국민대학교
KOOKMIN UNIVERSITY

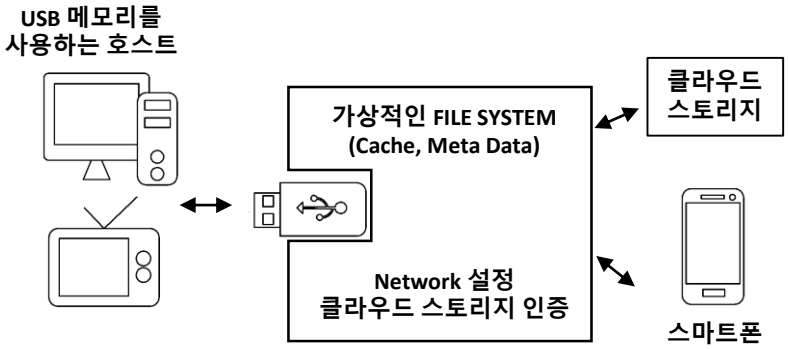
- 이름 : 이민석
- 소속 : 컴퓨터공학부
- 연구분야 : 컴퓨터공학

클라우드 스토리지

저장장치 없이 활용 가능한
클라우드 기반 메모리 장치

기술개요

- 본 기술은 물리 장치의 활용 없이 보호대상 파일 및 클라우드 인증 정보를 저장하는 기술이다.
- 본 기술은 호스트 시스템에서의 로그인 과정 없이 클라우드 스토리지의 파일을 이용 할 수 있다.



기술성

- 호스트 시스템에서 로그인 과정을 생략 하여 접근성 증대
- 물리적 저장 장치 활용을 요하지 않으므로 안정성 증대
- 사용자가 원하는 수준의 보안 레벨을 선택 가능 하므로 편의성 증대

대표청구항

- 사용 호스트 시스템에서의 로그인 과정없이 클라우드 스토리지의 파일을 이용할 수 있도록 하는 클라우드 저장소 기반 메모리 장치
- 클라우드 저장소 기반 메모리 장치가 접속되는 호스트 장치들
- 데이터 파일들을 저장하는 클라우드 스토리지
- 클라우드 저장소 기반 메모리 장치가 호스트 장치에 물리적으로 접속되면 보안 인증 절차를 수행하는 스마트 기기를 포함하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치

지식재산권

- 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법 (10-2017-0179983)

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년08월08일
(11) 등록번호 10-2008691
(24) 등록일자 2019년08월02일

(51) 국제특허분류(Int. Cl.)
G06F 21/34 (2013.01) *G06F 21/60* (2013.01)
G06F 21/78 (2013.01)
(52) CPC특허분류
G06F 21/34 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2017-0179983
(22) 출원일자 2017년12월26일
심사청구일자 2017년12월26일
(65) 공개번호 10-2019-0078198
(43) 공개일자 2019년07월04일
(56) 선행기술조사문헌
JP2011192154 A*
KR101758733 B1*
KR1020140066919 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
국민대학교산학협력단
서울특별시 성북구 정릉로 77 (정릉동, 국민대학교)
(72) 발명자
이민석
서울특별시 강남구 광평로51길 22, 103동 703호(수서동, 한아름아파트)
(74) 대리인
정부연

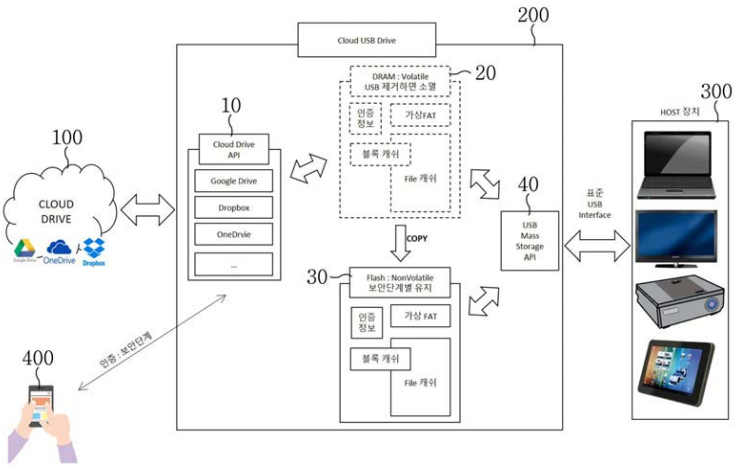
전체 청구항 수 : 총 15 항 심사관 : 문남두

(54) 발명의 명칭 **안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법**

(57) 요 약

본 발명은 호스트 시스템에서의 로그인 과정 없이 클라우드 스토리지의 파일을 이용할 수 있고, 보호 대상인 파일 및 클라우드 인증 정보를 비휘발성 물리적 저장 장치에 저장하지 않는 보안성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법에 관한 것으로, 사용 호스트 시스템에서의 로그인 과정없이 클라우드 스토리지의 파일을 이용할 수 있도록 하는 클라우드 저장소 기반 메모리 장치;클라우드 저장소 기반 메모리 장치가 접속되는 호스트 장치들;데이터 파일들을 저장하는 클라우드 스토리지;클라우드 저장소 기반 메모리 장치가 호스트 장치에 물리적으로 접속되면 보안 인증 절차를 수행하는 스마트 기기;를 포함하는 것이다.

대 표 도 - 도2



(52) CPC특허분류
G06F 21/604 (2013.01)
G06F 21/78 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 17-136 (IPA 관리번호)
부처명 미래창조과학부
연구관리전문기관 정보통신산업진흥원
연구사업명 창의도전형 SW R&D 지원 사업
연구과제명 클라우드 기반 USB 저장 매체
기 여 율 1/1
주관기관 한국IT비즈니스진흥협회
연구기간 2017.05.15 ~ 2017.11.30
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

데이터 파일들을 저장하는 클라우드 스토리지;

사용 호스트 시스템에서의 로그인 과정없이 클라우드 스토리지의 파일을 이용할 수 있고, 보호 대상인 파일 및 클라우드 인증 정보를 저장하지 않는 클라우드 저장소 기반 메모리 장치;

클라우드 저장소 기반 메모리 장치가 접속되는 호스트 장치들;

클라우드 저장소 기반 메모리 장치가 호스트 장치에 물리적으로 접속되면 상기 클라우드 저장소 기반 메모리 장치로부터 보안 인증 요청을 수신하여 상기 클라우드 저장소 기반 메모리 장치가 상기 클라우드 스토리지로의 보안 인증 절차를 수행할 수 있도록 인증 데이터를 상기 클라우드 저장소 기반 메모리 장치에 송신하는 스마트 기기;를 포함하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치.

청구항 2

삭제

청구항 3

제 1 항에 있어서, 상기 스마트 기기의 보안 인증을 통하여 인증된 사용자만 상기 클라우드 스토리지에 접근이 가능하고, 상기 스마트 기기를 통하여 원하는 수준의 보안 레벨을 설정하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치.

청구항 4

제 3 항에 있어서, 보안 레벨은,

암호화된 클라우드 ID 및 PWD, 암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 자동 로그인을 지원하는 0 단계와,

암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 인증정보의 유효기간동안 자동 로그인을 지원하는 1 단계와,

메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 File 및 Meta Data 암호화가 이루지는 2 단계와,

메타데이터, 읽기 쓰기 파일 데이터의 Block 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 File,Block 및 Meta Data 암호화가 이루어지는 3 단계와,

읽기 쓰기 파일 데이터의 Block 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 Block Data 암호화가 이루어지는 4 단계와,

클라우드 저장소 기반 메모리 장치에 아무 정보도 남지 않는 5 단계로 설정하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치.

청구항 5

제 1 항에 있어서, 클라우드 저장소 기반 메모리 장치는,

호스트 장치가 일반 USB와 동일한 형태로 인식하고, 클라우드 저장소 기반 메모리 장치가 호스트 장치에서 제거되는 순간 모든 파일 정보, 인증 정보가 삭제되는 구조인 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치.

청구항 6

제 1 항에 있어서, 클라우드 저장소 기반 메모리 장치는,

스마트 기기와 독립적으로 WiFi에 접속하거나 스마트 기기가 제공하는 테더링을 이용하여 인터넷에 접근할 수 있고,

인터넷 접속이 가능하지 않은 호스트 장치에 클라우드 저장소 기반 메모리 장치를 접속하여도 클라우드 스토리지의 데이터 파일을 이용 가능한 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치.

청구항 7

제 1 항에 있어서, 클라우드 저장소 기반 메모리 장치는,

클라우드 저장소 기반 메모리 장치와 클라우드 스토리지와의 인터페이스를 지원하는 클라우드 드라이브 인터페이스부와,

클라우드 저장소 기반 메모리 장치와 호스트 장치의 인터페이스를 지원하는 USB 인터페이스부와,

클라우드 저장소 기반 메모리 장치가 호스트 장치에서 제거되면 모든 정보가 삭제되는 제 1 인증 및 데이터 처리부와,

제 1 인증 및 데이터 처리부의 정보를 카피하고, 보안 단계 개별 유지를 지원하는 제 2 인증 및 데이터 처리부를 포함하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치.

청구항 8

보호 대상인 파일 및 클라우드 인증 정보를 저장하지 않는 클라우드 저장소 기반 메모리 장치가 호스트 장치에 물리적으로 연결되면 스마트 기기로 연결을 알리고, 파일 시스템 체크에 의해 상기 스마트 기기로 인증 요청을 하고, 상기 클라우드 저장소 기반 메모리 장치가 클라우드 스토리지로의 보안 인증 절차를 수행할 수 있도록 상기 스마트 기기가 인증 데이터를 상기 클라우드 저장소 기반 메모리 장치에 송신하는 클라우드 드라이브 인터페이스부;

상기 클라우드 저장소 기반 메모리 장치와 상기 호스트 장치의 인터페이스를 지원하는 USB 인터페이스부;

클라우드 인증 절차 및 메타데이터의 송수신 처리를 하고, 읽기 쓰기 동작시의 가상 FAT 구성, 블록 캐슁, 파일 캐슁을 지원하고, 상기 클라우드 저장소 기반 메모리 장치가 상기 호스트 장치에서 제거되면 모든 정보가 삭제되는 제 1 인증 및 데이터 처리부;

상기 제 1 인증 및 데이터 처리부의 정보를 카피하여, 사용자의 보안 단계 설정에 따라, 낮은 보안 단계에서의 성능 향상을 지원하는 제 2 인증 및 데이터 처리부를 포함하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치.

청구항 9

(S1)보호 대상인 파일 및 클라우드 인증 정보를 저장하지 않는 클라우드 저장소 기반 메모리 장치가 호스트 장치에 접속되면, (S2)이를 스마트 기기에 알리는 단계;

(S3)상기 호스트 장치가 파일 시스템 체크를 하는 단계;

(S4)상기 클라우드 저장소 기반 메모리 장치에서 상기 스마트 기기로 보안 인증 요청을 하면, (S5)상기 스마트 기기에서 보안 단계 설정을 하고, 인증 데이터(ID/PWD)를 클라우드 저장소 기반 메모리 장치로 제공하는 단계;

(S6)인증 데이터(ID/PWD)를 받은 클라우드 저장소 기반 메모리 장치에서 클라우드 스토리지로 인증을 시도하는 단계;

(S7)상기 클라우드 스토리지에서의 보안 인증이 완료되면, (S8)상기 클라우드 저장소 기반 메모리 장치에서 상기 호스트 장치로 파일 시스템 확인 정보를 전송하는 단계;

(S9)상기 클라우드 저장소 기반 메모리 장치가 상기 클라우드 스토리지로 메타데이터 참조 요청을 하고, (S10)최상위 메타데이터를 받아 (S11)초기 가상 FAT를 구성하는 단계를 포함하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법.

청구항 10

제 9 항에 있어서, 메타데이터(Meta Data)는 FAT(File Allocation Table)를 포함하는 파일 관리 정보인 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법.

청구항 11

제 9 항에 있어서, (S1) ~ (S11)의 인증 절차는 클라우드 저장소 기반 메모리 장치가 호스트 장치에 물리적으로 연결될 때마다 수행하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법.

청구항 12

제 9 항에 있어서, 스마트 기기를 통하여 (S1) ~ (S11)의 인증 절차가 이루어진 사용자만 클라우드 스토리지에 접근이 가능하고, 스마트 기기를 통하여 원하는 수준의 보안 레벨 설정을 하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법.

청구항 13

제 12 항에 있어서, 보안 레벨은,

암호화된 클라우드 ID 및 PWD, 암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 자동 로그인을 지원하는 0 단계와,

암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 인증정보의 유효기간동안 자동 로그인을 지원하는 1 단계와,

메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 File 및 Meta Data 암호화가 이루지는 2 단계와,

메타데이터, 읽기 쓰기 파일 데이터의 Block 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 File,Block 및 Meta Data 암호화가 이루어지는 3 단계와,

읽기 쓰기 파일 데이터의 Block 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 Block Data 암호화가 이루어지는 4 단계와,

클라우드 저장소 기반 메모리 장치에 아무 정보도 남지 않는 5 단계로 설정하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법.

청구항 14

제 9 항에 있어서, (S1) ~ (S11)의 인증 절차가 이루어지면 클라우드 스토리지의 데이터를 읽기 위하여,

(R1)호스트 장치에서 리드 액세스를 하여 클라우드 저장소 기반 메모리 장치로 파일 데이터 참조 요청을 하는 단계;

(R2)클라우드 저장소 기반 메모리 장치에서 클라우드 스토리지로 파일 데이터 참조 요청을 하고, (R3)가상 FAT를 구성하는 단계;

(R4)클라우드 스토리지가 블록 스트림으로 파일 데이터를 클라우드 저장소 기반 메모리 장치로 전송하는 단계;

(R5)클라우드 저장소 기반 메모리 장치가 블록 캐쉉을 하고, (R6)파일 데이터를 호스트 장치로 제공하고, (R7)클라우드 저장소 기반 메모리 장치에서 파일 캐쉉을 하는 단계;를 수행하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법.

청구항 15

제 9 항에 있어서, (S1) ~ (S11)의 인증 절차가 이루어지면 클라우드 스토리지의 데이터를 쓰기 위하여,

(W1)호스트 장치에서 라이트 액세스를 하여 클라우드 저장소 기반 메모리 장치로 파일 목록 생성을 요청하는 단계;

(W2)클라우드 저장소 기반 메모리 장치가 가상 FAT 구성을 하는 단계;

(W3)가상 FAT 구성을 하면, 호스트 장치가 파일 데이터 기록을 하고, (W4)클라우드 저장소 기반 메모리 장치가 블록 캐싱을 하는 단계;

(W5)호스트 장치가 FAT 데이터 기록을 하고, (W6)클라우드 저장소 기반 메모리 장치가 클라우드 스토리지에 블록 데이터 쓰기를 하는 단계;

(W7)호스트 장치가 파일 쓰기 종료를 요청하면, (W8)클라우드 저장소 기반 메모리 장치가 파일 캐싱을 하고, (W9)클라우드 스토리지에 파일 데이터 쓰기를 하는 단계;를 포함하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법.

청구항 16

제 15 항에 있어서, 호스트 장치가 파일 데이터 기록을 하고(W3), 클라우드 저장소 기반 메모리 장치가 블록 캐싱을 하는 과정(W4)을 반복하면서,

클라우드 저장소 기반 메모리 장치의 공간이 부족하면 클라우드 스토리지에 중간 저장을 하고, 이후에 클라우드 저장소 기반 메모리 장치가 파일 캐싱을 하는 단계(W8)에서 조립을 하는 것을 특징으로 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 메모리 장치에 관한 것으로, 구체적으로 호스트 시스템에서의 로그인 과정 없이 클라우드 스토리지의 파일을 이용할 수 있고, 보호 대상인 파일 및 클라우드 인증 정보를 물리적 저장 장치에 저장하지 않는 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 USB(Universal Serial Bus)는 복잡한 PC 및 주변기기 설치 작업을 플러그 하나 꽂는 수준으로 단순화시킨 PC 주변기기 포트 규격을 말한다.

[0003] USB 메모리는 상기 USB에 연결시켜 사용하는 저장장치를 말하는데, USB 메모리는 초기의 높은 가격과 용량의 문제를 해결하고 지금은 누구나 손쉽게 사용하고 있다.

[0004] USB 메모리는 가격적인 측면에서 기타 다른 하드웨어 기기들에 비하여 저렴하며, 메모리 사용에 있어서 Password 기능을 추가해서 개인의 자료를 보호할 수 있는 기능이 있어 대중적으로 확대되고 있는 추세이다.

[0005] 특히, USB 메모리에 보호 받을 수 있는 개인 자료의 저장은 매우 일반화 되어 있고, 생활의 일부가 되어 있는 인터넷 금융 거래시 매우 높은 활용도를 나타내고 있다.

[0006] 그리고 클라우드 컴퓨팅은 개별적으로 존재하는 다수의 컴퓨팅 자원(resource)을 하나의 영역, 예를 들어, 컴퓨팅 기능이 있는 인터넷 환경인 클라우드 영역으로 옮겨두고, 언제, 어디서나, 인터넷에 접근해 필요한 만큼 컴퓨팅 자원을 사용하고 과금하는 서비스 형태의 분산 컴퓨팅 환경의 일종이다.

[0007] 클라우드 서버는 다수의 물리적 또는 논리적 서버가 네트워크를 통해 서로 연결되어 컴퓨팅 자원을 제공하므로 컴퓨터, 휴대 단말 등의 정보기기가 갖는 자원의 한계를 극복할 수 있다.

[0008] 클라우드 서버에 접속된 컴퓨터, 휴대단말 등의 정보기기는 사용자와의 인터랙션 또는 결과 출력만을 담당하고 실제 정보 처리 기능이나 대용량의 데이터 저장 기능은 클라우드 서버의 자원을 이용함으로써, 정보기기가 보유하고 있는 자원의 한계를 극복할 수 있다.

[0009] 그러나 클라우드 영역의 자원을 활용한다고 하더라도 정보기기 자체의 입출력부의 제약으로 인해 멀티미디어를 감상하거나 혹은 문서를 읽는데 한계가 있다.

[0010] 이에, 클라우드 서버에 저장된 데이터를 휴대 단말 혹은 PC에 다운로드 받은 다음, 다시, 메모리스틱 혹은 CD 등의 이동식 저장매체에 저장하여 해당 데이터를 최적의 상태로 처리할 수 있는 외부 장치를 이용하게 된다.

[0011] 최근에는 USB(Universal Serial Bus) 장치를 통해 회사의 기밀정보를 유출하는 사례가 많이 늘고 있으며, 클라우드 컴퓨팅 환경도 예외는 아니다.

[0012] 따라서, 클라우드 컴퓨팅 환경에서 인가되지 않은 USB(Universal Serial Bus) 장치를 통해 클라우드 어플리케이션 환경에 접근하여 중요 정보를 유출하는 것에 대해서 통제 방안이 필요하다.

[0013] 특히, 종래 기술의 비휘발성물리적 를 갖는 USB는 높은 호환성을 갖고 있으나, 분실 및 도난시에 물리적 매체에 접근할 수 있는 가능성 때문에 보안 위협이 존재하고, USB 자체만으로는 클라우드 스토리지에 있는 파일에의 접근이 불가능한 문제가 있다.

[0014] 클라우드 스토리지의 경우에는 네트워크 접속이 가능한 환경에서 편리하게 사용할 수 있으나, 로그인을 사용 호스트에서 수행함으로써, 공용 컴퓨터나 타인의 컴퓨터에 로그인 흔적이 남아 보안 위협이 존재하며 컴퓨터 및 스마트폰 등, 전용 응용프로그램이 있거나 브라우져가 있는 호스트 장치에서만 사용이 가능한 문제가 있다.

선행기술문헌

특허문헌

[0015] (특허문헌 0001) 대한민국 공개특허 제10-2014-0129714호

(특허문헌 0002) 대한민국 등록특허 제10-1758733호

(특허문헌 0003) 대한민국 공개특허 제10-2014-0066919호

발명의 내용

해결하려는 과제

[0016] 본 발명은 이와 같은 종래 기술의 클라우드 컴퓨팅 및 휴대용 메모리 장치의 문제를 해결하기 위한 것으로, 호스트 시스템에서의 로그인 과정 없이 클라우드 스토리지의 파일을 이용할 수 있고, 보호 대상인 파일 및 클라우드 인증 정보를 물리적 저장 장치에 저장하지 않는 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법을 제공하는데 그 목적이 있다.

[0017] 본 발명은 스마트폰의 인증을 통하여 본인만 클라우드 스토리지에 접근이 가능하고, 원하는 수준의 보안 레벨을 설정이 가능하도록 한 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법을 제공하는데 그 목적이 있다.

[0018] 본 발명은 사용자 파일 데이터를 가지고 있지 않는 USB 메모리 스틱 형태를 갖고 컴퓨터나 TV 등의 호스트 장치에 연결되어 클라우드 스토리지의 파일을 USB 메모리 스틱에 있는 파일처럼 볼 수 있게 하는 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법을 제공하는데 그 목적이 있다.

[0019] 본 발명은 USB가 연결되는 모든 장치에서 사용 가능하고, 네트워크 환경에서 편리하게 접근 및 공유가 가능하도록 하여 클라우드 스토리지를 USB 메모리처럼 접근하여 사용할 수 있도록 한 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법을 제공하는데 그 목적이 있다.

[0020] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0021] 이와 같은 목적을 달성하기 위한 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치는 사용 호스트 시스템에서의 로그인 과정없이 클라우드 스토리지의 파일을 이용할 수 있도록 하는 클라우드 저장소 기반 메모리 장치;클라우드 저장소 기반 메모리 장치가 접속되는 호스트 장치들;데이터 파일들을 저장하는 클라우드 스토리지;클라우드 저장소 기반 메모리 장치가 호스트 장치에 물리적으로 접속되면 보안 인증 절차를 수행하는 스마트 기기;를 포함하는 것을 특징으로 한다.

[0022] 여기서, 클라우드 저장소 기반 메모리 장치는, 보호 대상인 파일 및 클라우드 인증 정보를 물리적 저장 장치에 저장하지 않는 것을 특징으로 한다.

[0023] 그리고 스마트 기기의 인증을 통하여 인증된 사용자만 클라우드 스토리지에 접근이 가능하고, 스마트 기기를 통하여 원하는 수준의 보안 레벨을 설정하는 것을 특징으로 한다.

[0024] 그리고 보안 레벨은, 암호화된 클라우드 ID 및 PWD, 암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 자동 로그인을 지원하는 0 단계와,암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 인증정보의 유효기간동안 자동 로그인을 지원하는 1 단계와,메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 File 및 Meta Data 암호화가 이루지는 2 단계와,메타데이터, 읽기 쓰기 파일 데이터의 Block 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 File,Block 및 Meta Data 암호화가 이루어지는 3 단계와,읽기 쓰기 파일 데이터의 Block 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 Block Data 암호화가 이루어지는 4 단계와,클라우드 저장소 기반 메모리 장치에 아무 정보도 남지 않는 5 단계로 설정하는 것을 특징으로 한다.

[0025] 그리고 클라우드 저장소 기반 메모리 장치는, 호스트 장치가 일반 USB와 동일한 형태로 인식하고, 클라우드 저장소 기반 메모리 장치가 호스트 장치에서 제거되는 순간 모든 파일 정보, 인증 정보가 삭제되는 구조인 것을 특징으로 한다.

[0026] 그리고 클라우드 저장소 기반 메모리 장치는, 스마트 기기와 독립적으로 WiFi에 접속하거나 스마트 기기가 제공하는 테더링을 이용하여 인터넷에 접근할 수 있고, 인터넷 접속이 가능하지 않은 호스트 장치에 클라우드 저장소 기반 메모리 장치를 접속하여도 클라우드 스토리지의 데이터 파일을 이용 가능한 것을 특징으로 한다.

[0027] 그리고 클라우드 저장소 기반 메모리 장치는, 클라우드 저장소 기반 메모리 장치와 클라우드 스토리지와의 인터페이스를 지원하는 클라우드 드라이브 인터페이스부와,클라우드 저장소 기반 메모리 장치와 호스트 장치의 인터페이스를 지원하는 USB 인터페이스부와,클라우드 저장소 기반 메모리 장치가 호스트 장치에서 제거되면 모든 정보가 삭제되는 제 1 인증 및 데이터 처리부와,제 1 인증 및 데이터 처리부의 정보를 카피하여, 사용자의 보안 단계 설정에 따라, 낮은 보안 단계에서의 성능 향상을 지원하는 제 2 인증 및 데이터 처리부를 포함하는 것을 특징으로 한다.

[0028] 다른 목적을 달성하기 위한 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치는 클라우드 저장소 기반 메모리 장치가 호스트 장치에 물리적으로 연결되면 스마트 기기로 연결을 알리고, 파일 시스템 체크에 의해 스마트 기기로 인증 요청을 하고 클라우드 인증 절차 및 메타데이터의 송수신을 하는 클라우드 드라이브 인터페이스부;클라우드 저장소 기반 메모리 장치와 호스트 장치의 인터페이스를 지원하는 USB 인터페이스부;클라우드 인증 절차 및 메타데이터의 송수신 처리를 하고, 읽기 쓰기 동작시의 가상 FAT 구성, 블록 캐싱, 파일 캐싱을 지원하고, 클라우드 저장소 기반 메모리 장치가 호스트 장치에서 제거되면 모든 정보가 삭제되는 제 1 인증 및 데이터 처리부;제 1 인증 및 데이터 처리부의 정보를 카피하고, 보안 단계 개별 유지를 지원하는 제 2 인증 및 데이터 처리부;를 포함하는 것을 특징으로 한다.

[0029] 다른 목적을 달성하기 위한 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법은 (S1)클라우드 저장소 기반 메모리 장치가 호스트 장치에 접속되면, (S2)이를 스마트 기기에 알리는 단계;(S3)호스트 장치가 파일 시스템 체크를 하는 단계;(S4)클라우드 저장소 기반 메모리 장치에서 스마트 기기로 인증 요청을 하면, (S5)스마트 기기에서 보안 단계 설정을 하고, 인증 데이터(ID/PWD)를 클라우드 저장소 기반 메모리 장치로 제공하는 단계;(S6)인증 데이터(ID/PWD)를 받은 클라우드 저장소 기반 메모리 장치에서 클라우드 스토리지로 인증을 시도하는 단계;(S7)클라우드 스토리지에서의 인증이 완료되면, (S8)클라우드 저장소 기반 메모리 장치에서 호스트 장치로 파일 시스템 확인 정보를 전송하는 단계;(S9)클라우드 저장소 기반 메모리 장치가 클라우드 스토리지로 메타데이터 참조 요청을 하고, (S10)최상위 메타데이터를 받아 (S11)초기 가상 FAT를 구성하는 단계;를 포함하는 것을 특징으로 한다.

[0030] 여기서, 메타데이터(Meta Data)는 FAT(File Allocation Table)를 포함하는 파일 관리 정보인 것을 특징으로 한다.

[0031] 그리고 (S1) ~ (S11)의 인증 절차는 클라우드 저장소 기반 메모리 장치가 호스트 장치에 물리적으로 연결될 때마다 수행하는 것을 특징으로 한다.

[0032] 그리고 스마트 기기를 통하여 (S1) ~ (S11)의 인증 절차가 이루어진 사용자만 클라우드 스토리지에 접근이 가능하고, 스마트 기기를 통하여 원하는 수준의 보안 레벨 설정을 하는 것을 특징으로 한다.

[0033] 그리고 보안 레벨은, 암호화된 클라우드 ID 및 PWD, 암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 자동 로그인을 지원하는 0 단계와,암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 인증정보의 유효기간동안 자동 로그인을 지원하는 1 단계와,메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 File 및 Meta Data 암호화가 이루지는 2 단계와,메타데이터, 읽기 쓰기 파일 데이터의 Block 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 File,Block 및 Meta Data 암호화가 이루어지는 3 단계와,읽기 쓰기 파일 데이터의 Block 캐쉬가 클라우드 저장소 기반 메모리 장치에 저장되고 Block Data 암호화가 이루어지는 4 단계와,클라우드 저장소 기반 메모리 장치에 아무 정보도 남지 않는 5 단계로 설정하는 것을 특징으로 한다.

[0034] 그리고 (S1) ~ (S11)의 인증 절차가 이루어지면 클라우드 스토리지의 데이터를 읽기 위하여, (R1)호스트 장치에서 리드 액세스를 하여 클라우드 저장소 기반 메모리 장치로 파일 데이터 참조 요청을 하는 단계;(R2)클라우드 저장소 기반 메모리 장치에서 클라우드 스토리지로 파일 데이터 참조 요청을 하고, (R3)가상 FAT를 구성하는 단계;(R4)클라우드 스토리지가 블록 스트림으로 파일 데이터를 클라우드 저장소 기반 메모리 장치로 전송하는 단계;(R5)클라우드 저장소 기반 메모리 장치가 블록 캐쉉을 하고, (R6)파일 데이터를 호스트 장치로 제공하고, (R7)클라우드 저장소 기반 메모리 장치에서 파일 캐쉉을 하는 단계;를 수행하는 것을 특징으로 한다.

[0035] 그리고 (S1) ~ (S11)의 인증 절차가 이루어지면 클라우드 스토리지의 데이터를 쓰기 위하여, (W1)호스트 장치에서 라이트 액세스를 하여 클라우드 저장소 기반 메모리 장치로 파일 목록 생성을 요청하는 단계;(W2)클라우드 저장소 기반 메모리 장치가 가상 FAT 구성을 하는 단계;(W3)가상 FAT 구성을 하면, 호스트 장치가 파일 데이터 기록을 하고, (W4)클라우드 저장소 기반 메모리 장치가 블록 캐쉉을 하는 단계;(W5)호스트 장치가 FAT 데이터 기록을 하고, (W6)클라우드 저장소 기반 메모리 장치가 클라우드 스토리지에 블록 데이터 쓰기를 하는 단계;(W7)호스트 장치가 파일 쓰기 종료를 요청하면, (W8)클라우드 저장소 기반 메모리 장치가 파일 캐쉉을 하고, (W9)클라우드 스토리지에 파일 데이터 쓰기를 하는 단계;를 포함하는 것을 특징으로 한다.

[0036] 그리고 호스트 장치가 파일 데이터 기록을 하고(W3), 클라우드 저장소 기반 메모리 장치가 블록 캐쉉을 하는 과정(W4)을 반복하면서, 클라우드 저장소 기반 메모리 장치의 공간이 부족하면 클라우드 스토리지에 중간 저장을 하고, 이후에 클라우드 저장소 기반 메모리 장치가 파일 캐쉉을 하는 단계(W8)에서 조립을 하는 것을 특징으로 한다.

발명의 효과

[0037] 이와 같은 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법은 다음과 같은 효과를 갖는다.

[0038] 첫째, 호스트 시스템에서의 로그인 과정 없이 클라우드 스토리지의 파일을 이용할 수 있다.

[0039] 둘째, 보호 대상인 파일 및 클라우드 인증 정보를 물리적 저장 장치에 저장하지 않아 안전성을 높일 수 있다.

[0040] 셋째, 스마트폰의 인증을 통하여 본인만 클라우드 스토리지에 접근이 가능하고, 원하는 수준의 보안 레벨을 설정이 가능하도록 보안성을 높이고, 효율적인 시스템 설계가 가능하도록 한다.

[0041] 넷째, 사용자 파일 데이터를 가지고 있지 않는 USB 메모리 스틱 형태를 갖고 컴퓨터나 TV 등의 호스트 장치에 연결되어 클라우드 스토리지의 파일을 USB 메모리 스틱에 있는 파일처럼 볼 수 있게 하여 편리성을 높일 수 있다.

[0042] 다섯째, USB가 연결되는 모든 장치에서 사용 가능하고, 네트워크 환경에서 편리하게 접근 및 공유가 가능하도록 하여 클라우드 스토리지를 USB 메모리처럼 접근하여 사용할 수 있도록 하여 보안성 및 편리성을 높일 수 있다.

도면의 간단한 설명

[0043] 도 1은 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 전체 시스템 구성도

도 2는 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 상세 구성도

도 3은 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법을 나타낸 동작 제어 흐름도

도 4는 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 데이터 입출력 과정을 나타낸 제어

흐름도

발명을 실시하기 위한 구체적인 내용

[0044] 이하, 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법의 바람직한 실시 예에 관하여 상세히 설명하면 다음과 같다.

[0045] 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법의 특징 및 이점들은 이하에서의 각 실시 예에 대한 상세한 설명을 통해 명백해질 것이다.

[0046] 도 1은 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 전체 시스템 구성도이고, 도 2는 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 상세 구성도이다.

[0047] 본 발명은 사용 호스트 시스템에서의 로그인 과정없이 클라우드 스토리지의 파일을 이용할 수 있도록 한 것으로, 파일 저장을 위한 비휘발성 물리적 공간을 갖지 않고 스마트폰과 독립적으로 WiFi에 접속을 하거나 스마트폰이 제공하는 테더링을 이용하여 인터넷에 접근할 수 있도록 하는 것이다.

[0048] 이와 같은 동작에서 모든 인증 과정은 스마트폰을 통하여 이루어지고, USB 장치의 제거시에 파일 정보 및 인증 정보를 삭제하는 구성을 포함한다.

[0049] 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 전체 시스템은 도 1 및 도 2에서와 같이, 사용 호스트 시스템에서의 로그인 과정없이 클라우드 스토리지의 파일을 이용할 수 있도록 하는 클라우드 저장소 기반 메모리 장치(200)와, 클라우드 저장소 기반 메모리 장치(200)가 접속되는 호스트 장치(300)들과, 데이터 파일들을 저장하는 클라우드 스토리지(100)와, 클라우드 저장소 기반 메모리 장치(200)가 호스트 장치(300)에 물리적으로 접속되면 보안 인증 절차를 수행하는 스마트 기기(400)를 포함한다.

[0050] 여기서, 클라우드 저장소 기반 메모리 장치(200)는 호스트 장치(300)에서의 로그인 과정 없이 클라우드 스토리지(100)의 파일을 이용할 수 있고, 보호 대상인 파일 및 클라우드 인증 정보를 비휘발성 물리적 저장 장치에 저장하지 않는다.

[0051] 또한, 스마트 기기(400)의 인증을 통하여 인증된 사용자만 클라우드 스토리지(100)에 접근이 가능하고, 스마트 기기(400)를 통하여 원하는 수준의 보안 레벨을 설정한다.

[0052] 이와 같은 본 발명에 따른 클라우드 저장소 기반 메모리 장치(200)는 호스트 장치(300)(운영체제와 상관없이 컴퓨터 , TV , 산업 기기 등) 입장에서 일반 USB와 동일한 형태로 인식한다.

[0053] 클라우드 저장소 기반 메모리 장치(200)는 호스트 장치(300)에서 제거되는 순간 모든 파일 정보, 인증 정보가 삭제되는 구조이다.

[0054] 클라우드 저장소 기반 메모리 장치(200)를 통하여 클라우드 스토리지(100)의 데이터 파일을 이용하기 위한 모든 인증 과정은 스마트 기기(400)에서 이루어지고, 클라우드 저장소 기반 메모리 장치(200)는 스마트 기기(400)와 독립적으로 WiFi에 접속하거나 스마트 기기(400)가 제공하는 테더링을 이용하여 인터넷에 접근할 수 있어 호스트 장치(300)가 인터넷 접속이 가능하지 않은 장치여도 클라우드 저장소 기반 메모리 장치(200)를 통하여 클라우드 스토리지(100)의 데이터 파일을 이용할 수 있다.

[0055] 본 발명에 따른 클라우드 저장소 기반 메모리 장치(200)의 상세 구성을 설명하면 다음과 같다.

[0056] 도 2에서와 같이, 클라우드 저장소 기반 메모리 장치(200)가 호스트 장치(300)에 물리적으로 연결되면 스마트 기기(400)로 연결을 알리고 파일 시스템 체크에 의해 스마트 기기(400)로 인증 요청을 하고 클라우드 인증 절차 및 메타데이터의 송수신을 하는 클라우드 드라이브 인터페이스부(10)와, 클라우드 저장소 기반 메모리 장치(200)와 호스트 장치(300)의 인터페이스를 지원하는 USB 인터페이스부(40)와, 클라우드 인증 절차 및 메타데이터의 송수신 처리를 하고, 읽기 쓰기 동작시의 가상 FAT 구성, 블록 캐싱, 파일 캐싱을 지원하고, 클라우드 저장소 기반 메모리 장치(200)가 호스트 장치(300)에서 제거되면 모든 정보가 삭제되는 제 1 인증 및 데이터 처리부(20)와, 제 1 인증 및 데이터 처리부(20)의 정보를 카피하고, 사용자가 낮은 수준의 보안 단계를 필요로 하는 경우, 성능 향상을 위한 저장소를 지원하는 제 2 인증 및 데이터 처리부(30)를 포함한다.

[0057] 이와 같은 구성을 포함하는 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치는,

[0058] 첫째, 호스트 장치에서의 로그인 과정없이 클라우드 스토리지의 파일을 이용할 수 있도록 하고,

[0059] 둘째, 스마트 기기와 독립적으로 WiFi 접속을 하거나 스마트 기기가 제공하는 테더링을 이용하여 인터넷에 접근할 수 있고,

[0060] 셋째, 스마트 기기를 이용하여 인증 과정이 진행되고,

[0061] 넷째, 클라우드 저장소 기반 메모리 장치의 제거시에 파일 정보 및 인증 정보가 삭제되는 특징을 갖는다.

[0062] 따라서, 이와 같은 구성을 포함하는 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치는 보안이 매우 중요한 파일을 어느 컴퓨터에서든 사용자의 흔적 없이 접근 가능하여 다른 사람의 컴퓨터,호텔이나 공공장소, PC방 등에서 클라우드 스토리지에 존재하는 보안이 필요한 파일, 콘텐츠 접근시에 유용하게 사용될 수 있다.

[0063] 또한, 메모리 장치를 분실한 경우에도 물리적인 저장 공간을 가지지 않음으로써, 사용자의 파일 내용이 유출될 가능성이 없다.

[0064] 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법을 구체적으로 설명하면 다음과 같다.

[0065] 도 3은 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 인증 제어 방법을 나타낸 동작 제어 흐름도이다.

[0066] 호스트 장치에서의 로그인 과정없이 클라우드 스토리지의 파일을 이용할 수 있도록 하기 위하여 다음과 같은 인증 절차를 진행한다.

[0067] 먼저, 클라우드 저장소 기반 메모리 장치(200)가 호스트 장치(300)에 접속되면(S1), 클라우드 저장소 기반 메모리 장치(200)의 제 1 인증 및 데이터 처리부(20)가 클라우드 드라이브 인터페이스부(10)를 통하여 스마트 기기(400)로 클라우드 저장소 기반 메모리 장치(200)가 연결되었음을 알린다(S2).

[0068] 그리고 호스트 장치(300)가 클라우드 저장소 기반 메모리 장치(200)의 첫 번째 블록을 Read하여 파일 시스템 체크를 한다(S3).

[0069] 이어, 클라우드 저장소 기반 메모리 장치(200)가 스마트 기기(400)로 인증 요청을 한다(S4).

[0070] 그리고 스마트 기기(400)를 통하여 보안 단계 설정을 하고, 스마트 기기(400)가 인증 데이터(ID/PWD)를 클라우드 저장소 기반 메모리 장치(200)로 제공한다.(S5)

[0071] 인증 데이터(ID/PWD)를 받은 클라우드 저장소 기반 메모리 장치(200)가 클라우드 스토리지(100)로 인증을 시도한다(S6).

[0072] 클라우드 스토리지(100)에서의 인증이 완료되면(S7), 클라우드 저장소 기반 메모리 장치(200)가 호스트 장치(300)로 파일 시스템 확인 정보를 전송한다(S8).

[0073] 그리고 클라우드 저장소 기반 메모리 장치(200)가 클라우드 스토리지(100)로 메타데이터 참조 요청을 하고(S9), 최상위 메타데이터를 받아(S10) 초기 가상 FAT를 구성한다(S11).

[0074] 메타데이터(Meta Data)는 FAT(File Allocation Table) 등 파일 관리 정보이다.

[0075] 이와 같은 인증 절차는 클라우드 저장소 기반 메모리 장치(200)가 호스트 장치(300)에 물리적으로 연결될 때마다 수행한다.

[0076] 그리고 스마트 기기(400)를 통하여 보안 단계를 설정하는 과정을 구체적으로 설명하면 다음과 같다.

표 1

[0077]

보안 단계	(암호화된) cloud ID	(암호화된) cloud PWD	(암호화된) 인증정보	Meta Data	Read File Data	Write File Data	
0단계	○	○	○	○	File 캐쉬	File 캐쉬	자동로그인
1단계	×	×	○	○	File 캐쉬	File 캐쉬	자동로그인 (인증정보 유효기간동안)

2단계	×	×	×	○	File 캐쉬	File 캐쉬	File 및 Meta Data 암호화
3단계	×	×	×	○	Block 캐쉬	Block 캐쉬	File,Block 및 Meta Data 암호화
4단계	×	×	×	×	Block 캐쉬	Block 캐쉬	Block Data 암호화
5단계	×	×	×	×	×	×	USB의 비휘발성 메모리에 아무 정보도 남지않음

[0078] 이와 같은 인증 단계별 설정 정보는 사용자의 보안 단계 설정에 따라 제 2 인증 및 데이터 처리부(30)에 저장될 수 있다.

[0079] 제 2 인증 및 데이터 처리부(30)에 저장되지 않는 정보는 클라우드 저장소 기반 메모리 장치(200)가 호스트 장치(300)에서 제거되면 모든 정보가 삭제되는 제 1 인증 및 데이터 처리부(20)에 저장된다.

[0080] 표 1에서는 0 단계 ~ 5 단계로 보안 레벨이 설정되는 것으로 설명하였으나, 이로 제한되지 않는다.

[0081] 일 예로, 0 단계에서 제 2 인증 및 데이터 처리부(30)에 저장되는 내역은 암호화된 클라우드 ID 및 PWD, 암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬이고, 자동 로그인을 지원한다.

[0082] 그리고 1 단계에서는 암호화된 인증 정보, 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬이고, 인증정보의 유효기간동안 자동 로그인을 지원한다.

[0083] 그리고 2 단계에서는 메타데이터, 읽기 쓰기 파일 데이터의 File 캐쉬이고, File 및 Meta Data 암호화가 이루어진다.

[0084] 그리고 3 단계에서는 메타데이터, 읽기 쓰기 파일 데이터의 Block 캐쉬이고, File,Block 및 Meta Data 암호화가 이루어진다.

[0085] 그리고 4 단계에서는 읽기 쓰기 파일 데이터의 Block 캐쉬이고, Block Data 암호화가 이루어진다.

[0086] 그리고 5 단계에서는 클라우드 저장소 기반 메모리 장치(200)의 제 2 인증 및 데이터 처리부(30)에 아무 정보도 남지 않는다.

[0087] 모든 단계에서 파일 캐쉬는 해당 파일의 전체 데이터 블록에 대한 캐쉬를 한다는 의미이다.

[0088] 이와 같이 본 발명의 일 예에 따른 보안 레벨 설정은 0, 1 단계에도 ID/PWD/인증정보는 모두 암호화되는 것이다.

[0089] 그리고 인증 정보는 클라우드 스토리지 서비스 사업자가 로그인 없이 접근할 수 있도록 보내준 해쉬이고, 파일, 블록, 캐쉬는 클라우드 스토리지의 정보를 로컬에 복사한다.

[0090] 1,2 단계에서는 성능 향상을 위하여 File, Meta Data 암호화를 하지 않는다.

[0091] 그리고 2 단계 이후에는 제 2 인증 및 데이터 처리부(30)에 저장되는 데이터는 모두 암호화한다.

[0092] 이와 같이 보안 레벨을 설정하는 것에 의해 4 단계 이후에는 클라우드 저장소 기반 메모리 장치(200)의 해킹 이후에도 암호화된 조각 데이터만 접근가능하여 거의 완벽한 보안이 유지될 수 있다.

[0093] 이와 같은 보안 인증 절차 이후에 진행되는 데이터 쓰기 및 읽기 과정을 설명하면 다음과 같다.

[0094] 도 4는 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치의 데이터 입출력 과정을 나타낸 제어 흐름도이다.

[0095] 먼저, 읽기 동작은, 호스트 장치(300)에서 리드 액세스를 하여 클라우드 저장소 기반 메모리 장치(200)로 파일 데이터 참조 요청을 한다.(R1)

[0096] 호스트 장치(300)로부터 파일 데이터 참조 요청을 받은 클라우드 저장소 기반 메모리 장치(200)는 클라우드 스

토리지(100)로 파일 데이터 참조 요청을 하고(R2), 가상 FAT를 구성한다.(R3)

[0097] 이어, 클라우드 스토리지(100)가 블록 스트림으로 파일 데이터를 클라우드 저장소 기반 메모리 장치(200)로 전송하면(R4), 클라우드 저장소 기반 메모리 장치(200)가 블록 캐싱을 하고(R5), 파일 데이터를 호스트 장치(300)로 제공하고(R6), 클라우드 저장소 기반 메모리 장치(200)에서 파일 캐싱을 한다.(R7)

[0098] 보안 단계 2 이하에서는 성능 향상을 위하여 (R7)에서와 같이 파일 단위로 캐싱을 한다. 블록 캐싱 및 파일 캐싱은사용자의 보안단계 설정에 따라 제 1 인증 및 데이터 처리부(20) 또는 제 2 인증 및 데이터 처리부(30)를 이용한다.

[0099] 그리고 쓰기 동작은, 호스트 장치(300)에서 라이트 액세스를 하여 클라우드 저장소 기반 메모리 장치(200)로 파일 목록 생성을 요청하면(W1), 클라우드 저장소 기반 메모리 장치(200)가 가상 FAT 구성을 한다.(W2)

[0100] 클라우드 저장소 기반 메모리 장치(200)가 가상 FAT 구성을 하면, 호스트 장치(300)가 파일 데이터 기록을 하고(W3), 클라우드 저장소 기반 메모리 장치(200)가 블록 캐싱을 한다.(W4)

[0101] 이어, 호스트 장치(300)가 FAT 데이터 기록을 하고(W5), 클라우드 저장소 기반 메모리 장치(200)가 클라우드 스토리지(100)에 블록 데이터 쓰기를 한다.(W6)

[0102] 그리고 호스트 장치(300)가 파일 쓰기 종료를 요청하면(W7), 클라우드 저장소 기반 메모리 장치(200)가 파일 캐싱을 하고(W8), 클라우드 스토리지(100)에 파일 데이터 쓰기를 한다.(W9)

[0103] 이와 같은 쓰기 동작에서 호스트 장치(300)가 파일 데이터 기록을 하고(W3), 클라우드 저장소 기반 메모리 장치(200)가 블록 캐싱을 하는 과정(W4)을 반복하면서, 클라우드 저장소 기반 메모리 장치(200)의 공간이 부족하면 클라우드 스토리지(100)에 중간 저장을 하고, 이후에 클라우드 저장소 기반 메모리 장치(200)가 파일 캐싱을 하는 단계(W8)에서 조립을 한다.

[0104] 그리고 이와 같은 쓰기 동작에서 성능 향상을 위하여 보안 단계 2이하에서는 (W8)으로 파일 단위 캐싱을 한다.

[0105] 그리고 호스트 장치(300)의 파일 시스템 운영 방식에 따라 클라우드 저장소 기반 메모리 장치(200)로 파일 목록 생성을 요청하는 단계(W1), 클라우드 저장소 기반 메모리 장치(200)가 가상 FAT 구성하는 단계(W2), 호스트 장치(300)가 파일 쓰기 종료를 요청하는 단계(W7)의 수행 방식은 달라질 수 있다.

[0106] 이상에서 설명한 본 발명에 따른 안전성을 높인 클라우드 저장소 기반 메모리 장치 및 이의 인증 제어 방법은 일반 USB 메모리와 클라우드 스토리지의 장점을 유지하고, 단점을 보완한 새로운 USB 메모리 스틱 형태의 클라우드 저장소 기반 메모리 장치로, 보호 대상인 파일 및 클라우드 인증 정보를 물리적 저장 장치에 저장하지 않고, 인증 환경 및 물리적 파일데이터, 호스트에의 접속 시스템을 분리하여 분실 또는 탈취에 따른 보안 위협이 없도록 한 것이다.

[0107] 특히, 사용 호스트 시스템에서의 로그인 과정 없이 클라우드 스토리지의 파일을 이용함으로써, 사용자 파일뿐만 아니라 클라우드 스토리지 접근을 위한 사용자 ID와 패스워드 등 인증 정보도 호스트 시스템에 남지 않도록 하고, 스마트 기기를 통한 인증 과정을 거쳐야 클라우드 스토리지에 접근 가능하도록 하여 보안성을 높인 것이다.

[0108] 이상에서의 설명과 같이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 본 발명이 구현되어 있음을 이해할 수 있을 것이다.

[0109] 그러므로 명시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 하고, 본 발명의 범위는 전술한 설명이 아니라 특허청구 범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

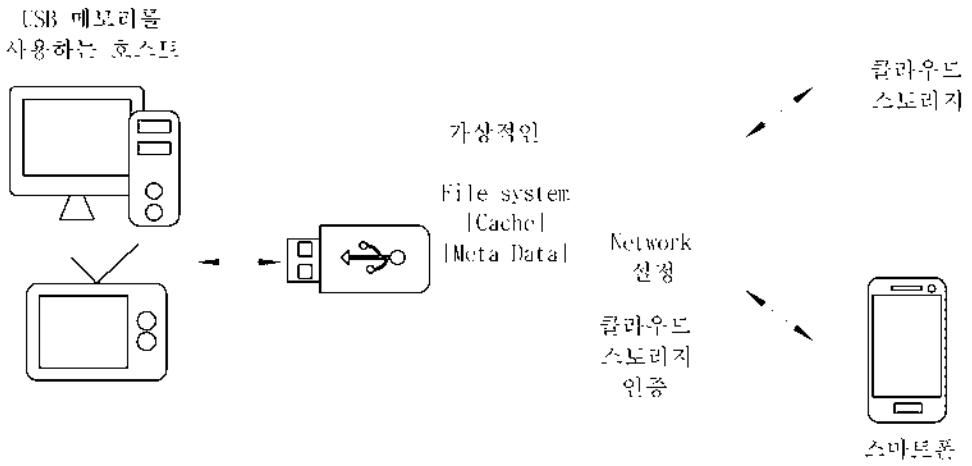
부호의 설명

[0110] 100. 클라우드 스토리지 200. 클라우드 기반 메모리 장치

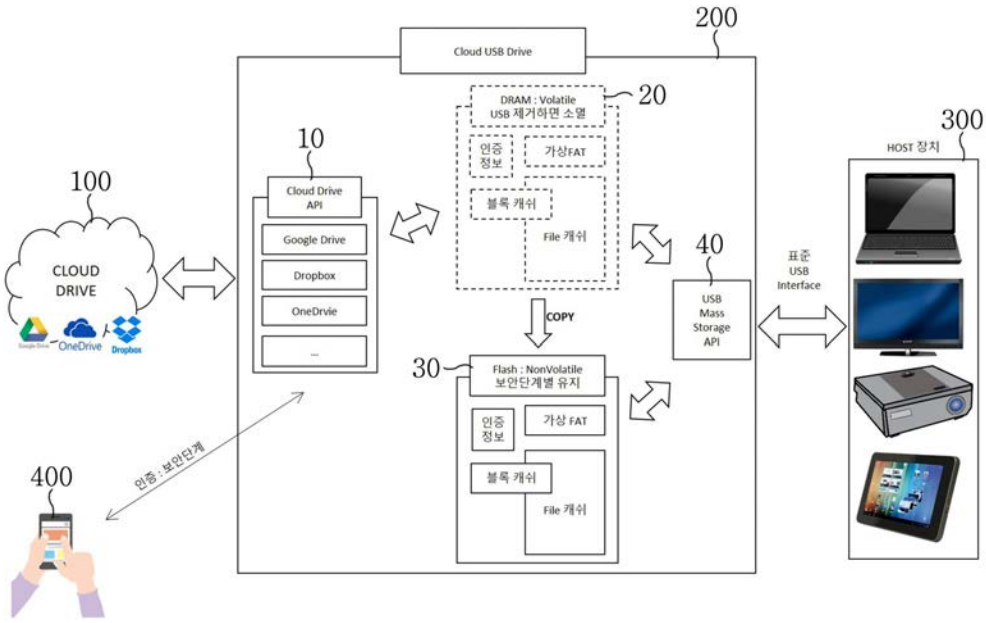
300. 호스트 장치 400. 스마트 기기

도면

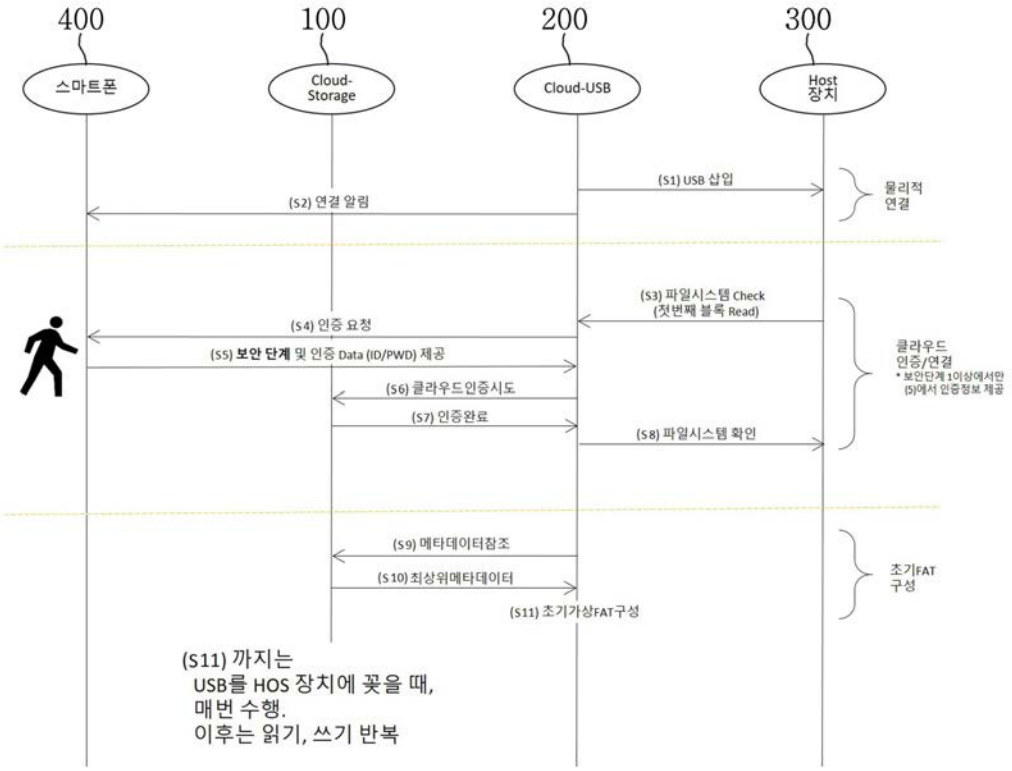
도면1


USB 메모리를
사용하는 호스트
가상적인
File system
|Cache|
|Meta Data|
Network
설정
클라우드
스토리지
클라우드
스토리지
인증
스마트폰

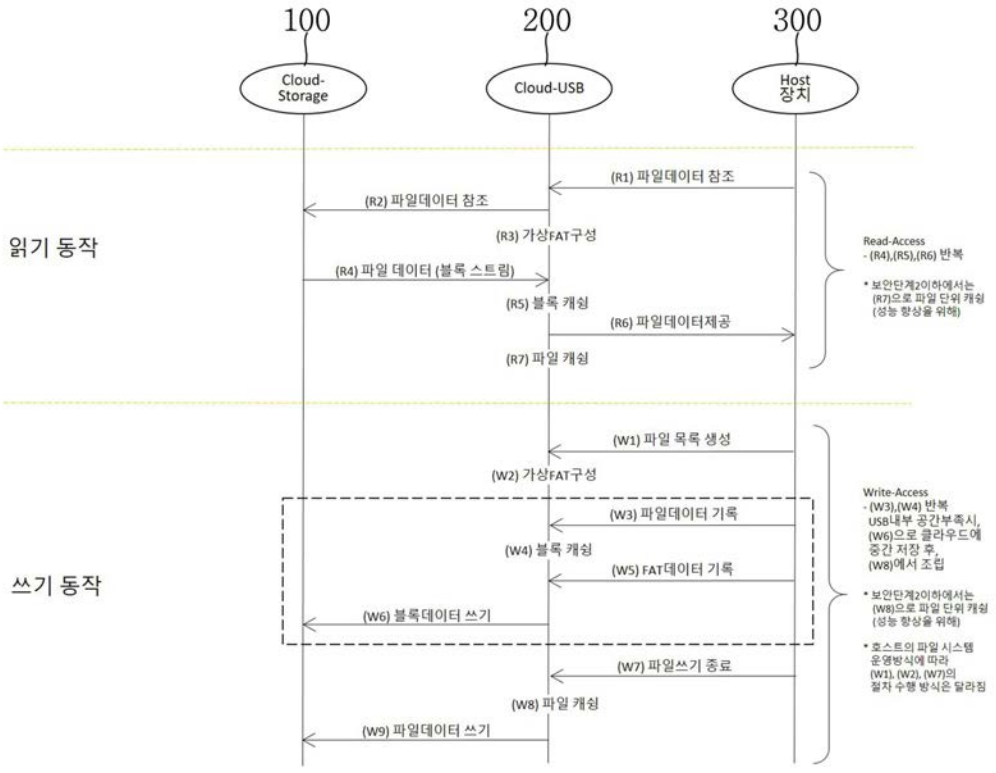
도면2


200
Cloud USB Drive
DRAM : Volatile
USB 제거하면 소멸
20
10
인증
정보
가상FAT
Cloud Drive
API
블록 캐쉬
Google Drive
File 캐쉬
Dropbox
OneDrvie
...
100
CLOUD
DRIVE
40
USB
Mass
Storage
API
COPY
30
Flash : NonVolatile
보안단계별 유지
인증
정보
가상 FAT
블록 캐쉬
File 캐쉬
400
인증 : 보안단계
표준
USB
Interface
300
HOST 장치

도면3


400
100
200
300
스마트폰
Cloud-Storage
Cloud-USB
Host 장치
(S1) USB 삽입
(S2) 연결 알림
물리적 연결
(S3) 파일시스템 Check (첫번째 블록 Read)
(S4) 인증 요청
(S5) 보안 단계 및 인증 Data (ID/PWD) 제공
(S6) 클라우드인증시도
(S7) 인증완료
(S8) 파일시스템 확인
클라우드 인증/연결
* 보안단계 1이상에서만 (5)에서 인증정보 제공
(S9) 메타데이터참조
(S10) 최상위메타데이터
(S11) 초기가상FAT구성
초기FAT 구성
(S11) 까지는
USB를 HOS 장치에 꽂을 때,
매번 수행.
이후는 읽기, 쓰기 반복

도면4


100
200
300
Cloud-Storage
Cloud-USB
Host 장치
읽기 동작
(R1) 파일데이터 참조
(R2) 파일데이터 참조
(R3) 가상FAT구성
(R4) 파일 데이터 (블록 스트림)
(R5) 블록 캐싱
(R6) 파일데이터제공
(R7) 파일 캐싱
Read-Access
- (R4),(R5),(R6) 반복
* 보안단계2이하에서는 (R7)으로 파일 단위 캐싱 (성능 향상을 위해)
쓰기 동작
(W1) 파일 목록 생성
(W2) 가상FAT구성
(W3) 파일데이터 기록
(W4) 블록 캐싱
(W5) FAT데이터 기록
(W6) 블록데이터 쓰기
(W7) 파일쓰기 종료
(W8) 파일 캐싱
(W9) 파일데이터 쓰기
Write-Access
- (W3),(W4) 반복
USB내부 공간부족시, (W6)으로 클라우드에 중간 저장 후, (W8)에서 조립
* 보안단계2이하에서는 (W8)으로 파일 단위 캐싱 (성능 향상을 위해)
* 호스트의 파일 시스템 운영방식에 따라 (W1), (W2), (W7)의 절차 수행 방식은 달라짐