



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0104552
(43) 공개일자 2022년07월26일

(51) 국제특허분류(Int. Cl.)

H04L 9/40 (2022.01) G06Q 30/06 (2012.01)
G06Q 50/30 (2012.01) G07C 5/08 (2006.01)
H04L 65/40 (2022.01) H04L 9/06 (2006.01)
H04L 9/08 (2006.01)

(52) CPC특허분류

H04L 63/10 (2013.01)
G06Q 30/0607 (2013.01)

(21) 출원번호 10-2021-0007016

(22) 출원일자 2021년01월18일

심사청구일자 2021년01월18일

(71) 출원인

부경대학교 산학협력단

부산광역시 남구 용소로 45, 부경대학교내 (대연동)

(72) 발명자

신상욱

부산광역시 남구 분포로 113, 208동 1401호(용호동, 엘지메트로시티)

정병규

부산광역시 남구 용소로7번길 63-3, 905호(대연동, 오름아파트)

조강우

경상남도 창원군 창녕읍 학산길 23

(74) 대리인

오위환, 나성곤, 정기택

전체 청구항 수 : 총 23 항

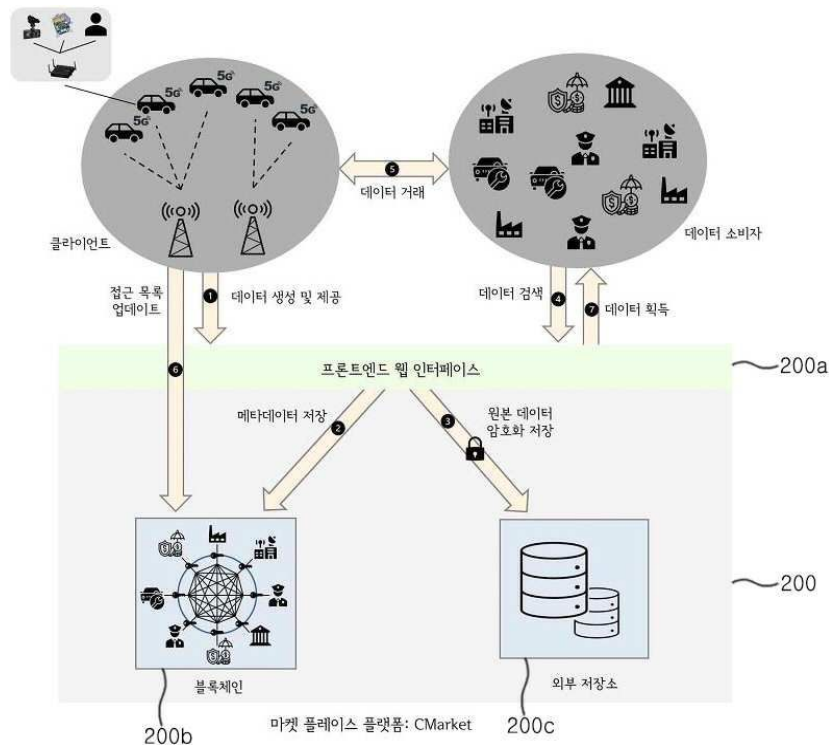
(54) 발명의 명칭 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법

(57) 요약

본 발명은 DO-ABE(data-owner-based attribute-based encryption) 암호화 체계를 블록체인 환경에서 동작할 수 있도록 재구성하고 이를 이용하여 커넥티드 카의 중요 데이터를 안전하고 효율적으로 공유하고 거래할 수 있도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법에 관한 것으로, 데이터에 접근하는 개

(뒷면에 계속)

대표도 - 도3



체를 직접 정의하고, 차량 데이터와 블랙박스 영상 데이터를 생산하고 블록체인 네트워크에 제공하는 주체가 되는 데이터 소유자 노드; 차량 데이터와 블랙박스 영상 데이터를 요구하는 개체로, 마켓플레이스 플랫폼 장치에서 필요한 데이터를 검색하고 접근 수단을 제출하여 데이터에 접근하는 데이터 소비자 노드; 데이터 소유자 노드와 데이터 소비자 노드를 연결하고 데이터와 자금의 거래를 위한 서비스 제공을 하고, 데이터 소유자 노드의 데이터 등록, 데이터 소비자 노드의 데이터 검색과 구매를 지원하는 데이터 거래 플랫폼 역할을 하는 마켓플레이스 플랫폼 장치;를 포함하고, 데이터 소비자 노드가 데이터를 구매하면, 데이터 소유자 노드는 보안 채널을 통해 암호화된 원본 데이터의 위치와 키값을 전달하고, 마켓플레이스 플랫폼은 오프체인 거래를 위한 보안 채널을 지원하는 것이다.

(52) CPC특허분류

G06Q 50/30 (2015.01)
G07C 5/0866 (2013.01)
H04L 67/1097 (2022.05)
H04L 9/0643 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/0827 (2013.01)
H04L 9/50 (2022.05)
H04L 2209/84 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1345312936
과제번호	2019R1I1A3A01060652
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	이공학학술연구기반구축(R&D)
연구과제명	블록체인을 이용한 커넥티드 카 서비스 보안기술 연구
기 여 율	1/1
과제수행기관명	부경대학교
연구기간	2020.03.01 ~ 2021.02.28

명세서

청구범위

청구항 1

데이터에 접근하는 개체를 직접 정의하고, 차량 데이터와 블랙박스 영상 데이터를 생산하고 블록체인 네트워크에 제공하는 주체가 되는 데이터 소유자 노드;

차량 데이터와 블랙박스 영상 데이터를 요구하는 개체로, 마켓플레이스 플랫폼 장치에서 필요한 데이터를 검색하고 접근 수단을 제출하여 데이터에 접근하는 데이터 소비자 노드;

데이터 소유자 노드와 데이터 소비자 노드를 연결하고 데이터와 자금의 거래를 위한 서비스 제공을 하고, 데이터 소유자의 데이터 등록, 데이터 소비자의 데이터 검색과 구매를 지원하는 데이터 거래 플랫폼 역할을 하는 마켓플레이스 플랫폼 장치;를 포함하고,

데이터 소비자 노드가 데이터를 구매하면, 데이터 소유자 노드는 보안 채널을 통해 암호화된 원본 데이터의 위치와 키값을 전달하고, 마켓플레이스 플랫폼 장치는 오프체인 거래를 위한 보안 채널을 지원하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 2

제 1 항에 있어서, 데이터 구매 거래시에,

데이터 소비자 노드는 데이터 소유자가 관리하는 접근 제어목록에 등록되어 있어야 하고, 데이터 소유자 노드가 사전 정의한 설정값에 따른 시간 또는 조건 동안에만 데이터의 접근이 허가되는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 3

제 1 항에 있어서, 데이터 소유자 노드가 되는 커넥티드 카의 게이트웨이는,

차량과 블랙박스에서 생성된 데이터를 수집하여 전처리하여 마켓플레이스 플랫폼 장치로 전송하고,

마켓플레이스 플랫폼 장치는 원본 데이터와 메타데이터를 분리하여 외부 스토리지와 블록체인으로 나누어 데이터를 저장하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 4

제 1 항에 있어서, 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위하여,

블록체인 네트워크에 참여하는 개체를 인증하고 제한할 수 있는 컨소시엄 블록체인을 채택하고,

컨소시엄은 차량사고 수사관, 법 집행 기관, 차량 보험사, 차량 유지보수 업체, 차량 제조업체, 이동 통신사를 포함한 데이터 소비자 노드에 의해 구성되며,

데이터 소유자 노드인 차량 블랙박스 소유자 및 차량 소유자는 블록체인 시스템에서 클라이언트로 참여하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 5

제 1 항에 있어서, 블록체인에 저장되는 데이터는 트랜잭션 단위로 생성되고, 이러한 트랜잭션을 모아서 블록으로 만들어 체인에 연결하고,

트랜잭션은 트랜잭션 헤더와 바디로 구성되는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 6

제 5 항에 있어서, 트랜잭션의 헤더에는 트랜잭션 식별자, 전송 금액, 디지털 서명, 수신자의 공개키 해시값 및

유형값 항목이 포함되고,

유형값을 통해 해당 트랜잭션이 DO-ABE와 관련된 트랜잭션인지 커넥티드 카와 관련된 트랜잭션인지 구분하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 7

제 5 항에 있어서, 트랜잭션 바디에는 차량 관련 데이터, 블랙박스 영상 관련 데이터, DO-ABE를 위한 데이터가 포함되는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 8

제 7 항에 있어서, 차량 관련 트랜잭션은 차량 내부에 있는 게이트웨이로부터 생성되고,

엣지 컴퓨팅(edge computing)이 가능한 차량 게이트웨이는 차량 내부의 각종 센서 및 컨트롤러와 블랙박스로부터 데이터를 수신하여 블록체인 네트워크로 데이터를 전송하기 위한 전처리 작업을 수행하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 9

제 7 항에 있어서, 트랜잭션에 포함되는 데이터의 종류는,

사전 정의된 조건에 의해 발생한 EDR 데이터, BSM, 차종, 차량 정보 등이 포함된 차량 관련 데이터와,

영상 시간, 출발 장소 및 도착 장소가 포함된 이동 경로, 영상의 크기, 그 외에 운행 정보가 포함된 블랙박스 영상 관련 데이터를 포함하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 10

제 5 항에 있어서, 블록은 헤더와 바디로 구성되고,

블록 바디에는 트랜잭션의 목록이 포함되고, 블록 헤더에는 트랜잭션 목록의 해시값, 이전 블록의 해시값, 타임스탬프, 버전값이 포함되는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 11

제 1 항에 있어서, 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위하여,

데이터 소유자 노드가 ACL을 등록하고 제어하는 기능, 새로운 데이터 세트의 구성, 데이터 거래에 필요한 프로세스를 포함하는 블록체인 상에서 이뤄지는 기능들의 강제성을 부여하기 위해 스마트 계약을 이용하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 12

제 11 항에 있어서, 스마트 계약 함수는,

데이터 소유자 노드가 데이터를 생성하고 블록체인에 저장하는 함수인 CreateData를 포함하고,

CreateData는 데이터 소유자 노드만 실행할 수 있는 함수로써 데이터 소유자 노드의 ID와 블록체인에 저장할 데이터를 매개 변수로 입력받고, 함수를 실행한 개체가 데이터 소유자 노드인지, 그리고 매개 변수의 개수와 포맷이 일치하는지 확인하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 13

제 12 항에 있어서, 포맷은 차량 게이트웨이에서 전처리한 데이터 포맷과 스마트 계약에서 정의한 포맷을 의미하고,

함수 실행 주체가 데이터 소유자 노드이고 저장할 데이터 또한 올바른 데이터임을 확인했다면 이를 블록체인에 저장하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 14

제 11 항에 있어서, 스마트 계약 함수는,

데이터 소비자 노드가 필요로 하는 데이터에 접근하고 획득하는 PurchaseData 함수를 포함하고,

PurchaseData는 데이터 소비자 노드의 ID와 구매할 데이터의 ID를 매개 변수로 입력받고, 데이터 소비자 노드의 ID를 통해 올바른 사용자인지 확인하고 데이터 소비자 노드는 구매할 데이터의 가격만큼 데이터 소유자 노드에 게 자산을 지불하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 15

제 14 항에 있어서, 자산의 입금을 확인한 데이터 소유자 노드는 본인이 관리하는 ACL에 해당 데이터 소비자 노드를 등록하고,

다시 데이터 소비자 노드의 ID와 데이터 소유자 노드가 보유하고 있는 ACL의 비교를 통해 소유자가 허가한 사용자인지 확인하여,

접근 권한이 없거나 적절하지 않으면 접근은 거부되고, 접근이 허가된 사용자의 경우에는 데이터 소유자 노드는 오프체인 프라이빗 컨트랙트를 통해 원본 데이터의 위치와 키값을 전달하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 16

제 11 항에 있어서, 스마트 계약 함수는,

데이터 소비자 노드의 요청에 대한 수신과 데이터 소유자 노드의 ACL 관리 기능을 하는 HandlingACL 함수를 포함하고,

HandlingACL은 RequestACL을 통해 수신된 요청을 토대로 자산의 입금을 확인하고 데이터 소유자 노드의 ACL에 해당 소비자를 등록하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 17

제 11 항에 있어서, 스마트 계약 함수는,

DeleteData는 등록한 데이터를 삭제하는 함수를 포함하고,

DeleteData 함수는 데이터의 키값으로 원장을 조회한 후 삭제했다는 트랜잭션을 생성하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치.

청구항 18

블록체인 기반 DO-ABE를 이용한 데이터 공유 및 거래 프로세스가,

신뢰 기관이 존재하는 컨소시엄 형 블록체인을 채택하고, 모든 참여자가 시스템에 참여하기 전에 신뢰 기관에 등록되도록 하는 시스템 설정 단계;

데이터 소유자 노드가 메타데이터를 커넥티드 카 트랜잭션을 통해 블록체인에 저장하고, 외부 스토리지에 암호화된 원본 데이터를 저장하는 콘텐츠 등록 및 업로드 단계;

데이터 소비자 노드가 데이터의 위치 정보나 시간 정보를 토대로 마켓플레이스 플랫폼 장치에서 원하는 데이터를 검색하고 해당 데이터의 메타데이터를 획득할 수 있도록 하는 콘텐츠 접근 및 다운로드 단계;를 포함하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 방법.

청구항 19

제 18 항에 있어서, DO-ABE와 관련된 데이터 중 공개 파라미터, 전체 속성들의 집합, 공개키, 콘텐츠의 식별자 및 암호화된 콘텐츠의 해시값을 블록체인에 공개하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 방법.

청구항 20

제 18 항에 있어서, 데이터 소유자 노드는 스마트 계약을 통해 거래가 완료된 소비자의 고유 식별자(UID, User

ID)를 ACL에 정의하고, 이를 암호화한 뒤에 블록체인 트랜잭션에 게시하고,

데이터 소비자 노드는 스마트 계약으로 ACL이 허용하는 경우에만 데이터에 접근하고 처리할 수 있는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 방법.

청구항 21

제 18 항에 있어서, 시스템 설정 단계에서,

각 참여자는 신뢰 기관으로부터 UID와 공개/개인키 쌍을 할당받고, 블록의 합의 및 검증에 참여하는 노드는 채택된 합의 메커니즘을 기반으로 선별되고,

각 데이터 소유자 노드는 Setup 함수를 이용하여 DO-ABE 공개 매개 변수를 생성하고, 이를 DO-ABE 트랜잭션을 통해 블록체인에 저장하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 방법.

청구항 22

제 18 항에 있어서, 콘텐츠 등록 및 업로드 단계에서,

데이터 소유자 노드는 KeyGen 함수를 이용하여 마스터 비밀키 $MSK = g^{\beta}$ 와 공개키 $PK = (e(g, g)^{\beta}, g^{\alpha})$ 를 계산하고, 생성된 공개키 PK는 DO-ABE 트랜잭션을 통해 블록체인에 저장하는 단계와,

암호화된 원본 데이터 EF는 임의로 생성된 대칭키 sk_F 로 원본 데이터 F를 암호화하여 생성 $(EF = SymEnc(F, sk_F))$ 하는 단계와,

접근 구조 ST를 정의하고 대칭키 sk_F 와 Encrypt 함수를 사용하여 암호문 CT를 계산 $(CT = Enc(PK, ST, sk_F))$ 하는 단계와,

소유자의 식별자 UID, 원본 데이터의 식별자 Fid , 암호화된 데이터의 해시값 $H(EF)$ 를 포함한 메타데이터는 커넥티드 카 트랜잭션을 통해 블록체인에 저장하고, (Fid, EF, CT) 는 외부(오프체인) 스토리지에 저장하는 단계;를 포함하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 방법.

청구항 23

제 18 항에 있어서, 콘텐츠 접근 및 다운로드 단계에서,

접근 속성 집합 S를 보유한 데이터 소비자 노드는 데이터 소유자 노드에게 오프체인 프라이빗 컨트랙트를 통해 원본 데이터에 접근하기 위한 비밀키 SK의 생성을 요청하는 단계와,

데이터 소유자 노드는 KeyGen 함수를 이용하여 데이터 소비자 노드의 속성 비밀키 $SK(K = g^{\beta} g^{\alpha t}, L = g^t, \forall x \in S, K_x = h_x^t)$ 을 생성하고 이 SK와 원본 데이터의 저장 위치 $H(F)$ 를 오프체인 프라이빗 컨트랙트에 의해 안전하게 전달하는 단계와,

데이터 소비자 노드는 저장 위치 $H(F)$ 에 저장된 암호화된 원본 데이터 (Fid, EF, CT) 를 획득하고 $sk_F = Dec(CT, SK)$ 를 계산하는 단계와,

데이터 소비자 노드는 대칭키 sk_F 를 복호화하여 원본 데이터 F를 얻고, 거래가 성공적으로 완료되면 블록체인에 기록되는 단계;를 포함하는 것을 특징으로 하는 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 방법.

발명의 설명

기술분야

[0001] 본 발명은 커넥티드 카 데이터 처리에 관한 것으로, 구체적으로 DO-ABE(data-owner-based attribute-based encryption) 암호화 체계를 블록체인 환경에서 동작할 수 있도록 재구성하고 이를 이용하여 커넥티드 카의 중요 데이터를 안전하고 효율적으로 공유하고 거래할 수 있도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법에 관한 것이다.

배경기술

[0002] 커넥티드 카는 V2X(Vehicle to Everything) 기술을 기반으로 차량, 사물을 포함한 모든 기기, 공간, 인프라와 네트워크로 연결된 차량을 의미한다.

[0003] 이는 운전자 없이 주행하는 자율주행 자동차, 그리고 지능적인 서비스를 제공하는 스마트카를 초월하는 개념이다. 온전한 커넥티드 카 서비스를 구축하기 위해서는 고성능 컴퓨팅 능력과 강력한 사이버 보안, 그리고 방대한 데이터를 관리할 수 있는 능력이 필요하다.

[0004] 커넥티드 카는 차량에 부착된 각종 센서나 다른 차량과 상호작용하여 자동 충돌 알림, 과속 및 안전 경고 알림 등의 자동적인 주행 조작이 가능하다. 뿐만 아니라 커넥티드 카에는 무선 통신 모듈이 장착되어 있어 개인 클라우드 서버나 외부 오라클 서버에 접속하는 등의 인터넷 활동도 가능하다.

[0005] 커넥티드 카에서 생성되는 데이터에는 차량의 각종 센서 데이터, 인포테인먼트(infortainment)를 위한 데이터, 텔레매틱스(telematics)를 위한 데이터, GPS(Global Positioning System) 데이터, 주변 차량이나 신호등과 같은 인프라와 통신을 위한 데이터, 자율주행 데이터 등 커넥티드 카에서 수집할 수 있는 데이터의 종류와 수는 무궁무진하다. 최근에는 많은 차량 제조업체와 IT 기업에서 커넥티드 카에서 수집된 데이터를 통한 수익화 방안을 연구개발하고 있다.

[0006] 해커나 악성코드가 운전 제어 장치나 각 차량에 사용되는 데이터에 접근할 수 없도록 차량을 보호하는 것이 중요하다. 커넥티드 카에서 생성되는 데이터에는 개인정보와 같은 민감한 데이터가 다수 포함되어 있다.

[0007] 특히 운행 영상 데이터(블랙박스 영상 데이터)는 사생활이 침해될 우려가 있는 데이터가 존재한다. 또한, 자율주행과 관련된 데이터는 악의적인 공격이나 오류로부터 보호되어야 한다. 자율주행 시스템이 공격이나 오류로 인해 주행 제어권을 잃는다면 심각한 사고로 이어질 수 있기 때문이다.

[0008] 그러나 오늘날 일반적으로 사용되는 차량 보안 기술은 커넥티드 카의 빠른 네트워크 환경과 복잡한 시스템에 적합하지 않다.

[0009] 도 1은 서버-클라이언트 구조의 차량 데이터 관리 방식을 나타낸 구성도이다.

[0010] 도 1에서와 같이, 현재 차량 데이터를 처리하고 관리하는 방식은 중앙집중 형태의 서버-클라이언트 구조이다.

[0011] 차량에서 수집된 데이터는 차량 제조사의 서버(클라우드)로 전송되고 저장된다. 수많은 개인정보와 민감정보가 한 곳에 저장되는데, 이러한 중앙 집중화된 데이터 관리는 공격 및 오류 등 내외부의 다양한 요인으로 인해 가용성이 훼손될 수 있는 단일 실패 지점 문제를 내포하며 성능 병목 현상을 일으킬 수 있다.

[0012] 또한, 현재 차량 보안 아키텍처의 대부분은 사용자의 개인정보를 고려하지 않으며 데이터 소유자는 아웃소싱된 데이터를 직접 제어할 수 없는 구조이기 때문에 데이터 저장과 관리에 있어서 제3자를 신뢰할 수밖에 없다.

[0013] 따라서, 커넥티드 카 데이터를 중앙 신뢰기관 없이 안전하게 관리할 수 있도록 무결성, 불변성, 추적성, 안전성과 같은 특성을 이용하는 커넥티드 카 데이터 관리를 위한 새로운 기술의 개발이 요구되고 있다.

선행기술문헌

특허문헌

[0014] (특허문헌 0001) 대한민국 공개특허 제10-2019-0057881호

(특허문헌 0002) 대한민국 공개특허 제10-2020-0068776호

(특허문헌 0003) 대한민국 등록특허 제10-1974345호

발명의 내용

해결하려는 과제

- [0015] 본 발명은 종래 기술의 커넥티드 카 데이터 관리 기술의 문제점을 해결하기 위한 것으로, 커넥티드 카의 빠른 네트워크 환경과 복잡한 시스템에 유용하게 적용할 수 있는 차량 보안 기술을 적용하는 것에 의해 커넥티드 카 데이터 관리가 가능하도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법을 제공하는 데 그 목적이 있다.
- [0016] 본 발명은 DO-ABE(data-owner-based attribute-based encryption) 암호화 체계를 블록체인 환경에서 동작할 수 있도록 재구성하고 이를 이용하여 커넥티드 카의 중요 데이터를 안전하고 효율적으로 공유하고 거래할 수 있도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법을 제공하는데 그 목적이 있다.
- [0017] 본 발명은 허가형 컨소시엄 블록체인을 채택하여 대용량 및 프라이버시에 민감한 블랙박스 영상 데이터의 접근을 허가된 참여자로 제한하여 안전한 데이터 저장과 프라이버시를 보호할 수 있도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법을 제공하는데 그 목적이 있다.
- [0018] 본 발명은 블록체인의 기본 속성인 무결성과 추적성으로 인해 이를 기반으로 하여 개발된 DApp(Decentralized Application)을 통해 누구나 검증 가능하도록 하여 데이터에 대한 신뢰성을 보장할 수 있도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법을 제공하는데 그 목적이 있다.
- [0019] 본 발명은 스마트 계약에 의해 보호되는 데이터 소유자 정의 접근 제어 목록과 데이터 소유자 기반의 속성 기반 암호화를 사용하여 데이터 소유자의 데이터 소유권을 주장하고 데이터를 제어하는 등 데이터 주권을 확보할 수 있도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법을 제공하는데 그 목적이 있다.
- [0020] 본 발명은 커넥티드 카 데이터를 안전하게 거래하고 공유하여 차량 사고 수사관은 무결성과 신뢰성이 보장된 데이터를 증거로 사용할 수 있으며 사고 원인을 빠르고 정확하게 분석할 수 있도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법을 제공하는데 그 목적이 있다.
- [0021] 본 발명은 차량 보험사, 유지보수 업체, 차량 제조업체, 이동 통신사를 비롯한 관련 서비스 업체들이 블록체인 기반으로 저장되는 차량 운행 정보와 차량 정보를 토대로 보험비, 수리비, 통신비 등 각종 서비스에 대한 가격을 정확하게 책정하고 사용자 맞춤형 서비스를 고품질로 제공할 수 있도록 한 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법을 제공하는데 그 목적이 있다.
- [0022] 본 발명의 다른 목적들은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0023] 상기와 같은 목적을 달성하기 위한 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치는 데이터에 접근하는 개체를 직접 정의하고, 차량 데이터와 블랙박스 영상 데이터를 생산하고 블록체인 네트워크에 제공하는 주체가 되는 데이터 소유자 노드; 차량 데이터와 블랙박스 영상 데이터를 요구하는 개체로, 마켓플레이스 플랫폼 장치에서 필요한 데이터를 검색하고 접근 수단을 제출하여 데이터에 접근하는 데이터 소비자 노드; 데이터 소유자 노드와 데이터 소비자 노드를 연결하고 데이터와 자금의 거래를 위한 서비스 제공을 하고, 데이터 소유자의 데이터 등록, 데이터 소비자의 데이터 검색과 구매를 지원하는 데이터 거래 플랫폼 역할을 하는 마켓플레이스 플랫폼 장치;를 포함하고, 데이터 소비자 노드에서 데이터를 구매하면, 데이터 소유자 노드는 보안 채널을 통해 암호화된 원본 데이터의 위치와 키값을 전달하고, 마켓플레이스 플랫폼 장치는 오프체인 거래를 위한 보안 채널을 지원하는 것을 특징으로 한다.
- [0024] 여기서, 데이터 구매 거래시에, 데이터 소비자 노드는 데이터 소유자 노드가 관리하는 접근 제어목록에 등록되어 있어야 하고, 데이터 소유자 노드가 사전 정의한 설정값에 따른 시간 또는 조건 동안에만 데이터의 접근이 허가되는 것을 특징으로 한다.
- [0025] 그리고 데이터 소유자 노드가 되는 커넥티드 카의 게이트웨이는, 차량과 블랙박스에서 생성된 데이터를 수집하

여 전처리하여 마켓플레이스 플랫폼 장치로 전송하고, 마켓플레이스 플랫폼 장치는 원본 데이터와 메타데이터를 분리하여 외부 스토리지와 블록체인으로 나누어 데이터를 저장하는 것을 특징으로 한다.

[0026] 그리고 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위하여, 블록체인 네트워크에 참여하는 개체를 인증하고 제한할 수 있는 컨소시엄 블록체인을 채택하고, 컨소시엄은 차량사고 수사관, 법 집행 기관, 차량 보험사, 차량 유지보수 업체, 차량 제조업체, 이동 통신사를 포함한 데이터 소비자에 의해 구성되며, 데이터 소유자인 차량 블랙박스 소유자 및 차량 소유자는 블록체인 시스템에서 클라이언트로 참여하는 것을 특징으로 한다.

[0027] 그리고 블록체인에 저장되는 데이터는 트랜잭션 단위로 생성되고, 이러한 트랜잭션을 모아서 블록으로 만들어 체인에 연결하고, 트랜잭션은 트랜잭션 헤더와 바디로 구성되는 것을 특징으로 한다.

[0028] 그리고 트랜잭션의 헤더에는 트랜잭션 식별자, 전송 금액, 디지털 서명, 수신자의 공개키 해시값 및 유형값 항목이 포함되고, 유형값을 통해 해당 트랜잭션이 DO-ABE와 관련된 트랜잭션인지 커넥티드 카와 관련된 트랜잭션인지 구분하는 것을 특징으로 한다.

[0029] 그리고 트랜잭션 바디에는 차량 관련 데이터, 블랙박스 영상 관련 데이터, DO-ABE를 위한 데이터가 포함되는 것을 특징으로 한다.

[0030] 그리고 차량 관련 트랜잭션은 차량 내부에 있는 게이트웨이로부터 생성되고, 엣지 컴퓨팅(edge computing)이 가능한 차량 게이트웨이는 차량 내부의 각종 센서 및 컨트롤러와 블랙박스로부터 데이터를 수신하여 블록체인 네트워크로 데이터를 전송하기 위한 전처리 작업을 수행하는 것을 특징으로 한다.

[0031] 그리고 트랜잭션에 포함되는 데이터의 종류는, 사전 정의된 조건에 의해 발생한 EDR 데이터, BSM, 차종, 차량 정보 등이 포함된 차량 관련 데이터와, 영상 시간, 출발 장소 및 도착 장소가 포함된 이동 경로, 영상의 크기, 그 외에 운행 정보가 포함된 블랙박스 영상 관련 데이터를 포함하는 것을 특징으로 한다.

[0032] 그리고 블록은 헤더와 바디로 구성되고, 블록 바디에는 트랜잭션의 목록이 포함되고, 블록 헤더에는 트랜잭션 목록의 해시값, 이전 블록의 해시값, 타임스탬프, 버전값이 포함되는 것을 특징으로 한다.

[0033] 그리고 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위하여, 데이터 소유자가 ACL을 등록하고 제어하는 기능, 새로운 데이터 세트의 구성, 데이터 거래에 필요한 프로세스를 포함하는 블록체인 상에서 이뤄지는 기능들의 강제성을 부여하기 위해 스마트 계약을 이용하는 것을 특징으로 한다.

[0034] 그리고 스마트 계약 함수는, 데이터 소유자 노드가 데이터를 생성하고 블록체인에 저장하는 함수인 CreateData를 포함하고, CreateData는 데이터 소유자 노드만 실행할 수 있는 함수로써 데이터 소유자 노드의 ID와 블록체인에 저장할 데이터를 매개 변수로 입력받고, 함수를 실행한 개체가 데이터 소유자 노드인지, 그리고 매개 변수의 개수와 포맷이 일치하는지 확인하는 것을 특징으로 한다.

[0035] 그리고 포맷은 차량 게이트웨이에서 전처리한 데이터 포맷과 스마트 계약에서 정의한 포맷을 의미하고, 함수 실행 주체가 데이터 소유자 노드이고 저장할 데이터 또한 올바른 데이터임을 확인했다면 이를 블록체인에 저장하는 것을 특징으로 한다.

[0036] 그리고 스마트 계약 함수는, 데이터 소비자 노드가 필요로 하는 데이터에 접근하고 획득하는 PurchaseData 함수를 포함하고, PurchaseData는 데이터 소비자 노드의 ID와 구매할 데이터의 ID를 매개 변수로 입력받고, 데이터 소비자 노드의 ID를 통해 올바른 사용자인지 확인하고 데이터 소비자 노드는 구매할 데이터의 가격만큼 데이터 소유자 노드에게 자산을 지불하는 것을 특징으로 한다.

[0037] 그리고 자산의 입금을 확인한 데이터 소유자 노드는 본인이 관리하는 ACL에 해당 데이터 소비자를 등록하고, 다시 데이터 소비자 노드의 ID와 데이터 소유자 노드가 보유하고 있는 ACL의 비교를 통해 소유자가 허가한 사용자인지 확인하여, 접근 권한이 없거나 적절하지 않으면 접근은 거부되고, 접근이 허가된 사용자의 경우에는 데이터 소유자 노드는 오프체인 프라이빗 컨트랙트를 통해 원본 데이터의 위치와 키값을 전달하는 것을 특징으로 한다.

[0038] 그리고 스마트 계약 함수는, 데이터 소비자 노드의 요청에 대한 수신과 데이터 소유자 노드의 ACL 관리 기능을 하는 HandlingACL 함수를 포함하고, HandlingACL은 RequestACL을 통해 수신된 요청을 토대로 자산의 입금을 확인하고 데이터 소유자 노드의 ACL에 해당 소비자를 등록하는 것을 특징으로 한다.

[0039] 그리고 스마트 계약 함수는, DeleteData는 등록된 데이터를 삭제하는 함수를 포함하고, DeleteData 함수는 데이터의 키값으로 원장을 조회한 후 삭제했다는 트랜잭션을 생성하는 것을 특징으로 한다.

- [0040] 다른 목적을 달성하기 위한 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 방법은 블록체인 기반 DO-ABE를 이용한 데이터 공유 및 거래 프로세스가, 신뢰 기관이 존재하는 컨소시엄 형 블록체인을 채택하고, 모든 참여자가 시스템에 참여하기 전에 신뢰 기관에 등록되도록 하는 시스템 설정 단계; 데이터 소유자 노드가 메타데이터를 커넥티드 카 트랜잭션을 통해 블록체인에 저장하고, 외부 스토리지에 암호화된 원본 데이터를 저장하는 콘텐츠 등록 및 업로드 단계; 데이터 소비자 노드가 데이터의 위치 정보나 시간 정보를 토대로 마켓플레이스 플랫폼 장치에서 원하는 데이터를 검색하고 해당 데이터의 메타데이터를 획득할 수 있도록 하는 콘텐츠 접근 및 다운로드 단계;를 포함하는 것을 특징으로 한다.
- [0041] 여기서, DO-ABE와 관련된 데이터 중 공개 파라미터, 전체 속성들의 집합, 공개키, 콘텐츠의 식별자 및 암호화된 콘텐츠의 해시값을 블록체인에 공개하는 것을 특징으로 한다.
- [0042] 그리고 데이터 소유자 노드는 스마트 계약을 통해 거래가 완료된 소비자 노드의 고유 식별자(UID, User ID)를 ACL에 정의하고, 이를 암호화한 뒤에 블록체인 트랜잭션에 게시하고, 데이터 소비자 노드는 스마트 계약으로 ACL이 허용하는 경우에만 데이터에 접근하고 처리할 수 있는 것을 특징으로 한다.
- [0043] 그리고 시스템 설정 단계에서, 각 참여자는 신뢰 기관으로부터 UID와 공개/개인키 쌍을 할당받고, 블록의 합의 및 검증에 참여하는 노드는 채택된 합의 메커니즘을 기반으로 선별되고, 각 데이터 소유자 노드는 Setup 함수를 이용하여 DO-ABE 공개 매개 변수를 생성하고, 이를 DO-ABE 트랜잭션을 통해 블록체인에 저장하는 것을 특징으로 한다.
- [0044] 그리고 콘텐츠 등록 및 업로드 단계에서, 데이터 소유자 노드는 KeyGen 함수를 이용하여 마스터 비밀키 $MSK = g^{\beta}$ 와 공개키 $PK = (e(g, g)^{\beta}, g^{\alpha})$ 를 계산하고, 생성된 공개키 PK는 DO-ABE 트랜잭션을 통해 블록체인에 저장하는 단계와, 암호화된 원본 데이터 EF는 임의로 생성된 대칭키 sk_F 로 원본 데이터 F를 암호화하여 생성 $(EF = SymEnc(F, sk_F))$ 하는 단계와, 접근 구조 ST를 정의하고 대칭키 sk_F 와 Encrypt 함수를 사용하여 암호문 CT를 계산 $(CT = Enc(PK, ST, sk_F))$ 하는 단계와, 소유자의 식별자 UID, 원본 데이터의 식별자 Fid , 암호화된 데이터의 해시값 $H(EF)$ 를 포함한 메타데이터는 커넥티드 카 트랜잭션을 통해 블록체인에 저장하고, (Fid, EF, CT) 는 외부(오프체인) 스토리지에 저장하는 단계;를 포함하는 것을 특징으로 한다.
- [0045] 그리고 콘텐츠 접근 및 다운로드 단계에서, 접근 속성 집합 S를 보유한 데이터 소비자 노드는 데이터 소유자 노드에게 오프체인 프라이빗 컨트랙트를 통해 원본 데이터에 접근하기 위한 비밀키 SK의 생성을 요청하는 단계와, 데이터 소유자 노드는 KeyGen 함수를 이용하여 데이터 소비자 노드의 속성 비밀키 $SK(K = g^{\beta} g^{\alpha t}, L = g^t, \forall x \in S, K_x = h_x^t)$ 을 생성하고 이 SK와 원본 데이터의 저장 위치 $H(F)$ 를 오프체인 프라이빗 컨트랙트에 의해 안전하게 전달하는 단계와, 데이터 소비자 노드는 저장 위치 $H(F)$ 에 저장된 암호화된 원본 데이터 (Fid, EF, CT) 를 획득하고 $sk_F = Dec(CT, SK)$ 를 계산하는 단계와, 데이터 소비자 노드는 대칭키 sk_F 를 복호화하여 원본 데이터 F를 얻고, 거래가 성공적으로 완료되면 블록체인에 기록되는 단계;를 포함하는 것을 특징으로 한다.

발명의 효과

- [0046] 이상에서 설명한 바와 같은 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법은 다음과 같은 효과가 있다.
- [0047] 첫째, 커넥티드 카의 빠른 네트워크 환경과 복잡한 시스템에 유용하게 적용할 수 있는 차량 보안 기술을 적용하는 것에 의해 커넥티드 카 데이터 관리가 가능하도록 한다.
- [0048] 둘째, DO-ABE(data-owner-based attribute-based encryption) 암호화 체계를 블록체인 환경에서 동작할 수 있도록 재구성하고 이를 이용하여 커넥티드 카의 중요 데이터를 안전하고 효율적으로 공유하고 거래할 수 있도록 한다.

- [0049] 셋째, 허가형 컨소시엄 블록체인을 채택하여 대용량 및 프라이버시에 민감한 블랙박스 영상 데이터의 접근을 허가된 참여자로 제한하여 안전한 데이터 저장과 프라이버시를 보호할 수 있도록 한다.
- [0050] 넷째, 블록체인의 기본 속성인 무결성과 추적성으로 인해 이를 기반으로 하여 개발된 DApp(Decentralized Application)을 통해 누구나 검증 가능하도록 하여 데이터에 대한 신뢰성을 보장할 수 있도록 한다.
- [0051] 다섯째, 스마트 계약에 의해 보호되는 데이터 소유자 정의 접근 제어 목록과 데이터 소유자 기반의 속성 기반 암호화를 사용하여 데이터 소유자의 데이터 소유권을 주장하고 데이터를 제어하는 등 데이터 주권을 확보할 수 있도록 한다.
- [0052] 여섯째, 커넥티드 카 데이터를 안전하게 거래하고 공유하여 차량 사고 수사관은 무결성과 신뢰성이 보장된 데이터를 증거로 사용할 수 있으며 사고 원인을 빠르고 정확하게 분석할 수 있도록 한다.
- [0053] 일곱째, 차량 보험사, 유지보수 업체, 차량 제조업체, 이동 통신사를 비롯한 관련 서비스 업체들이 블록체인 기반으로 저장되는 차량 운행 정보와 차량 정보를 토대로 보험비, 수리비, 통신비 등 각종 서비스에 대한 가격을 정확하게 책정하고 사용자 맞춤형 서비스를 고품질로 제공할 수 있도록 한다.

도면의 간단한 설명

- [0054] 도 1은 서버-클라이언트 구조의 차량 데이터 관리 방식을 나타낸 구성도
- 도 2는 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치의 전체 구성도
- 도 3은 본 발명에 따른 마켓 플레이스 플랫폼(CMarket) 장치의 상세 구성도
- 도 4는 본 발명에 적용되는 블록 체인 구조를 나타낸 구성도
- 도 5는 본 발명에 따른 블록 및 트랜잭션 구조도
- 도 6a 내지 도 6d는 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치에서 사용하는 스마트 계약 함수의 예를 나타낸 구성도
- 도 7은 블록체인 기반 DO-ABE를 이용한 데이터 공유 및 거래 프로세스를 나타낸 동작 흐름도

발명을 실시하기 위한 구체적인 내용

- [0055] 이하, 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법의 바람직한 실시 예에 관하여 상세히 설명하면 다음과 같다.
- [0056] 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법의 특징 및 이점들은 이하에서의 각 실시 예에 대한 상세한 설명을 통해 명백해질 것이다.
- [0057] 도 2는 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치의 전체 구성도이다.
- [0058] 본 발명은 DO-ABE(data-owner-based attribute-based encryption) 암호화 체계를 블록체인 환경에서 동작할 수 있도록 재구성하고 이를 이용하여 커넥티드 카의 중요 데이터를 안전하고 효율적으로 공유하고 거래할 수 있도록 한 것이다.
- [0059] 본 발명은 이와 같은 차량에서 블록체인 네트워크로 데이터 전송을 위하여 다음과 같은 특징적인 구성을 포함한다.
- [0060] 블록체인의 유형은 컨소시엄 블록체인이며 클라이언트 조직을 구성하는 각각의 노드들을 차량으로 가정한다.
- [0061] 블록체인 네트워크는 일반적으로 속도가 느리며 블록체인의 가용성을 최대화하기 위해 블록체인 네트워크 내에서의 트랜잭션을 최소화한다.
- [0062] 그리고 차량은 블록체인 네트워크의 구성원이기도 하지만 블록체인 네트워크에 데이터를 제공하는 주체이기도 하다. 따라서, 차량에서 블록체인 네트워크로의 데이터 이동 전 트랜잭션화 수행하고, 이를 위해 차량에는 엣지 컴퓨팅이 가능한 차량용 게이트웨이를 구비한다.
- [0063] 이와 같은 차량용 게이트웨이의 역할은 차량내 생성되는 데이터들을 수집후 블록체인 네트워크에 전송하는 데, 전송 전 트랜잭션화(=구조화) 진행하는 것이다.

- [0064] 여기서, 트랜잭션(=구조화)은 블록체인 네트워크에서 오더러가 트랜잭션을 모아 블록을 만들기 위한 포맷에 맞게, 즉 오더러가 (1)차량데이터들을 하나하나 모아 트랜잭션으로 만들고 또 (2)트랜잭션을 모아 블록으로 만드는 과정에서 (1)과정의 역할을 차량으로 위임한다.
- [0065] 이는 본 발명에서의 트랜잭션은 차량 정보, 운행 속도, 거리, 출발지, 도착지, 영상 길이, 충돌 유무 등등 관련 데이터들의 집합 자체이기 때문에 이러한 데이터를 분리해서 블록체인 네트워크에 전송할 수 없기 때문이다.
- [0066] 트랜잭션은 전처리 과정이자 원본데이터에서 메타데이터를 추출하는 과정으로 설명될 수 있다.
- [0067] 그리고 차량 데이터의 수집 구간 은 차량 시동 On-Off, Off-On 구간으로, 차량의 시동을 키고부터 끝때까지는 차량데이터와 운행데이터, 블랙박스 영상 데이터를 포함하고, 차량의 시동을 끄고부터 끝때까지는 차량데이터와 블랙박스 영상 데이터의 일부분을 포함한다.
- [0068] 차량용 게이트웨이는 이렇게 두 구간으로 구분하여 데이터를 실시간으로 수집하고 모든 전처리과정이 끝난 후 전송한다. 이후 시동이 켜지거나, 꺼질때 한 구간의 데이터를 모아서 트랜잭션화한 후 전송한다.
- [0069] 수집 도중 오류나 파손으로 인한 데이터 손실을 방지하기 위해 사용자가 지정한 단위 시간마다 차량용 게이트웨이는 백업 및 이어쓰기를 한다.
- [0070] 이를 위하여, 차량용 게이트웨이는 네트워크가 가능해야 하고, 엣지 컴퓨팅(트랜잭션화)을 위한 약간의 컴퓨팅 성능 및 백업을 위한 자체 스토리지를 갖는다.
- [0071] 그리고 차량용 게이트웨이에서 블록체인 네트워크로 데이터를 전송할 시 접근 권한, 인가 방법 등은 컨소시엄 블록체인의 MSP와 같은 신뢰개체에 의한 설정값에 기반한다.
- [0072] 블록체인은 영상데이터와 같이 대용량의 데이터를 저장하기에 적합한 구조가 아니므로 이러한 데이터들을 블록체인을 이용하여 저장하기 위해서는 오프체인 스토리지 기법을 사용한다. 따라서, 원본데이터는 오프체인(=외부 스토리지), 메타데이터는 블록체인에 DApp 을 거쳐서 저장한다.
- [0073] 차량 내부에서 차량 게이트웨이로 데이터가 전송되는 것은 유무선으로 이루어지고, 차량 게이트웨이에서 DApp으로 데이터를 전송하기 위한 통신 채널은 자율주행을 위한 통신채널과 분리한다.
- [0074] 본 발명에 적용되는 블록체인 기반 DO-ABE를 구체적으로 설명하면 다음과 같다.
- [0075] 속성 기반 암호화(ABE, Attributed-Based Encryption)는 사용자의 비밀키와 암호문이 속성에 의존하는 공개키 암호화 방법이다.
- [0076] ABE에서 사용자를 위한 비밀키 생성을 위해 PKG를 요구했던 것과는 달리, 본 발명에 적용되는 데이터 소유자 기반 ABE(DO-ABE, Data Owner based ABE)에서는 암호화에 사용되는 임의성을 사용하여 키를 생성한다.
- [0077] 따라서, 암호화된 콘텐츠에 대한 메시지 수준 기반의 세분화된 제어를 쉽게 달성할 수 있다.
- [0078] 그러나 이러한 DO-ABE 체계는 클라우드 스토리지와 같은 중앙화된 애플리케이션에 적합한 암호화이다. 이를 블록체인 환경에서 사용하기 위해 본 발명에서는 스토리지 기능을 블록체인과 외부 스토리지로 분산시키는 등의 적절한 재구성을 수행한다.
- [0079] 공개 허가형 블록체인(Public-Permissioned blockchain) 모델에 관하여 설명하면 다음과 같다.
- [0080] 공개 허가형 블록체인은 비트코인과 같은 공개 비허가형(Public-Permissionless) 블록체인과 프라이빗(Private-Permissioned) 블록체인의 사이에 위치하는 형태로, 컨소시엄(consortium) 블록체인 모델이다.
- [0081] 블록체인에 대한 접근 권한을 인가된 개체만이 새로운 데이터(또는 트랜잭션)을 블록체인에 기록(write)할 수 있으며, 반면에 블록체인에 기록된 데이터(또는 트랜잭션)에 대한 읽기(read) 권한은 모두에게 허가하는 형태이다.
- [0082] 참여 개체의 인증을 위한 멤버십 서비스를 필요로 하지만, 인가된 개체만이 블록체인에 쓰기 권한을 가지므로, 블록체인의 성능에서 이점이 있다.
- [0083] 본 발명에서는 블록체인 기반 DO-ABE를 이용한 데이터 공유 및 거래 방식과 블록체인 기반 차량 데이터 마켓플레이스 플랫폼 모델을 제안한다.
- [0084] 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법에서는 메타데이터를 블록

체인(온체인, On-chain)에 저장하고 암호화된 원본 데이터를 외부(오프체인, Off-Chain) 스토리지에 저장한다.

- [0085] 컨소시엄 블록체인을 채택하여 대용량 및 프라이버시에 민감한(privacy-sensitive) 블랙박스 영상 데이터를 안전하고 효율적으로 처리한다.
- [0086] 또한, 데이터 소유자는 블록체인 기반 DO-ABE 및 소유자 정의 접근 제어 목록(ACL, Access Control List)을 적용하여 자신의 데이터를 직접 제어할 수 있다.
- [0087] 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치는 도 2에서와 같이, 데이터 소유자 노드(100), 데이터 소비자 노드(300), 블록체인 네트워크 및 DApp(Decentralized Application)으로 구현된 마켓플레이스 플랫폼 장치(200), 외부 스토리지로 구성된다.
- [0088] 시스템 참여자, 즉 블록체인 네트워크에 가입하여 활동하는 개체는 크게 데이터 소유자 노드(100)와 데이터 소비자 노드(300)로 구분된다. 블록체인 네트워크의 한 피어는 데이터 소유자 또는 데이터 소비자가 될 수 있으며, 둘다 일 수도 있다.
- [0089] 데이터 소유자 노드(100)는 차량 데이터와 블랙박스 영상 데이터를 생산하고 블록체인 네트워크에 제공하는 주체이다. 데이터 소유자 노드는 본인이 소유한 데이터에 대해 직접 관리하고 제어할 수 있으며 소유권을 주장할 수 있다. 따라서 데이터에 접근하는 개체를 직접 정의할 수 있다.
- [0090] 데이터 소비자 노드(300)는 차량 데이터와 블랙박스 영상 데이터를 요구하는 개체로, 차량사고 수사관, 차량 유지보수 업체, 차량 보험 회사, 차량제조업체, 이동통신사 그리고 법 집행 기관을 포함한다. 데이터 소비자 노드는 DApp인 마켓플레이스 플랫폼에서 필요한 데이터를 검색하고 적절한 접근 수단을 제출하여 데이터에 접근할 수 있다.
- [0091] 거래가 이루어지면 데이터 소유자 노드(100)는 데이터 소비자 노드(300)에게 원본 데이터에 접근할 수 있는 저장 위치와 복호화 키를 전달한다. 이때, 데이터 소비자 노드(300)는 데이터 소유자 노드(100)가 관리하는 접근 제어목록에 등록되어 있어야 하고 데이터 소유자 노드(100)가 사전 정의한 설정값에 따른 시간 또는 조건 동안에만 데이터의 접근이 허가된다.
- [0092] 데이터 소유자 노드, 즉 클라이언트와 데이터 소비자 노드로 예를 든 여섯 개의 기관이 컨소시엄을 구성하고 블록체인 시스템에 참여한다. 조직을 구성하는 모든 피어는 동일한 원장을 가지고 있지만, 조직을 대표하는 소수의 피어만 트랜잭션을 모아 블록으로 만들고 어떤 블록을 체인으로 연결할지 합의한다.
- [0093] 도 3은 본 발명에 따른 마켓 플레이스 플랫폼(CMarket) 장치의 상세 구성도이다.
- [0094] 데이터 거래 플랫폼 장치는 데이터 소유자 노드(100)와 데이터 소비자 노드(300)를 연결하고 데이터와 자금의 거래를 위한 서비스 제공자이다.
- [0095] 즉, 블록체인 기반 커넥티드 카 데이터 공유 모델의 서비스 제공자인 마켓플레이스 플랫폼 장치(200)는 이하의 설명에서 'CMarket'으로 설명되고, 데이터 소유자 노드의 데이터 등록, 데이터 소비자 노드의 데이터 검색과 구매를 도와주는 분산 애플리케이션이다.
- [0096] CMarket은 중재자의 역할을 한다. 데이터 소비자 노드를 대신하여 계정 정보를 관리하고 데이터를 구매하며 접근하는 등의 거래 과정에서의 주요 기능을 포함한다.
- [0097] 데이터 소비자 노드가 적절한 결제수단을 통해 데이터를 구매하면, 데이터 소유자 노드(100)는 보안 채널을 통해 암호화된 원본 데이터의 위치와 키값을 전달하게 된다. 이때 CMarket은 이러한 오프체인 거래를 위한 보안 채널을 지원한다.
- [0098] 데이터와 자산을 거래하면서 CMarket을 신뢰해야 한다. 대부분의 DApp과 마찬가지로 CMarket도 오픈소스로 배포된다. 소스 코드가 오픈되어 있으므로 누구나 CMarket을 검증할 수 있다. 따라서 CMarket은 반신뢰적(semi-trust)인, 즉 정직하지만, 호기심이 많은(honest-but-curious) 개체라고 가정한다.
- [0099] 도 3은 CMarket의 구조와 거래의 흐름을 나타낸 것이다.
- [0100] 먼저, 커넥티드 카의 게이트웨이는 차량과 블랙박스에서 생성된 데이터를 수집하여 전처리한다.
- [0101] 이후 게이트웨이에서 5G 무선 통신 기술을 이용하여 CMarket에 전송되고, CMarket은 다시 원본 데이터와 메타데이터를 분리하여 외부 스토리지와 블록체인으로 데이터를 저장한다.

- [0102] CMarket은 가공된 차량 데이터와 블랙박스 영상 데이터를 수신한후 해당 데이터들을 관련 특성별로 분류하여 화면에 출력한다.
- [0103] 데이터 소비자 노드들은 가공되고 분류된 데이터들을 토대로 더욱 효율적인 검색 및 조작을 할 수 있다. 이후 데이터 소비자 노드는 CMarket을 이용하여 필요한 데이터를 구매하고 요청할 수 있게 된다.
- [0104] CMarket의 개발 및 구현을 위해 컨소시엄 블록체인을 위한 대표적인 플랫폼인 Hyperledger Fabric을 사용할 수 있고 이로 제한되지 않는다.
- [0105] 도 4는 본 발명에 적용되는 블록 체인 구조를 나타낸 구성도이다.
- [0106] 본 발명은 차량 데이터나 블랙박스 영상 데이터와 같은 사생활 침해가 우려되는 데이터를 다룬다. 또한, 차량사고 수사관, 법 집행기관, 차량 보험사 등 블록체인 네트워크에 참여하는 각 조직의 역할과 요구되는 데이터가 다르다.
- [0107] 따라서, 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치에서는 블록체인 네트워크에 참여하는 개체를 인증하고 제한할 수 있는 컨소시엄 블록체인을 채택한다.
- [0108] 컨소시엄은 차량사고 수사관, 법 집행 기관, 차량 보험사, 차량 유지보수 업체, 차량 제조업체, 이동 통신사를 포함한 데이터 소비자 노드에 의해 구성되며 데이터 소유자 노드 즉, 차량 블랙박스 소유자 및 차량 소유자는 블록체인 시스템에서 클라이언트로 참여한다.
- [0109] 도 4에서 예로 나타낸 바와 같이, 컨소시엄을 이루는 여섯 개의 조직은 수사그룹과 서비스 그룹으로 분류된다.
- [0110] 수사그룹에는 차량사고 수사관, 법집행 기관이 포함되며 차량사고의 수사를 위해 차량 데이터와 블랙박스 영상 데이터 등 블록체인에 저장된 모든 데이터가 요구된다.
- [0111] 서비스 그룹에는 차량 보험사, 차량 유지보수 업체, 차량 제조업체, 이동 통신사를 포함하며 수사그룹과는 달리 블랙박스 영상 데이터는 요구되지 않는다.
- [0112] 오직 차량 데이터와 운행 데이터를 가지고 운전자의 안전과 편의 서비스를 제공한다. 이렇게 그룹마다 요구되는 데이터가 다르고 이에 따라 관리와 처리 방법도 다르므로 하나의 블록체인 시스템에서 그룹별로 거래와 원장을 구분하여 사용한다.
- [0113] 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치의 블록체인 시스템에는 CA와 MSP가 존재한다. 이는 퍼블릭 블록체인의 이념과는 어긋나지만 컨소시엄 블록체인에서는 참여 개체를 인증하고 제한해야 하므로 허용되는 개념이다. MSP는 블록체인 네트워크에 인증 서비스를 제공하는 역할을 한다.
- [0114] 모든 참여자에게 해당하는 책임을 부여하고, 행위를 추적하는 책임성을 보장하며, 프라이버시 보호를 위해 트랜잭션 익명성 및 트랜잭션 비 연결성도 보장한다. 다시 말해 MSP는 블록체인 네트워크에 참여하는 피어노드의 신원, 역할, 소속, 권한을 관리하고 조직 구조를 설계하는 역할을 한다. CA는 MSP에서 암호화 인증을 위해 필요한 인증기관이며, 공개키 인증서 및 이에 대응하는 개인키를 발급한다.
- [0115] 차량 데이터와 블랙박스 영상 데이터는 일반적으로 블록체인에 저장되는 데이터에 비해 용량이 크다. 그러나 블록체인은 이미 저장된 데이터에 대해 수정과 삭제를 할 수 없는 비가역적인 특성을 지니며 P2P 네트워크의 모든 노드가 동일한 원장으로 공유하는 분산 저장 데이터베이스이다.
- [0116] 따라서 대용량인 영상 데이터를 블록체인에 그대로 저장하는 것은 비효율적인 방법이다. 이를 위해 본 발명에서는 오프체인 스토리지를 고려한다.
- [0117] 원본 데이터는 외부 오프체인 스토리지에 저장하고 원본 데이터의 메타데이터, 해시값, 저장된 주소와 같은 적은 용량의 데이터만 블록체인에 저장한다.
- [0118] 이때 외부 스토리지로써 클라우드 스토리지, IPFS 또는 DApp의 웹서버를 고려할 수 있고, 이로 제한되지 않는다.
- [0119] 이와 같은 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치에서 합의 알고리즘 설정을 위한 고려 사항은 다음과 같다.
- [0120] (i)컨소시엄 블록체인에 적합해야 한다.

- [0121] (ii)초당 트랜잭션은 대량의 차량 데이터를 처리할 수 있을 만큼 충분히 빨라야 한다.
- [0122] (iii)채굴 보상이 요구되지 않는다.
- [0123] (iv)사물인터넷 환경에 적합해야 한다.
- [0124] (v)블록체인 참여자 중 클라이언트의 역할을 하는 데이터 소유자를 제외한 데이터 소비자 피어들로만 합의할 수 있는 메커니즘이 필요하다.
- [0125] (vi)합의에 참여할 수 있는 피어 중 리더를 정할 수 있는 메커니즘이 필요하다.
- [0126] 프라이빗 또는 컨소시엄 블록체인에서는 참여자가 이미 인증되고 허가된 개체이므로 상호 간의 신뢰성이 보장되어 있으며 거래가 정상적인지 검증하는 데 많은 에너지가 요구되지 않기 때문에 블록을 생성하고 체인에 연결하는 행위에 대한 보상은 고려하지 않는다.
- [0127] 따라서, 본 발명에서는 블록을 어떻게 생성할 것인지, 어떠한 블록을 채택할 것인지에 대한 합의 알고리즘은 단순 수신된 트랜잭션을 시간순으로 정렬하는 순서화 알고리즘으로 대체될 수 있다.
- [0128] 이러한 순서화 알고리즘으로 Pub/Sub 구조의 메시지 큐 미들웨어인 카프카 기반의 오더링 서비스 또는 CFT(Crash Fault Tolerant) 알고리즘 기반의 오더링 서비스인 RAFT를 사용할 수 있고, 이로 제한되지 않는다.
- [0129] 도 5는 본 발명에 따른 블록 및 트랜잭션 구조도이다.
- [0130] 블록체인에 저장되는 데이터는 트랜잭션 단위로 생성된다. 채굴자 노드는 이러한 트랜잭션을 모아서 블록으로 만들고 체인에 연결한다. 하나의 블록을 만들기 위한 트랜잭션의 개수나 양은 블록체인 시스템 마다 다르다.
- [0131] 트랜잭션은 트랜잭션 헤더와 바디로 구성된다.
- [0132] 도 5에서와 같이, 트랜잭션의 헤더에는 트랜잭션 식별자, 전송 금액, 디지털 서명, 수신자의 공개키 해시값 및 유형값과 같은 일반적인 항목이 포함된다.
- [0133] 유형값을 통해 해당 트랜잭션이 DO-ABE와 관련된 트랜잭션인지 커넥티드 카와 관련된 트랜잭션인지 구분할 수 있다.
- [0134] 트랜잭션 바디에는 차량 관련 데이터, 블랙박스 영상 관련 데이터, DO-ABE를 위한 데이터가 포함된다.
- [0135] 차량 관련 트랜잭션은 차량 내부에 있는 게이트웨이로부터 생성된다. 엣지 컴퓨팅(edge computing)이 가능한 차량 게이트웨이는 차량 내부의 각종 센서 및 컨트롤러와 블랙박스로부터 데이터를 수신한다.
- [0136] 그리고 블록체인 네트워크로 데이터를 전송하기 위한 전처리 작업을 수행한다.
- [0137] 트랜잭션에 포함되는 데이터의 종류에는 사전 정의된 조건에 의해 발생한 EDR 데이터, BSM, 차종, 차량 정보 등이 포함된 차량 관련 데이터와 영상 시간, 출발 장소 및 도착 장소가 포함된 이동 경로, 영상의 크기, 그 외에 운행 정보가 포함된 블랙박스 영상 관련 데이터가 있다. 또한, DO-ABE와 관련된 데이터가 있다.
- [0138] 이처럼 블록체인의 확장성과 높은 전송 성공률, 그리고 낮은 전송 지연을 위해 블록체인에는 차량 데이터, 영상 데이터의 메타데이터만 저장하고 원본 데이터는 외부 저장소에 분리하여 저장한다.
- [0139] 트랜잭션과 마찬가지로 블록도 헤더와 바디로 구성된다. 블록 바디에는 위에서 언급한 트랜잭션의 목록이 포함된다. 블록 헤더에는 트랜잭션 목록의 해시값, 이전 블록의 해시값, 타임스탬프, 그리고 버전값이 포함된다.
- [0140] 도 6a 내지 도 6d는 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치에서 사용하는 스마트 계약 함수의 예를 나타낸 구성도이다.
- [0141] 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치에서는 데이터 소유자 노드가 ACL을 등록하고 제어하는 기능, 새로운 데이터 세트의 구성, 그리고 데이터 거래에 필요한 프로세스 등 블록체인 상에서 이뤄지는 기능들의 강제성을 부여하기 위해 스마트 계약을 이용한다.
- [0142] 의사 코드(pseudo code)로 표현된 도 6a 내지 도 6d는 본 발명에서 사용하는 주요 스마트 계약 함수를 나타낸다.
- [0143] 도 6a는 데이터 소유자 노드가 데이터를 생성하고 블록체인에 저장하는 함수인 CreateData이다.
- [0144] CreateData는 데이터 소유자 노드만 실행할 수 있는 함수로써 데이터 소유자의 ID와 블록체인에 저장할 데이터

를 매개 변수로 입력받는다.

- [0145] 먼저 함수를 실행한 개체가 데이터 소유자 노드인지, 그리고 매개 변수의 개수와 포맷이 일치하는지 확인한다.
- [0146] 여기서, 포맷은 차량 게이트웨이에서 전처리한 데이터 포맷과 스마트 계약에서 정의한 포맷을 의미한다. 함수 실행 주체가 데이터 소유자 노드이고 저장할 데이터 또한 올바른 데이터임을 확인했다면 이를 블록체인에 저장한다.
- [0147] 도 6b는 데이터 소비자 노드가 필요로 하는 데이터에 접근하고 획득하는 PurchaseData 함수이다.
- [0148] PurchaseData는 데이터 소비자 노드의 ID와 구매할 데이터의 ID를 매개 변수로 입력받는다.
- [0149] 먼저 데이터 소비자 노드의 ID를 통해 올바른 사용자인지 확인한다. 이후, 데이터 소비자 노드는 구매할 데이터의 가격만큼 데이터 소유자 노드에게 자산을 지불한다.
- [0150] 자산의 입금을 확인한 데이터 소유자 노드는 본인이 관리하는 ACL에 해당 데이터 소비자를 등록한다.
- [0151] 그리고 다시 데이터 소비자 노드의 ID와 데이터 소유자가 보유하고 있는 ACL의 비교를 통해 사용자가 허가한 사용자인지 확인한다.
- [0152] 접근 권한이 없거나 적절하지 않으면 접근은 거부된다. 접근이 허가된 사용자의 경우, 데이터 소유자 노드는 오프체인 프라이빗 컨트랙트를 통해 원본 데이터의 위치와 키값을 전달한다.
- [0153] 데이터 소비자 노드는 암호화된 원본 데이터를 획득하고 복호화할 수 있으며 사전 정의된 설정값에 따른 시간 또는 조건 동안에만 데이터의 열람이 가능하다.
- [0154] 이와 같은 PurchaseData 함수를 실행하기 전에 수행되어야 하는 함수가 있다.
- [0155] 데이터 소비자 노드는 데이터를 구매하고 원본 데이터의 위치와 키값을 받기 전, 데이터 소유자 노드로부터 허가받아야 한다.
- [0156] 즉, 데이터 소유자 노드는 직접 관리하는 ACL에 본인의 데이터에 접근하는 사용자를 등록해야 한다.
- [0157] 이는 데이터 소유자 노드가 단순히 데이터를 생성하고 제공하는 클라이언트의 역할을 넘어서 정보 주체에게 자기 정보통제권 확보를 위한 선택권을 최대한 보장해주고 시스템의 신뢰를 구축하기 위함이다.
- [0158] 도 6c는 이러한 데이터 소비자 노드의 요청에 대한 수신과 데이터 소유자의 ACL 관리 기능을 하는 HandlingACL을 나타낸다.
- [0159] HandlingACL은 RequestACL을 통해 수신된 요청을 토대로 자산의 입금을 확인하고 데이터 소유자 노드의 ACL에 해당 소비자를 등록하는 함수이다.
- [0160] 도 6d는 DeleteData는 등록된 데이터를 삭제하는 함수이다.
- [0161] 블록체인 시스템에서는 이미 저장된 데이터는 삭제할 수 없다. 따라서 DeleteData 함수는 데이터의 키값으로 원장을 조회한 후 삭제했다는 트랜잭션을 생성하므로 구현할 수 있다.
- [0162] 즉, 실제 블록체인에는 데이터가 저장되어 있지만 조회할 수 없도록 구현한다.
- [0163] 이러한 기능들을 스마트 계약으로 구현함에 따라 데이터 소유자 노드가 ACL을 등록하고 제어하는 기능, 데이터 세트를 구성하고 블록체인에 저장하는 기능, 데이터 거래에 필요한 모든 기능에 대해 강제성을 부여하고 서로의 계약 이행을 관찰할 수 있다. 더 나아가 데이터에 대한 정합성과 무결성 검증 시간이 단축될 수 있으며 상호 약속된 규칙에 따른 절차에 의해 컨소시엄 내에서 신뢰를 구축할 수 있다.
- [0164] 도 7은 블록체인 기반 DO-ABE를 이용한 데이터 공유 및 거래 프로세스를 나타낸 동작 흐름도이다.
- [0165] DO-ABE는 클라우드 스토리지와 같은 중앙집중화된 애플리케이션에 적합한 암호화 기법이기 때문에 이를 제안 모델에 적용하기 위해서는 블록체인 기반으로 재구성할 필요가 있다.
- [0166] 우선 클라우드 스토리지의 저장 기능을 블록체인과 외부 스토리지로 분리한다.
- [0167] DO-ABE와 관련된 데이터 중 공개 파라미터, 전체 속성들의 집합, 공개키, 콘텐츠의 식별자 및 암호화된 콘텐츠의 해시값을 블록체인에 공개한다.
- [0168] 여기서, 콘텐츠란 원본 데이터, 즉 차량 운행 데이터와 블랙박스 영상 데이터를 의미한다. 그리고 콘텐츠의 식

별자, 암호화된 콘텐츠, 암호화된 콘텐츠에 사용되는 대칭키의 암호문은 외부 스토리지에 저장한다.

- [0169] 도 7은 블록체인 기반 DO-ABE를 사용하여 데이터 공유 및 거래 프로세스를 나타낸다.
- [0170] 데이터 소유자 노드는 스마트 계약을 통해 거래가 완료된 소비자의 고유 식별자(UID, User ID)를 ACL에 정의하고, 이를 암호화한 뒤에 블록체인 트랜잭션에 게시한다. 데이터 소비자 노드는 스마트 계약으로 ACL이 허용하는 경우에만 데이터에 접근하고 처리할 수 있다.
- [0171] 구체적으로 먼저 '시스템 설정'을 설명한다.
- [0172] 본 발명에서는 신뢰 기관이 존재하는 컨소시엄 형 블록체인을 채택한다.
- [0173] 따라서 모든 참여자는 시스템에 참여하기 전 신뢰 기관에 등록되어야 한다.
- [0174] 다시 말해, 각 참여자는 신뢰 기관으로부터 UID와 공개/개인키 쌍을 할당받는다. 블록의 합의 및 검증에 참여하는 노드는 채택된 합의 메커니즘을 기반으로 선별된다. 그리고 각 데이터 소유자 노드는 Setup 함수를 이용하여 DO-ABE 공개 매개 변수를 생성하고, 이를 DO-ABE 트랜잭션을 통해 블록체인에 저장한다.
- [0175] 그리고 '콘텐츠 등록 및 업로드'를 설명한다.
- [0176] 먼저 데이터 소유자 노드는 KeyGen 함수를 이용하여 마스터 비밀키 $MSK = g^\beta$ 와 공개키 $PK = (e(g, g)^\beta, g^\alpha)$ 를 계산한다.
- [0177] 이렇게 생성된 공개키 PK는 DO-ABE 트랜잭션을 통해 블록체인에 저장된다.
- [0178] 암호화된 원본 데이터 EF는 임의로 생성된 대칭키 sk_F 로 원본 데이터 F를 암호화하여 생성된다. ($EF = SymEnc(F, sk_F)$)
- [0179] 이후 적절한 접근 구조 ST를 정의하고 대칭키 sk_F 와 Encrypt 함수를 사용하여 암호문 CT를 계산한다. ($CT = Enc(PK, ST, sk_F)$)
- [0180] 소유자의 식별자 UID, 원본 데이터의 식별자 Fid , 암호화된 데이터의 해시값 $H(EF)$ 를 포함한 메타데이터는 커넥티드 카 트랜잭션을 통해 블록체인에 저장된다.
- [0181] 여기서, 메타데이터는 타임스탬프 정보와 GPS와 같은 위치 정보를 포함할 수 있다.
- [0182] 그리고 (Fid, EF, CT) 는 외부(오프체인) 스토리지에 저장한다.
- [0183] 이때, $H(F)$ 로 외부 스토리지에서 암호화된 원본 데이터를 저장하는 위치를 계산할 수 있다.
- [0184] 그리고 '콘텐츠 접근 및 다운로드'를 설명한다.
- [0185] 데이터 소비자 노드는 데이터의 위치 정보나 시간 정보를 토대로 마켓플레이스 플랫폼에서 원하는 데이터를 검색하고 해당 데이터의 메타데이터를 획득할 수 있다.
- [0186] 접근 속성 집합 S를 보유한 데이터 소비자 노드는 데이터 소유자 노드에게 오프체인 프라이빗 컨트랙트를 통해 원본 데이터에 접근하기 위한 비밀키 SK의 생성을 요청한다.
- [0187] 데이터 소유자는 KeyGen 함수를 이용하여 소비자의 속성 비밀키
- [0188] $SK(K = g^\beta g^{\alpha t}, L = g^t, \forall x \in S, K_x = h_x^t)$ 을 생성하고 이 SK와 원본 데이터의 저장 위치 $H(F)$ 를 오프체인 프라이빗 컨트랙트에 의해 안전하게 전달한다.
- [0189] 소비자는 저장 위치 $H(F)$ 에 저장된 암호화된 원본 데이터 (Fid, EF, CT) 를 획득하고 $sk_F = Dec(CT, SK)$ 를 계산한다.

- [0190] 소비자는 대칭키 sk_F 를 복호화하여 원본 데이터 F를 얻을 수 있다. 이 거
- [0191] 래가 성공적으로 완료되면 블록체인에 기록된다. 여기에서 데이터 구매를 위한 결제 프로세스는 커밋 체인 또는 상태 채널과 같은 오프체인 기술을 통해 수행될 수 있다.
- [0192] 이상에서 설명한 본 발명에 따른 블록체인 기반 커넥티드 카 데이터 거래 및 공유를 위한 장치 및 방법은 DO-ABE(data-owner-based attribute-based encryption) 암호화 체계를 블록체인 환경에서 동작할 수 있도록 재구성하고 이를 이용하여 커넥티드 카의 중요 데이터를 안전하고 효율적으로 공유하고 거래할 수 있도록 한 것이다.
- [0193] 본 발명에 의해 커넥티드 카 데이터를 안전하게 거래하고 공유하여 차량 사고 수사관은 무결성과 신뢰성이 보장된 데이터를 증거로 사용할 수 있으며 사고 원인을 빠르고 정확하게 분석할 수 있도록 하고, 차량 보험사, 유지보수 업체, 차량 제조업체, 이동 통신사를 비롯한 관련 서비스 업체들이 블록체인 기반으로 저장되는 차량 운행 정보와 차량 정보를 토대로 보험비, 수리비, 통신비 등 각종 서비스에 대한 가격을 정확하게 책정하고 사용자 맞춤형 서비스를 고품질로 제공할 수 있도록 한다.
- [0194] 이상에서의 설명에서와 같이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 본 발명이 구현되어 있음을 이해할 수 있을 것이다.
- [0195] 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

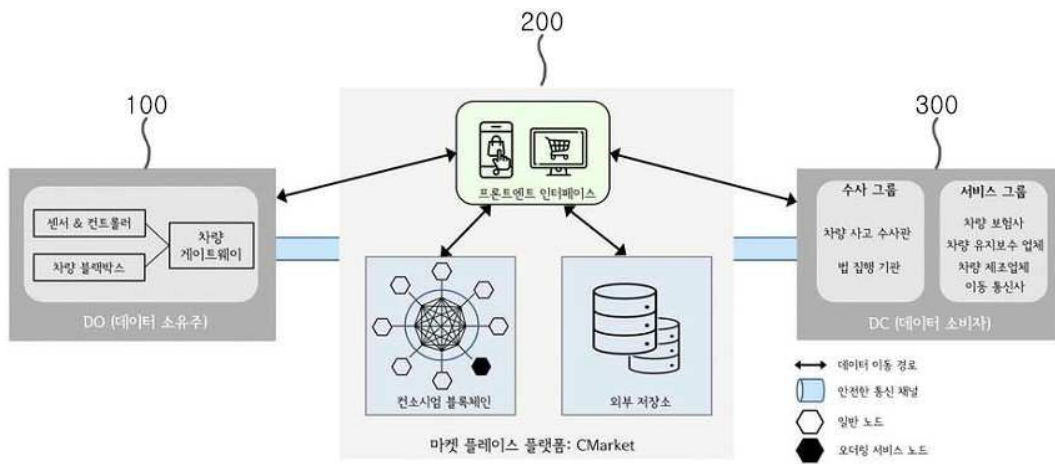
- [0196] 100. 데이터 소유자 노드
200. 마켓플레이스 플랫폼 장치
300. 데이터 소비자 노드

도면

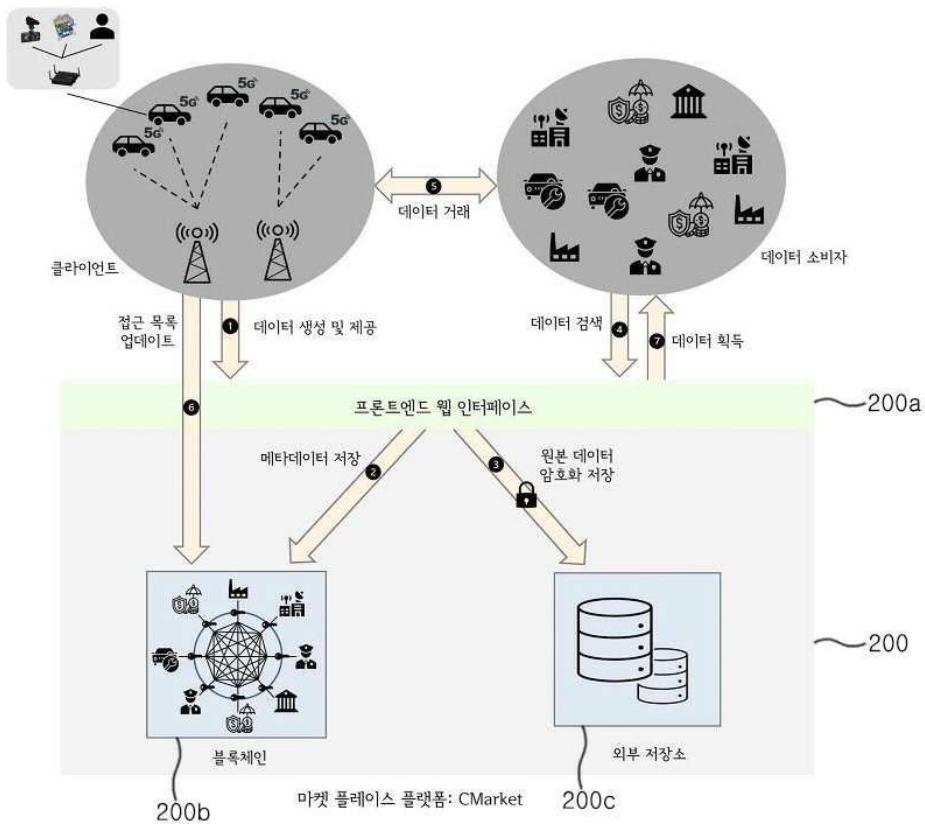
도면1



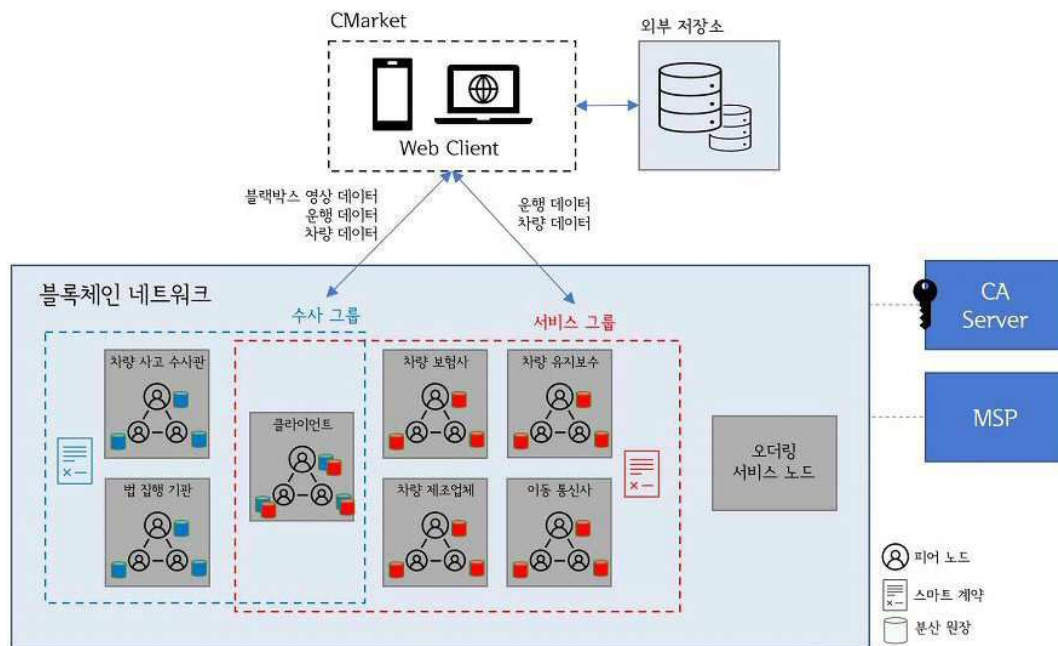
도면2



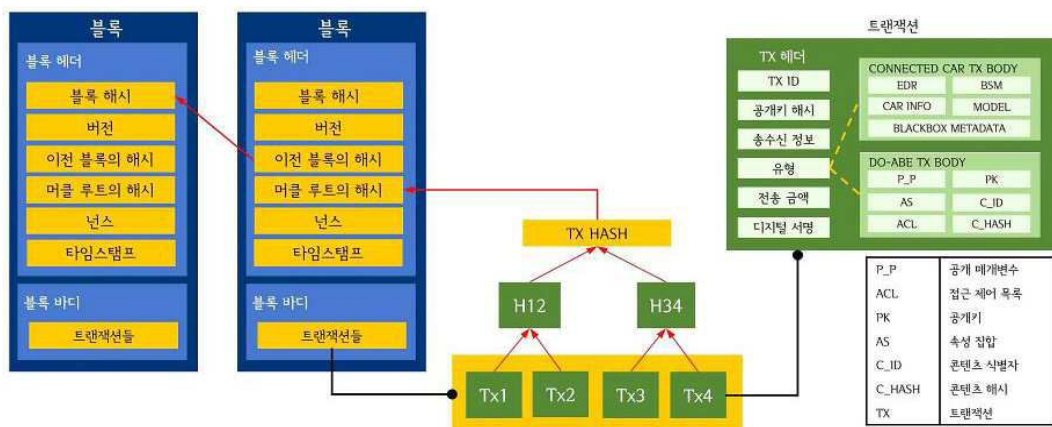
도면3



도면4



도면5



도면6a

Algorithm 1 CreateData

Require: DO's ID, Data

onlyOwner

if Validation(*DO's ID*) **then**

if (Data.length = format.length) **then**

$MSK, PK = KeyGen()$

 PutState(PK)

$EF = Sym_Enc(F, sk_F)$

$CT = Encrypt(PK, ST, sk_F)$

metadata of Vehicle data = timestamp, location

metadata of DO-ABE data = $UID, Fid, F, H(EF)$

 PutState(*metadata of Vehicle data*)

 PutState(*public param of DO-ABE data*)

else

 REJECT *Creating*

endif

도면6b

Algorithm 2 PurchaseData

Require: DC's ID, ContentID

payable

if Validation(*DC's ID*) **then**

 PaytoOwner(*data value*, *DO's address*)

 RequestACL(*DC's ID*)

$SK, H(F) = \text{GetfromOwner}(\text{set of attributes } S)$

 OffChainTransaction{

$(Fid, EF, CT) = \text{GetfromOffChain}()$

$sk_F = \text{Decrypt}(CT, SK)$

$F = Sym_Dec(EF, sk_F)$

 }

else

 REJECT *Access*

endif

도면6c

Algorithm 3 HandlingACL

```

Require: DC's ID
onlyOwner
if CheckACL(DC's ID) then
    Compute(data key)
else GetState(transaction.dataValue == dataValue) then
    AddtoACL(DC's ID)
    PutState(ACL)
    Compute(data key)
return (data key, location)
endif
    
```

도면6d

Algorithm 4 DeleteData

```

Require: DO's ID, ContentID
onlyOwner
if ContentID's Owner == DO's ID then
    GetState(ContentID)
    Key = ContentID's Key
    DelState(Key)
else
    REJECT Delete
endif
    
```

도면7

