칭키 Client_AS KEY와, 생성한 삭제완료메시지를 상기 제1 사용자단말(320)로 전송한다(S510).
- [0081] 이하, 도 7을 참조하여, 스토리지 서버 내 개별 파일에 대한 무결성을 검증하는 과정에 대하여 자세히 살펴보도록 한다.
- [0082] 도 7은 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- [0083] 도 7에 도시된 바와 같이, 먼저, 제1 사용자단말(420)이 제1 사용자단말(420)과 인증서버(440)간 공개키 Client_AS KEY와, 상기 제1 사용자단말(420)의 고유 ID 정보 및 파일의 무결성 검증을 시작하는 검증메시지 M(verify)를 인증서버(440)로 전송한다(S610).
- [0084] 상기 인증서버(440)가 무결성 검증을 수행하고자 하는 파일을 파일 리스트 File Table 로부터 로딩하여, 상기 제1 사용자단말(420)과 로딩한 파일 리스트 File Table 를 상기 제1 사용자단말(420)로 전송한다(S620).
- [0085] 상기 제1 사용자단말(420)이 수신한 파일 리스트 File Table 중 무결성 검증을 수행하고자 하는 파일을 선택한 후, 선택한 파일 리스트 File name 과, 상기 제1 사용자단말(420)과 인증서버(440)간 대칭키 Client_AS KEY 를 상기 인증서버(440)로 전송한다(S630).
- [0086] 이에 따라, 상기 인증서버(440)가 스토리지 서버(460)의 공개키 SS_{PUB} KEY 와, 선택받은 파일의 해시값 BF(f) 요청 메시지를 상기 스토리지 서버(460)로 전송한다(S640).
- [0087] 이후, 상기 스토리지 서버(460)가 스토리지 디스크로부터 요청받은 파일의 블록필터값 BF(f)을 로딩하여, 상기 인증서버(440)의 공개키 AS_{PUB} KEY와, 요청받은 파일File 및 상기 파일의 블록필터값 BF(f) 을 상기 인증서버(440)로 전송한다(S650).
- [0088] 이어서, 상기 인증서버(440)가 파일의 블록필터값에 대하여 카운트 민 스케치(Count Min Sketch) 방식에 의해 무결성을 검증한다(S660).
- [0089] 이후, 상기 인증서버(440)가 상기 제1 사용자단말(420)과 인증서버(440)간 대칭키 Client_AS KEY와, 검증결과 메시지를 상기 제1 사용자단말(420)로 전송한다(S670).
- [0090] 이하, 도 8을 참조하여 스토리지 서버 내 디렉토리 무결성을 검증하는 과정에 대하여 자세히 살펴보도록 한다.
- [0091] 도 8은 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- [0092] 특히, 스토리지 서버 내 존재하는 다수의 파일이 블록으로 나누어지고, 나누어진 블록이 트리구조로 형성됨에 따라 디렉토리 형태로 이루어진다.
- [0093] 도 8에 도시된 바와 같이, 먼저 제1 사용자단말(520)이 제1 사용자단말(520)과 인증서버(540)간의 대칭키 Client_AS KEY 와, 상기 제1 사용자단말(520)의 고유 ID 정보 User_ID 및 디렉토리의 무결성 검증을 시작하는 검증메시지 M(Verify) 를 인증서버(540)로 전송한다(S710).
- [0094] 이후, 상기 인증서버(540)가 디렉토리의 무결성 검증을 수행하기 위한 파일 리스트 File Table 와, 상기 제1 사용자단말(520)과 인증서버(540)간 대칭키 Client_AS KEY 를 상기 제1 사용자단말(520)로 전송한다(S720).

- [0095] 이어서, 상기 제1 사용자단말(520)이 수신한 파일리스트로부터 무결성을 검증하고자 하는 디렉토리를 선택하고, 선택한 디렉토리 이름 Directory name 과, 상기 제1 사용자단말(520)과 인증서버(540)간 대칭키 Client_AS KEY 를 상기 인증서버(540)로 전송한다(S730).
- [0096] 이에 따라, 상기 인증서버(540)가 디렉토리별 카운트 민 스케치(Count Min Sketch) 방식에 따라 저장된 데이터 블록 중 선택받은 특정 데이터 블록의 해시값을 요청하는 해시값 요청메시지 request h(movie)와, 스토리지 서버(560)의 공개키 SS_{PUB} KEY 를 스토리지 서버(560)로 전송한다(S740). 이때, 선택받은 특정 데이터 블록은 영화에 대한 데이터블록이라고 가정한다.
- [0097] 이후, 상기 스토리지 서버(560)가 수신한 해시값 요청메시지 request h(movie) 에 응답하여 디렉토리별 카운트 민 스케치 방식에 따라 선택받은 특정 데이터 블록의 해시값 h(movie')을 생성한다(S750).
- [0098] 이에 따라, 상기 스토리지 서버(560)가 생성한 특정 데이터 블록의 해시값 h(movie')과, 인증서버(540)의 공개키 AS_{PUB} KEY 를 상기 인증서버(540)로 전송한다(S760).
- [0099] 상기 인증서버(540)가 상기 스토리지 서버(560)로부터 수신한 데이터 블록의 해시값을 머클 해시트리(Merkle Hash Tree) 연산방법에 적용하여 연산함으로써 디렉토리별 무결성을 검증한다(S770). 즉, 상기 인증서버(540)는 상기 스토리지 서버(560)로부터 수신한 영화에 대한 데이터블록의 해시값 h(movie')과, 내부에 기저장되며 상기 영화 데이터블록과 인접하여 배열되는 문서에 대한 데이터블록의 해시값 h(document)간 XOR 연산을 수행한 후, 이를 다시 해시한다. 이때, 생성된 해시값은 h(m'd)이다.
- [0100] 또한, 영화와 문서를 제외한 나머지 디렉토리인 음악에 대한 데이터블록의 해시값인 h(music) 와, 사진에 대한 데이터블록의 해시값인 h(picture)간 XOR 연산을 수행하고, 이를 다시 해시연산을 수행하여 해시값 h(mp)를 생성한다.
- [0101] 결국, 상기 인증서버(540)는 디렉토리 무결성 검증을 수행하기 위해, 앞서 생성한 영화와 문서간 데이터블록의 해시값인 h(m'd)와, 음악과 사진간 데이터블록의 해시값인 h(mp)간 XOR 연산을 수행하고, 이를 다시 해시연산한 값을 전체 루트해시값 h(root') 과 비교하여 디렉토리에 대한 무결성을 검증한다(S770). 상기 머클 해시트리 연산방법에 대하여 도 9를 참조하여 보다 자세히 살펴보도록 한다.
- [0102] 도 9는 머클 해시 트리 구조를 나타낸 도면이다.
- [0103] 상기 머클 해시 트리 구조란, 대용량 데이터가 변경되었는지 여부를 확인할 수 있는 자료구조로서, 대용량의 데이터를 여러 블록으로 분할하여 각 블록별 해시값을 이용하여 트리형태로 이루어지는 구성을 말한다. 이러한 머클 해시 트리구조는 트리형태로 이루어지기 때문에, 대용량 데이터의 어느 부분에서 데이터의 변조가 발생하였는지 여부를 확인할 수 있는 용이하게 알 수 있다.
- [0104] 도 9에 도시된 바와 같이, 다수의 데이터 블록 a, b, c, d, e, f, g, h 로 이루어지는 대용량 데이터에 대하여, 데이터 블록 a의 해시값은 h(a)가 되고, 인접하여 배치되는 데이터블록 b의 해시값 h(b)가 된다. 이때, 상기 데이터블록 a의 해시값 h(a)와 데이터 블록 b의 해시값 h(b)를 상호 XOR 연산을 수행한 후, 이를 다시 해시연산 h(h(a)|| h(b))하면, 데이터 블록의 해시값과 트리구조를 이루는 해시값 h(i)이 획득하게 된다. 이러한 연산과정을 반복하여 전체 대용량 데이터를 데이터 블록으로 분할한 후, 각 데이터 블록별 트리구조로 이어가는 경우, 최종적으로, 전체 루트해시값 h(r)을 획득하게 되고, 이와 같이 획득한 전체 루트해시값 h(r)을 미리 설정된 루트해시값과 비교하여 동일한지 여부를 판단함으로써, 디렉토리에 대한 무결성 여부를 검증할 수 있다.
- [0105] 다시 도 8로 돌아가서, 이러한 무결성 검증결과를 수행한 후, 상기 인증서버(540)가 상기 디렉토리의 무결성 검증결과 메시지와, 스토리지 서버(560)의 공개키 SS_{PUB} KEY 를 상기 스토리지 서버(560)로 전송한다(S780).
- [0106] 이어서, 상기 인증서버(540)가 상기 디렉토리의 무결성 검증결과 메시지와, 상기 제1 사용자단말(520)과 인증서버(540)간 대칭키 Client_AS KEY 를 상기 제1 사용자단말(520)로 전송한다(S790).
- [0107] 이하, 도 10을 참조하여 스토리지 서버 내 전체 파일에 대한 무결성 검증 과정에 대하여 자세히 살펴보도록 한다.
- [0108] 도 10은 본 발명의 또 다른 실시 예에 따른 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법의 순서도이다.
- [0109] 도 10에 도시된 바와 같이, 먼저 제1 사용자단말(620)이 전체 파일의 무결성을 검증하기 위한 검증 시작메시지

M 와, 상기 제1 사용자단말(620)의 고유 ID 정보 User_ID 및 상기 제1 사용자단말(620)과 인증서버(640)간 대칭키 Client_AS KEY를 인증서버(640)로 전송한다(S810).

[0110] 이에 따라, 상기 인증서버(640)가 카운트 민 스케치(Count Min Sketch) 방식에 따라 다차원 배열형태로 기저장된 다수의 데이터 블록의 해시값 중 적어도 하나를 로딩하여(S820), 선택한 디렉토리별 카운트 민 스케치 방식에 따라 저장된 해시값 전송을 요청하는 해시값 요청메시지와, 스토리지 서버(660)의 공개키 SS_{PUB} KEY 와, 상기 제1 사용자단말(620)의 고유 ID 정보 User_ID 를 스토리지 서버(660)로 전송한다(S830).

[0111] 이어서, 상기 스토리지 서버(660)가 수신한 해시값 요청메시지에 응답하여 스토리지 디스크로부터 복수 개의 디렉토리별 카운트 민 스케치의 해시값을 생성한다(S840). 예를 들어, 상기 스토리지 서버(660)가 영화에 대한 카운트 민 스케치의 해시값 h(mpvie') 과, 사진에 대한 카운트 민 스케치의 해시값 h(picture')을 생성할 수 있다.

[0112] 이와 같이, 복수 개의 디렉토리별 카운트 민 스케치의 해시값을 생성한 상기 스토리지 서버(660)는 생성한 복수 개의 디렉토리별 카운트 민 스케치의 해시값과, 인증서버(640)의 공개키 AS_{PUB} KEY 를 인증서버(640)로 전송한다(S850).

[0113] 상기 인증서버(640)가 상기 스토리지 서버(660)로부터 수신한 해시값과, 자신이 기저장하고 있는 해시값을 머클 해시 트리(Merkle Hash Tree) 연산방법을 이용하여 전체 파일에 대한 무결성 검증을 수행한다(S860). 예를 들어, 상기 인증서버(640)가 문서에 대한 카운트 민 스케치 방식으로 기저장된 배열로부터 문서에 대한 해시값 h(document)와, 음악에 대한 해시값 h(music)을 획득한다. 이후, 상기 인증서버(640)는 상기 스토리지 서버(660)로부터 수신한 영화에 대한 해시값 h(movie')와, 기저장하고 있는 문서에 대한 해시값 h(document)를 상호 XOR 연산하고, 이를 다시 해시연산함으로써, 영화와 문서간 해시값을 연산한다 h(m'd). 이어서, 상기 인증서버(640)는 음악에 대한 해시값 h(music)과 사진에 대한 해시값 h(picture')간 XOR 연산을 수행하고, 이를 다시 해시연산하여 음악과 사진에 대한 해시값 h(mp')을 획득할 수 있다. 이후, 상기 인증서버(640)는 전체 루트해시값을 연산하기 위해, 앞서 연산한 영화와 문서간 해시값 h(m'd) 와 음악과 사진간 해시값 h(mp')를 상호 XOR 연산하고, 이를 다시 해시연산하여 전체 파일에 대한 루트 해시값 Root(h')을 획득한다. 이에 따라, 상기 인증서버(640)는 앞서 연산한 루트 해시값 Root(h')과 기저장하고 있는 루트해시값 Root(h)을 상호 비교하여 동일한지 여부를 판단한 후, 전체 파일에 대한 무결성 검증을 완료한다.

[0114] 이처럼, 상기 인증서버(640)가 전체 파일에 대한 무결성 검증을 완료함에 따라 무결성 검증 완료메시지를 생성하고, 생성한 무결성 검증 완료메시지와, 스토리지 서버(660)의 공개키 SS_{PUB} KEY 를 상기 스토리지 서버(660)로 전송한다(S870).

[0115] 이어서, 상기 인증서버(640)는 앞서 생성한 전체 파일에 대한 무결성 검증 완료메시지와, 상기 제1 사용자단말(620)과 인증서버(640)간 대칭키 Client_AS KEY 를 상기 제1 사용자단말(620)로 전송한다(S880).

[0116] 또한, 이러한 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0117] 본 발명의 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 사용자단말로 발급된 일회용 패스워드의 확인을 통해 스토리지 서버에 허용되지 않는 사용자가 접속하거나, 정상 사용자가 스토리지 서버에 접속한 이력을 부인하는 것을 방지할 수 있는 효과가 있다. 이에 따라, 추후 발생하는 사용자에게 의한 파일의 상태변경을 용이하게 확인할 수 있는 효과가 있다.

[0118] 또한 본 발명의 본 발명의 스토리지 서비스 이용에 따른 사용자 부인방지 및 데이터 무결성 검증 방법은 스토리지 서버에 저장되어 있는 데이터의 손실 및 변경을 확인함에 따라 데이터의 무결성을 용이하게 검증할 수 있는 효과가 있다.

[0119] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

[0120]

120: 제1 사용자단말

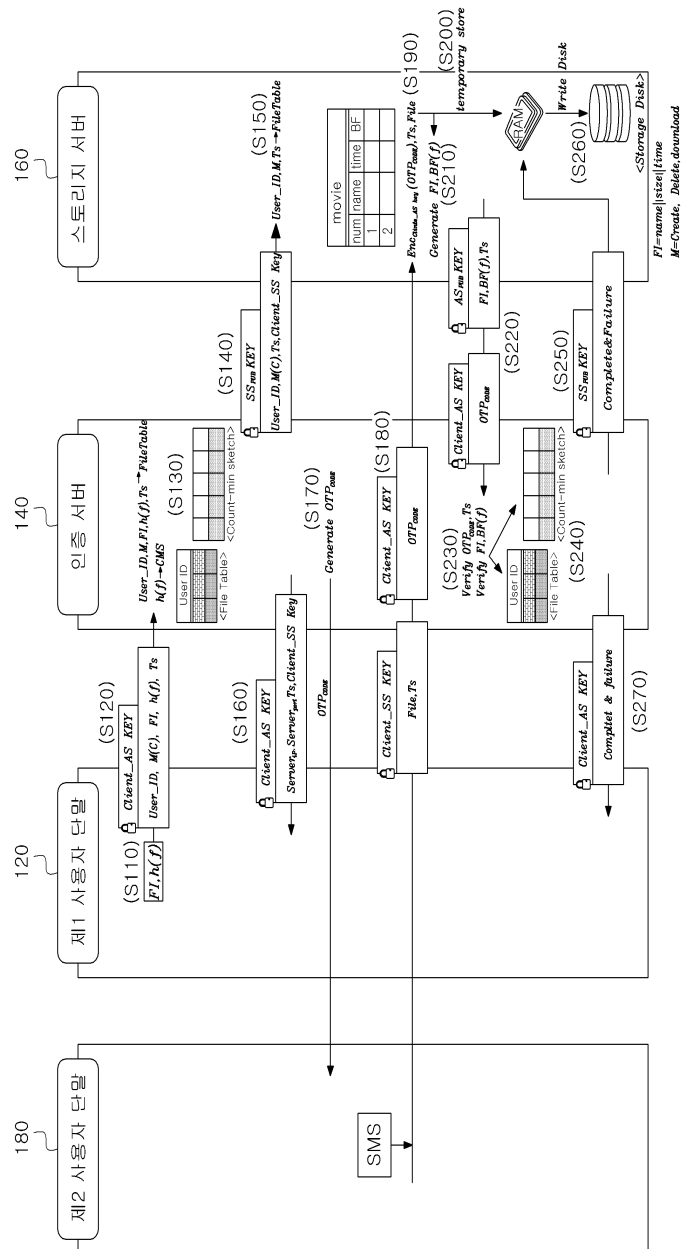
140: 인증서버

160: 스토리지 서버

180: 제2 사용자단말

도면

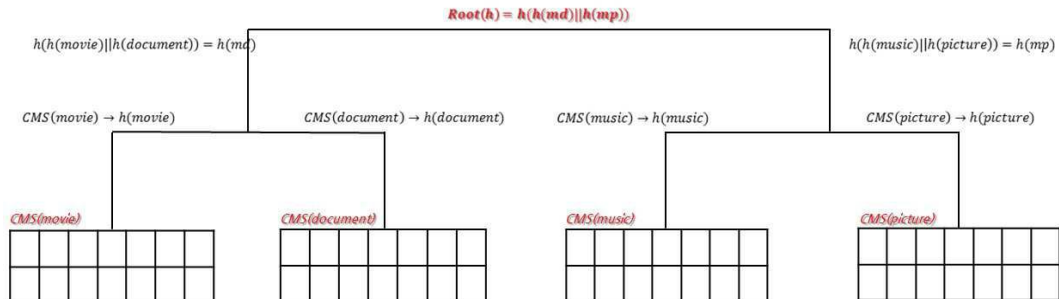
도면1



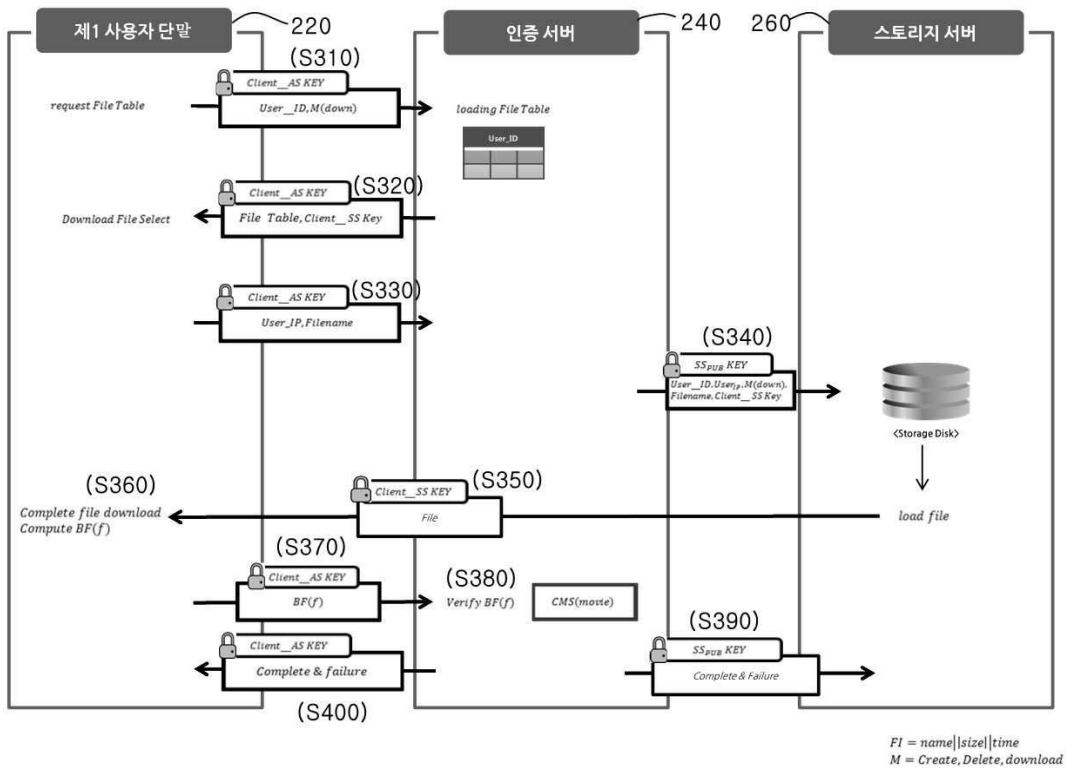
도면2

movie				document				music				picture			
num	name	time	BF	num	name	time	BF	num	name	time	BF	num	name	time	BF
1				1				1				1			
2				2				2				2			

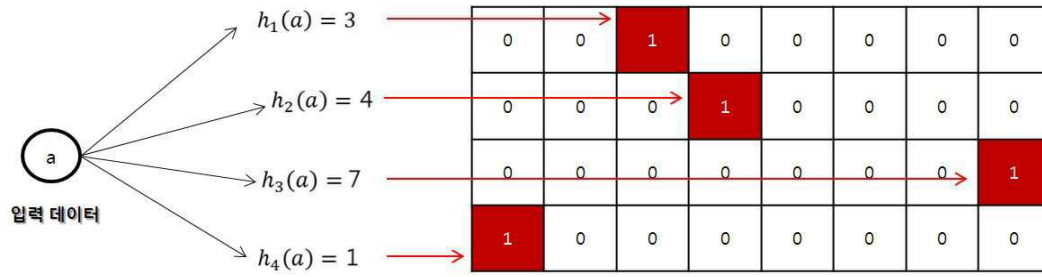
도면3



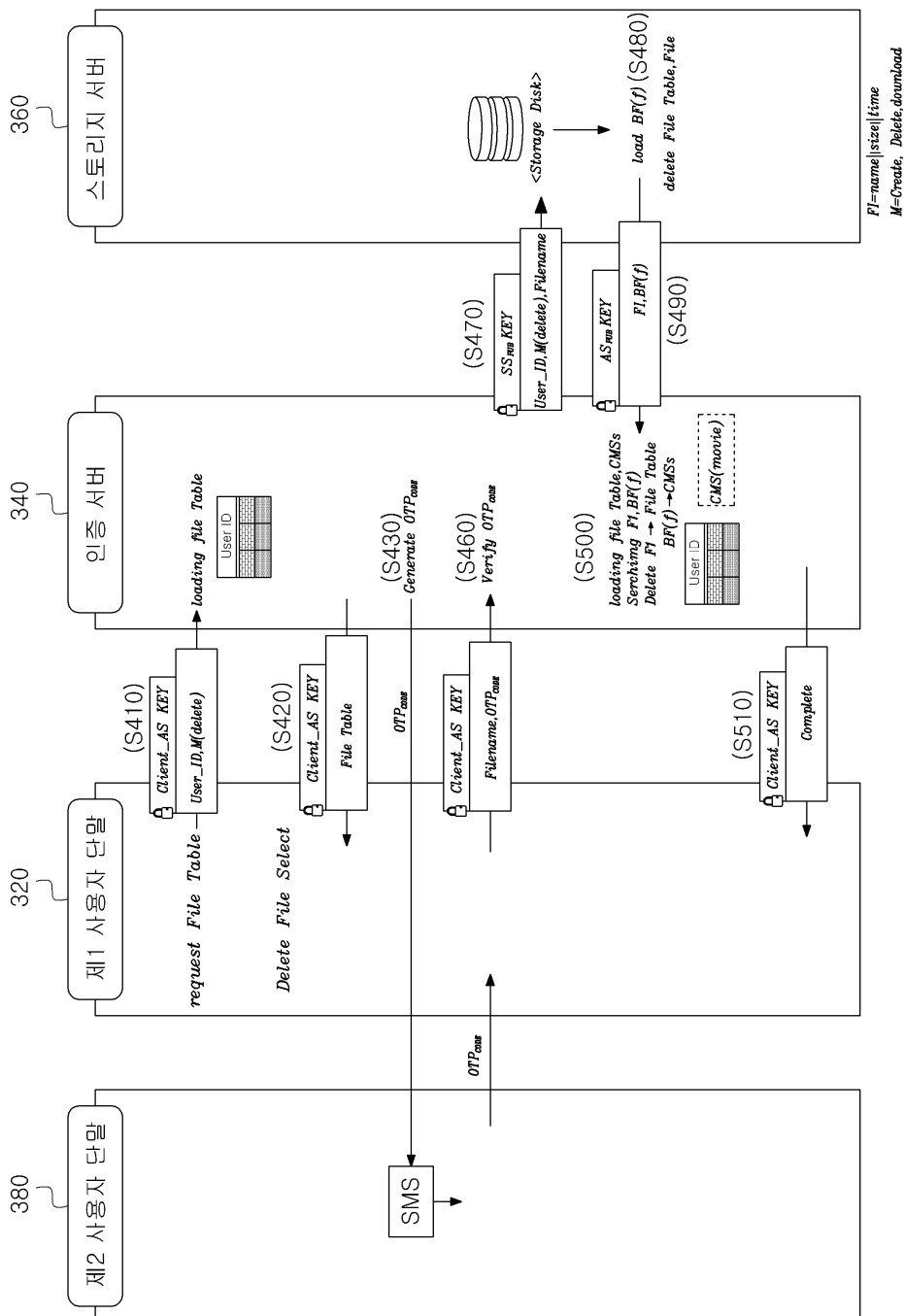
도면4



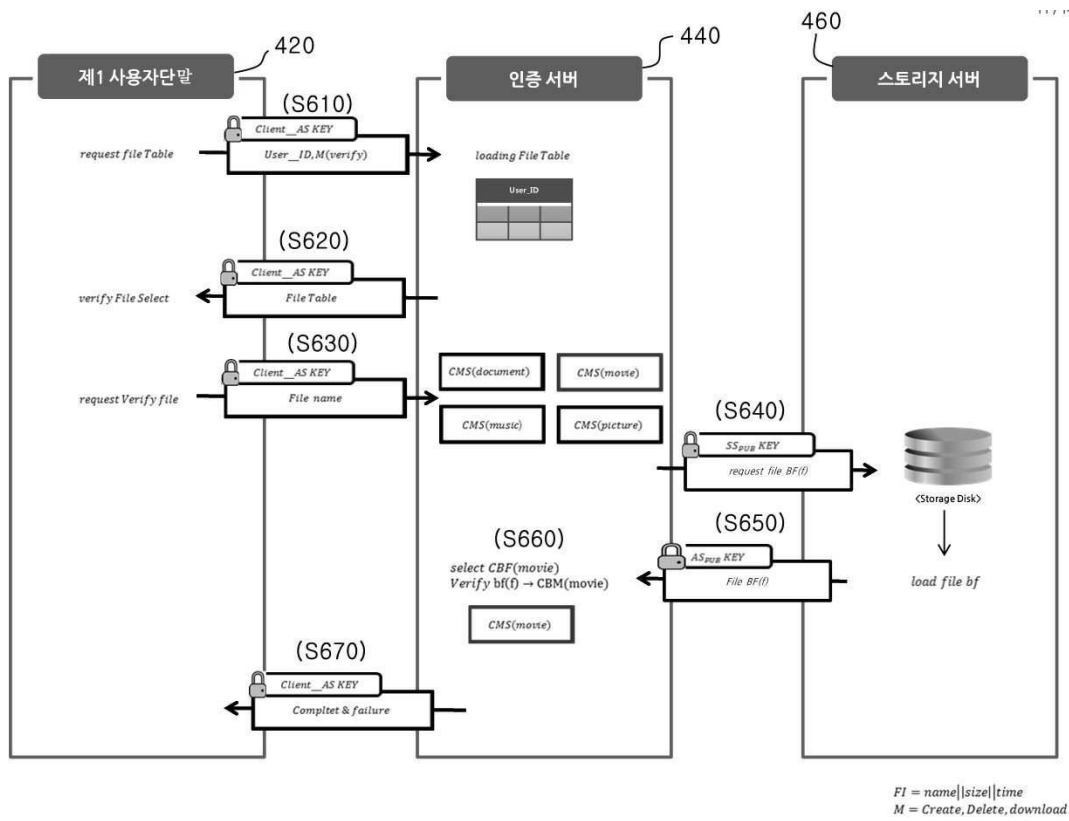
도면5



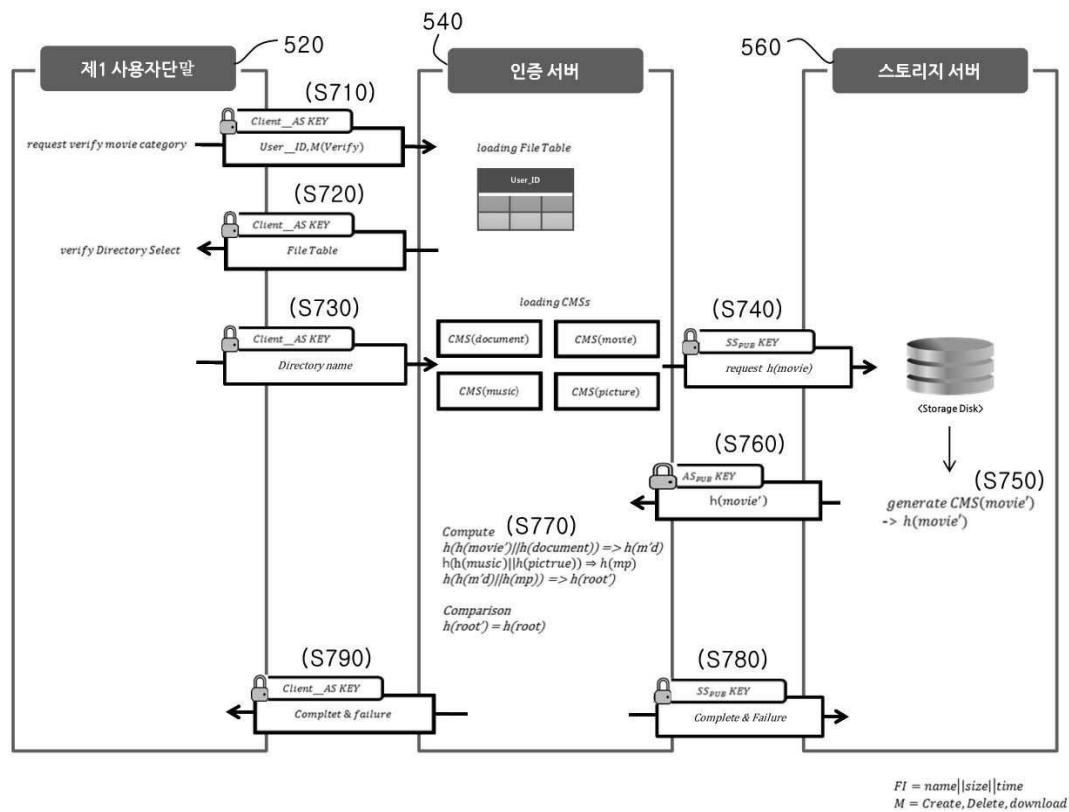
도면6



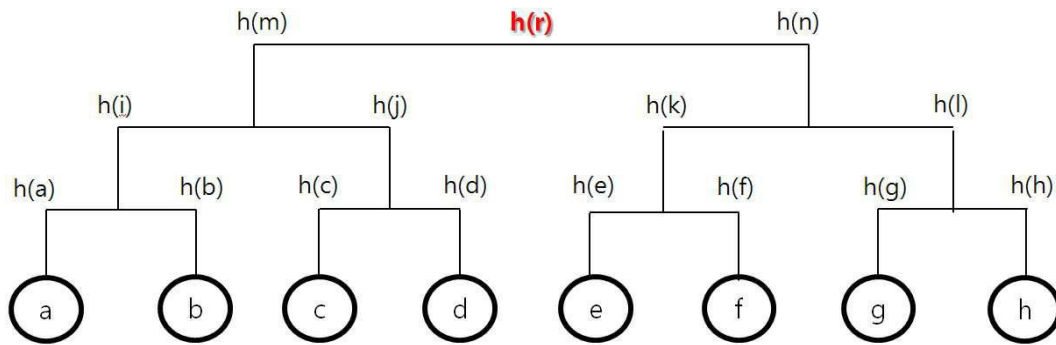
도면7



도면8



도면9



도면10

