(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년03월11일
(11) 등록번호 10-1957064
(24) 등록일자 2019년03월05일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/60* (2013.01)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
G06F 21/6245 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2017-0184037
(22) 출원일자 2017년12월29일
심사청구일자 2017년12월29일
(56) 선행기술조사문헌
KR101590076 B1*
(뒷면에 계속)

(73) 특허권자
건양대학교산학협력단
충청남도 논산시 대학로 121 (내동)
(72) 발명자
정승욱
대전광역시 서구 청사로 281, 샘머리아파트 218동 204호
(74) 대리인
김대영

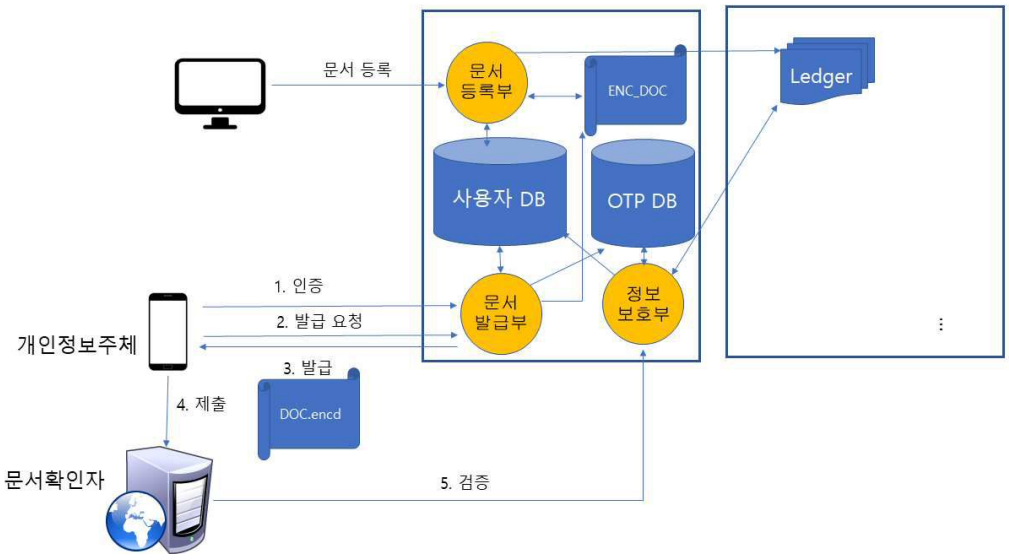
전체 청구항 수 : 총 1 항 심사관 : 구대성

(54) 발명의 명칭 **블록체인 상의 개인정보보호를 위한 OTP 기반 복호화 시스템**

(57) 요 약

본 발명은 블록체인 상에서 개인정보가 포함된 디지털 문서 자체를 블록체인 상에 저장하지 않고 개인정보파일의 일방향 해쉬값을 저장하되, 전달되는 개인정보파일을 암호화하고 제출하고자 하는 기관에서 한 번(또는 개인정보 주체가 정한 수만큼) 복호화하여 열람 가능하도록 하는 one-time 특성으로 디지털 문서의 무한 복제 후 배포를 막을 수 있는 블록체인 상의 개인정보보호를 위한 OTP 기반 복호화 시스템에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/0863 (2013.01)
H04L 2209/38 (2013.01)

(56) 선행기술조사문헌
KR101637854 B1*
KR10201300121348 A
KR10201700085423 A
KR10201700099152 A
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업
과제고유번호 NRF-2017R1D1A3B03036404
부처명 교육부
연구관리전문기관 한국연구재단
연구사업명 지역대학우수과학자지원사업
연구과제명 밀성이 향상된 블록체인 플랫폼 연구 및 개발
기 여 율 1/1
주관기관 건양대학교 산학협력단
연구기간 2017.06.01 ~ 2020.05.31

명 세 서

청구범위

청구항 1

등록되는 정보파일에 대하여 암호화키를 생성하고 상기 암호화 키를 통해 상기 정보파일을 암호화하여 저장하는 디지털문서관리부(111)와, 사용자식별정보와 상기 암호화 키와 암호화된 정보파일의 저장위치정보가 저장되는 사용자DB(112)와, 상기 정보파일의 일방향 해시값을 생성하여 사용자식별정보와 함께 블록체인에 기록하는 해시부(113)를 구비하는 문서등록부(110);

인증된 정보주체의 정보파일 발급요청에 따라 상기 정보주체의 사용자식별정보를 이용하여 상기 사용자DB(112)로부터 저장위치정보에 따른 암호화된 정보파일을 읽는 검색부(121)와, 난수 OTP를 생성하고 복호화 횟수를 설정받아 사용자식별정보와 상기 OTP와 함께 저장하는 OTP부(122)와, 읽어들인 암호화된 정보파일에 상기 OTP를 포함시킨 변환파일을 정보주체에게 발급하는 변환부(123)를 구비하는 문서발급부(120);

상기 정보주체로부터 전송된 변환파일에서 OTP를 추출하고 상기 OTP부에 존재하는 것으로 확인 후 사용자식별정보를 추출하는 검증부(131)와, 상기 사용자DB(112)로부터 추출된 사용자식별정보에 대응하는 암호화 키를 찾아 암호화된 정보파일을 복호화하는 복호화부(132)와, 복호화된 정보파일의 해시값을 생성하고 상기 블록체인에 저장된 해시값과 일치시 정보주체에게 복호화된 정보파일을 보여주는 해시확인부(133)와, 상기 검증부(131)를 통해 상기 OTP부에서 복호화 횟수 확인하여 차감하되, 횟수가 0이면 해당 OTP와 사용자식별정보 및 복호화 횟수를 제거하는 차감부(134)를 구비하는 정보보호부(130); 로 이루어지는 것을 특징으로 하는 블록체인 상의 개인정보보호를 위한 OTP 기반 복호화 시스템.

청구항 2

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 OTP 기반의 개인정보보호 시스템에 관한 것으로, 자세하게는 블록체인 상에서 개인정보가 포함된 디지털 문서 자체를 블록체인 상에 저장하지 않고 개인정보파일의 일방향 해쉬값을 저장하되, 전달되는 개인정보파일을 암호화하고 제출하고자 하는 기관에서 한 번(또는 개인정보주체가 정한 수만큼) 복호화하여 열람 가능하도록 하는 one-time 특성으로 디지털 문서의 무한 복제 후 배포를 막을 수 있는 블록체인 상의 개인정보보호를 위한 OTP 기반 복호화 시스템에 관한 것이다.

배 경 기 술

[0002] 블록체인(blockchain security technology)은 온라인 금융이나 가상화폐 거래에서 해킹을 막는 기술로서, 기존 금융회사들은 중앙 서버에 거래기록을 보관하지만 블록체인은 거래에 관여한 모든 컴퓨터가 동시에 기록을 보유한 상태에서 추가적인 거래가 일어나면 각 참여자의 승인을 받도록 하여 거래 내역을 고치려면 네트워크상의 모든 컴퓨터가 기록을 바꿔야 해 사실상 해킹이 불가능하다.

[0003] 이러한 블록체인은 대표적으로 비트코인의 거래를 위한 보안 기술로 활용되고 있으며 비트코인처럼 특허가 없는 오픈 소스인 데다 활용 가치가 커 관심이 높아지고 있는 가운데 이를 활용함으로 고객 데이터베이스(DB) 유지 보수와 보안에 따른 막대한 비용을 줄일 수 있어 글로벌 금융회사들이 이 기술에 눈독을 들이고 있다.

[0004] 이와 같이 블록체인은 한번 기록한 정보를 변경할 수 없어 기록한 정보의 무결성을 제공하며 이러한 무결성 특성으로 인해 위조방지가 필요한 문서기록에 대한 적용 논의도 활발하다. 예를 들어, 주민등록등본과 같은 정보에 대한 진위를 판별하기 위해서 주민등록등본의 원본을 블록체인 상에 기록하여 보관하면 누구도 변경할 수 없어 진본임을 확인할 수 있으며 종이문서의 위조를 막을 수 있어 매우 유용하다.

[0005] 하지만, 무결성이라는 특성과 함께 블록체인은 특성상 블록체인 네트워크에 참여하고 있는 누구나 확인 가능한 투명성(transparency)도 함께 제공하며, 이는 개인정보보호 관점 나의 개인정보를 누구나 확인 가능하여 개인정

보유출에 관한 심각한 문제를 발생시킬 수 있다는 약점으로 작용할 수 있다.

[0006] 이에 본 특허에서는 블록체인 상에서 개인정보를 보호하기 위해서 개인정보가 들어있는 디지털 문서(예 주민등록등본, 이하 개인정보파일이라고 함) 자체를 블록체인 상에 저장하지 않고 개인정보파일의 일방향 해쉬값을 저장하여 블록체인 상에 저장된 정보자체로는 개인정보가 유출될 수 없도록 한다.

[0007] 하지만, 이 경우 개인정보파일을 요청하는 기관에 제출할 경우 수령한 기관은 디지털 파일의 특성상 무한대로 복제할 수 있어, 무한대로 복제한 개인정보파일이 개인정보주체가 원치 않은 수많은 제3자에게 전달되어 개인정보 유출이 발생할 가능성도 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 등록특허공보 제10-1723405호(2017.03.30)

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 문제점을 해결하기 위하여 창출된 것으로, 본 발명의 목적은 블록체인 상에서 개인정보가 포함된 디지털 문서 자체를 블록체인 상에 저장하지 않고 개인정보파일의 일방향 해쉬값을 저장하여 블록체인 상에 저장된 정보만으로는 개인정보가 유출될 수 없도록 하되, 전달되는 개인정보파일을 암호화하고 제출받은 기관에서 복호화할 때 한번 또는 정해진 횟수만큼만 복호화할 수 있도록 하여 디지털 문서의 무한 복제 후 배포를 막을 수 있는 블록체인 상의 개인정보보호를 위한 OTP 기반 복호화 시스템을 제공하는 것이다.

과제의 해결 수단

[0010] 상기와 같은 목적을 위한 본 발명은 등록되는 정보파일에 대하여 암호화키를 생성하고 상기 암호화 키를 통해 상기 정보파일을 암호화하여 저장하는 디지털문서관리부와, 사용자식별정보와 상기 암호화 키와 암호화된 정보파일의 저장위치정보가 저장되는 사용자DB와, 상기 정보파일의 일방향 해시값을 생성하여 사용자식별정보와 함께 블록체인에 기록하는 해시부를 구비하는 문서등록부; 인증된 정보주체의 정보파일 발급요청에 따라 상기 정보주체의 사용자식별정보를 이용하여 상기 사용자DB로부터 저장위치정보에 따른 암호화된 정보파일을 읽는 검색부와, 난수 OTP를 생성하고 사용자식별정보와 함께 상기 OTP를 저장하는 OTP부와, 읽어들인 암호화된 정보파일에 상기 OTP를 포함시킨 변환파일을 정보주체에게 발급하는 변환부를 구비하는 문서발급부; 상기 정보주체로부터 전송된 변환파일에서 OTP를 추출하고 상기 OTP부에 존재하는 것으로 확인 후 사용자식별정보를 추출하는 검증부와, 상기 사용자DB로부터 추출된 사용자식별정보에 대응하는 암호화 키를 찾아 암호화된 정보파일을 복호화하는 복호화부와, 복호화된 정보파일의 해시값을 생성하고 상기 블록체인에 저장된 해시값과 일치시 정보주체에게 복호화된 정보파일을 보여주는 해시확인부를 구비하는 정보보호부; 로 이루어지는 것을 특징으로 한다.

[0011] 이때 상기 OTP부는 복호화 횟수를 설정받아 상기 OTP와 함께 저장하고, 상기 검증부를 통해 상기 OTP부에서 복호화 횟수 확인하여 차감하되, 횟수가 0이면 해당 OTP와 사용자식별정보 및 복호화 횟수를 제거하는 차감부를 더 포함하는 것이 바람직하다.

발명의 효과

[0012] 본 특허는 기본적으로 블록체인을 이용하므로 저장파일의 진본을 확인할 수 있으며 투명성을 제공한다. 이때 블록체인 상에서 개인정보를 보호가 이루어질 수 있도록 주민등록등본과 같이 개인정보가 들어있는 디지털 문서 자체는 블록체인 상에 저장하지 않고 개인정보파일의 일 방향 해쉬값을 저장함으로 블록체인 상에 저장된 정보자체로 개인정보가 유출될 수 없도록 하여 개인정보를 효과적으로 보호하게 된다.

[0013] 또한, OTP를 이용하여 한 번 또는 정해진 횟수만 복호화가 가능하도록 하여 디지털 문서의 특성인 무한 복제 후 전송 문제를 차단하여 뛰어난 정보보안이 이루어질 수 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 개념도,

도 2는 본 발명의 실시예에 따른 구성 및 연결관계를 나타낸 블록도 이다.

발명을 실시하기 위한 구체적인 내용

[0015] 이하 첨부된 도면을 참조하여 본 발명 블록체인 상의 개인정보보호를 위한 OTP 기반 복호화 시스템의 구성을 구체적으로 설명한다.

[0016] 도 1은 본 발명의 개념도, 도 2는 본 발명의 실시예에 따른 구성 및 연결관계를 나타낸 블록도로서, 본 발명은 기본적으로 문서등록, 문서발급, 복호화라는 세 가지 주요기능을 통해 동작하며 이를 위한 문서등록부(110)와, 문서발급부(120) 및 정보보호부(130)의 주요 구성을 구비하게 된다.

[0017] 본 발명에서는 개인정보를 취급 및 보호하는 전체 시스템은 사용자의 정보를 수집을 하였다고 가정한다. 예를 들어, 주요 개인정보의 일례인 주민등록등본의 관련 정보를 관청에서 이미 가지고 있을 것이다.

[0018] 도 1과 같이 사용자DB(112)에는 사용자를 인증할 수 있는 정보가 저장되고 추가로 FILE_PATH(ENC_DOC) 정보와 ENC_KEY가 저장되며 사용자식별정보도 저장된다. 여기서 FILE_PATH 함수는 입력 파일의 URL를 나타내는 함수이다. ENC_DOC은 암호화된 개인정보파일이며 ENC_KEY는 암호화 키, OTP DB는 일회용 비밀번호(OTP), 사용자 식별값 및 복호화 횟수가 저장된다.

[0019] 먼저, 상기 문서등록부(110)는 이러한 관청과 같은 정보취급주체가 디지털화된 문서를 등록하기 위한 구성으로 디지털문서관리부(111)와 사용자DB(112)와, 해시부(113)의 세부구성을 구비하게 된다.

[0020] 상기 디지털문서관리부(111)는 등록되는 정보파일에 대하여 암호화키를 생성하고 상기 암호화 키를 통해 상기 정보파일을 암호화하여 저장하는 구성으로, 정보취급주체가 개인정보파일을 필요시 또는 최종 변경사항이 적용된 개인정보파일을 디지털문서관리부를 통하여 등록한다. 여기서 정보취급주체는 공무원과 같은 사람과 자동화된 문서 등록 프로그램을 포괄하는 것으로, 관청뿐 아니라 병원, 은행, 학교, 기업, 공공기관 등 개인정보를 취급하는 다양한 대상을 포함한다.

[0021] 상기 사용자DB(112)는 사용자식별정보와 상기 암호화 키와 암호화된 정보파일의 저장위치정보가 저장되는 구성이다.

[0022] 즉 상기 디지털문서관리부(111)는 우선 랜덤하게 암호화키는 ENC_KEY 값을 생성하고 생성된 암호화 키를 이용하여 암호화된 정보파일 ENC_DOC := EncENC_KEY(DOC)를 만든다. (여기에서 Enc은 암호화 알고리즘이고 DOC은 개인정보파일을 의미한다.)

[0023] 이와 같은 암호화된 정보파일 ENC_DOC은 사용자DB(112)에 저장되며, 구체적으로 ENC_KEY 값과 FILE_PATH(ENC_DOC) 파일을 사용자DB에 입력한다. 또한, 여기서 FILE_PATH 함수는 암호화된 정보파일의 저장위치 즉 URL을 나타내는 함수이다. 또한, 상기 사용자DB(112)에는 사용자를 인증할 수 있는 정보인 사용자 식별정보가 저장된다.

[0024] 상기 해시부(113)는 상기 정보파일의 일방향 해시값을 생성하여 사용자식별정보와 함께 블록체인에 기록하는 구성이다. 즉 h(DOC)를 만들어 블록체인 상에 사용자식별정보와 함께 기록하게 되며, h는 안전한 일방향 hash 함수이다.

[0025] 상기 문서발급부(120)는 개인과 같은 정보주체가 개인정보가 담긴 문서인 암호화된 정보파일을 발급받기 위한 구성으로, 검색부(121)와, OTP부(122)와, 변환부(123) 및 차감부(134)의 세부 구성을 구비하게 된다.

[0026] 상기 검색부(121)는 인증된 정보주체의 정보파일 발급요청에 따라 상기 정보주체의 사용자식별정보를 이용하여 상기 사용자DB(112)로부터 저장위치정보에 따른 암호화된 정보파일을 읽게 된다.

[0027] 이를 위해 정보파일을 발급받고자 하는 개인인 정보주체가 암호화된 정보파일(DOC 파일) 발급을 위해서 사용자식별정보를 이용한 인증을 한다. 이는 아이디/패스워드나, 공인인증서를 비롯한 다양한 공지의 인증방식을 통해 진행될 수 있으며 인증이 성공함에 따라 정보주체가 정보파일 발급을 요청하게 된다.

[0028] 이때 정보주체가 정보파일을 요청하는 시점에 앞서 설명된 문서등록절차가 진행될 수도 있고, 사전에 미리 등록절차가 진행될 수도 있다.

[0029] 이러한 발급요청에 따라 상기 검색부는 정보주체가 입력한 사용자식별정보를 이용하여 사용자DB(112)에서 암호

화된 정보파일(ENC_DOC)의 위치를 확인하고 해당 파일을 읽어들인다.

[0030] 상기 OTP부(122)는 난수 OTP를 생성하고 사용자식별정보와 함께 상기 OTP를 별도의 저장부-OPT DB 등에 저장하게 된다. 이때 상기 OTP부(122)는 복호화 횟수를 설정받아 상기 OTP와 함께 저장할 수 있다.

[0031] 즉 상기 OTP부(122)에서 난수 OTP를 생성하고 OTP DB에 OTP와 사용자식별정보 그리고 설정된 복호화 횟수를 기록한다. 이하의 설명에서는 기본적으로 복호화 횟수를 1이라 가정하나, 필요한 복호화 즉 발급 횟수를 이를 통해 조정할 수 있다.

[0032] 상기 변환부(123)는 상기 검색부를 읽어들인 암호화된 정보파일에 상기 OTP부(122)를 통해 생성된 OTP를 포함시켜 형성된 변환파일을 정보주체에게 발급하게 된다. 즉 DOC.encd(확장자를 encd라고 가정) := ENC_DOC|OTP파일을 만들어서 정보주체에게 전달하게 되며, 정보주체는 발급받은 파일인 DOC.encd를 검증을 위한 기관에 제출한다.

[0033] 상기 정보보호부(130)는 정보주체가 받은 파일을 복호화하기 위하여 검증 및 복호화하는 구성으로, 검증부(131)와 복호화부(132)와 해시확인부(133)의 세부구성을 구비하게 되며, 별도의 검증기관을 비롯하여 문서를 발급한 관청 등의 기관을 통해서도 이루어질 수 있다.

[0034] 상기 검증부(131)는 상기 정보주체로부터 전송된 변환파일에서 OTP를 추출하고 상기 OTP부에 존재하는 것으로 확인 후 사용자식별정보를 추출하는 구성이다.

[0035] 즉 정보주체가 발급받은 암호화된 정보파일(DOC.encd)을 상기 정보보호부(130)에 전송하면 상기 검증부(131)는 DOC.encd 파일에서 OTP를 추출하고 상기 OTP DB에서 해당 OTP가 존재하는지 확인한다.

[0036] 이때 상기 검증부(131)를 통해 상기 OTP부(122)에서 복호화 횟수 확인하여 차감하되, 횟수가 0이면 해당 OTP와 사용자식별정보 및 복호화 횟수를 제거하는 차감부(134)를 포함할 수 있다.

[0037] 즉 만약 OTP가 존재한다면 복호화 횟수를 확인하고 1 이상이면 복호화 횟수를 -1 차감하고 OTP DB에서 사용자식별값을 추출한다. 이때 앞서 설정된 복호화 횟수에 따른 복호화가 가능하며 상기 검증부(131)에서 사용자 식별정보를 추출하고 복호화 횟수를 확인하여 0이면 OTP DB에서 해당 OTP, 사용자식별정보, 복호화 횟수를 삭제한다.

[0038] 상기 복호화부(132)는 상기 사용자DB(112)로부터 추출된 사용자식별정보에 대응하는 암호화 키를 찾아 암호화된 정보파일을 복호화하게 된다. 즉 사용자식별정보를 이용하여 사용자 DB에서 ENC_KEY를 찾아 DOC.encd파일에서 ENC_DOC을 복호화한다.

[0039] 상기 해시확인부(133)는 복호화된 정보파일의 해시값을 생성하고 상기 블록체인에 저장된 해시값과 일치시 정보주체에게 복호화된 정보파일을 보여주어 내용확인이 이루어질 수 있도록 한다. 복호화된 DOC 파일의 해쉬값을 생성, 즉 h(DOC)를 만들고 블록체인 상에 사용자식별정보를 통해 저장된 h(DOC)를 검색한다. 두 개의 해쉬값을 비교하여 맞으면 사용자에게 DOC파일을 보여 준다.

[0040] 이때 복호화된 정보파일(DOC 파일)을 보여주는 것은 별도의 애플리케이션을 이용하여 보여주게 되며 해당 애플리케이션은 문서 다운로드 금지 및 출력 횟수를 제한하여 다운로드 후 무한 복제를 차단하여 개인정보 유출을 방지할 수도 있다.

[0041] 본 발명의 권리는 위에서 설명된 실시 예에 한정되지 않고 청구범위에 기재된 바에 의해 정의되며, 본 발명의 분야에서 통상의 지식을 가진 자가 청구범위에 기재된 권리범위 내에서 다양한 변형과 개작을 할 수 있다는 것은 자명하다.

부호의 설명

[0042]

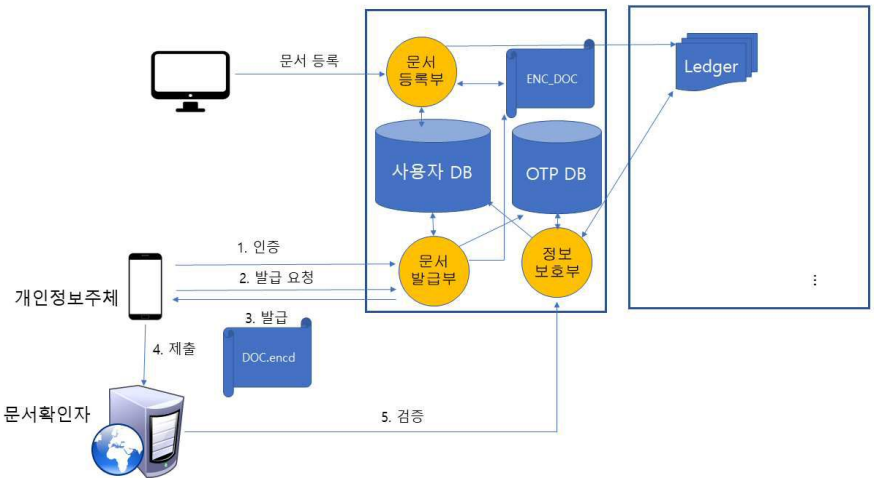
110: 문서등록부	111: 디지털문서관리부
112: 사용자DB	113: 해시부
120: 문서발급부	121: 검색부
122: OTP부	123: 변환부
130: 정보보호부	131: 검증부

132: 복호화부 133: 해시확인부

134: 차감부

도면

도면1



도면2