



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0140538
(43) 공개일자 2024년09월24일

- | | |
|--|---|
| <p>(51) 국제특허분류(Int. Cl.)
H04W 12/02 (2021.01) G06F 16/182 (2019.01)
H04L 9/32 (2006.01) H04W 12/041 (2021.01)
H04W 4/44 (2018.01)</p> <p>(52) CPC특허분류
H04W 12/02 (2021.01)
G06F 16/182 (2019.01)</p> <p>(21) 출원번호 10-2023-0035039
(22) 출원일자 2023년03월17일
심사청구일자 2023년03월17일</p> | <p>(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 갯벌로 27, 인천대학교 이노베이션센터(송도동)</p> <p>(72) 발명자
전광길
인천광역시 연수구 해송로 70, 209동 805호(송도동, 송도웹카운티2단지)</p> <p>(74) 대리인
특허법인충정</p> |
|--|---|

전체 청구항 수 : 총 11 항

(54) 발명의 명칭 블록체인 기반 개인 보호 인증 시스템

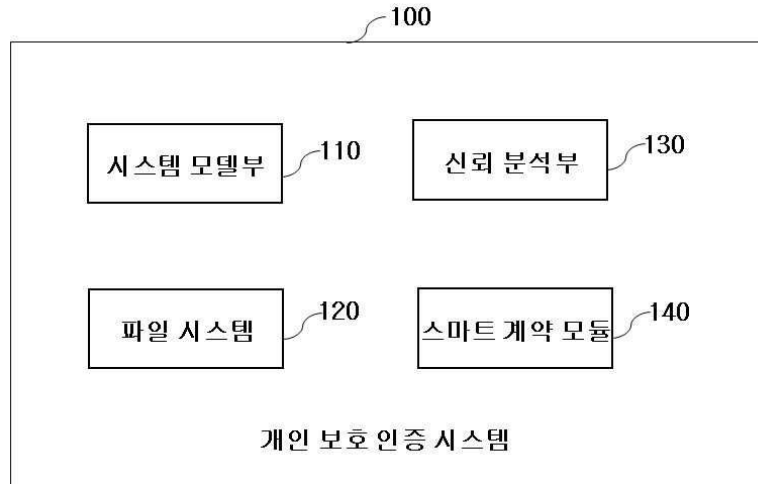
(57) 요약

블록체인 기반 개인 보호 인증 시스템은 사용자의 프라이버시와 보안을 보장하기 위한 지능형 교통 시스템(Intelligent Transportation System, ITS) 네트워크용 블록체인 기반 개인 보호 인증 모델을 제공하고, ITS 네트워크를 위한 안전하고 분산된 솔루션을 제공하여 데이터 저장, 데이터 액세스 및 처리 관리를 수행한다.

본 발명은 차량 노드 위치 및 데이터 프라이버시가 필요한 ITS 네트워크의 모든 영역에서 중요한 요소 중 하나인 보안 및 프라이버시를 제공할 수 있는 효과가 있다.

본 발명은 ITS 네트워크 데이터를 활용하여 데이터 저장, 액세스 및 처리 메커니즘을 통해 프라이버시와 보안을 보장할 수 있는 효과가 있다.

대표도 - 도1



(52) CPC특허분류

H04L 9/3247 (2013.01)

H04W 12/041 (2021.01)

H04W 4/44 (2020.05)

H04L 2209/84 (2013.01)

H04L 2463/102 (2024.08)

명세서

청구범위

청구항 1

차량단말기가 장착되어 서로 통신할 수 있고, 지능형 교통 시스템 네트워크에서 길가에 배치되어 액세스 포인트로 작동하는 로드 사이드 유니트와 통신하는 이동 노드 엔터티(Entity)를 포함하는 하나 이상의 차량 노드와, 등록 단계에서 상기 각 차량 노드의 이동 노드 엔터티가 외부 소유 계정 주소를 등록하고, 가져오고, 트랜잭션 단계에서 API(Application Programming Interface) 호출 및 계약 트랜잭션을 포함한 메시지는 이더리움 네트워크를 통해 스마트 계약으로 전송하는 시스템 모델을 포함하며,

상기 시스템 모델부는 상기 각 차량 노드의 개인 정보 보호를 보장하기 위해 블록체인과 스마트 계약을 사용하는 블록체인 기반 개인 보호 인증 시스템.

청구항 2

청구항 1에 있어서,

상기 시스템 모델부는 이더리움 블록체인을 확인하기 위해서 고유한 외부 소유 계정 주소를 생성하는 공개키와, 상기 차량 노드의 모든 메시지를 인증용 개인키에 의해 디지털 서명하는 블록체인 기반 개인 보호 인증 모델을 더 포함하는 블록체인 기반 개인 보호 인증 시스템.

청구항 3

청구항 2에 있어서,

상기 차량 노드는 신뢰 평가를 위한 비밀키(SK_{TE})를 공유하고, 분산 저장소에 데이터 전송과 고유 식별자의 할당을 위해 데이터 암호화용 대칭키(SK_{DE})를 생성하는 블록체인 기반 개인 보호 인증 시스템.

청구항 4

청구항 3에 있어서,

상기 시스템 모델부는,

상기 분산 저장소로부터 데이터를 다운받기 위해서 데이터 식별자를 사용하고, 데이터 SK_{DE}^{TE} 를 해독하여 상기 대칭키(SK_{DE})를 얻은 다음, 데이터 실행 전에 데이터를 다운로드하는 신뢰 실행부; 및

상기 스마트 계약의 함수를 이용하여 데이터를 요청하고, 사용자 인증 목록에 속할 때마다 데이터 식별자와 상기 데이터 SK_{DE}^{TE} 가 리턴되고, 상기 신뢰 실행부의 링크를 수신하며, 실행용 코드를 상기 신뢰 실행부로 전송하는 서비스 제공부를 더 포함하는 블록체인 기반 개인 보호 인증 시스템.

청구항 5

청구항 4에 있어서,

중앙 집중식 클라우드 스토리지와 같은 단일 장애 지점을 회피하기 위하여 분산 파일 시스템을 사용하는 파일 시스템;

데이터를 운영 체제 및 요청된 응용 프로그램의 인증, 무결성 및 기밀성을 보장하기 위해 처리되고, 트랜잭션 기록을 위한 합의 프로토콜을 사용하여 상기 로드 사이드 유니트와 차량 노드 데이터를 통해 상기 서비스 제공부를 액세스하는 신뢰 분석부; 및

상기 차량 노드의 식별 및 권한 부여, 데이터 검색 및 스마트 계약 완료를 수행하는 스마트 계약 모듈을 포함하

는 블록체인 기반 개인 보호 인증 시스템.

청구항 6

청구항 5에 있어서,

상기 신뢰 분석부는 운영체제(OS)의 유효성 및 애플리케이션의 신뢰성을 확인하라는 사용자 요청이 수신되면, 스토리지, 입출력 실행 프로세스, 통신의 서비스 액세스 가능성에 대한 액세스 권한이 부여되고, 상기 액세스 권한이 부여된 응용 프로그램의 신뢰성을 확인하고, 상기 애플리케이션을 구동시키는 블록체인 기반 개인 보호 인증 시스템.

청구항 7

청구항 5에 있어서,

상기 스마트 계약 모듈은 상기 차량 노드의 식별 및 권한 부여, 데이터 검색 및 스마트 계약 완료를 세 가지 주요 함수를 사용하여 수행하고,

첫 번째 식별 함수 및 권한 부여 함수에서, 상기 차량 노드는 스마트 계약을 통해 데이터 식별자를 업로드하고, 두 번째 함수는 상기 서비스 제공부가 데이터 식별자를 검색하는 데이터 검색이고, 세 번째 함수는 상기 차량 노드가 스마트 계약을 완료하고, 상기 세 번째 함수를 다시 호출하지 않고, 계약 업데이트를 일시 중지하는 스마트 계약 완료를 수행하는 블록체인 기반 개인 보호 인증 시스템.

청구항 8

청구항 7에 있어서,

상기 스마트 계약 모듈은 상기 시스템 모델로부터 차량 노드 id(VN_id), 데이터 id(Data_id), 서비스 제공부 주소(SP_address), 데이터 키(data_key), 신뢰 분석부 주소(TE_address), 상기 차량 노드의 스마트 계약(VN_smartcontract)을 입력받고,

상기 권한 부여 함수에서 서비스 제공부 주소를 매핑을 시작하고, 상기 차량 노드가 유효한 경우, 성공 메시지를 반환하고, 상기 식별 함수에서 상기 차량 노드의 신뢰성이 있다고 판단하는 경우, 상기 차량 노드 id(VN_id)를 이용하여 데이터 식별자(data_identifier), 데이터 키(data_key), 신뢰 분석부 주소(TE_address)를 획득하고, 상기 식별 함수에서 데이터 id(Data_id), 데이터 키(data_key), 신뢰 분석부 주소(TE_address)를 반환하는 블록체인 기반 개인 보호 인증 시스템.

청구항 9

차량단말기가 장착되어 서로 통신할 수 있고, 지능형 교통 시스템 네트워크에서 길가에 배치되어 액세스 포인트로 작동하는 로드 사이드 유닛과 통신하는 이동 노드 엔터티(Entity)를 포함하는 하나 이상의 차량 노드와, 등록 단계에서 상기 각 차량 노드의 이동 노드 엔터티가 외부 소유 계정 주소를 등록하고, 가져오고, 트랜잭션 단계에서 API(Application Programming Interface) 호출 및 계약 트랜잭션을 포함한 메시지는 이더리움 네트워크를 통해 스마트 계약으로 전송하며, 상기 이더리움 블록체인을 확인하기 위해서 고유한 외부 소유 계정 주소를 생성하는 공개키와, 상기 차량 노드의 모든 메시지를 인증용 개인키에 의해 디지털 서명하는 블록체인 기반 개인 보호 인증 모델을 제공하는 시스템 모델부;

데이터를 운영 체제 및 요청된 응용 프로그램의 인증, 무결성 및 기밀성을 보장하기 위해 처리되고, 트랜잭션 기록을 위한 합의 프로토콜을 사용하여 상기 로드 사이드 유닛과 차량 노드 데이터를 통해 상기 서비스 제공부를 액세스하는 신뢰 분석부; 및

상기 차량 노드의 식별 및 권한 부여, 데이터 검색 및 스마트 계약 완료를 수행하는 스마트 계약 모듈을 포함하는 블록체인 기반 개인 보호 인증 시스템.

청구항 10

청구항 9에 있어서,

상기 시스템 모델부는,

상기 이더리움 네트워크 측에 설치되어 온라인 서비스를 상기 차량 노드로 제공하고, 상기 지능형 교통 시스템 네트워크에서 수신한 데이터를 수집 및 처리하는 서비스 제공부;

상기 차량 노드에서 송신되는 데이터를 안전하게 저장, 유지 관리 및 배포할 수 있는 P2P 분산 오픈 소스 파일 공유 시스템을 제공하는 분산 저장소;

상기 차량 노드의 스마트 계약 코드 실행, 이더리움을 통한 저장의 상기 지능형 교통 시스템 네트워크의 분산 응용 프로그램을 지원하는 P2P 플랫폼을 제공하는 블록체인 네트워크; 및

상기 분산 저장소로부터 데이터를 다운받기 위해서 데이터 식별자를 사용하고, 데이터 SK_{DE}^{TE} 를 해독하여 상기 대칭키(SK_{DE})를 얻은 다음, 데이터 실행 전에 데이터를 다운로드하는 신뢰 실행부를 포함하는 블록체인 기반 개인 보호 인증 시스템.

청구항 11

청구항 10에 있어서,

상기 차량 노드는 신뢰 평가를 위한 비밀키(SK_{TE})를 공유하고, 분산 저장소에 데이터 전송과 고유 식별자의 할당을 위해 데이터 암호화용 대칭키(SK_{DE})를 생성하고,

상기 서비스 제공부는 상기 스마트 계약의 함수를 이용하여 데이터를 요청하고, 사용자 인증 목록에 속할 때마다 데이터 식별자와 상기 데이터 SK_{DE}^{TE} 가 리턴되고, 상기 신뢰 실행부의 링크를 수신하며, 실행용 코드를 상기 신뢰 실행부로 전송하는 블록체인 기반 개인 보호 인증 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 기반 개인 보호 인증 시스템에 관한 것으로서, 더욱 상세하게는 사용자의 프라이버시와 보안을 보장하기 위한 지능형 교통 시스템(Intelligent Transportation System, ITS) 네트워크용 블록체인 기반 개인 보호 인증 모델을 제공하고, ITS 네트워크를 위한 안전하고 분산된 솔루션을 제공하여 데이터 저장, 데이터 액세스 및 처리 관리를 수행하는 블록체인 기반 개인 보호 인증 시스템에 관한 것이다.

배경 기술

[0002] 지능형 교통 시스템(Intelligent Transportation System, ITS) 네트워크는 도로에서 사용자를 용이하게 하는 스마트 서비스 및 애플리케이션으로 인해 인기를 얻었다. 이러한 네트워크에서 사용자가 증가함에 따라 새롭고 복잡한 데이터 처리, 저장, 보안 및 개인 정보 보호 문제가 발생하였다. 지능형 교통 시스템은 데이터 관리를 위해 중앙 집중식 에지, 포그 또는 클라우드 아키텍처를 사용하고 있다.

[0003] 지능형 교통 시스템 네트워크는 다양한 이점과 기능으로 인해 안전한 데이터 통신 프로세스를 보장하기 위한 데이터 보안, 사용자 개인 정보 보호와 관련된 몇 가지 심각한 문제로 어려움을 겪었다.

[0004] 지능형 교통 시스템 네트워크는 안전한 데이터 전송을 위해 인증 및 무결성이 네트워크에 대한 사용자의 신뢰를 보장해야 한다. 그러나 기존의 솔루션은 데이터 보안 및 사용자 프라이버시를 위해 ITS 네트워크에 적용되지만 차량 노드의 특수한 특성 및 이동성 패턴으로 인해 라우팅 프로토콜과 함께 보안 및 프라이버시 프로세스가 지연, 단절, 다양한 취약성 및 공격에 시달리는 문제점이 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국 등록특허번호 제10-2273549호

발명의 내용

해결하려는 과제

- [0006] 이와 같은 문제점을 해결하기 위하여, 본 발명은 사용자의 프라이버시와 보안을 보장하기 위한 지능형 교통 시스템(Intelligent Transportation System, ITS) 네트워크용 블록체인 기반 개인 보호 인증 모델을 제공하고, ITS 네트워크를 위한 안전하고 분산된 솔루션을 제공하여 데이터 저장, 데이터 액세스 및 처리 관리를 수행하는 블록체인 기반 개인 보호 인증 시스템을 제공하는데 그 목적이 있다.

과제의 해결 수단

- [0007] 상기 목적을 달성하기 위한 본 발명의 특징에 따른 블록체인 기반 개인 보호 인증 시스템은,
- [0008] 차량단말기가 장착되어 서로 통신할 수 있고, 지능형 교통 시스템 네트워크에서 길가에 배치되어 액세스 포인트로 작동하는 로드 사이드 유닛과 통신하는 이동 노드 엔터티(Entity)를 포함하는 하나 이상의 차량 노드와, 등록 단계에서 상기 각 차량 노드의 이동 노드 엔터티가 외부 소유 계정 주소를 등록하고, 가져오고, 트랜잭션 단계에서 API(Application Programming Interface) 호출 및 계약 트랜잭션을 포함한 메시지는 이더리움 네트워크를 통해 스마트 계약으로 전송하는 시스템 모델부를 포함하며, 상기 시스템 모델부는 상기 각 차량 노드의 개인 정보 보호를 보장하기 위해 블록체인과 스마트 계약을 사용한다.
- [0009] 본 발명의 특징에 따른 블록체인 기반 개인 보호 인증 시스템은,
- [0010] 차량단말기가 장착되어 서로 통신할 수 있고, 지능형 교통 시스템 네트워크에서 길가에 배치되어 액세스 포인트로 작동하는 로드 사이드 유닛과 통신하는 이동 노드 엔터티(Entity)를 포함하는 하나 이상의 차량 노드와, 등록 단계에서 상기 각 차량 노드의 이동 노드 엔터티가 외부 소유 계정 주소를 등록하고, 가져오고, 트랜잭션 단계에서 API(Application Programming Interface) 호출 및 계약 트랜잭션을 포함한 메시지는 이더리움 네트워크를 통해 스마트 계약으로 전송하며, 상기 이더리움 블록체인을 확인하기 위해서 고유한 외부 소유 계정 주소를 생성하는 공개키와, 상기 차량 노드의 모든 메시지를 인증용 개인키에 의해 디지털 서명하는 블록체인 기반 개인 보호 인증 모델을 제공하는 시스템 모델부; 데이터를 운영 체제 및 요청된 응용 프로그램의 인증, 무결성 및 기밀성을 보장하기 위해 처리되고, 트랜잭션 기록을 위한 합의 프로토콜을 사용하여 상기 로드 사이드 유닛과 차량 노드 데이터를 통해 상기 서비스 제공부를 액세스하는 신뢰 분석부; 및 상기 차량 노드의 식별 및 권한 부여, 데이터 검색 및 스마트 계약 완료를 수행하는 스마트 계약 모듈을 포함한다.

발명의 효과

- [0011] 전술한 구성에 의하여, 본 발명은 차량 노드 위치 및 데이터 프라이버시가 필요한 ITS 네트워크의 모든 영역에서 중요한 요소 중 하나인 보안 및 프라이버시를 제공할 수 있는 효과가 있다.
- [0012] 본 발명은 ITS 네트워크 데이터를 활용하여 데이터 저장, 액세스 및 처리 메카니즘을 통해 프라이버시와 보안을 보장할 수 있는 효과가 있다.

도면의 간단한 설명

- [0013] 도 1은 본 발명의 실시예에 따른 블록체인 기반 개인 보호 인증 시스템의 구성을 나타낸 도면이다.
- 도 2는 본 발명의 실시예에 따른 시스템 모델부의 내부 구성을 나타낸 도면이다.
- 도 3은 본 발명의 실시예에 따른 파일 시스템의 데이터 저장 프로세스를 나타낸 도면이다.
- 도 4는 본 발명의 실시예에 따른 OS 및 애플리케이션 요청에 대한 신뢰 분석부의 프로세스를 나타낸 도면이다.
- 도 5는 본 발명의 실시예에 따른 스마트 계약 프로세스를 나타낸 도면이다.
- 도 6은 본 발명의 실시예에 따른 데이터 크기에 따른 트랜잭션 비용 분석을 나타낸 도면이다.
- 도 7은 본 발명의 실시예에 따른 이벤트가 다른 트랜잭션 비용 및 실행 비용을 나타낸 그래프이다.
- 도 8은 본 발명의 실시예에 따른 300000 GAS 제한을 이용한 초당 트랜잭션 분석을 나타낸 도면이다.
- 도 9는 본 발명의 실시예에 따른 800000 GAS 제한을 이용한 초당 트랜잭션 분석을 나타낸 도면이다.

도 10은 본 발명의 실시예에 따른 1000000 GAS 제한을 이용한 초당 트랜잭션 분석을 나타낸 도면이다.

도 11은 본 발명의 실시예에 따른 서로 다른 아키텍처에서 트랜잭션 수 측면에서 시간 분석을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0014] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0015] 도 1은 본 발명의 실시예에 따른 블록체인 기반 개인 보호 인증 시스템의 구성을 나타낸 도면이고, 도 2는 본 발명의 실시예에 따른 시스템 모델부의 내부 구성을 나타낸 도면이고, 도 3은 본 발명의 실시예에 따른 파일 시스템의 데이터 저장 프로세스를 나타낸 도면이다.
- [0016] 본 발명의 실시예에 따른 블록체인 기반 개인 보호 인증 시스템(100)은 시스템 모델부(System Model)(110), 파일 시스템(File System, FS)(120), 신뢰 분석부(Trust Evaluation, TE)(130) 및 스마트 계약 모듈(Smart Contract Module)(140)을 포함한다.
- [0017] 시스템 모델부(System Model)(110)는 차량 노드(Vehicle Nodes, VN)(111), 로드 사이드 유닛(Road Side Units, RSU)(112), 서비스 제공부(Service Providers, SP)(113), 분산 저장소(Distributed Storage, DS)(114), 신뢰 실행부(Trusted Execution, TE)(115) 및 블록체인 네트워크(Blockchain Network, BN)(116)를 포함한다.
- [0018] 차량 노드(111)는 차량단말기(On-Board Unit, OBU)가 장착되어 서로 통신할 수 있고, ITS 네트워크에서 RSU(120)와 통신할 수 있는 이동 노드 엔터티(Entity)를 포함한다.
- [0019] 차량단말기는 차량에 장착되는 다양한 장치와 센서들이 있다.
- [0020] 차량단말기는 애플리케이션 유형에 따라 환경을 감지하고, 차량 노드(111)의 속도 및 위치를 모니터링할 수 있다.
- [0021] RSU(112)는 길가에 배치되어 액세스 포인트로 작동하고, 유선 및 무선 매체를 사용하여 차량 노드(111)에서 데이터를 수집한다.
- [0022] 차량이 데이터를 전달할 때, 차량 노드(111)는 데이터를 전송하고, 액세스 권한을 부여하고 승인 처리를 할 수 있다.
- [0023] 서비스 제공부(113)는 이더리움 네트워크 측에 설치되어 온라인 서비스를 차량 노드(111)로 제공하고, ITS 네트워크에서 수신한 데이터를 수집 및 처리한다.
- [0024] 분산 저장소(114)의 엔터티(Entity)는 차량 노드(111)에서 송신되는 데이터를 안전하게 저장, 유지 관리 및 배포할 수 있는 P2P 분산 오픈 소스 파일 공유 시스템을 제공한다.
- [0025] 신뢰 분석부(130)는 데이터 실행을 위한 안전한 환경을 제공하고, 차량 노드 데이터의 무결성을 보장한다.
- [0026] 블록체인 네트워크(116)는 차량 노드(111)의 스마트 계약 코드 실행, 이더리움을 통한 저장과 같은 ITS 네트워크의 분산 응용 프로그램을 지원하는 P2P 플랫폼을 제공한다.
- [0027] 시스템 모델부(System Model)(110)는 등록 단계 및 트랜잭션 단계의 동작을 수행한다.
- [0028] 시스템 모델부(System Model)(110)는 등록 단계에서 이더리움 네트워크에 등록해야 한다.
- [0029] 시스템 모델부(System Model)(110)에서 등록하는 동안, 각 차량 노드의 이동 노드 엔터티는 EOA(외부 소유 계정, Externally Owned Account) 주소를 등록하고, 가져온다.
- [0030] 차량 노드(111)는 고유한 계약 주소를 얻어서 계약 계정을 생성한다.
- [0031] 블록체인 기반 개인 보호 인증(Blockchain Based Privacy-Preserving Authentication, BPPAU) 모델은 각 차량 노드의 이동 노드 엔터티가 한 쌍의 공개키(PUK_a^{Eth}), 개인키(PRK_a^{Eth})를 생성하는 암호화를 제공한다.
- [0032] 공개키(PUK_a^{Eth})는 이더리움 블록체인을 확인하기 위해서 고유한 20바이트 EOA 주소를 생성한다.
- [0033] 본 발명의 BPPAU 모델을 통한 차량 노드(111)의 모든 메시지는 인증용 개인키(PRK_a^{Eth})에 의해 디지털 서명

한다.

- [0034] 데이터 암호화용 대칭키(SK_{DE})는 분산 저장소(114)에 데이터 전송과 저장되기 전에 차량 노드(111) 측에서 생성되고, 고유 식별자를 할당한다.
- [0035] 차량 노드(111)는 신뢰 평가를 위한 비밀키(SK_{TE})를 공유한다.
- [0036] 차량 노드(111)는 데이터 식별자가 있는 스마트 계약을 위해 차량 노드(111)와 신뢰 실행부(115) 간에 공유되는 비밀키(SK_{TE})를 사용하여 데이터 암호화용 대칭키(SK_{DE})를 추가로 암호화한다.
- [0037] 시스템 모델부(System Model)(110)는 트랜잭션 단계에서 API(Application Programming Interface) 호출 및 계약 트랜잭션을 포함한 메시지는 이더리움 네트워크를 통해 스마트 계약으로 전송된다.
- [0038] API 메시지는 상호 작용을 위해 사용되고, 계약 트랜잭션을 이더리움 네트워크로 전송된다.
- [0039] 시스템 모델부(System Model)(110)의 트랜잭션 단계는 스마트 계약 게시, 데이터 저장, 데이터 식별자 업데이트, 요청 및 전송, 전송 및 처리, 공유 및 서비스 제공을 포함한 여러 단계로 구성된다.
- [0040] 차량 노드(111)는 스마트 계약을 게시하는 반면, 스마트 계약에는 서비스 제공부(Service Providers, SP)들(113)의 목록을 가진다.
- [0041] 데이터 저장소에서 차량 노드(111)는 분산 저장 시스템을 통해 데이터를 암호화하고, 스마트 계약을 통해 데이터 식별자를 업데이트한다.
- [0042] 서비스 제공부(Service Providers, SP)(113)는 스마트 계약의 함수를 이용하여 데이터를 요청한다.
- [0043] 서비스 제공부(113)가 사용자 인증 목록에 속할 때마다 데이터 식별자와 데이터 SK_{DE}^{TE} 가 리턴되고, 신뢰 실행부(Trusted Execution, TE)(115)의 링크를 수신한다.
- [0044] 서비스 제공부(113)는 실행용 코드를 신뢰 실행부(115)로 전송한다.
- [0045] 신뢰 실행부(115)는 분산 저장소(114)로부터 데이터를 다운받기 위해서 데이터 식별자를 사용하고, 데이터 SK_{DE}^{TE} 를 해독하여 대칭키(SK_{DE})를 얻은 다음, 데이터 실행 전에 데이터를 다운로드한다.
- [0046] 데이터 공유 및 서비스 제공은 서비스 제공을 위해 데이터를 처리하고, 서비스 제공부(113)와 공유하는 마지막 단계이다.
- [0047] 차량 노드들(111)은 스마트 계약들을 게시하고, 데이터를 데이터베이스에 저장한 후에 식별자를 업데이트한다. 업데이트 후에, 다음 프로세스는 데이터 식별자를 업데이트하고, 서비스 제공부(113)에게 데이터 액세스 요청을 전송한다.
- [0048] 서비스 제공부(113)는 요청 메시지를 생성하여 신뢰 실행부(115)로 전송한 후, 분산 저장소(Distributed Storage, DS)(114)로 전송한다.
- [0049] 블록체인 기반 개인 보호 인증 시스템(100)은 차량 노드(111) 또는 데이터를 소유한 사용자에게 완전한 제어를 제공한다.
- [0050] 차량 노드(111)는 EOA 주소 목록을 유지하고, 데이터를 활용한다. 블록체인 기반 개인 보호 인증 시스템(100)은 스토리지 시스템에 암호화된 데이터를 저장하고, 사용자 개인 정보를 보호하는 보안을 보장한다.
- [0051] ITS 네트워크에서 데이터를 요청하면, 해시 식별자(Hash Identifier)를 사용하여 데이터 접근성을 유지한다.
- [0052] 데이터가 변경되거나 업데이트되면, 새로운 버전의 데이터에 액세스할 수 있다. 데이터는 블록체인 기반 개인 보호 인증 시스템(100)의 파일 시스템(File System, FS)(120)에 업로드하기 전에 암호화하고 디지털 서명한다.
- [0053] 파일 시스템(File System, FS)(120)은 중앙 집중식 클라우드 스토리지와 같은 단일 장애 지점을 회피하기 위하여 IPFS(InterPlanetary File System)라는 분산 파일 시스템을 사용한다.
- [0054] 중앙 집중식 스토리지는 높은 대역폭 및 처리 기능 측면에서 더 많은 리소스가 필요하다.

- [0055] 파일 시스템(File System, FS)(120)은 피어 투 피어 프로토콜을 정의하는 분산 시스템을 제공한다.
- [0056] 파일 시스템(File System, FS)(120)은 중앙 집중식 시스템에 비해 빠르고 안정적이며, 안전하다.
- [0057] 파일 시스템(120)은 위치 주소 지정이 아닌 콘텐츠 주소 지정을 사용하기 때문에 데이터 중복성 문제도 해결할 수 있다.
- [0058] 차량 노드(111)의 사용자는 업로드 데이터를 선택하고, 데이터는 AES(Advanced Encryption Standard)와 대칭키(SK_{DE})를 사용하여 암호화된 다음, 데이터 파일은 디지털 방식으로 사용자에게 의해 서명되고, 개인키(PRK_a^{Eth})는 이더리움 EOA용으로 사용된다.
- [0059] 그리고 공개키(PUK_a^{Eth})는 데이터가 이더리움 네트워크에 등록되어 있고, 스마트 계약을 맺은 실제 차량 노드(111)에 속하는지 확인하는데 사용된다. SHA 256은 데이터 식별자의 해싱에 사용된다.
- [0060] 데이터 필드 및 링크 식별자를 포함하여 데이터가 파일 시스템(120)에 업로드된다.
- [0061] 큰 데이터 크기는 더 작은 청크로 분할되어 피어 네트워크에 저장된다.
- [0062] 도 3은 파일 시스템(120)의 데이터 저장 프로세스를 보여준다.
- [0063] 블록체인 기반 개인 보호 인증 시스템(100)에서 신뢰 분석부(Trust Evaluation, TE)(130)는 신뢰할 수 있는 프로세스를 사용하여 차량 노드 데이터를 처리하는데 사용된다.
- [0064] 신뢰 분석부(130)는 데이터를 운영 체제 및 요청된 응용 프로그램의 인증, 무결성 및 기밀성을 보장하기 위해 처리된다.
- [0065] 신뢰 분석부(130)를 통해 서비스 제공부(113)는 데이터 액세스 없이 사용자 암호화 데이터를 처리할 수 있다.
- [0066] 신뢰 분석부(130)는 트랜잭션 기록을 위한 합의 프로토콜을 사용하여 로드 사이드 유닛(Road Side Units, RSU)(112)와 차량 노드 데이터를 통해 서비스 제공부(113)를 액세스할 수 있다.
- [0067] RSU(112)는 공개키(PUK_a^{Eth}), 개인키(PRK_a^{Eth}) 측면에서 블록체인 노드의 신뢰값에 대해 문의하고, 검증을 위한 차량 노드들을 선택한다.
- [0068] 본 발명에서 제공한 신뢰 분석부(130)의 모델은 기본적인 동작 흐름을 도 4에 제시되어 있다.
- [0069] 도 4는 본 발명의 실시예에 따른 OS 및 애플리케이션 요청에 대한 신뢰 분석부의 프로세스를 나타낸 도면이다.
- [0070] 신뢰 분석부(130)의 모델은 보안 실행을 위한 사용자와 서비스 제공자(113)에 액세스할 수 있다.
- [0071] 사용자가 운영체제(OS) 또는 애플리케이션에 액세스하려는 경우, OS의 유효성 및 응용 프로그램의 신뢰성을 확인하라는 사용자 요청이 신뢰 분석부(130)에 수신된다.
- [0072] 신뢰 분석부(130)는 OS의 유효성이 있는지 판단한다(S100).
- [0073] 신뢰 분석부(130)는 OS 또는 애플리케이션이 유효하지 않으면, 세션이 10초 후에 종료된다(S101).
- [0074] 신뢰 분석부(130)는 OS 또는 애플리케이션이 유효한 경우, 스토리지, 입출력 실행 프로세스, 통신과 같은 서비스 액세스 가능성에 대한 액세스 권한이 부여된다(S102).
- [0075] 신뢰 분석부(130)는 액세스 권한이 부여된 애플리케이션의 신뢰성을 확인하여 신뢰할 수 있는지 판단하고(S103), 신뢰할 수 없는 경우, 애플리케이션의 세션이 10초 후에 종료된다는 경고 메시지를 생성하여 전송한다(S104).
- [0076] 신뢰 분석부(130)는 액세스 권한이 부여된 애플리케이션의 신뢰성을 확인하여 신뢰할 수 있다고 판단하는 경우, 애플리케이션을 구동시키고, 30초 안에 사용자 승인 메시지를 생성하여 전송한다(S105, S106).
- [0077] 블록체인 기반 개인 보호 인증 시스템(100)의 스마트 계약 모듈(Smart Contract Module)(140)은 차량 노드(111) 측에 배치된다. EOA는 데이터 식별자, 데이터 암호화키, 서비스 공급자 주소, 신뢰 분석부 주소, 서비스 제공자(113)의 신뢰 평가 결과와 같은 정보가 저장되는 차량 노드 사용자 측에 저장한다.

[0078] 다음은 신뢰 분석부의 프로세스를 알고리즘으로 나타낸 것이다.

Algorithm 1 Trust Execution (TE)

Input: VN_id; Data_id; SP_address; data_key; TE_address

if OS==valid **then**

 Start mapping

 SP_address-to-Data_id

 Sp_address-to-Data_key

 Sp_address-to-TE_address

 (Services accessible)

return true

else

return false; (OS not verified; Dismiss in 10 Sec)

if App==valid **then**

 Start booting; **return** true

else

return false; (Warn about APP; Dismiss in 10 Sec)

end

[0079]

[0080]

도 5는 본 발명의 실시예에 따른 스마트 계약 프로세스를 나타낸 도면이다.

[0081]

스마트 계약 모듈(140)은 차량 노드(111)의 식별 및 권한 부여, 데이터 검색 및 스마트 계약 완료를 세 가지 주요 함수를 사용하여 수행한다.

[0082]

첫 번째 식별 함수 및 권한 부여 함수에서, 차량 노드(111)는 스마트 계약을 통해 데이터 식별자를 업로드한다.

[0083]

EOA 주소는 식별자, 암호화키 및 신뢰 분석부 주소를 포함하는 인수들을 서비스 제공자(113)로 전송한다.

[0084]

사용자 데이터가 업데이트될 때마다 동일한 함수가 반복된다. 인증 함수에서, 차량 노드(111)는 신뢰할 수 있는 서비스 목록을 유지하여 서비스 제공자 신뢰 또는 신뢰할 수 없는 상태를 확인한다.

[0085]

두 번째 함수는 서비스 제공부(113)가 데이터 식별자를 검색하는 데이터 검색이다.

[0086]

서비스 제공부(113)가 호출할 때마다 EOA 주소가 저장되어 서비스 제공자(113)가 신뢰할 수 있는 목록에 있는지 여부를 확인한다.

[0087]

서비스 제공부(113)가 신뢰할 수 있는 경우, 함수는 데이터 식별자와 신뢰 분석부(130)의 주소를 반환한다. 이에 반해, 서비스 제공자(113)가 목록에 없으면, 액세스 권한에서 거부된다.

[0088]

세 번째 함수는 차량 노드(111)가 스마트 계약을 완료하고, 함수를 다시 호출하지 않고, 계약 업데이트를 일시 중지하는 스마트 계약 완료를 수행한다. 도 5는 스마트 계약 프로세스를 보여준다.

[0089]

스마트 계약 모듈(140)은 시스템 모델부(110)로부터 차량 노드 id(VN_id), 데이터 id(Data_id), 서비스 제공부 주소(SP_address), 데이터 키(data_key), 신뢰 분석부 주소(TE_address), 차량 노드(111)의 스마트 계약(VN_smartcontract)을 입력받는다(S200).

[0090]

스마트 계약 모듈(140)은 권한 부여 함수에서 서비스 제공부 주소를 매핑을 시작하고, 차량 노드(111)가 유효하다고 판단하는 경우, 성공 메시지를 반환한다(S201).

[0091]

스마트 계약 모듈(140)은 식별 함수에서 차량 노드(111)의 신뢰성이 있다고 판단하는 경우(S202), 차량 노드 id(VN_id)를 이용하여 데이터 식별자(data_identifier), 데이터 키(data_key), 신뢰 분석부 주소(TE_address)를 획득하고, 식별 함수에서 데이터 id(Data_id), 데이터 키(data_key), 신뢰 분석부 주소(TE_address)를 반환한다(S203).

[0092]

스마트 계약 모듈(140)은 차량 노드(111)의 신뢰성이 있다고 판단하는 경우, 스마트 계약을 완료한다(S204, S205).

[0093] 다음은 스마트 계약 프로세스를 알고리즘으로 나타낸 것이다.

Algorithm 2 Smartcontract Execution

Input: *VN_id*; *Data_id*; *SP_address*; *data_key*; *TE_address*; *VN_smartcontract*

For Authorization

if *VN (sender)*==*valid* **then**
 Start mapping
 SP_address;
 return true;
else
 return false;
end

For Identifier

if *VN trusted*==*valid* **then**
 get data_identifier, data_key, TE_address using VN_id
 return *data_id, data_key, TE_address*;
else
 return false;
end

Smartcontract Completion

if *VN trusted*==*valid* **then**
 terminate smartcontract
 pause VN_smartcontract
 return true;

else
 return false;
end

[0094]

[0095] 도 6은 본 발명의 실시예에 따른 데이터 크기에 따른 트랜잭션 비용 분석을 나타낸 도면이고, 도 7은 본 발명의 실시예에 따른 이벤트가 다른 트랜잭션 비용 및 실행 비용을 나타낸 그래프이다.

[0096] 이더리움 플랫폼은 차량 노드 id(*VN_id*), 데이터 id(*Data_id*), 서비스 제공부 주소(*SP_address*), 데이터 키(*data_key*), 신뢰 분석부 주소(*TE_address*), 차량 노드의 스마트 계약(*VN_smartcontract*)와 같은 스마트 계약에 규칙을 설정하는데 사용된다.

[0097] 블록체인 네트워크에서 Proof of Work(PoW) 합의는 블록체인 네트워크를 검증하는데 사용된다.

[0098] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)은 16개의 GM RAM, GeForce 920M 카드가 장착된 Core i7이 포함되어 있고, 초당 250K 해시 계산을 완료할 수 있다. 결과는 전체 트랜잭션 수로 생성된다. 시뮬레이션의 개수는 성능 평가를 위해 실행된다.

[0099] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)의 솔루션은 기존의 DKM for ITS 및 UGG/IPP와 비교된다.

[0100] 이더리움 블록체인에서는 GAS 비용을 네트워크에서 트랜잭션을 수행한다. GAS는 이더리움 블록체인에서 트랜잭션을 검증하고, 확인하기 위한 최소 단위이다.

[0101] 트랜잭션 및 실행 비용을 포함하여 블록체인 네트워크에서 관찰되는 두 가지 유형의 비용이 있다.

[0102] 트랜잭션 비용은 데이터를 블록체인으로 보내는데 필요한 총 가스 수를 의미하는 반면, 실행 비용은 함수에서 수행되는 작업을 나타낸다.

[0103] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)은 트랜잭션 비용과 실행 비용은 도 6 및 도 7에 나와 있다.

[0104] 트랜잭션 비용은 도 6과 같이 다양한 데이터 크기로 평가되고, 데이터 크기가 증가함에 따라 트랜잭션 비용이 점차 증가하는 것을 관찰할 수 있다.

[0105] 또 다른 요인은 스마트 계약을 배포하는 실행 비용보다 더 큰 트랜잭션 비용을 나타낸다.

[0106] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)의 주요 목표는 정보를 저장하는 어레이 대신 매핑 기능을

사용하여 GAS 비용을 가능한 한 낮게 유지하는 것이다. 도 6은 데이터 크기에 따른 트랜잭션 비용을 보여준다.

- [0107] 트랜잭션 비용은 일반적으로 데이터 크기를 늘릴 때마다 높아진다. 데이터 범위는 30바이트에서 210바이트까지 사용된다.
- [0108] 도 7은 스마트 계약에서 발생하는 다양한 이벤트에 대한 트랜잭션 비용 및 실행 비용의 분석을 보여준다.
- [0109] 이벤트 1은 서명 생성, 이벤트 2는 초기화, 이벤트 3은 응답 백 프로세스, 이벤트 4는 확인, 이벤트 5는 게시자 계정 초기화, 이벤트 6은 증인에게 인센티브를 전송하는 등 총 6가지 이벤트가 있다.
- [0110] 본 발명의 실험은 블록체인 기반 개인 보호 인증 시스템(100)을 서로 다른 트랜잭션이 있는 상태에서 분석했다. 먼저, 블록 GAS 한도를 300000, 800000, 1000000으로 설정한다.
- [0111] 결과는 본 발명의 솔루션이 초당 더 높은 트랜잭션을 보여주고, 낮은 블록 시간과 높은 GAS 블록 제한을 사용했다.
- [0112] 적절한 블록 시간 선택은 프로세스의 모든 종류의 지연을 방지하는데 중요하다. 세 가지 다른 트랜잭션은 함수 블록의 성능을 평가하는데 사용된다.
- [0113] 도 8은 본 발명의 실시예에 따른 300000 GAS 제한을 이용한 초당 트랜잭션 분석을 나타낸 도면이고, 도 9는 본 발명의 실시예에 따른 800000 GAS 제한을 이용한 초당 트랜잭션 분석을 나타낸 도면이고, 도 10은 본 발명의 실시예에 따른 1000000 GAS 제한을 이용한 초당 트랜잭션 분석을 나타낸 도면이고, 도 11은 본 발명의 실시예에 따른 서로 다른 아키텍처에서 트랜잭션 수 측면에서 시간 분석을 나타낸 도면이다.
- [0114] 도 8은 300000 GAS 제한이 있을 때 초당 트랜잭션 결과를 보여준다.
- [0115] 도 9는 800000 GAS 제한을 사용하여 초당 트랜잭션을 분석한 것으로, 블록 가스 한도가 증가할 때마다 높은 초당 트랜잭션이 급격히 감소하는 것을 관찰할 수 있다. 반면에 블록 시간이 증가하면, 초당 트랜잭션이 감소한다.
- [0116] 도 10은 1000000 GAS 제한을 사용하여 초당 트랜잭션을 분석한 결과이며, 블록 가스 한도가 증가할 때마다 높은 초당 트랜잭션이 급격히 감소하는 것을 다시 한 번 관찰할 수 있다. 반면에, 블록 시간이 증가하면, 초당 트랜잭션이 감소한다.
- [0117] 이러한 결과는 본 발명의 솔루션이 더 나은 성능을 보여준다.
- [0118] 도 11은 서로 다른 아키텍처에서 트랜잭션 수 측면에서 시간 분석을 위한 첫 번째 실험을 보여준다.
- [0119] 시스템 테스트를 위한 총 트랜잭션은 1500이고, 트랜잭션 수가 증가하면, 시스템 시간이 증가한다.
- [0120] 기존의 2개의 솔루션은 모두 블록체인을 기반으로 하지만, 대기 시간 및 처리로 인해 시스템 시간 측면에서 여전히 어려움을 겪고 있다.
- [0121] DKM과 UGG/IPP 솔루션은 분산 아키텍처로 인해 시스템 시간이 적다.
- [0122] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)은 DKM과 UGG/IPP 솔루션에 비해 시스템 시간이 더 짧다.
- [0123] 두 기존의 DKM과 UGG/IPP 솔루션은 동일한 시스템 시간으로 수행하는 것보다 트랜잭션의 수가 적을 때 배포된다.
- [0124] 본 발명의 솔루션이 트랜잭션 수가 200에 도달할 때마다, 트랜잭션이 1500에 도달할 때까지 결과에서 관찰된다.
- [0125] 800 트랜잭션에서 DKM의 시간 소비가 증가하고, 1500에서 5.3에 도달한다.
- [0126] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)의 전반적인 추세는 기존 개인 정보 보호 솔루션보다 좋고 시간이 덜 걸린다.
- [0127] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)은 기존의 개인 정보 보호 솔루션에 비해 더 나은 결과를 얻었다.
- [0128] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)은 데이터 유용성, 정확성, 복잡성과 오버헤드 측면에서 더 우수하다.
- [0129] 보안 및 프라이버시는 차량 노드 위치 및 데이터 프라이버시가 필요한 ITS 네트워크의 모든 영역에서 중요한 요

소 중 하나이다.

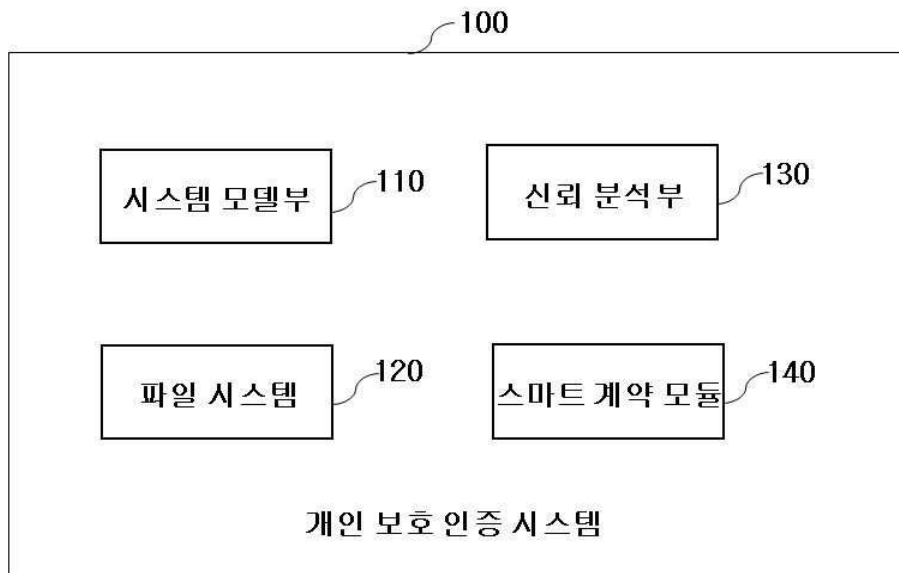
- [0130] 기존의 ITS 네트워크는 사용자의 수요 증가와 함수를 제공하는 다양한 서비스 제공업체로 인해 사용자 개인 정보가 침해되는 클라우드 및 에지 네트워크를 사용하고 있다.
- [0131] 본 발명에서는 수요 함수 기반의 접근 통제 정책과 스마트 계약 시스템을 이용하여 데이터 저장 접근, 처리 메카니즘을 통해 사용자의 프라이버시와 보안을 보장하기 위하여 블록체인 기반 개인 보호 인증이라는 데이터 프라이버시 모델을 제공한다.
- [0132] 본 발명의 블록체인 기반 개인 보호 인증 시스템(100)은 데이터 크기에 따른 트랜잭션 비용 측면에서도 좋은 성능을 보이며, 초당 트랜잭션 분석에서 낮은 블록 시간으로 달성할 수 있는 효과가 있다.
- [0133] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

부호의 설명

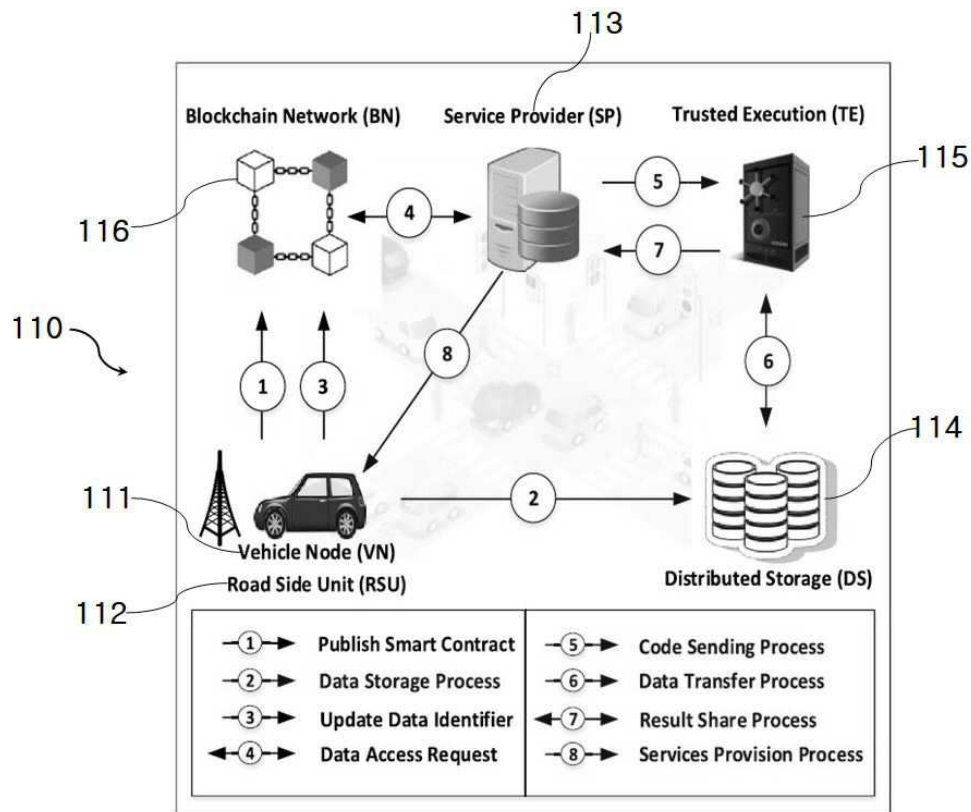
- [0134] 100: 블록체인 기반 개인 보호 인증 시스템 110: 시스템 모델부
- 111: 차량 노드 112: 로드 사이드 유니트
- 113: 서비스 제공부 114: 분산 저장소
- 115: 신뢰 실행부 116: 블록체인 네트워크
- 120: 파일 시스템 130: 신뢰 분석부
- 140: 스마트 계약 모듈

도면

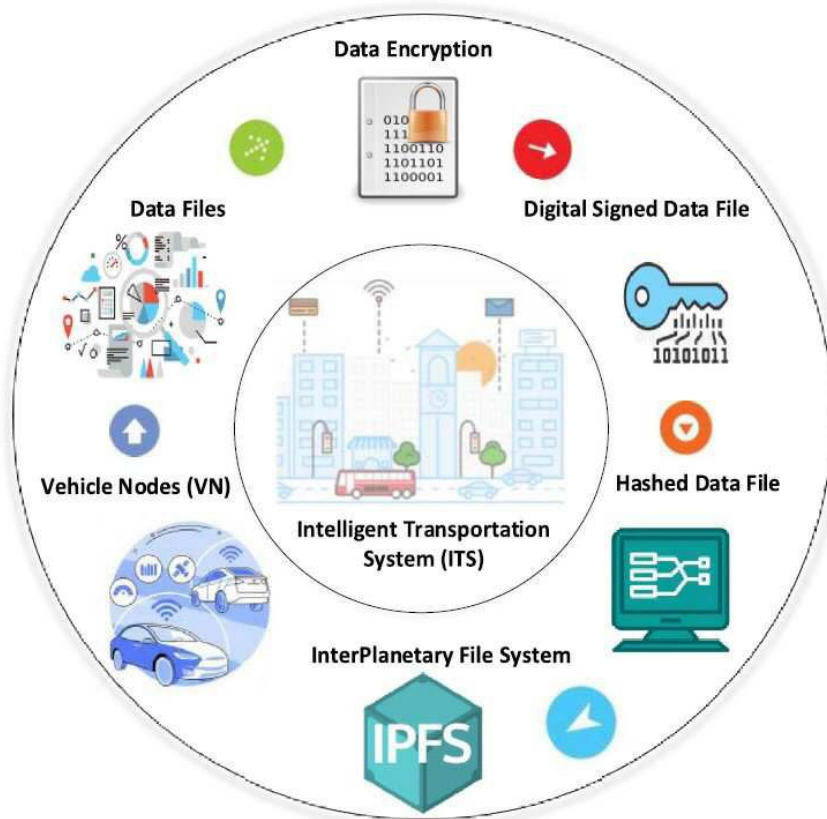
도면1



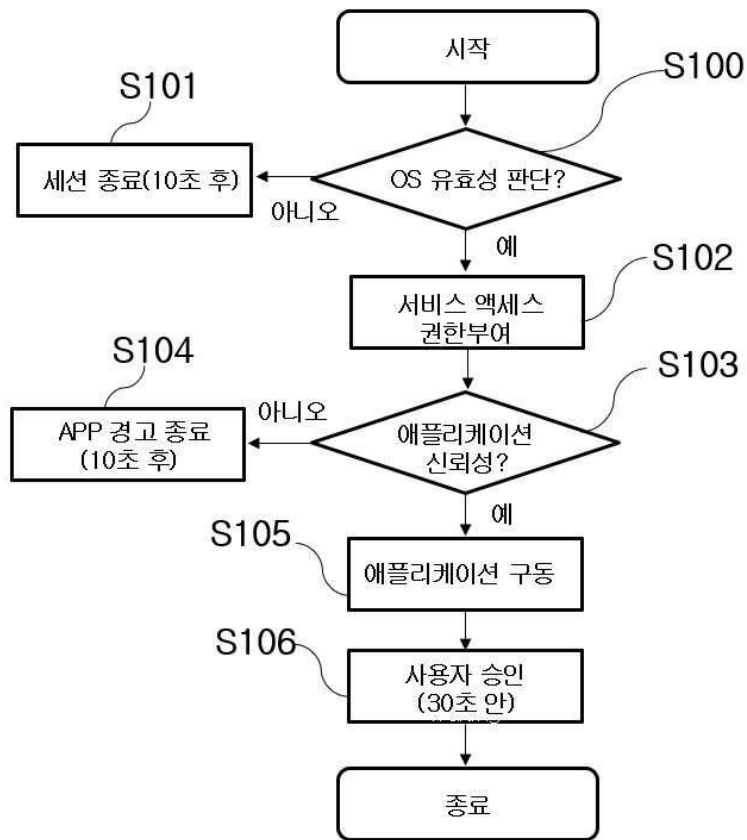
도면2



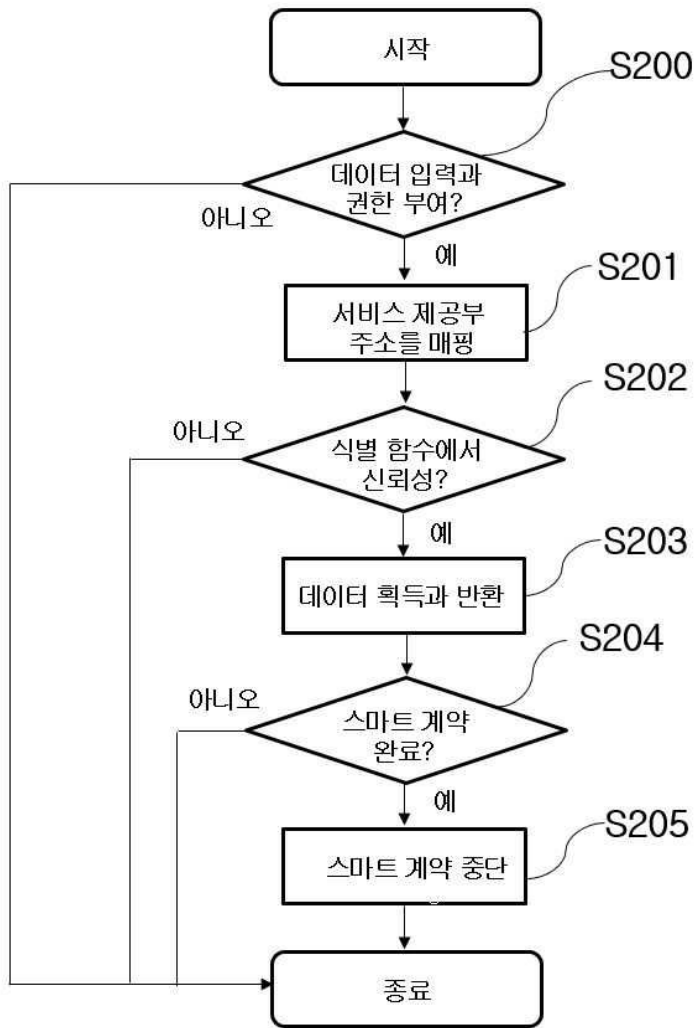
도면3



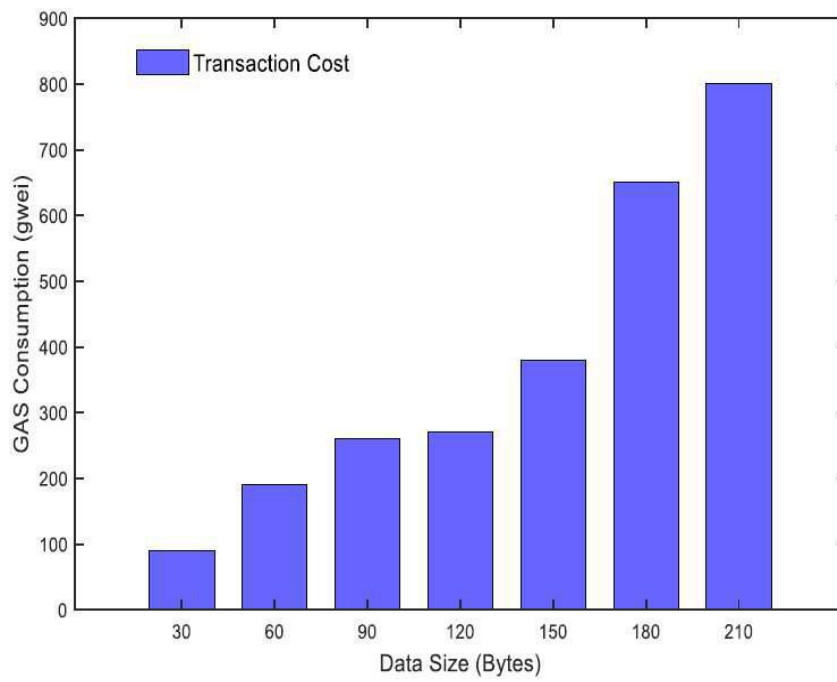
도면4



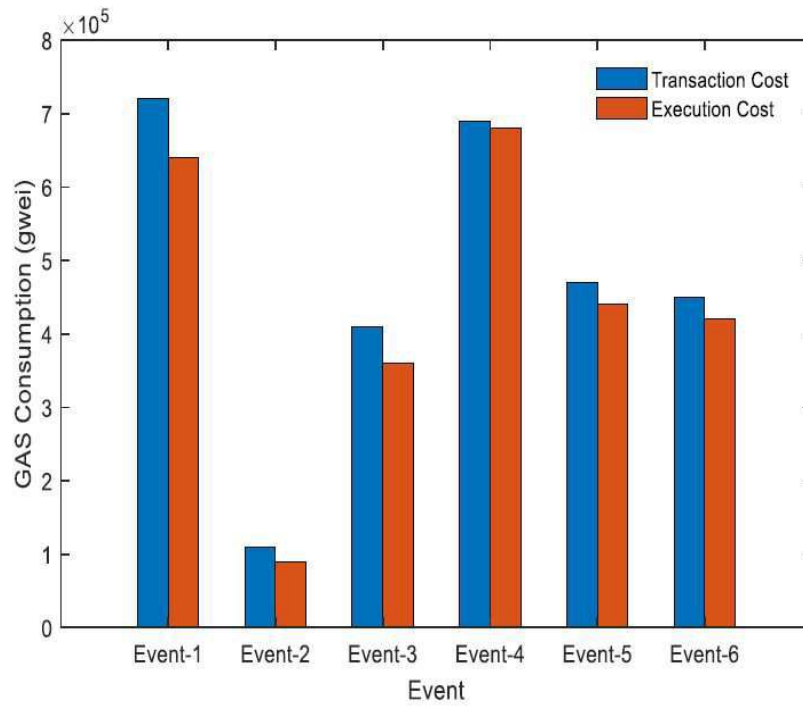
도면5



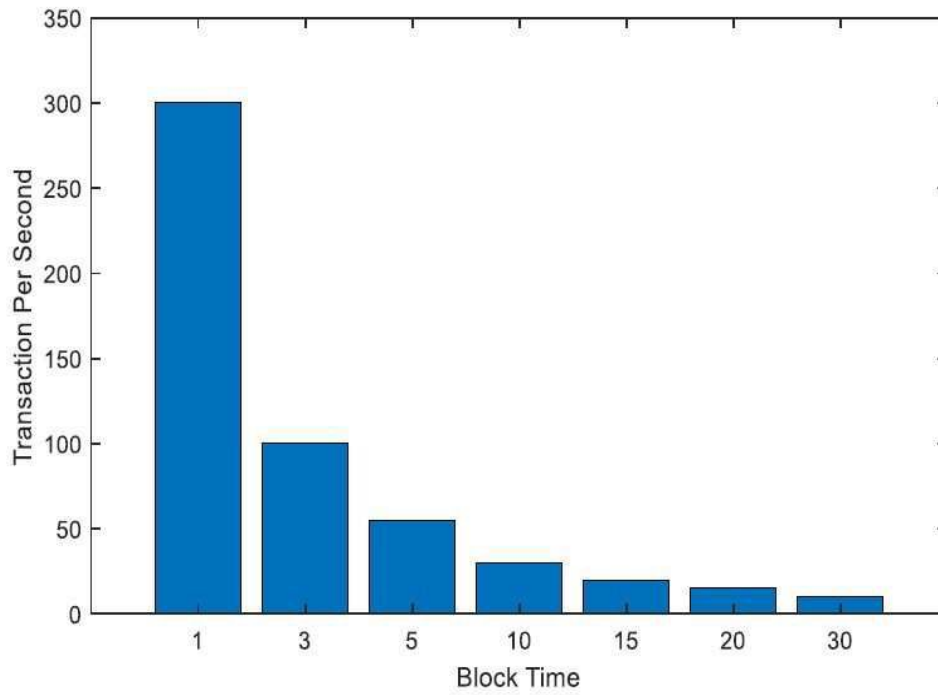
도면6



도면7

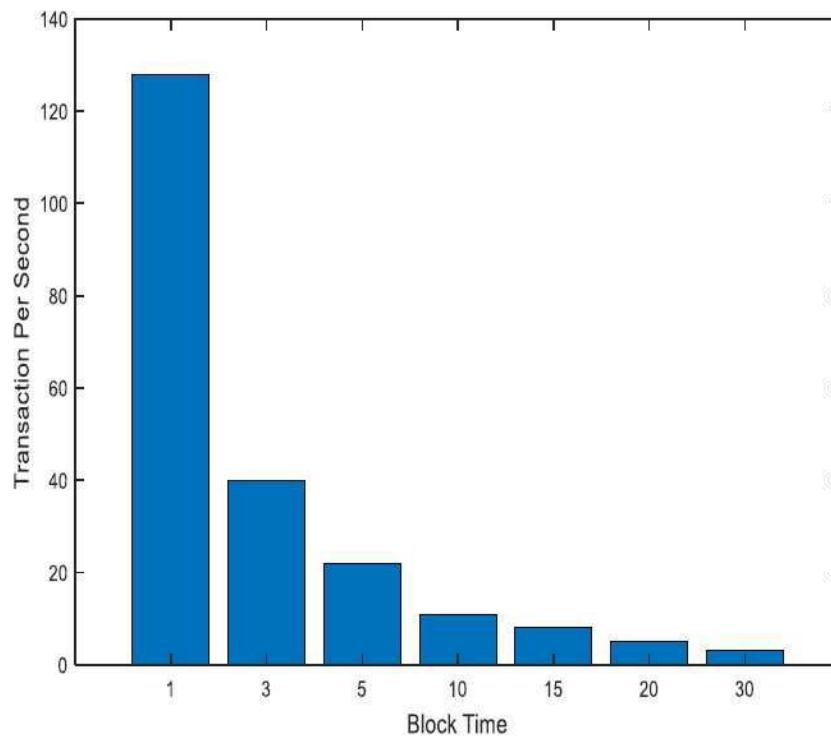


도면8



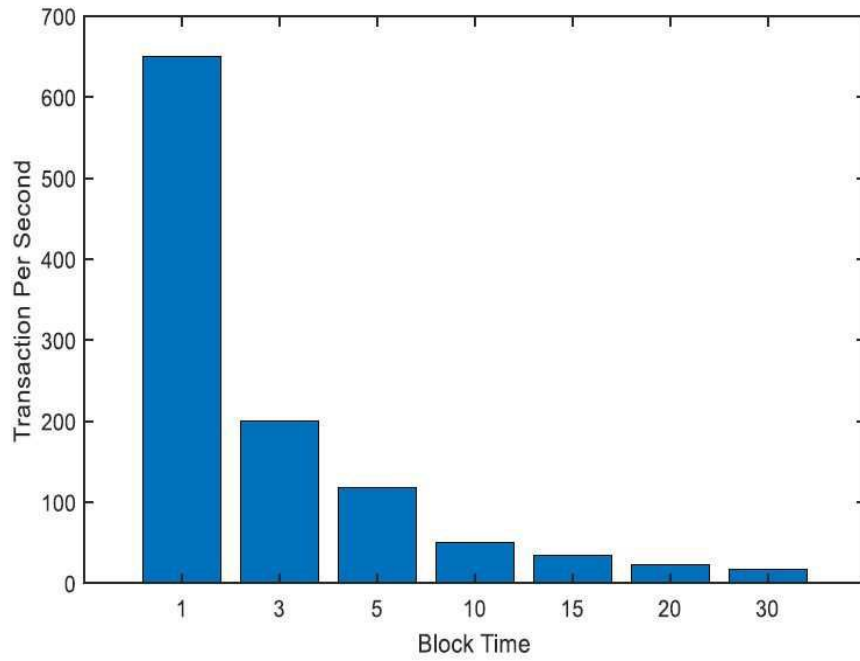
Transaction per seconds analysis by using 800000 GAS limit.

도면9



Transaction per seconds analysis by using 300000 GAS limit.

도면10



Transaction per seconds analysis by using 1000000 GAS limit.

도면11

