(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년04월22일
(11) 등록번호 10-1971225
(24) 등록일자 2019년04월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/60* (2013.01)
H04L 29/08 (2006.01)
(52) CPC특허분류
H04L 9/3234 (2013.01)
G06F 21/606 (2013.01)
(21) 출원번호 10-2018-0120934
(22) 출원일자 2018년10월11일
심사청구일자 2018년10월11일
(56) 선행기술조사문헌
KR101719129 B1*
(뒷면에 계속)

(73) 특허권자
옥임식
경기도 고양시 일산서구 일산로 488, 1302동 301호 (일산동, 후곡마을)
구재모
세종특별자치시 누리로 54, 524동 603호 (한솔동, 첫마을아파트)
(72) 발명자
옥임식
경기도 고양시 일산서구 일산로 488, 1302동 301호 (일산동, 후곡마을)
구재모
세종특별자치시 누리로 54, 524동 603호 (한솔동, 첫마을아파트)
(74) 대리인
안재열

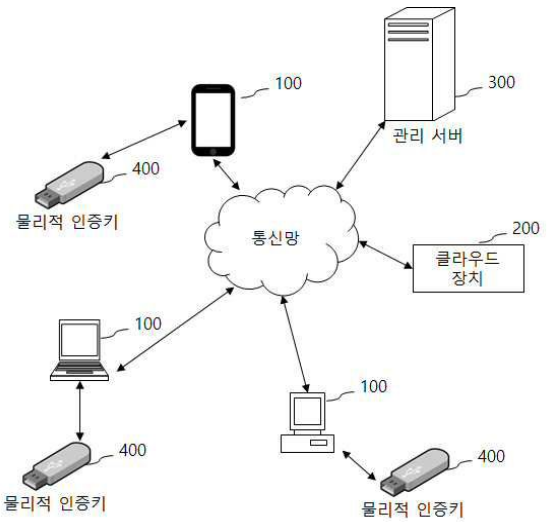
전체 청구항 수 : 총 5 항 심사관 : 양종필

(54) 발명의 명칭 **클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법**

(57) 요 약

본 발명은 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법에 관한 것으로서, 더욱 상세하게는 등록된 다수의 사용자 단말에 대하여 물리적 인증키를 이용하여 추가 인증을 수행함으로써 활성화되는 전용 업로드/다운로드 브라우저를 통해 상기 사용자 단말이 클라우드 장치에 접속하여 대용량의 파일에 대한 보안이 강화된 클라우드 서비스를 제공 받으며, 상기 물리적 인증키에 구비된 암호화 프로그램 및 보안키를 이용하여 상기 대용량의 파일의 업로드시 암호화를, 다운로드시 복호화를 수행함으로써, 그룹으로 등록된 사용자들만 상기 대용량 파일의 재생 또는 편집이 가능하도록 하기 위한, 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법을 제공한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 67/06 (2013.01)
H04L 2209/60 (2013.01)

(56) 선행기술조사문헌
KR1020170011469 A*
KR1020170109126 A*
KR101709276 B1
KR101758733 B1
KR101619286 B1
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

클라우드 서버의 데이터 전송 보안 시스템에 있어서,

전용 업로드/다운로드 브라우저의 활성상태에서 클라우드 서비스가 제공되는 다수의 사용자 단말(100);

상기 사용자 단말과 통신망을 통해 연결되며, 상기 사용자 단말로부터 클라우드 서비스에 대한 요청에 응답하여 저장공간으로 하나 이상의 데이터에 대한 탐색, 다운로드, 업로드, 삭제, 백업 및 중복제거 중, 적어도 하나를 실행하는 클라우드 장치(200);

상기 사용자 단말과 물리적으로 접속함에 따라 추가적인 인증을 수행하기 위한 물리적 인증키(400); 및

상기 클라우드 장치로부터 클라우드 장치의 장치정보, 사용자 단말의 장치정보 및 회원정보를 제공받아 상기 사용자 단말 및 클라우드 장치를 등록 및 인증하고, 상기 물리적 인증키를 등록하고, 등록된 물리적 인증키가 접속됨에 따라, 인증된 클라우드 장치에 대하여 상기 클라우드 서비스 제공과 관련된 설정을 처리하는 관리 서버(300)

를 포함하고,

상기 사용자 단말은,

상기 클라우드 서비스에 대한 요청에 따라 상기 물리적 인증키가 추가 인증됨에 따라, 상기 전용 업로드/다운로드 브라우저가 활성화되는 것을 특징으로 하고,

상기 사용자 단말(100)은,

통신망을 통해 클라우드 서비스를 제공하는 클라우드 장치와 연결되어 데이터를 송수신하는 단말 통신부(101);

상기 클라우드 장치를 인증 및 등록하는 단말 인증부(102);

상기 물리적 인증키와 물리적으로 접속하는 인증키 접속부(104);

상기 사용자 단말의 동작 제어를 위한 사용자 요청을 입력받기 위한 입력부(105);

클라우드 서비스에 대응하는 화면을 제공하는 출력부(106);

상기 클라우드 장치에 정의된 하나 이상의 저장공간으로 하나 이상의 데이터에 대한 탐색, 다운로드, 업로드, 삭제, 백업 및 중복제거 중, 적어도 하나를 실행 요청하는 제어부(103);

상기 저장공간으로부터 다운로드된 데이터를 저장하는 단말 저장부(107); 및

상기 물리적 인증키에 구비된 암호화 프로그램 및 보안키가 로딩됨으로써, 상기 보안키를 이용하여 파일을 암호화 또는 복호화하기 위한 암호화/복호화부(108)

를 포함하는 것을 특징으로 하고,

상기 클라우드 장치(200)는,

통신망을 통해 하나 이상의 사용자 단말과 연결되어 상기 클라우드 서비스에 따른 데이터를 송수신하는 클라우드 통신부(201);

상기 사용자 단말을 인증 및 등록하는 클라우드 인증부(202);

상기 사용자 단말로부터 상기 물리적 인증키 관련 정보를 수신하여 확인하는 인증키 확인부(203);

하나 이상의 데이터에 대한 관리, 미디어 콘텐츠 제공 및 저장된 데이터에 대한 백업을 포함하는 클라우드 서비스를 제공하는 서비스 제공부(204); 및

상기 클라우드 서비스를 위한 데이터를 저장하는 하나 이상의 저장공간이 정의된 클라우드 저장부(205)

를 포함하는 것을 특징으로 하고,

상기 관리 서버(300)는,

통신망을 통해 하나 이상의 클라우드 장치와 연결되어 데이터를 송수신하는 서버 통신부(301);

클라우드 장치 및 클라우드 장치에 등록된 사용자 단말을 인증 및 등록하는 서버 인증부(302);

상기 사용자 단말을 통해 전달받은 상기 물리적 인증키 관련 정보를 인증하는 인증키 인증부(303);

인증된 클라우드 장치로부터 클라우드 서비스 제공과 관련된 설정을 처리하는 서버 관리부(304);

사용자의 회원정보를 저장하는 회원 DB(305); 및

각 회원의 계정별 등록된 클라우드 장치의 장치정보 및 각 회원의 물리적 인증키의 장치정보를 저장하는 장치 DB(306)

를 포함하는 것을 특징으로 하고,

상기 물리적 인증키는,

범용 직렬 버스(USB: Universal Serial Bus) 형태를 가지며, 복제 방지 기능이 적용된 하드웨어이고, 암호화 프로그램 및 파일 암호화 및 복호화를 위한 보안키가 구비되는 것을 특징으로 하고,

상기 USB의 고유번호가 암호화되어 기록되고, 상기 사용자 단말에서의 전용 업로드/다운로드 브라우저 프로그램의 실행시에 상기 USB의 고유번호와 암호화되어 복호화된 고유번호를 비교하여 복제 여부가 확인되는 것을 특징으로 하는 클라우드 서버의 데이터 전송 보안 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 전용 업로드/다운로드 브라우저는,

파일 전송 프로토콜(FTP : File Transfer Protocol) 접속 형태의 소프트웨어인 것을 특징으로 하는 클라우드 서버의 데이터 전송 보안 시스템.

청구항 6

청구항 1의 클라우드 서버의 데이터 전송 보안 시스템에서 클라우드 서버의 데이터 전송 보안 제공 방법에 있어서,

사용자 단말의 등록 요청에 따라 관리 서버가 회원 및 장치를 등록하는 회원및장치등록단계(S501 내지 S505);

상기 관리 서버가 수신한 등록 요청에 따라 물리적 인증키를 등록하는 물리적인증키등록단계(S506);

상기 물리적 인증키가 접속됨에 따라, 상기 물리적 인증키의 인증이 수행되는 물리적인증키인증단계(S507 내지 S511);

상기 물리적 인증키가 인증됨에 따라, 상기 사용자 단말에 전용 업로드/다운로드 브라우저가 활성화되는 전용브

라우저활성화단계(S512); 및

상기 활성화된 업로드/다운로드 브라우저를 통해 상기 사용자 단말 및 클라우드 장치간의 데이터가 관리 및 전송되는 데이터관리및전송단계(S513)

를 포함하고,

상기 물리적인증키인증단계는,

상기 물리적 인증키가 상기 사용자 단말을 통해 물리적으로 접속되는 단계(S507);

상기 사용자 단말이 상기 클라우드 장치로 상기 물리적 인증키의 확인을 요청하는 단계(S508);

상기 클라우드 장치가 상기 관리 서버로 상기 물리적 인증키의 인증을 요청하는 단계(S509);

상기 관리 서버에서 상기 물리적 인증키가 인증되는 단계(S510); 및

상기 물리적 인증키가 인증됨에 따라 상기 사용자 단말과 상기 클라우드 장치 간에 세션이 연결되는 단계(S511)

를 포함하는 것을 특징으로 하고,

상기 데이터관리및전송단계(S513)는,

상기 물리적 인증키로부터 암호화 프로그램 및 보안키가 로딩되는 단계(S601);

상기 사용자 단말에 상기 암호화 프로그램이 설치되는 단계(S602);

상기 사용자 단말의 요청에 따라 상기 클라우드 장치로부터 대용량 파일이 다운로드되는 단계(S603);

상기 사용자 단말에서 상기 다운로드된 대용량 파일이 복호화되는 단계(S604);

상기 사용자 단말의 요청에 따라 상기 복호화된 대용량 파일이 재생 또는 편집되는 단계(S605);

상기 사용자 단말에서 편집된 대용량 파일을 암호화하는 단계(S606); 및

상기 사용자 단말의 요청에 따라 상기 암호화된 대용량 파일이 업로드되는 단계(S607)

를 포함하는 것을 특징으로 하고,

상기 물리적 인증키는,

범용 직렬 버스(USB: Universal Serial Bus) 형태를 가지며, 복제 방지 기능이 적용된 하드웨어이고, 암호화 프로그램 및 파일 암호화 및 복호화를 위한 보안키가 구비되는 것을 특징으로 하고,

상기 USB의 고유번호가 암호화되어 기록되고, 상기 사용자 단말에서의 전용 업로드/다운로드 브라우저 프로그램의 실행시에 상기 USB의 고유번호와 암호화되어 복호화된 고유번호를 비교하여 복제 여부가 확인되는 것을 특징으로 하는 클라우드 서버의 데이터 전송 보안 제공 방법.

청구항 7

제6항에 있어서,

상기 회원및장치등록단계는,

상기 사용자 단말을 상기 클라우드 장치에 인식시키고, 계정, 및 패스워드를 포함하는 회원정보를 입력하여 단말의 등록을 요청하는 단계(S501);

상기 클라우드 장치가 상기 사용자 단말에 대한 최초 인증을 수행하는 단계(S502);

상기 사용자 단말이 정상 회원의 사용자 단말인 경우, 상기 클라우드 장치가 상기 관리 서버로 단말 및 장치의 등록을 요청하는 단계(S503);

상기 관리 서버가 회원 및 장치를 등록하는 단계(S504); 및

정상적으로 회원 및 장치가 등록되면, 상기 관리 서버가 상기 클라우드 장치에 대하여 사용을 승인하는 단계(S505)

를 포함하는 것을 특징으로 하는 클라우드 서버의 데이터 전송 보안 제공 방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

제6항에 있어서,

상기 전용 업로드/다운로드 브라우저는,

파일 전송 프로토콜(FTP : File Transfer Protocol) 접속 형태의 소프트웨어인 것을 특징으로 하는 클라우드 서버의 데이터 전송 보안 제공 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법에 관한 것으로서, 더욱 상세하게는 등록된 다수의 사용자 단말에 대하여 물리적 인증키를 이용하여 추가 인증을 수행함으로써 활성화되는 전용 업로드/다운로드 브라우저를 통해 상기 사용자 단말이 클라우드 장치에 접속하여 대용량의 파일에 대한 보안이 강화된 클라우드 서비스를 제공 받으며, 상기 물리적 인증키에 구비된 암호화 프로그램 및 보안키를 이용하여 상기 대용량의 파일의 업로드시 암호화를, 다운로드시 복호화를 수행함으로써, 그룹으로 등록된 사용자들만 상기 대용량 파일의 재생 또는 편집이 가능하도록 하기 위한, 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법에 관한 것이다.

배 경 기 술

[0002] 컴퓨터 네트워크의 기술발전에 따라, 각 단말의 독립적인 하드웨어 성능에 의존하던 기존의 컴퓨팅 환경은, 네트워크 상의 모든 컴퓨팅 자원을 활용하여 단말의 요청에 따라 해당 서비스를 제공하는 클라우드 컴퓨팅(Cloud Computing) 형태로 진화하고 있다.

[0003] 클라우드 컴퓨팅 서비스란, 인터넷과 같은 네트워크를 통한 '컴퓨팅 자원의 온 디맨드 아웃소싱 서비스'라고 정의할 수 있다. 클라우드 컴퓨팅 환경에서는, 서비스 제공자는 여러 곳에 분산되어 있는 데이터 센터를 가상화 기술로 통합하여 사용자들이 필요로 하는 서비스를 제공하게 된다. 서비스 사용자는 어플리케이션(Application), 스토리지(Storage), 운영체제(Operation System, OS), 보안(Security)등의 필요한 컴퓨팅 자원을 각 사용자 소유의 단말에 설치하여 사용하는 것이 아니라, 가상화 기술을 통해 생성된 가상공간상의 서비스를 원하는 시점에 원하는 만큼 골라서 사용하게 된다. 사용자는 각 컴퓨팅 자원의 구입비용을 지불하는 것이 아니라 사용량에 기반하여 대가를 지불하게 된다.

[0004] 이러한 클라우드 컴퓨팅 서비스에 따르면, 사용자들은 어떠한 장소에서든 네트워크 접속과 기본적인 연산기능만을 수행하는 단말을 통해 클라우드 망에 접속하여 대용량의 저장장치와 고성능 컴퓨팅 리소스가 필요한 작업들을 수행하고, 고도화된 서비스들도 제공받을 수 있는 장점이 있다.

[0005] 최근에는 스마트폰의 대중화에 따라 언제 어디서나 인터넷에 접속이 가능하게 되어, 클라우드 서비스(cloud service)가 활성화되고 있다. 클라우드 서비스란, 영화, 사진, 음악 등 미디어 파일 문서 주소록 등 사용자의 콘텐츠를 외부의 서버에 저장해 두고 스마트폰이나, 태블릿 PC를 포함한 어느 기기에서든 다운로드 후 사용 할 수 있는 서비스이다.

[0006] 그러나, 이러한 클라우드 서비스에서 제공하는 저장 공간의 크기는 제한적이며, 통상적으로 일정 공간 이상을 사용하기 위해서는 일정 금액의 사용료를 지불하여야 한다. 또한, 컴퓨팅 장치에도 다운로드 한 대용량의 데이터를 저장할 수 있는 저장공간이 확보되어야만 한다.

[0007] 이러한 클라우드 서비스를 이용하고, 대용량 데이터를 저장 및 관리할 수 있는 수단으로는 웹 하드 서비스, 네트워크 스토리지 서비스(NAS) 및 외장하드 장치 등이 있다.

[0008] 이중, 웹 하드 서비스는 장치의 휴대가 불필요하고, 클라우드 방식으로 운영되나, 정기적으로 이용료를 지급하거나, 데이터 패킷 이용에 따른 비용을 지불하여야 한다. 또한, 네트워크 스토리지 서비스는 전문 지식이 없는 개인이 도움없이 혼자서 구축하는 데는 어려움이 있으며, 휴대가 불필요하다는 장점이 있으나, 미디어 스트리밍, 서버로의 데이터 백업 등의 클라우드 서비스를 제공하지는 못한다는 한계가 있다.

[0009] 또한, 외장하드 장치는 장치를 한번 구입하면 이후 추가 비용이 발생하지 않는다는 장점만이 있을 뿐, 사용을 위해서는 항상 소지하여야 하는 번거로움이 있으며, 별도의 클라우드 서비스를 제공하지 못하는 단순 데이터 저장장치로만 사용해야 하는 한계가 있다.

[0010] 한국등록특허 [10-1081489]에는 인터넷을 통한 컴퓨팅 자원의 온 디맨드(On Demand) 아웃소싱을 제공하는 클라우드 컴퓨팅(Cloud Computing) 기술을 기반으로 하여, 기존의 사용자 개인단말 이외에 타 단말에서도 동일한 사용자환경을 적용하여 사용할 수 있도록 하는 통합사용자환경 제공방법 및 시스템이 개시되어 있다.

[0011] 한편, 한국등록특허 [10-1545146]에는 클라우드 스토리지 기반 작업 수행 시스템 및 방법이 개시되어 있다.

[0012] 현재, 기하급수적으로 늘어가고 있는 데이터 량에 따라서 자료의 보관은 물론 보관된 자료의 활용에 대한 요구도가 늘어가고 있다. 보편적으로 데이터의 저장 및 다른 사람에게 자료를 전송하는 방법으로써 주로 이메일을 사용하고 있으나 이 경우 광대한 용량을 가진 이메일 서버를 구축 및 유지해야만 하며, 고용량, 다량의 데이터가 서버로 전송되면서 메일서버는 대량의 부하를 감당해야만 하는 문제가 발생되고 있다.

[0013] 또 다른 방법으로 웹하드 서비스 및 클라우드 서비스를 이용하는 것으로 서비스 제공업자는 지속적으로 대용량 서버를 늘려가야만 하고 늘어난 시스템을 유지 관리해야만 하는 부담이 있으며 사용자의 입장에서는 제공받을 수 있는 용량의 한계와 비용의 부담은 물론 한 곳에서 관리되는 여러 사용자의 저장공간으로 인해 해킹에 의한 자료의 안전성 등에 대한 부담을 감수해야 하는 불편함이 있다.

[0014] 한편, 이러한 클라우드 컴퓨팅 환경에서 클라우드 서버의 스토리지(Storage)에 저장된 파일 데이터에 대해서 인가된 사용자에 의한 정상적인 루틴이 아닌 다른 루틴에 의해서 유출되는 것을 막기 위해서는 스토리지 보안이 필요하다. 즉, 네트워크 해킹을 통한 파일 유출과 직접적인 저장 매체를 통한 파일 유출을 막는 보안이 필요한 실정이다.

[0015] 예를 들어, 영화나 드라마 등과 같은 영상물에 관련된 데이터는 테라바이트급의 사이즈를 가지고 있으며, 이를 편집하는 사용자가 다수인 경우, 각 사용자가 저장장치를 구비할 수 없으므로, 클라우드 서비스를 이용하는 것이 바람직하다. 그러나, 클라우드 서비스에 있어서, 암호화, 접근통제, 데이터 손실방지 및 이상행위 탐지가 중요한 이슈이므로, 이를 보완하기 위한 대책이 필요하다.

선행기술문헌

특허문헌

[0016] (특허문헌 0001) 한국등록특허 [10-1081489](등록일자: 2011. 11. 02.)

(특허문헌 0002) 한국등록특허 [10-1545146](공개일자: 2015. 08. 11.)

(특허문헌 0003) 한국공개특허 [10-2016-0026951](공개일자: 2016. 03. 09.)

(특허문헌 0004) 한국등록특허 [10-0875964](등록일자: 2008. 12. 18.)

발명의 내용

해결하려는 과제

[0017] 따라서, 본 발명은 상기한 바와 같은 문제점을 해결하기 위하여 안출된 것으로, 본 발명의 목적은 등록된 다수의 사용자 단말에 대하여 물리적 인증키를 이용하여 추가 인증을 수행함으로써 활성화되는 전용 업로드/다운로드 브라우저를 통해 상기 사용자 단말이 클라우드 장치에 접속하여 대용량의 파일에 대한 보안이 강화된 클라우드 서비스를 제공 받으며, 상기 물리적 인증키에 구비된 암호화 프로그램 및 보안키를 이용하여 상기 대용량의

파일의 업로드시 암호화를, 다운로드시 복호화를 수행함으로써, 그룹으로 등록된 사용자들만 상기 대용량 파일의 재생 또는 편집이 가능하도록 하기 위한, 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법에 관한 것이다.

[0018] 본 발명의 실 시예들의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0019] 상기한 바와 같은 목적을 달성하기 위한 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 시스템에 있어서, 전용 업로드/다운로드 브라우저의 활성상태에서 클라우드 서비스가 제공되는 다수의 사용자 단말(100); 상기 사용자 단말과 통신망을 통해 연결되며, 상기 사용자 단말로부터 클라우드 서비스에 대한 요청에 응답하여 저장공간으로 하나 이상의 데이터에 대한 탐색, 다운로드, 업로드, 삭제, 백업 및 중복제거 중, 적어도 하나를 실행하는 클라우드 장치(200); 상기 사용자 단말과 물리적으로 접속함에 따라 추가적인 인증을 수행하기 위한 물리적 인증키(400); 및 상기 클라우드 장치로부터 클라우드 장치의 장치정보, 사용자 단말의 장치정보 및 회원정보를 제공받아 상기 사용자 단말 및 클라우드 장치를 등록 및 인증하고, 상기 물리적 인증키를 등록하고, 등록된 물리적 인증키가 접속됨에 따라, 인증된 클라우드 장치에 대하여 상기 클라우드 서비스가 제공과 관련된 설정을 처리하는 관리 서버(300)를 포함하고, 상기 사용자 단말은, 상기 클라우드 서비스에 대한 요청에 따라 상기 물리적 인증키가 추가 인증됨에 따라, 상기 전용 업로드/다운로드 브라우저가 활성화되는 것을 특징으로 한다.

[0020] 상기 사용자 단말(100)은, 통신망을 통해 클라우드 서비스를 제공하는 클라우드 장치와 연결되어 데이터를 송수신하는 단말 통신부(101); 상기 클라우드 장치를 인증 및 등록하는 단말 인증부(102); 상기 물리적 인증키와 물리적으로 접속하는 인증키 접속부(104); 상기 사용자 단말의 동작 제어를 위한 사용자 요청을 입력받기 위한 입력부(105); 클라우드 서비스에 대응하는 화면을 제공하는 출력부(106); 상기 클라우드 장치에 정의된 하나 이상의 저장공간으로 하나 이상의 데이터에 대한 탐색, 다운로드, 업로드, 삭제, 백업 및 중복제거 중, 적어도 하나를 실행 요청하는 제어부(103); 및 상기 저장공간으로부터 다운로드된 데이터를 저장하는 단말 저장부(107); 및 상기 물리적 인증키에 구비된 암호화 프로그램 및 보안키가 로딩됨으로써, 상기 보안키를 이용하여 파일을 암호화 또는 복호화하기 위한 암호화/복호화부(108)를 포함하는 것을 특징으로 한다.

[0021] 상기 클라우드 장치(200)는, 통신망을 통해 하나 이상의 사용자 단말과 연결되어 상기 클라우드 서비스에 따른 데이터를 송수신하는 클라우드 통신부(201); 상기 사용자 단말을 인증 및 등록하는 클라우드 인증부(202); 상기 사용자 단말로부터 상기 물리적 인증키 관련 정보를 수신하여 확인하는 인증키 확인부(203); 하나 이상의 데이터에 대한 관리, 미디어 콘텐츠 제공 및 저장된 데이터에 대한 백업을 포함하는 클라우드 서비스를 제공하는 서비스 제공부(204); 상기 클라우드 서비스를 위한 데이터를 저장하는 하나 이상의 저장공간이 정의된 클라우드 저장부(205)를 포함하는 것을 특징으로 한다.

[0022] 상기 관리 서버(300)는, 통신망을 통해 하나 이상의 클라우드 장치와 연결되어 데이터를 송수신하는 서버 통신부(301); 클라우드 장치 및 클라우드 장치에 등록된 사용자 단말을 인증 및 등록하는 서버 인증부(302); 상기 사용자 단말로부터 전달받은 물리적 인증키를 인증하는 인증키 인증부(303); 인증된 클라우드 장치로부터 클라우드 서비스 제공과 관련된 설정을 처리하는 서버 관리부(304); 사용자의 회원정보를 저장하는 회원 DB(305); 및 각 회원의 계정별 등록된 클라우드 장치의 장치정보 및 각 사용자의 물리적 인증키의 장치정보를 저장하는 장치 DB(306)를 포함한다.

[0023] 상기 물리적 인증키는, 범용 직렬 버스(USB: Universal Serial Bus) 형태를 가지며, 복제 방지 기능이 적용된 하드웨어인 것을 특징으로 한다.

[0024] 상기 물리적 인증키는, 범용 직렬 버스(USB: Universal Serial Bus) 형태를 가지며, 복제 방지 기능이 적용된 하드웨어이고, 암호화 프로그램 및 파일 암호화 및 복호화를 위한 보안키가 구비되는 것을 특징으로 하고, 상기 전용 업로드/다운로드 브라우저는, 파일 전송 프로토콜(FTP : File Transfer Protocol) 접속 형태의 소프트웨어인 것을 특징으로 한다.

[0025] 또한, 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 제공 방법에 있어서, 사용자 단말의 등록 요청에 따라 관리 서버가 회원 및 장치를 등록하는 회원및장치등록단계(S501 내지 S505); 상기 관리 서버가 수신한 등록 요청에 따라 물리적 인증키를 등록하는 물리적인증키등록단계(S506); 상기 물리적 인증키가 접속됨에 따라, 상기 물리적 인증키의 인증이 수행되는 물리적인증키인증단계(S507 내지 S511); 상기 물리적 인증키가 인

증됨에 따라, 상기 사용자 단말에 전용 업로드/다운로드 브라우저가 활성화되는 전용브라우저활성화단계(S512); 및 상기 활성화된 업로드/다운로드 브라우저를 통해 상기 사용자 단말 및 상기 클라우드 장치간의 데이터가 관리 및 전송되는 데이터관리및전송단계(S513)를 포함한다.

[0026] 상기 회원및장치등록단계는, 상기 사용자 단말을 상기 클라우드 장치에 인식시키고, 계정, 패스워드 등의 회원 정보를 입력하여 단말의 등록을 요청하는 단계(S501); 상기 클라우드 장치가 상기 사용자 단말에 대한 최초 인증을 수행하는 단계(S502); 상기 사용자 단말이 정상 사용자인 경우, 상기 클라우드 장치가 상기 관리 서버로 단말 및 장치의 등록을 요청하는 단계(S503); 상기 관리 서버가 회원 및 장치를 등록하는 단계(S504); 및 정상적으로 회원 및 장치가 등록되면, 상기 관리 서버가 상기 클라우드 장치에 대하여 사용을 승인하는 단계(S505)를 포함하는 것을 특징으로 한다.

[0027] 상기 물리적인증키인증단계는, 상기 물리적 인증키가 상기 사용자 단말을 통해 접속되는 단계(S507); 상기 사용자 단말이 상기 클라우드 장치로 상기 물리적 인증키의 확인을 요청하는 단계(S508); 상기 클라우드 장치가 상기 관리 서버로 상기 물리적 인증키의 인증을 요청하는 단계(S509); 상기 관리 서버에서 상기 물리적 인증키가 인증되는 단계(S510); 및 상기 물리적 인증키가 인증됨에 따라 상기 사용자 단말과 상기 클라우드 장치 간에 세션이 연결되는 단계(S511)를 포함하는 것을 특징으로 한다.

[0028] 상기 데이터관리및전송단계(S513)는, 상기 물리적 인증키로부터 암호화 프로그램 및 보안키가 로딩되는 단계(S601); 상기 사용자 단말에 상기 암호화 프로그램이 설치되는 단계(S602); 상기 사용자 단말의 요청에 따라 상기 클라우드 장치로부터 대용량 파일이 다운로드되는 단계(S603); 상기 다운로드된 대용량 파일이 복화화되는 단계(S604); 상기 사용자 단말의 요청에 따라 상기 복호화된 대용량 파일이 재생 또는 편집되는 단계(S605); 편집된 대용량 파일을 암호화하는 단계(S606); 및 상기 사용자 단말의 요청에 따라 상기 암호화된 대용량 파일이 업로드되는 단계(S607)를 포함하는 것을 특징으로 한다.

[0029] 상기 물리적 인증키는, 범용 직렬 버스(USB: Universal Serial Bus) 형태를 가지며, 복제 방지 기능이 적용된 하드웨어이고, 암호화 프로그램 및 파일 암호화 및 복호화를 위한 보안키가 구비되는 것을 특징으로 하고, 상기 전용 업로드/다운로드 브라우저는, 파일 전송 프로토콜(FTP : File Transfer Protocol) 접속 형태의 소프트웨어인 것을 특징으로 한다.

발명의 효과

[0030] 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법에 의하면, 등록된 다수의 사용자 단말에 대하여 물리적 인증키를 이용하여 추가 인증을 수행함으로써 활성화되는 전용 업로드/다운로드 브라우저를 통해 상기 사용자 단말이 클라우드 장치에 접속할 수 있으므로, 보안이 강화된 클라우드 서비스를 제공 받는 것이 가능한 효과가 있다.

[0031] 또한, 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법에 의하면, 영화나 드라마와 같은 영상물 제작을 위해 촬영된 데이터의 용량은 매우 큰데, 이를 편집하기 위해 사용자 개별적으로 보관을 위한 디스크가 필요 없이 클라우드 장치를 통해 쉽게 업로드 및 다운로드 할 수 있으므로, 사용자 편의가 제공될 수 있다.

[0032] 또한, 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법에 의하면, 상기 물리적 인증키에 구비된 암호화 프로그램 및 보안키를 이용하여 대용량의 파일의 업로드시 암호화를 수행하고, 다운로드시 복호화를 수행함으로써, 그룹으로 등록된 사용자들만 상기 대용량 파일의 재생 또는 편집이 가능하므로, 보안이 더욱 강화된 그룹핑 작업이 가능한 효과가 있다.

[0033] 또한, 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 시스템 및 그 제공 방법에 의하면, 물리적 인증키를 사용함으로써, 정상적인 사용자가 아닌 네트워크 해킹을 통해 자료가 유출되는 것을 방지할 수 있다.

도면의 간단한 설명

[0034] 도 1은 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 시스템의 구성도.

도 2는 도 1의 사용자 단말의 일실시예 상세 구성도.

도 3은 도 1의 클라우드 장치의 일실시예 상세 구성도.

도 4는 도 1의 관리 서버의 일실시예 상세 구성도.

도 5는 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 제공 방법에 대한 흐름도.

도 6은 도 5의 데이터 관리 및 전송 단계에 대한 상세 흐름도.

도 7은 본 발명의 일 실시예에 따른 전용 업로드/다운로드 브라우저를 설명하기 위한 도면.

발명을 실시하기 위한 구체적인 내용

[0035] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는바, 특정 실시예들을 도면에 예시하고 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 이해되어야한다.

[0036] 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.

[0037] 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0038] 본 명세서에서 사용되는 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, 공정, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 공정, 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 의미가 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미가 있는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0040] 이하, 첨부된 도면을 참조하여 본 발명을 더욱 상세하게 설명한다. 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정하여 해석되어서는 아니 되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여, 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다. 또한, 사용되는 기술 용어 및 과학 용어에 있어서 다른 정의가 없다면, 이 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 통상적으로 이해하고 있는 의미를 가지며, 하기의 설명 및 첨부 도면에서 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 설명은 생략한다. 다음에 소개되는 도면들은 당업자에게 본 발명의 사상이 충분히 전달될 수 있도록 하기 위해 예로서 제공되는 것이다. 따라서, 본 발명은 이하 제시되는 도면들에 한정되지 않고 다른 형태로 구체화될 수도 있다. 또한, 명세서 전반에 걸쳐서 동일한 참조번호들은 동일한 구성요소들을 나타낸다. 도면들 중 동일한 구성요소들은 가능한 한 어느 곳에서든지 동일한 부호들로 나타내고 있음에 유의해야 한다.

[0041] 도 1은 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 시스템의 구성도이다.

[0042] 도 1을 참조하면, 본 발명에 따른 클라우드 서버의 데이터 전송 보안 시스템은, 전용 업로드/다운로드 브라우저를 실행하여, 클라우드 서비스를 요청하는 하나 이상의 사용자 단말(100), 상기 사용자 단말(100)과 통신망을 통해 연결되며, 클라우드 서비스에 대한 요청에 응답하여 저장공간으로 하나 이상의 데이터에 대한 탐색, 다운로드, 업로드, 삭제, 백업 및 중복제거 중, 적어도 하나를 실행하는 클라우드 장치(200), 상기 사용자 단말과 물리적으로 접속함에 따라 추가적인 인증을 수행하기 위한 물리적 인증키(400), 상기 사용자 단말(100), 클라우드 장치(200) 및 물리적 인증키를 등록 및 인증하고, 인증된 클라우드 장치에 대하여 클라우드 서비스 제공과 관련된 설정을 처리하는 관리 서버(300)를 포함한다.

[0043] 사용자 단말(100)은 설치된 전용 업로드/다운로드 브라우저 프로그램을 실행하여 내부망 또는 외부망을 통해 클라우드 장치(200)에 접속하고, 클라우드 장치(200)에 탑재된 대용량 저장소에 기반한 클라우드 서비스를 제공받을 수 있다.

[0044] 또한, 사용자 단말(100)은 상기 물리적 인증키(400)에 구비된 암호화 프로그램 및 보안키를 이용하여, 상기 대용량의 파일을 상기 클라우드 장치(200)로 업로드시 암호화를 수행하고, 다운로드시 복호화를 수행할 수 있다. 이에 따라, 암호화 프로그램을 구비한 단말기에서만 상기 대용량 파일의 재생 또는 편집이 가능하다.

[0045] 즉, 대용량 파일이 리마스터링을 위한 영상 파일인 경우를 예를 들어 설명하면, 리마스터링 작업을 위해 상기 영상 파일을 재생 또는 편집을 해야 하는데, 상기 물리적 인증키(400) 없이는 업로드 및 다운로드가 불가능하고, 재생 또는 편집도 불가능하도록 하는 것이 가능하다.

[0046] 상기 사용자 단말(100)은 내부망 또는 외부망을 통해 상기 클라우드 장치(200)에 접속할 수 있다.

[0047] 이러한 기능을 수행하기 위해, 사용자 단말(100)은 내부망 또는 외부망에 접속하여 데이터를 송수신하는 통신모듈, 클라이언트 프로그램이 기록된 기록매체, 그 클라이언트 프로그램을 실행하는 AP, 클라이언트 프로그램의 실행화면 및 클라우드 장치(200)로부터 제공되는 콘텐츠를 표시하는 디스플레이 등의 하드웨어 수단등을 탑재할 수 있다.

[0048] 또한, 사용자 단말(100)은 구동초기 WiFi, 블루투스, NFC 태그 방식 등을 통해 클라우드 장치(200)와 연결되어 서로 간 장치등록 및 인증을 수행할 수 있고, WiFi 방식으로 가정 또는 사무실내 공유기(미도시됨)에 접속함으로써 내부망에 연결될 수 있으며, 다시 내부망을 통해 클라우드 장치(200)와 연동할 수도 있다.

[0049] 이러한 사용자 단말(100)은 다수개가 그룹으로 등록 및 인증될 수 있다.

[0050] 본 발명의 사용자 단말(100)은 예를 들면, 네비게이션 장치, 노트북, 이동통신 단말, 스마트폰(Smart phone), PMP(Portable Media Player), PDA(Personal Digital Assistant), 타블렛 PC(Tablet PC), 셋탑박스(Set-top box), 스마트 TV 등 다양한 장치가 될 수 있다.

[0051] 한편, 상기 클라우드 장치(200)는 클라우드 서비스를 제공하기 위한 대용량 클라우드 플랫폼이 설치될 수 있다. 클라우드 플랫폼은 미디어 파일의 자동백업, 미디어 콘텐츠 스트리밍, 외부 시스템으로부터의 파일 다운로드, 데이터에 대한 이중백업 및 문서편집 등의 기능을 제공할 수 있고, 이를 위한 대용량 저장소를 탑재할 수 있다.

[0052] 상기 클라우드 장치(200)는 사용자 단말(100)의 전용 업로드/다운로드 브라우저(클라이언트 프로그램)와 연동하여 클라우드 플랫폼에 의한 클라우드 서비스를 제공할 수 있고, 이러한 클라우드 서비스는 관리 서버(300)의 설정에 따라 제공방식이 결정될 수 있다.

[0053] 한편, 물리적 인증키(400)는 범용 직렬 버스(USB: Universal Serial Bus) 형태를 가지며, 복제 방지 기능이 적용된 하드웨어이다.

[0054] 상기 물리적 인증키(400) 내에는 사설 인증서가 저장되어 있고, 이를 클라우드 장치(200)로 전달하여 인증키의 확인을 요청하고 받고, 상기 클라우드 장치(200)는 상기 관리 서버(300)로 전달하여 인증키의 인증을 받는다.

[0055] 상기 물리적 인증키(400)의 접속이 확인되어야만 상기 사용자 단말(100)에서 전용 업로드/다운로드 브라우저 프로그램이 활성화될 수 있다.

[0056] 따라서, 물리적 인증키(400)가 없이 사용자 단말을 통해 클라우드 장치(200)로 접속하는 것이 불가능하다.

[0057] 또한, 상기 물리적 인증키(400)에는 암호화 프로그램 및 파일 암호화 및 복호화를 위한 보안키가 구비될 수 있다. 따라서, 대용량 파일은 상기 클라우드 장치(200)로 업로드되기 전에 암호화되어야 하며, 다운로드받은 대용량 파일에 대해서는 복호화된 이후에 해당 파일에 대한 편집 또는 재생이 가능하다.

[0058] 한편, 상기 물리적 인증키(400)의 복제 방지를 위해, USB의 고유번호를 암호화하여 기록하고, 이후 상기 USB를 이용하여 전용 업로드/다운로드 브라우저 프로그램의 실행시에 해당 USB의 고유번호와 암호화되어 복호화된 고유번호를 비교하여 복제 여부를 확인할 수도 있다.

[0059] 한편, 관리 서버(300)는 각 가정 또는 사무실에 설치된 하나 이상의 클라우드 장치(200)를 관리하는 기능을 제공할 수 있다. 또한, 관리 서버(300)는 사용자 단말(100) 및 클라우드 장치(200)와 통신망으로 연결되고, 상기 사용자 단말(100)이 상기 클라우드 장치(200)를 이용할 수 있도록 지원한다.

[0060] 본 발명의 시스템에 따른 사용자 단말(100), 클라우드 장치(200) 및 물리적 인증키(400)는 사용전 관리 서버(300)에 등록 및 인증되어야 하고, 관리 서버(300)는 등록 및 인증된 장치들에 대한 정보를 데이터베이스에 기록 및 저장할 수 있다.

[0061] 또한, 관리 서버(300)는 각 클라우드 장치(200)의 클라우드 서비스 제공을 위한 장치별 설정을 저장할 수 있고, 구동시 그 설정값을 제공하여 클라우드 장치(200)들이 정상적으로 동작할 수 있도록 지원할 수 있다. 또한, 관리 서버(300)는 클라우드 장치(200)의 서비스 및 보안을 위한 최신 펌웨어(firmware)를 제공함으로써 클라우드 장치(200)의 펌웨어가 항상 최신상태를 유지할 수 있도록 한다.

[0062] 특히, 관리 서버(300)는 클라우드 장치(200)의 요청에 따라 그에 저장된 데이터의 일부 또는 전부를 회원별 또는 장치별로 백업하는 기능을 제공할 수 있다.

[0063] 전술한 구조에 따라, 본 발명의 실시예에 의한 클라우드 서버의 데이터 전송 보안 시스템은 각 가정 또는 사무실 등에 클라우드 장치를 설치하고, 사용자가 자신의 사용자 단말, 클라우드 장치 및 물리적 인증키를 등록하며, 그 클라우드 장치가 제공하는 클라우드 플랫폼을 통해 대용량 클라우드 서비스를 이용할 수 있다.

[0064] 이하, 도2를 참조하여 본 발명의 실시예에 따른 사용자 단말을 설명하기로 한다.

[0065] 도 2는 도 1의 사용자 단말의 일실시예 상세 구성도이다.

[0066] 도 2를 참조하면, 본 발명에 따른 클라우드 서버의 데이터 전송 보안 시스템의 사용자 단말(100)은, 통신망을 통해 클라우드 서비스를 제공하는 클라우드 장치와 연결되어 데이터를 송수신하는 단말 통신부(101), 클라우드 장치를 인증 및 등록하는 단말 인증부(102), 물리적 인증키와 물리적으로 접속하는 인증키 접속부(104), 사용자 단말(100)의 동작 제어를 위한 사용자 요청을 입력받기 위한 입력부(105), 클라우드 서비스에 대응하는 화면을 제공하는 출력부(106), 클라우드 장치에 정의된 하나 이상의 저장공간으로 하나 이상의 데이터에 대한 탐색, 다운로드, 업로드, 삭제, 백업 및 중복제거 중, 적어도 하나를 실행 요청하는 제어부(103), 상기 저장공간으로부터 다운로드된 데이터를 저장하는 단말 저장부(107) 및 상기 물리적 인증키에 구비된 암호화 프로그램 및 보안키가 로딩됨으로써, 상기 보안키를 이용하여 파일을 암호화 또는 복호화하기 위한 암호화/복호화부(108)를 포함한다.

[0067] 단말 통신부(101)는 통신망을 통해 클라우드 장치와 연동하여 데이터를 송수신할 수 있다. 여기서, 통신망은 내부망 또는 외부망일 수 있고, 게이트웨이로서 공유기를 통해 클라우드 장치(200)에 접속할 수도 있다.

[0068] 이러한 단말 통신부(101)는 와이파이(WiFi) 모듈, 블루투스 모듈, 근거리 무선통신(NFC) 모듈 및 엘티이(LTE) 모뎀 등 중, 어느 하나를 포함할 수 있고, 상황에 따라 적절한 프로토콜을 통해 클라우드 장치(200)와 통신을 수행할 수 있다.

[0069] 또한, 단말 통신부(101)는 사용자 단말(100)과 관리 서버(300)를 통신망을 통해 상호 연결시키는 통신 수단으로서, 예를 들어 이동통신, 위성통신 등의 무선 통신모듈, 인터넷 등의 유선 통신모듈, 와이파이 등의 근거리 무선 통신모듈 등을 포함할 수 있다.

[0070] 상기 단말 인증부(102)는 연동되는 클라우드 장치를 등록 및 인증할 수 있다. 본 발명의 실시예에서 클라우드 서비스는 사용자 단말(100)과 클라우드 장치(200)는 서로 간 장치등록절차 및 인증절차가 선행되어야 하며, 최초 구동시 사용자 단말(100)은 NFC 태그를 통한 블루투스 프로토콜로 클라우드 장치와 접속 및 페어링을 수행하거나, 또는 사용자 단말(100)을 통한 사용자의 직접 설정 입력에 따라, 계정을 등록하여 서로 간에 장치를 등록 및 인증 절차를 수행할 수 있다.

[0071] 제어부(103)는 클라우드 장치와 연동하여 클라우드 서비스 주요 기능인 파일탐색, 다운로드, 업로드, 삭제 및 공유설정 등의 기능을 실행할 수 있다.

[0072] 파일 탐색 기능은 제어부(103)가 제공하는 파일 탐색기에 파일명, 확장자명, 종류, 크기, 날짜 및 태그 등을 입력하여 클라우드 장치 또는 사용자 단말에 저장된 파일을 검색할 수 있도록 하는 기능이다. 파일 탐색기는 정렬방식에 따라 탐색순서를 변경할 수 있고, 보기방식에 따라 목록, 아이콘, 미리보기 등의 기능을 제공할 수 있다.

[0073] 또한, 파일 탐색 기능에 의한 검색결과는 데이터의 종류에 따라, 사진, 동영상, 문서 등의 파일 유형별로 표시될 수 있고, 그 파일의 저장위치에 따라 구분되어 표시될 수 있다.

[0074] 파일 다운로드 기능은 클라우드 장치 내 저장된 복수의 파일 중, 하나 이상이 선택되면, 이를 사용자 단말의 기본 폴더에 저장할 수 있도록 하는 기능이다.

[0075] 파일 업로드 기능은 사용자 단말 내 저장된 복수의 파일 중, 하나 이상이 선택되면, 이를 클라우드 장치의 저장

공간 내 업로드 하는 기능이다.

[0076] 파일 삭제 기능은 클라우드 장치 또는 사용자 단말에 대하여, 파일 탐색에 따라 하나 이상이 선택되면 확인절차 이후 삭제를 수행하는 기능이다.

[0077] 파일 공유 기능은 클라우드 장치 또는 사용자 단말에 대하여, 파일 탐색에 따라 타 회원 또는 시스템으로부터의 접속권한을 부여하여 회원간 데이터의 공유를 설정하는 기능이다.

[0078] 또한, 상기 제어부(103)는 저장공간 내 저장된 데이터에 대하여, 동일한 둘 이상이 파일이 존재하는 경우, 중복되는 파일을 선택적으로 삭제하는 중복 제거 기능을 더 포함할 수 있다.

[0079] 상기 인증키 접속부(104)는 물리적 인증키와 물리적으로 접속하며, 접속여부를 제어부(103)로 알려준다.

[0080] 상기 입력부(105)는 사용자 단말(100)의 동작 제어를 위한 사용자 요청을 입력받기 위한 수단으로서, 사용자의 조작에 따라서 사용자의 요청을 전기 신호로 변환한다. 입력부(105)는 사용자로부터 문자, 숫자, 텍스트, 음성, 움직임, 촉각, 시각 등을 입력받는 입력 수단으로 예컨대, 입력 수단은 키보드, 키패드, 터치 스크린, 시각 감지 수단, 촉각 감지 수단, 움직임 감지 수단, 음성 입력 수단 등 다양한 형태로 구현될 수 있다.

[0081] 사용자는 상기 입력부(105)를 통해 인증키 및 작업 파일 지정정보를 입력할 수 있다. 여기서, 인증키는 ID/비밀번호, 개인키 등을 포함할 수 있다.

[0082] 상기 출력부(106)는 다양한 애플리케이션 구동에 따른 화면 정보를 디스플레이하는 디스플레이 수단, 예를 들어 LCD(Liquid Crystal Display) 또는 OLED(Organic Light Emitting Diodes) 등 평판 디스플레이장치로 구현되는 것이 바람직하다.

[0083] 상기 출력부(106)는 전용 업로드/다운로드 브라우저의 실행에 따른 클라우드 서비스에 대한 화면을 제공할 수 있다. 클라우드 장치의 저장공간내 데이터인 폴더 및 파일은 리스트 형태로 제공될 수 있고, 사용자는 화면상에서 구현된 인터페이스를 통해 폴더 또는 파일을 선택하여 의도한 작업을 수행할 수 있다.

[0084] 상기 단말 저장부(107)는 사용자 단말(100)의 동작 제어 시 필요한 프로그램과, 그 프로그램 수행 중에 발생되는 데이터를 저장한다. 단말 저장부(107)에는 클라우드 스토리지 기반 작업 수행을 위한 애플리케이션이 저장되어 있다.

[0085] 상기 제어부(103)는 단말 통신부(101), 인증키 접속부(104), 입력부(105), 출력부(106), 단말 저장부(107), 및 암호화/복호화부(108)의 각각의 동작을 감지 및 제어한다.

[0086] 이에 따라, 본 발명의 실시예에 의한 사용자 단말은 클라우드 장치를 등록 및 인증하고, 정보통신망을 통해 인증된 클라우드 장치에 접속하여 대용량 데이터 파일을 관리하거나 전송하는 등의 클라우드 서비스를 제공받을 수 있다.

[0087] 도 3은 도 1의 클라우드 장치의 일실시예 상세 구성도이다.

[0088] 도 3을 참조하면, 본 발명에 따른 클라우드 서버의 데이터 전송 보안 시스템의 클라우드 장치(200)는, 통신망을 통해 하나 이상의 사용자 단말과 연결되어 클라우드 서비스에 따른 데이터를 송수신하는 클라우드 통신부(201); 상기 사용자 단말을 인증 및 등록하는 클라우드 인증부(202); 상기 사용자 단말로부터 물리적 인증키 관련 정보를 수신하여 확인하는 인증키 확인부(203); 하나 이상의 데이터에 대한 관리, 미디어 콘텐츠 제공 및 저장된 데이터에 대한 백업을 포함하는 클라우드 서비스를 제공하는 서비스 제공부(204); 및 상기 클라우드 서비스를 위한 데이터를 저장하는 하나 이상의 저장공간이 정의된 클라우드 저장부(205)를 포함한다.

[0089] 상기 클라우드 통신부(201)는 등록 및 인증된 사용자 단말이 내부망 또는 외부망을 통해 접속하면, 대용량 클라우드 서비스를 제공할 수 있다. 클라우드 장치(200)는 서비스를 제공하기 위한 클라우드 플랫폼이 적용되어 있으며, 사용자 단말의 요청에 따라, 미디어 콘텐츠를 실시간으로 전송하거나 저장 요청되는 데이터 파일을 전송받아 저장한다.

[0090] 상기 클라우드 인증부(202)는 사용자 단말 및 관리 서버와의 연동을 위한 장치 등록 및 인증절차를 수행한다.

[0091] 본 발명의 클라우드 서비스를 이용하기 위해서는, 관리 서버로의 장치 등록 및 인증뿐만 아니라, 연동하는 사용자 단말과 서로 장치 등록 및 인증절차가 선행되어야 하며, 사용자 단말간의 초기 접속에 따른 연결에 따라, 사용자의 회원정보 및 장치정보를 입력받아 등록하고, 이후, 해당 사용자 단말의 접속이 요청되면, 인증을 거쳐 사용자 단말의 요청에 응답한다.

[0092] 또한, 상기 클라우드 인증부(202)는 초기등록시 입력되는 회원정보 및 장치정보를 관리 서버에 제공하여 두 장치를 해당 계정에 등록하여 서비스 제공을 승인 받는다. 또한, 상기 클라우드 인증부(202)는 상기 물리적 인증키 정보를 관리 서버에 제공하여 물리적 인증키를 등록한다.

[0093] 상기 인증키 확인부(203)는, 상기 사용자 단말로부터 물리적 인증키 관련 정보를 수신하여 확인한다.

[0094] 상기 서비스 제공부(204)는 사용자 단말의 요청에 따라, 데이터에 대한 관리, 미디어 콘텐츠 제공 및 데이터 백업 등의 클라우드 서비스를 구현할 수 있다. 특히, 서비스 제공부(204)는 사용자 단말의 제어부(도 2의 103)과 연동하여 그로부터 요청되는 파일탐색, 다운로드, 업로드, 삭제 및 공유설정 등에 응답하여 절차를 수행할 수 있다.

[0095] 이를 위해, 서비스 제공부(204)는 사용자 단말의 제어부와 연동하여 저장공간으로 데이터에 대한 탐색, 다운로드, 업로드, 삭제, 백업 및 중복제거 중, 적어도 하나를 수행하는 파일관리모듈과, 사용자 단말의 요청에 따라 저장공간에 저장된 미디어 콘텐츠를 스트리밍 방식으로 제공하는 미디어 모듈 및, 저장공간에 데이터를 정보 통신망을 통해 관리 서버에 더 저장하는 백업 모듈을 포함할 수 있다.

[0096] 상기 클라우드 저장부(205)는 클라우드 서비스를 위한 데이터를 저장할 수 있다. 클라우드 저장부(205)는 초기 설정에 따라, 하나의 루트 폴더 이하로 복수의 폴더 및 파일로 구성될 수 있고, FAT32, NTFS 및 ExFAT 등의 파일 시스템이 적용될 수 있다.

[0097] 상기 클라우드 저장부(205)로는 데이터 저장을 위한 대용량 자기 디스크, HDD, SHDD 및 SDD 등의 저장매체가 이용될 수 있고, 클라우드 장치가 지원하는 장치 관리자에 의해 저장매치 용량 증설 또는 교체 등의 기능을 지원할 수 있다. 또한, RAID 방식이 적용되어 둘 이상의 저장매체가 하나의 장치로서 동작할 수도 있다.

[0098] 전술한 구조에 따라, 본 발명의 실시예에 의한 클라우드 장치는 사용자 단말과 연동하여 요청에 따라 클라우드 서비스를 제공할 수 있고, 또한 통신망을 통해 관리 서버에 접속하여 클라우드 저장부에 저장된 데이터를 백업할 수 있다.

[0099] 도 4는 도 1의 관리 서버의 일실시예 상세 구성도이다.

[0100] 도 4를 참조하면, 본 발명에 따른 클라우드 서버의 데이터 전송 보안 시스템의 관리 서버(300)는, 통신망을 통해 하나 이상의 클라우드 장치와 연결되어 데이터를 송수신하는 서버 통신부(301), 클라우드 장치 및 클라우드 장치에 등록된 사용자 단말을 인증 및 등록하는 서버 인증부(302), 상기 사용자 단말로부터 전달받은 물리적 인증키를 인증하는 인증키 인증부(303), 인증된 클라우드 장치로부터 클라우드 서비스 제공과 관련된 설정을 처리하는 서버 관리부(304), 사용자의 회원정보를 저장하는 회원 DB(305) 및 각 회원의 계정별 등록된 클라우드 장치의 장치정보 및 각 사용자의 물리적 인증키의 장치정보를 저장하는 장치 DB(306)를 포함한다.

[0101] 상기 서버 통신부(301)는 통신망을 통해 각 사용자들의 클라우드 장치에 연결되어 클라우드 서비스를 제공하고, 각 클라우드 장치를 관리하기 위해 요구되는 데이터를 송수신할 수 있다.

[0102] 서버 인증부(302)는 클라우드 서비스를 제공하기 위해, 사용자 계정 및 클라우드 장치의 등록 및 인증절차를 수행할 수 있다.

[0103] 본 발명의 실시예에 따른 클라우드 서비스를 제공하기 위해서는 사용자의 계정과 그의 클라우드 장치 및 물리적 인증키가 등록되어 있어야 하고, 정상 사용자 및 장치의 인증이 완료되어 클라우드 장치의 승인이 요구된다. 서버 인증부(320)는 등록된 사용자, 즉 회원의 계정별로 클라우드 장치를 관리할 수 있고, 정상적인 인증완료시 해당 클라우드 장치에 클라우드 서비스의 제공을 승인하게 된다.

[0104] 상기 인증키 인증부(303)는 상기 사용자 단말로부터 전달받은 물리적 인증키의 정보를 받아 해당 계정 및 해당 클라우드 장치에서 사용가능한 인증키인지 확인하여 인증한다.

[0105] 상기 서버 관리부(304)는 등록 및 인증된 클라우드 장치를 관리할 수 있다. 클라우드 장치는 사용자 계정별로 등록될 수 있고, 클라우드 장치의 구동시 주기적으로 그 장치가 정상적으로 동작하는 여부를 확인할 수 있으며, 버전업에 따른 펌웨어 업데이트 등의 기능을 제공할 수 있다.

[0106] 또한, 서버 관리부(304)는 클라우드 장치의 요청에 따라, 저장공간내 데이터의 일부 또는 전부를 정기적 또는 비정기적으로 백업할 수 있다. 이는 온-라인 백업기능으로서, 데이터 보존에 대한 신뢰성을 확보할 수 있도록 한다.

[0107] 회원 DB(305)는 사용자의 회원정보를 저장할 수 있다. 회원정보를 계정을 포함할 수 있고, 클라우드 장치는 계정별로 등록되어 관리될 수 있다. 또한, 장치 DB(306)는 계정별 등록된 장치정보를 저장할 수 있고, 특히 온-라인 백업요청시 그 백업데이터를 계정별로 저장할 수 있다.

[0108] 한편, 관리 서버(300)는 통신망을 통해 접속 시도하는 임의의 시스템에 대하여, 정상 접속 여부를 판단하고, 그에 따른 접속승인 또는 차단을 수행하며, 불법적인 비인가 접속시도에 대한 보안 솔루션을 제공하는 보안부(미도시)를 더 포함할 수 있다.

[0109] 전술한 구조에 따라, 본 발명의 실시예에 의한 관리 서버(300)는 통신망을 통해 클라우드 장치의 요청에 따라 사용자 단말과 클라우드 장치를 최초 등록 및 인증하고, 회원들이 클라우드 장치를 통한 클라우드 서비스를 제공받을 수 있도록 각 장치에 대한 관리 기능을 제공할 수 있다.

[0110] 도 5는 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 제공 방법에 대한 흐름도이다.

[0111] 도 5를 참조하면, 본 발명의 실시예에 따른 클라우드 서버의 데이터 전송 보안 제공 방법에서는, 최초 등록시 사용자가 자신이 소지한 사용자 단말(100)을 클라우드 장치(200)에 인식시키고, 계정, 패스워드 등의 회원정보를 입력하여 단말의 등록을 요청한다(S501). 이러한 요청에 따라, 클라우드 장치(200)는 해당 사용자 단말(100)에 대한 최초 인증을 수행하고(S502), 정상 사용자일 경우 클라우드 장치(200)는 관리 서버(300)에 단말 및 장치의 등록을 요청한다(S503).

[0112] 등록 요청 단계(S503)는, 클라우드 장치(200)가 이미 각 가정 또는 사무실에 대한 네크워크 설정이 전제되어야 한다.

[0113] 이에 따라, 관리 서버(300)는 시스템에 회원 및 장치를 등록한다.(S504). 회원정보 및 장치정보를 각각 데이터베이스에 저장되며, 회원의 계정과 장치간 연관관계가 설정됨에 따라, 관리 서버(300)는 이후 계정별로 클라우드 장치(200)를 관리하게 된다. 정상적으로 회원 및 장치가 등록되면, 관리 서버(300)는 해당 클라우드 장치(200)에 대하여 사용을 승인한다(S505).

[0114] 한편, 관리 서버(300)는 사용자 단말(100)로부터 전달받거나 관리자로부터 직접 입력받은 물리적 인증키에 대한 정보를 기반으로 물리적 인증키를 등록한다(S506).

[0115] 이후, 물리적 인증키(400)가 접속됨에 따라(S507), 상기 사용자 단말(100)은 상기 클라우드 장치(200)로 인증키 확인을 요청한다(S508).

[0116] 이후, 상기 클라우드 장치(200)는 상기 관리 서버(300)로 상기 물리적 인증키(400)에 대한 인증을 요청한다(S509).

[0117] 이후, 상기 물리적 인증키(400)에 대하여 인증키 인증이 완료되면(S510), 클라우드 장치(200)는 등록된 사용자 단말(100)에 대하여 하나 이상의 세션을 연결하여 클라우드 서비스 제공을 준비한다(S511). S511 단계에서, 클라우드 장치(200)는 세션 연결된 사용자 단말(100)의 요청이 수신될 때까지 대기상태를 유지할 수 있다.

[0118] 이후, 사용자 단말(100)에서는 전용 업로드/다운로드 브라우저가 활성화되고(S512), 사용자 단말(100)은 사용자의 요청에 따라, 대용량 저장소를 이용한 파일 복사, 이동, 삭제 및 공유 등의 파일관리와 같은 클라우드 서비스를 요청하고, 상기 클라우드 장치(200)는 이에 응답하여 관리 절차를 수행하고(S513), 결과를 회신할 수 있다. 또한, 그 결과가 사용자 단말(100)의 화면에 표시될 수 있다.

[0119] 또한, 사용자는 클라우드 서비스로서, 파일저장과 같은 대용량 저장소를 활용하는 기능 이외에도 실시간 동영상 시청과 같은 미디어 콘텐츠를 이용할 수 있으며, 사용자 단말(100)을 통해 클라우드 장치(200)에 미리 저장되어 있는 동영상 파일과 같은 미디어 콘텐츠를 실행함으로써, 미디어 스트리밍을 요청할 수 있고, 클라우드 장치(200)는 이에 응답하여 해당 동영상 파일을 스트리밍 방식으로 전송함으로써, 사용자 단말(100)에서 재생할 수 있도록 한다.

[0120] 도 6은 도 5의 데이터 관리 및 전송 단계(S513)에 대한 상세 흐름도이다.

[0121] 도 6을 참조하면, 사용자 단말(100)에 물리적 인증키(400)가 접속되면, 암호화 프로그램 및 보안키가 로딩되며(S601), 상기 사용자 단말(100)에 암호화 프로그램이 설치된다(S602).

[0122] 이후, 사용자 단말(100)이 클라우드 장치(200)로부터 대용량 파일을 다운로드 받으면(S603), 이를 상기 보안키를 이용하여 복호화하여(S604), 재생 또는 편집(S605)을 수행할 수 있다.

[0123] 이후, 상기 사용자 단말(100)은 재생 또는 편집된 대용량 파일을 상기 보안키를 이용하여 암호화하여(S606), 상기 클라우드 장치(200)에 업로드 한다(S607).

[0124] 도 7은 본 발명의 일 실시예에 따른 전용 업로드/다운로드 브라우저를 설명하기 위한 도면이다.

[0125] 본 발명에서는 관리 서버(300)에서 물리적 인증키의 인증이 완료되면, 사용자 단말에 전용 업로드/다운로드 브라우저가 활성화된다. 한편, 상기 전용 업로드/다운로드 브라우저 소프트웨어로써 FTP 접속 프로그램이 사용될 수 있다.

[0126] 도 7에는 본 발명에서 사용될 수 있는 전용 업로드/다운로드 브라우저 프로그램으로 파일질라(FileZilla) 프로그램의 실행 화면이 도시되어 있다.

[0127] ①은 호스트로, 접속하고자 하는 서버의 주소를 입력하는 부분이고, ②는 사용자명으로, 아이디가 되고, ③은 비밀번호이고, ④는 사용자 단말기에 있는 폴더와 파일들이 표시되는 부분이고, ⑤는 접속한 서버의 폴더 및 파일들이 표시되는 부분이다. 파일을 업로드할 경우는 ④ 영역에서 ⑤ 영역으로 파일을 드래그하면 되고, 파일을 다운로드할 경우에는 ⑤ 영역에서 ④ 영역으로 파일을 드래그하면 된다.

[0128] 일반적으로, FTP는 인터넷 익스플로러 등의 웹 브라우저나 윈도우 탐색기 등으로도 사용할 수 있지만, 아무래도 FTP 클라이언트 프로그램을 별도로 설치해 접속하는 것이 여러 모로 편하다. FTP 서버에 접속하기 위해서는 해당 서버의 IP 주소나 인터넷 주소(URL)가 필요하다. FTP 서버의 인터넷 주소는 WWW(http://)와는 달리 'ftp://'의 형태로 사용된다. 예를 들어, 마이크로소프트 사의 WWW 주소는 'http://www.microsoft.com'이지만, FTP 주소는 'ftp://ftp.microsoft.com'이 된다.

[0129] 즉, FTP 클라이언트 프로그램을 사용하는 경우, 접속할 서버 사이트의 IP 주소 또는 인터넷 주소, 승인된 사용자 계정 및 암호를 입력하고 접속하면 최상위 폴더(디렉토리)가 출력된다. 이후부터는 윈도우 탐색기를 사용하듯 폴더/파일을 선택, 자신의 PC내 원하는 폴더에 내려받을 수 있다(다운로드). 반대로 자신의 PC에 있는 파일/폴더를 FTP 서버로 올릴 수도 있다(업로드).

[0130] FTP 서비스는 기본적으로 능동(active) 모드와 수동(passive) 모드의 두 가지 데이터 접속 방식을 제공한다. 앞서 언급한 서버와 클라이언트 간 네트워크 포트 20번(데이터 전송용)/21번(신호 제어용)을 사용하는 방식은 능동 모드다. 다만 일부의 네트워크 보안 장비(방화벽 등)에서 이들 포트(특히 20번)를 차단하는 경우 사용자가 FTP 서버에 접속하더라도 제대로 출력되지 않는 등의 문제가 발생할 수 있다.

[0131] 수동 모드는 이런 경우 데이터 전송용 포트를 20번이 아닌 다른 임의의 번호로 할당하여 데이터 전송을 진행할 수 있게 한다. 수동 모드 접속은 일반적으로 FTP 클라이언트 프로그램에서 설정하여 접속할 수 있으며, 수동 모드로도 FTP 서버의 파일 목록이 나타나지 않으면 해당 인터넷 서비스 제공사 또는 업체 네트워크 담당자에게 문의하여 보안 장비의 포트 차단 설정을 확인해야 한다.

[0132] 한편 SFTP 연결은 일반 FTP 연결에 보안성(secure)을 강화한 것으로, 서버와 클라이언트 간의 데이터 전송 시 계정 정보 등을 암호화하여 해킹이나 보안 상의 문제를 사전에 방지할 수 있다. 접속하는 방법은 일반 FTP 접속 방식과 동일하지만, FTP 서버에서 이를 지원해야 하며 신호 제어용 네트워크 포트가 21번이 아닌 22번을 사용한다는 점이 다르다.

[0133] 아울러 SFTP 연결은 보안 강화용 공개 키 또는 개인 인증 키 등을 사용할 수 있어 보다 안전한 데이터 송수신이 가능하다. 참고로 SFTP 모드로 연결하면 FTP 서버의 숨김파일까지 모두 출력된다. SFTP 연결 역시 FTP 클라이언트 프로그램을 통해 손쉽게 설정, 사용할 수 있다.

[0134] 이상에서 본 발명의 일 실시예에 따른 클라우드 서버의 데이터 전송 보안 제공 방법에 대하여 설명하였지만, 클라우드 서버의 데이터 전송 보안 제공 방법을 구현하기 위한 프로그램이 저장된 컴퓨터 판독 가능한 기록매체 및 클라우드 서버의 데이터 전송 보안 제공 방법을 구현하기 위한 컴퓨터 판독 가능한 기록매체에 저장된 프로그램 역시 구현 가능함은 물론이다.

[0135] 즉, 상술한 클라우드 서버의 데이터 전송 보안 제공 방법은 이를 구현하기 위한 명령어들의 프로그램이 유형적으로 구현됨으로써, 컴퓨터를 통해 판독될 수 있는 기록매체에 포함되어 제공될 수도 있음을 당업자들이 쉽게 이해할 수 있을 것이다. 다시 말해, 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어, 컴퓨터 판독 가능한 기록매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공

지되어 사용 가능한 것일 수도 있다. 상기 컴퓨터 판독 가능한 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리, USB 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 컴퓨터 판독 가능한 기록매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0136] 본 발명은 상기한 실시예에 한정되지 아니하며, 적용범위가 다양함은 물론이고, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 다양한 변형 실시가 가능한 것은 물론이다.

부호의 설명

[0137]

100: 사용자 단말 200: 클라우드 장치

300: 관리 서버 400: 물리적 인증키

101: 단말 통신부 102: 단말 인증부

103: 제어부 104: 인증키 접속부

105: 입력부 106: 출력부

107: 단말 저장부 108: 암호화/복호화부

201: 클라우드 통신부 202: 클라우드 인증부

203: 인증키 확인부 204: 서비스 제공부

205: 클라우드 저장부 301: 서버 통신부

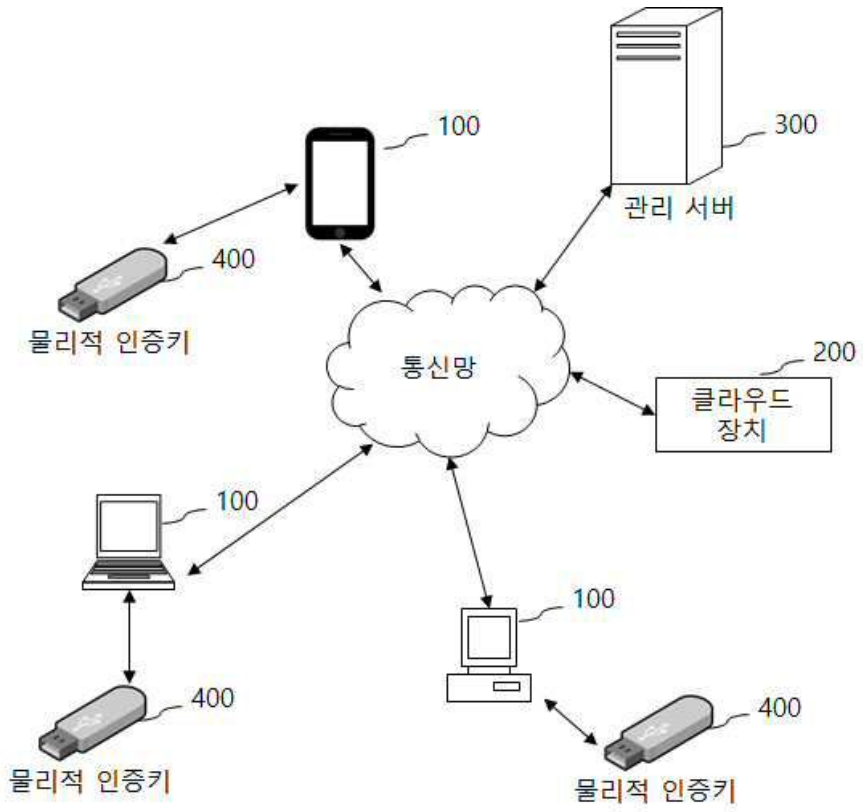
302: 서버 인증부 303: 인증키 인증부

304: 서버 관리부 305: 회원 데이터베이스

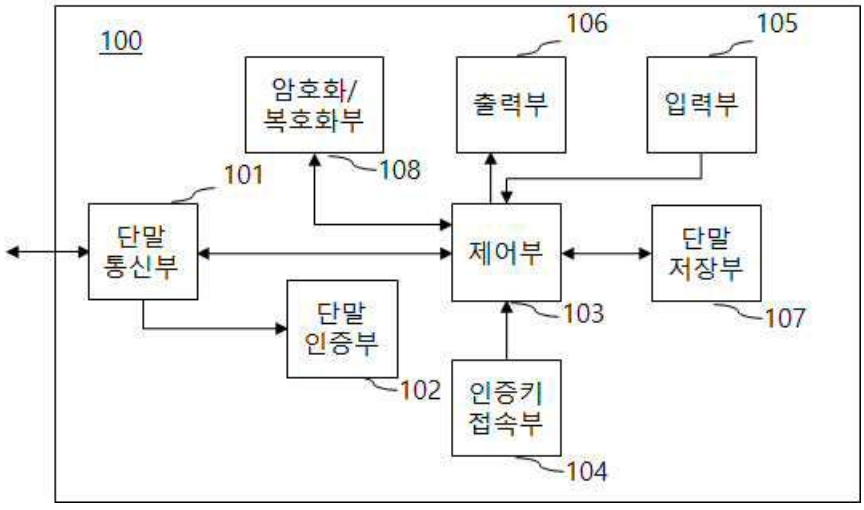
306: 장치 데이터베이스

도면

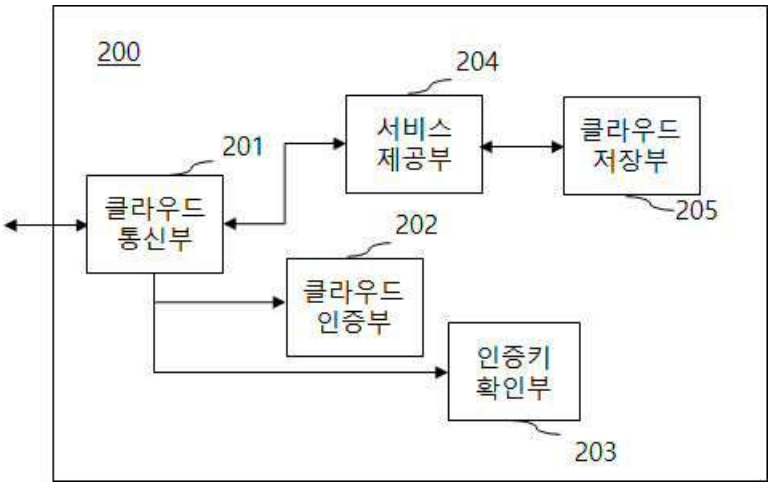
도면1


100
300
관리 서버
400
물리적 인증키
통신망
200
클라우드
장치
100
100
400
물리적 인증키
400
물리적 인증키

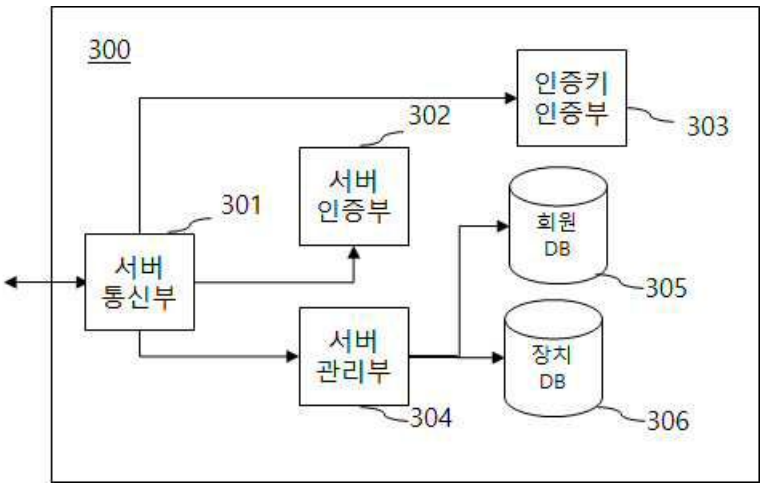
도면2


100
106
105
암호화/
복호화부
출력부
입력부
101
108
단말
통신부
제어부
단말
저장부
단말
인증부
103
107
102
인증키
접속부
104

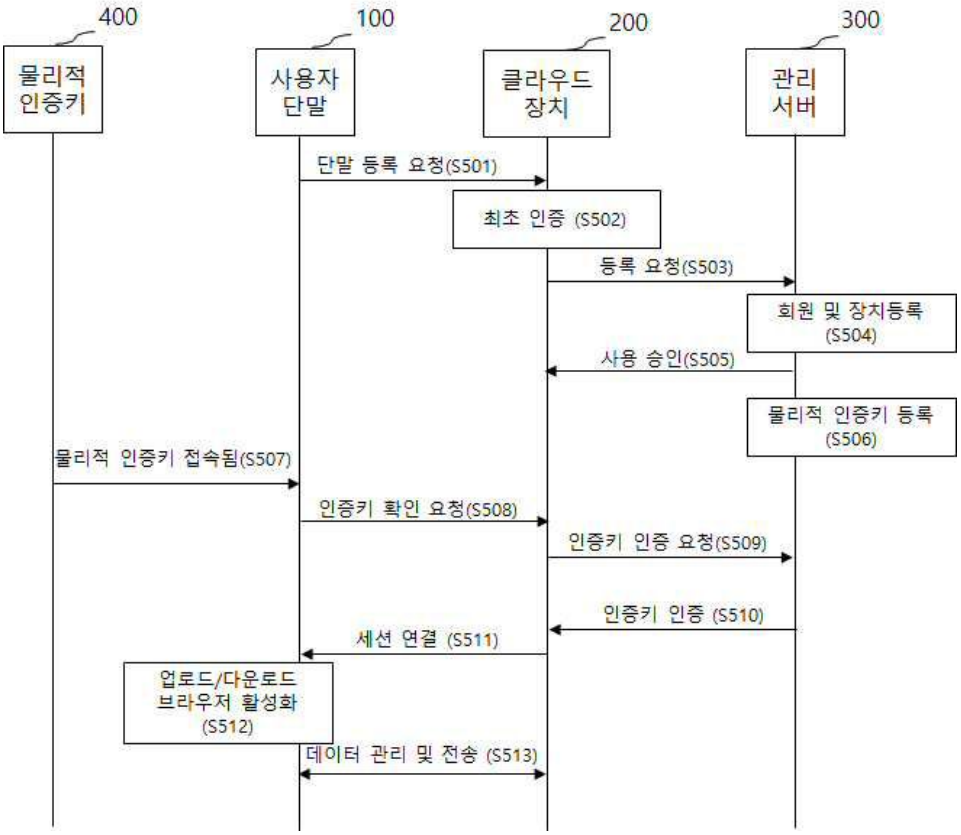
도면3


200
204
서비스
제공부
클라우드
저장부
205
201
클라우드
통신부
202
클라우드
인증부
인증키
확인부
203

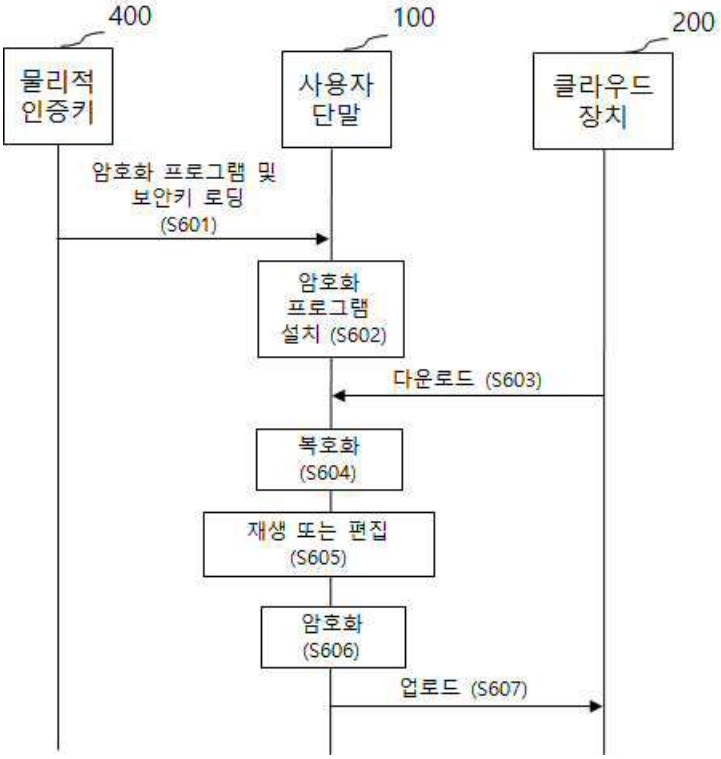
도면4


300
인증키
인증부
303
302
서버
인증부
301
서버
통신부
회원
DB
305
서버
관리부
장치
DB
304
306

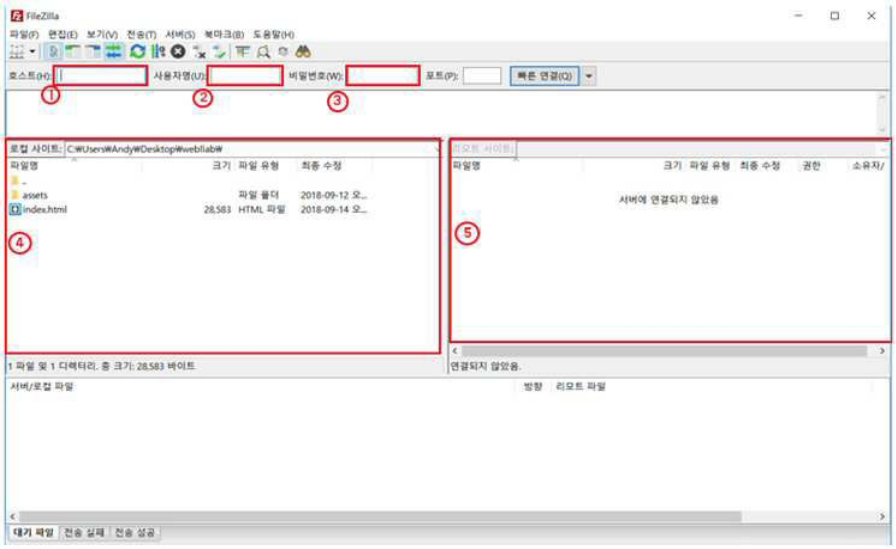
도면5


400
100
200
300
물리적 인증키
사용자 단말
클라우드 장치
관리 서버
단말 등록 요청(S501)
최초 인증 (S502)
등록 요청(S503)
회원 및 장치등록 (S504)
사용 승인(S505)
물리적 인증키 등록 (S506)
물리적 인증키 접속됨(S507)
인증키 확인 요청(S508)
인증키 인증 요청(S509)
인증키 인증 (S510)
세션 연결 (S511)
업로드/다운로드 브라우저 활성화 (S512)
데이터 관리 및 전송 (S513)

도면6


400
100
200
물리적 인증키
사용자 단말
클라우드 장치
암호화 프로그램 및 보안키 로딩 (S601)
암호화 프로그램 설치 (S602)
다운로드 (S603)
복호화 (S604)
재생 또는 편집 (S605)
암호화 (S606)
업로드 (S607)

도면7


FileZilla
파일(F) 편집(E) 보기(V) 전송(T) 서버(S) 북마크(B) 도움말(H)
호스트(H):
사용자명(U):
비밀번호(W):
포트(P):
빠른 연결(Q)
①
②
③
로컬 사이트: C:₩Users₩Andy₩Desktop₩webllab₩
파일명 크기 파일 유형 최종 수정
assets 파일 폴더 2018-09-12 오...
index.html 28,583 HTML 파일 2018-09-14 오...
④
원격 사이트:
파일명 크기 파일 유형 최종 수정 권한 소유자/
서버에 연결되지 않았음
⑤
1 파일 및 1 디렉터리. 총 크기: 28,583 바이트
연결되지 않았음.
서버/로컬 파일
방향
리모트 파일
대기 파일
전송 실패
전송 성공