



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2023년07월06일

(11) 등록번호 10-2552295

(24) 등록일자 2023년07월03일

(51) 국제특허분류(Int. Cl.)

H04L 9/40 (2022.01) G16Y 30/10 (2020.01)

H04L 41/40 (2022.01) H04L 67/1097 (2022.01)

H04L 9/00 (2022.01) H04L 9/08 (2006.01)

H04L 9/32 (2006.01)

(52) CPC특허분류

H04L 63/083 (2013.01)

G16Y 30/10 (2020.01)

(21) 출원번호 10-2022-0044445

(22) 출원일자 2022년04월11일

심사청구일자 2022년04월11일

(56) 선행기술조사문헌

KR1020200032412 A

KR1020150034463 A

KR1020210150271 A

KR101979586 B1

(73) 특허권자

세종대학교산학협력단

서울특별시 광진구 능동로 209 (군자동, 세종대학교)

(72) 발명자

김영갑

서울특별시 광진구 능동로 209, 대양AI센터 701호(군자동)

강길욱

서울특별시 광진구 능동로 209, 대양AI센터 732호(군자동)

(74) 대리인

양성보

전체 청구항 수 : 총 14 항

심사관 : 천대식

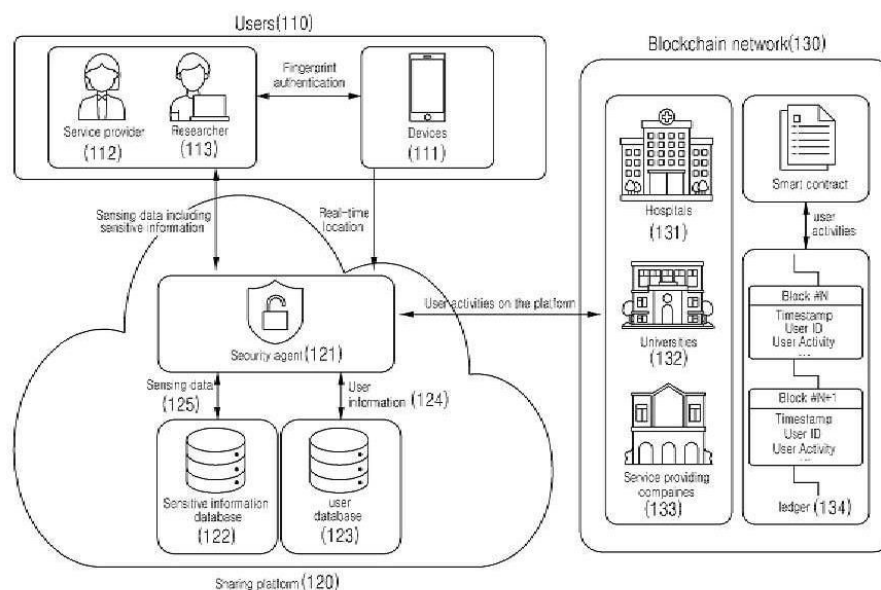
(54) 발명의 명칭 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 방법 및 시스템

(57) 요약

민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 방법 및 시스템이 제시된다. 본 발명에서 제안하는 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 방법은 사용자 단말을 통해 민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해

(뒷면에 계속)

대표도



지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화(Attribute-based encryption)의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록 단계, 개방형 클라우드 플랫폼에 저장된 센싱 데이터 내 민감정보에 대한 열에 대해 상기 개방형 클라우드 플랫폼에 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 개방형 클라우드 플랫폼에 저장하는 센싱 데이터 저장 단계, 사용자 단말을 통해 활용하고자 하는 센싱 데이터를 다운로드하는 센싱 데이터 다운로드 단계 및 상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계를 포함한다.

(52) CPC특허분류

H04L 41/40 (2022.05)

H04L 63/0861 (2013.01)

H04L 63/1425 (2013.01)

H04L 67/1097 (2022.05)

H04L 9/0872 (2013.01)

H04L 9/3297 (2013.01)

H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711131006
과제번호	2019-0-00231
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)(R&D)
연구과제명	클라우드 기반 블록체인, 자가적응 기술을 이용한 이기종 IoT 플랫폼 간 보안 상호
운용 기술 연구	
기 여 율	1/1
과제수행기관명	세종대학교 산학협력단
연구기간	2022.03.01 ~ 2023.02.28

명세서

청구범위

청구항 1

사용자 단말을 통해 민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해 지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화(Attribute-based encryption)의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록 단계;

개방형 클라우드 플랫폼에 저장된 센싱 데이터 내 민감정보에 대한 열에 대해 상기 개방형 클라우드 플랫폼에 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 개방형 클라우드 플랫폼에 저장하는 센싱 데이터 저장 단계;

사용자 단말을 통해 활용하고자 하는 센싱 데이터를 다운로드하는 센싱 데이터 다운로드 단계; 및

상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계

를 포함하는 사용자 인증 방법.

청구항 2

제1항에 있어서,

상기 사용자 단말을 통해 민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해 지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록 단계는,

상기 사용자 단말을 통해 사용자가 사용할 아이디, 패스워드를 포함하는 사용자 정보를 입력 받아 개방형 클라우드 플랫폼 내 보안 에이전트에 전달하고,

상기 보안 에이전트가 상기 사용자 정보를 사용자 데이터베이스에 저장하고,

상기 사용자 단말을 통해 상기 보안 에이전트에 사용자 정보와 함께 사용자 단말 등록을 요청하면, 상기 보안 에이전트가 해당 사용자 정보를 전달받아 패스워드 기반 인증을 수행하고 사용자 인증에 성공하면 사용자 단말 정보를 사용자 데이터베이스에 추가하고, 사용자 등록 결과를 반환하는

사용자 인증 방법.

청구항 3

제1항에 있어서,

상기 개방형 클라우드 플랫폼에 저장된 센싱 데이터 내 민감정보에 대한 열에 대해 상기 개방형 클라우드 플랫폼에 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 개방형 클라우드 플랫폼에 저장하는 센싱 데이터 다운로드 단계는,

상기 개방형 클라우드 플랫폼에 센싱 데이터를 업로드하기 전에 해당 센싱 데이터에 대한 추가 데이터를 미리 등록된 기관들로부터 전달 받아 데이터 연계 및 민감정보에 대한 비식별화를 진행하고,

해당 기관로부터 비식별화된 센싱 데이터를 민감정보를 포함한 열에 대한 정보와 함께 상기 개방형 클라우드 플랫폼에 업로드하고,

상기 개방형 클라우드 플랫폼 내 보안 에이전트는 업로드된 정보에 기초하여 민감정보를 포함한 열에 대해 해당 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고,

상기 보안 에이전트는 민감정보 데이터베이스에 해당 데이터를 업로드하고, 업로드에 관한 결과를 업로드를 요청한 기관에 전달하는

사용자 인증 방법.

청구항 4

제1항에 있어서,

상기 사용자 단말을 통해 활용하고자 하는 센싱 데이터를 다운로드하는 센싱 데이터 다운로드 단계는,

사용자 단말을 통해 상기 개방형 클라우드 플랫폼에 로그인한 후, 다운로드를 원하는 센싱 데이터를 선택하고, 선택된 센싱 데이터를 개방형 클라우드 플랫폼에 요청하고,

개방형 클라우드 플랫폼 내 보안 에이전트는 해당 센싱 데이터를 민감정보 데이터베이스에서 검색하여 가져오고, 상기 보안 에이전트는 사용자 데이터베이스에서 다운로드를 요청한 사용자 정보를 가져오고,

가져온 사용자의 정보를 이용하여 센싱 데이터에 대해 속성기반 암호화를 한 번 더 수행하고, 데이터 내용 전체를 암호화하여 암호화된 센싱 데이터를 사용자 단말에게 반환하는

사용자 인증 방법.

청구항 5

제1항에 있어서,

상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계는,

상기 사용자 단말을 통해 상기 개방형 클라우드 플랫폼에 로그인 및 인증을 수행하고,

상기 개방형 클라우드 플랫폼 내 보안 에이전트가 사용자의 실시간 위치정보와 사용자 정보를 이용하여 암호화된 센싱 데이터의 복호화를 시도하여 복호화에 성공하면, 해당 사용자 활동을 타임 스탬프와 함께 블록체인 네트워크의 분산원장에 기록하도록 개방형 클라우드 플랫폼 내 등록된 기관들에 요청하고,

상기 블록체인 네트워크를 통해 해당 기관들에 대한 스마트 계약을 실행하여, 분산원장에 해당 사용자 활동을 기록하고, 상기 보안 에이전트에게 요청 결과를 반환하며,

상기 보안 에이전트가 기록에 성공했음을 반환 받으면, 최종적으로 복호화된 데이터를 활용하도록 활용 페이지와 복호화된 데이터를 사용자 단말에게 전달하는

사용자 인증 방법.

청구항 6

제5항에 있어서,

상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계는,

센싱 데이터 활용을 위해 플랫폼에 사용자가 로그인하는 과정에서 발생하는 상기 개방형 클라우드 플랫폼 내 인증되지 않은 불법 사용자가 정당한 사용자의 아이디를 탈취하여 무작위 대입 공격을 수행하는 경우를 실시간으로 탐지하는

사용자 인증 방법.

청구항 7

제5항에 있어서,

상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계는,

센싱 데이터의 복호화를 수행하는 과정에서 발생하는 상기 개방형 클라우드 플랫폼에서 인가된 사용자가 다운로드한 센싱 데이터가 불법적으로 인가되지 않은 사용자에게 공유되어 활용을 시도하는 경우를 실시간으로 탐지하는

사용자 인증 방법.

청구항 8

민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해 지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화(Attribute-based encryption)의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록을 수행하고, 활용하고자 하는 센싱 데이터를 개방형 클라우드 플랫폼으로부터 다운로드하는 사용자 단말;

저장된 센싱 데이터 내 민감정보에 대한 열에 대해 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행 및 저장하는 개방형 클라우드 플랫폼; 및

상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하도록 하고, 상기 개방형 클라우드 플랫폼 내 보안 에이전트가 암호화된 센싱 데이터의 복호화를 시도하여 복호화에 성공하면, 분산원장에 기록하는 블록체인 네트워크

를 포함하는 사용자 인증 시스템.

청구항 9

제8항에 있어서,

상기 사용자 단말은 사용자가 사용할 아이디, 패스워드를 포함하는 사용자 정보를 입력 받아 상기 개방형 클라우드 플랫폼 내 보안 에이전트에 전달하고,

상기 보안 에이전트는 상기 사용자 정보를 사용자 데이터베이스에 저장하고,

상기 사용자 단말이 상기 보안 에이전트에 사용자 정보와 함께 사용자 단말 등록을 요청하면, 상기 보안 에이전트가 해당 사용자 정보를 전달받아 패스워드 기반 인증을 수행하고 사용자 인증에 성공하면 사용자 단말 정보를 사용자 데이터베이스에 추가하고, 사용자 등록 결과를 반환하는

사용자 인증 시스템.

청구항 10

제8항에 있어서,

상기 사용자 단말은 상기 개방형 클라우드 플랫폼에 센싱 데이터를 업로드하기 전에 해당 센싱 데이터에 대한 추가 데이터를 미리 등록된 기관들로부터 전달 받아 데이터 연계 및 민감정보에 대한 비식별화를 진행하고, 해당 기관로부터 비식별화된 센싱 데이터를 민감정보를 포함한 열에 대한 정보와 함께 상기 개방형 클라우드 플랫폼에 업로드하고,

상기 개방형 클라우드 플랫폼 내 보안 에이전트는 업로드된 정보에 기초하여 민감정보를 포함한 열에 대해 해당 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 보안 에이전트는 민감정보 데이터베이스에 해당 데이터를 업로드하고, 업로드에 관한 결과를 업로드를 요청한 기관에 전달하는

사용자 인증 시스템.

청구항 11

제8항에 있어서,

상기 사용자 단말은 상기 개방형 클라우드 플랫폼에 로그인한 후, 다운로드를 원하는 센싱 데이터를 선택하고, 선택된 센싱 데이터를 개방형 클라우드 플랫폼에 요청하고,

상기 개방형 클라우드 플랫폼 내 보안 에이전트는 해당 센싱 데이터를 민감정보 데이터베이스에서 검색하여 가져오고, 상기 보안 에이전트는 사용자 데이터베이스에서 다운로드를 요청한 사용자 정보를 가져오고, 가져온 사용자의 정보를 이용하여 센싱 데이터에 대해 속성기반 암호화를 한 번 더 수행하고, 데이터 내용 전체를 암호화하여 암호화된 센싱 데이터를 사용자 단말에게 반환하는

사용자 인증 시스템.

청구항 12

제8항에 있어서,

상기 사용자 단말은 상기 개방형 클라우드 플랫폼에 로그인 및 인증을 수행하고,

상기 개방형 클라우드 플랫폼 내 보안 에이전트가 사용자의 실시간 위치정보와 사용자 정보를 이용하여 암호화된 센싱 데이터의 복호화를 시도하여 복호화에 성공하면, 해당 사용자 활동을 타임 스탬프와 함께 블록체인 네트워크의 분산원장에 기록하도록 개방형 클라우드 플랫폼 내 등록된 기관들에 요청하고,

상기 블록체인 네트워크는 해당 기관들에 대한 스마트 계약을 실행하여, 분산원장에 해당 사용자 활동을 기록하고, 상기 보안 에이전트에게 요청 결과를 반환하며,

상기 보안 에이전트가 기록에 성공했음을 반환 받으면, 최종적으로 복호화된 데이터를 활용하도록 활용 페이지와 복호화된 데이터를 사용자 사용자 단말에게 전달하는

사용자 인증 시스템.

청구항 13

제12항에 있어서,

상기 사용자 단말은,

상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하기 위해 센싱 데이터 활용을 위해 플랫폼에 사용자가 로그인하는 과정에서 발생하는 상기 개방형 클라우드 플랫폼 내 인증되지 않은 불법 사용자가 정당한 사용자의 아이디를 탈취하여 무작위 대입 공격을 수행하는 경우를 실시간으로 탐지하는

사용자 인증 시스템.

청구항 14

제12항에 있어서,

상기 사용자 단말은,

상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하기 위해 센싱 데이터의 복호화를 수행하는 과정에서 발생하는 상기 개방형 클라우드 플랫폼에서 인가된 사용자가 다운로드한 센싱 데이터가 불법적으로 인가되지 않은 사용자에게 공유되어 활용을 시도하는 경우를 실시간으로 탐지하는

사용자 인증 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 방법 및 시스템에 관한 것이다.

배경 기술

[0002] 사물인터넷이 발전되면서 일상생활에 다양한 사물인터넷 기기들이 많이 보급되었고, 기기 내 많은 센서로부터 센싱 데이터들이 수집되고 있다. 이러한 데이터들이 공유되면 다양한 서비스와 부가가치를 창출할 수 있지만, 해당 데이터는 민감정보(예를 들어, 헬스케어 관련 정보 등)를 포함하고 있으므로 비인증 및 인가자에게 불법적으로 공유될 시에 개인정보 유출과 같은 사회적 문제를 일으킬 수 있다. 따라서, 민감정보를 포함하는 센싱 데이터를 안전하게 공유할 수 있도록 개방형 클라우드 플랫폼에서 비인증 사용자 및 비인가 사용자를 식별하고 차단할 수 있는 연구가 필요하다.

선행기술문헌

특허문헌

[0003] (특허문헌 0001) 한국등록특허 제10-2302351호(2021.09.09)

발명의 내용

해결하려는 과제

[0004] 본 발명이 이루고자 하는 기술적 과제는 민감정보를 포함하고 있는 센싱 데이터를 공유하기 위한 개방형 클라우드 플랫폼에서 발생하는 인증되지 않은 사용자 및 인가되지 않은 사용자를 포함하는 불법 사용자를 탐지하기 위한 허가형 블록체인 기반 사용자 인증 방법 및 시스템을 제공하는데 있다. 본 발명의 실시예에 따르면 허가형 블록체인 내의 분산원장(Distributed Ledger) 이용하여 플랫폼 내 모든 사용자의 활동에 대해서 무결성 및 부인방지를 보장하고, 책임 추적성(Accountability)을 제공하고자 한다.

과제의 해결 수단

[0005] 일 측면에 있어서, 본 발명에서 제안하는 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 방법은 사용자 단말을 통해 민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해 지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화(Attribute-based encryption)의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록 단계, 개방형 클라우드 플랫폼에 저장된 센싱 데이터 내 민감정보에 대한 열에 대해 상기 개방형 클라우드 플랫폼에 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 개방형 클라우드 플랫폼에 저장하는 센싱 데이터 저장 단계, 사용자 단말을 통해 활용하고자 하는 센싱 데이터를 다운로드하는 센싱 데이터 다운로드 단계 및 상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계를 포함한다.

[0006] 상기 사용자 단말을 통해 민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해 지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록 단계는 상기 사용자 단말을 통해 사용자가 사용할 아이디, 패스워드를 포함하는 사용자 정보를 입력 받아 개방형 클라우드 플랫폼 내 보안 에이전트에 전달하고, 상기 보안 에이전트가 상기 사용자 정보를 사용자 데이터베이스에 저장하고, 상기 사용자 단말을 통해 상기 보안 에이전트에 사용자 정보와 함께 사용자 단말 등록을 요청하면, 상기 보안 에이전트가 해당 사용자 정보를 전달받아 패스워드 기반 인증을 수행하고 사용자 인증에 성공하면 사용자 단말 정보를 사용자 데이터베이스에 추가하고, 사용자 등록 결과를 반환한다.

[0007] 상기 개방형 클라우드 플랫폼에 저장된 센싱 데이터 내 민감정보에 대한 열에 대해 상기 개방형 클라우드 플랫폼에 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 개방형 클라우드 플랫폼에 저장하는 센싱 데이터 다운로드 단계는 상기 개방형 클라우드 플랫폼에 센싱 데이터를 업로드하기 전에 해당 센싱 데이터에 대한 추가 데이터를 미리 등록된 기관들로부터 전달 받아 데이터 연계 및 민감정보에 대한 비식별화를 진행하고, 해당 기관들로부터 비식별화된 센싱 데이터를 민감정보를 포함한 열에 대한 정보와 함께 상기 개방형 클라우드 플랫폼에 업로드하고, 상기 개방형 클라우드 플랫폼 내 보안 에이전트는 업로드된 정보에 기초하여 민감정보를 포함한 열에 대해 해당 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 보안 에이전트는 민감정보 데이터베이스에 해당 데이터를 업로드하고, 업로드에 관한 결과를 업로드를 요청한 기관에 전달한다.

[0008] 상기 사용자 단말을 통해 활용하고자 하는 센싱 데이터를 다운로드하는 센싱 데이터 다운로드 단계는 사용자 단말을 통해 상기 개방형 클라우드 플랫폼에 로그인한 후, 다운로드를 원하는 센싱 데이터를 선택하고, 선택된 센싱 데이터를 개방형 클라우드 플랫폼에 요청하고, 개방형 클라우드 플랫폼 내 보안 에이전트는 해당 센싱 데이터를 민감정보 데이터베이스에서 검색하여 가져오고, 상기 보안 에이전트는 사용자 데이터베이스에서 다운로드를 요청한 사용자 정보를 가져오고, 가져온 사용자의 정보를 이용하여 센싱 데이터에 대해 속성기반 암호화를 한 번 더 수행하고, 데이터 내용 전체를 암호화하여 암호화된 센싱 데이터를 사용자 단말에게 반환한다.

[0009] 상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계는 상기 사용자 단말을 통해 상기 개방형 클라우드 플랫폼에 로그인 및 인증을 수행하고, 상기 개방형 클라우드 플랫폼 내 보안 에이전트가 사용자의 실시간 위치정보와 사용자 정보를 이용하여 암호화된 센싱 데이터의 복호화를 시도하여 복호화에 성공하면, 해당 사용자 활동을 타임 스탬프와 함께 블

록체인 네트워크의 분산원장에 기록하도록 개방형 클라우드 플랫폼 내 등록된 기관들에 요청하고, 상기 블록체인 네트워크를 통해 해당 기관들에 대한 스마트 계약을 실행하여, 분산원장에 해당 사용자 활동을 기록하고, 상기 보안 에이전트에게 요청 결과를 반환하며, 상기 보안 에이전트가 기록에 성공했음을 반환 받으면, 최종적으로 복호화된 데이터를 활용하도록 활용 페이지와 복호화된 데이터를 사용자 사용자 단말에게 전달한다.

[0010] 상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계는 센싱 데이터 활용을 위해 플랫폼에 사용자가 로그인하는 과정에서 발생하는 상기 개방형 클라우드 플랫폼 내 인증되지 않은 불법 사용자가 정당한 사용자의 아이디를 탈취하여 무작위 대입 공격을 수행하는 경우를 실시간으로 탐지한다.

[0011] 상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계는 센싱 데이터의 복호화를 수행하는 과정에서 발생하는 상기 개방형 클라우드 플랫폼에서 인가된 사용자가 다운로드한 센싱 데이터가 불법적으로 인가되지 않은 사용자에게 공유되어 활용을 시도하는 경우를 실시간으로 탐지한다.

[0012] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 시스템은 민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해 지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화(Attribute-based encryption)의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록을 수행하고, 활용하고자 하는 센싱 데이터를 개방형 클라우드 플랫폼으로부터 다운로드하는 사용자 단말, 저장된 센싱 데이터 내 민감정보에 대한 열에 대해 등록된 기관들의 위치 정보를 이용하여 속성기반 암호화를 수행 및 저장하는 개방형 클라우드 플랫폼 및 상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하도록 하고, 상기 개방형 클라우드 플랫폼 내 보안 에이전트가 암호화된 센싱 데이터의 복호화를 시도하여 복호화에 성공하면, 분산원장에 기록하는 블록체인 네트워크를 포함한다.

발명의 효과

[0013] 본 발명의 실시예들에 따르면 개방형 클라우드 플랫폼에서 민감정보를 포함한 센싱 데이터를 안전하게 저장 및 관리하도록 할 뿐만 아니라 비인증된 사용자 및 비인가된 사용자들을 허가형 블록체인 기술을 이용해 실시간으로 탐지할 수 있도록 하고, 신뢰성 있는 분산 로깅 및 강력한 책임 추적성을 제공할 수 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예에 따른 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 시스템의 전체 구성을 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 방법을 설명하기 위한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 사용자 등록 단계를 설명하기 위한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 센싱 데이터 저장 단계를 설명하기 위한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 센싱 데이터 다운로드 단계를 설명하기 위한 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 센싱 데이터 활용 단계를 설명하기 위한 흐름도이다.

도 7은 본 발명의 일 실시예에 따른 플랫폼 내 인증되지 않은 불법 사용자 탐지 과정을 설명하기 위한 도면이다.

도 8은 본 발명의 일 실시예에 따른 플랫폼 내에서 인가되지 않은 불법 사용자 탐지 과정을 설명하기 위한 도면이다.

도 9는 본 발명의 일 실시예에 따른 보안 에이전트의 의사코드 알고리즘을 나타내는 도면이다.

도 10은 본 발명의 일 실시예에 따른 블록체인 네트워크 구성에 따른 평균 지연율을 나타내는 그래프이다.

도 11은 본 발명의 일 실시예에 따른 블록체인 네트워크 구성에 따른 처리량을 나타내는 그래프이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0017] 도 1은 본 발명의 일 실시예에 따른 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 시스템의 전체 구성을 나타내는 도면이다.
- [0018] 개방형 클라우드 플랫폼에서 민감정보를 포함한 센싱 데이터를 안전하게 보호하고 불법 사용자를 탐지하기 위해 제안하는 사용자 인증 시스템은 도 1과 같이 사용자 단말(110), 클라우드 기반 플랫폼(120) 및 블록체인 네트워크(130)로 구성된 프레임워크로 구성되어 있다.
- [0019] 본 발명의 실시예에 따른 사용자 단말(110), 클라우드 기반 플랫폼(120) 및 블록체인 네트워크(130)는 도 2의 단계들(210~240)을 수행하기 위해 구성될 수 있다.
- [0020] 특히, 비인가 사용자 및 비인증 사용자로 식별되는 허가형 블록체인을 이용하여 무차별 대입 공격(brute-force attack)을 수행하는 사용자, 인가되지 않은 센싱 데이터를 사용하려고 시도하려는 불법 사용자들을 플랫폼 내 보안 에이전트(121)가 블록체인 네트워크(130)의 분산원장(134)을 토대로 실시간으로 차단할 뿐 아니라 플랫폼 관리자가 이들을 쉽게 탐지하고 보안 사고 발생 시에 사후 관리를 용이하게 한다.
- [0021] 본 발명의 실시예에 따른 사용자 단말(110)은 개방형 클라우드 기반 플랫폼(120) 내 민감정보(122)를 포함한 센싱 데이터(125)를 공유하거나 이용하려는 연구자(113) 및 서비스 제공자들(112)이 이용하는 단말로서 이들은 기본적으로 플랫폼(120)에 등록된 기관 사용자이어야만 사용자 단말(예를 들어, 스마트폰(111))을 통해 플랫폼(120) 내에서 데이터를 이용할 수 있다. 또한, 이들은 소속, 직위 등에 따라 플랫폼(120) 내에서 다운로드할 수 있는 센싱 데이터(125)가 존재한다.
- [0022] 본 발명의 실시예에 따른 개방형 클라우드 기반 플랫폼(120)은 보안 에이전트(121)와 두 개의 데이터베이스(122, 123)로 구성되어 있다. 특히, 보안 에이전트(121)는 민감정보(122)를 포함한 센싱 데이터(125)를 안전하게 플랫폼(120) 내에 저장하고 관리할 수 있도록 도울 뿐만 아니라 블록체인 클라이언트로서 블록체인 네트워크(130)의 분산원장(134)에 플랫폼(120) 내 사용자의 활동이 기록되도록 요청하고 분산원장에 기록된 사용자의 활동을 조회하는 역할을 한다. 두 개의 데이터베이스는 사용자의 소속, 아이디, 해시화된 비밀번호 등을 포함하고 있는 사용자 데이터베이스(123)와 민감정보를 포함한 센싱 데이터를 컬럼 암호화(Column-level encryption) 후에 저장하고 있는 민감정보 데이터베이스(122)가 있다.
- [0023] 본 발명의 실시예에 따른 블록체인 네트워크(130)는 플랫폼에 등록된 기관들(131, 132, 133)이 피어로 참여하는 네트워크로서, 신뢰할 수 있는 기관들이 보안 에이전트(121)가 전달한 플랫폼(120) 내 사용자의 활동을 분산원장(134)에 저장하고 관리하게 되어 높은 로그의 신뢰성을 보장한다. 또한, 탈중앙화라는 블록체인의 특징으로 인해 특정 기관의 시스템이 장애가 발생하더라도 단일 장애점(Single Point of Failure; SPoF) 문제가 발생하지 않는다. 본 발명의 실시예에 따른 사용자 인증 시스템 동작의 구체적인 단계는 사용자 등록 단계, 센싱 데이터 저장 단계, 센싱 데이터 다운로드 및 활용 단계로 구성되어 있으며, 도 2 내지 도 6을 참조하여 각 단계에 대해 더욱 상세히 설명한다.
- [0025] 도 2는 본 발명의 일 실시예에 따른 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 방법을 설명하기 위한 흐름도이다.
- [0026] 제안하는 민감정보를 포함하는 개방형 클라우드 플랫폼에서의 허가형 블록체인 기반 사용자 인증 방법은 사용자 단말을 통해 민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해 지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화(Attribute-based encryption)의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록 단계(210), 개방형 클라우드 플랫폼에 저장된 센싱 데이터 내 민감정보에 대한 열에 대해 상기 개방형 클라우드 플랫폼에 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 개방형 클라우드 플랫폼에 저장하는 센싱 데이터 저장 단계(220), 사용자 단말을 통해 활용하고자 하는 센싱 데이터를 다운로드하는 센싱 데이터 다운로드 단계(230) 및 상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계(240)을 포함한다.
- [0027] 단계(210)에서, 사용자 단말을 통해 민감정보를 포함하는 개방형 클라우드 플랫폼에 저장된 데이터를 활용하기 위해 지문 인증 및 GPS 기능을 사용하고, 속성기반 암호화(Attribute-based encryption)의 속성으로 활용하기 위한 사용자 정보를 저장하는 사용자 등록 단계를 수행한다.
- [0028] 이때, 상기 사용자 단말을 통해 사용자가 사용할 아이디, 패스워드를 포함하는 사용자 정보를 입력 받아 개방형 클라우드 플랫폼 내 보안 에이전트에 전달한다. 상기 보안 에이전트는 상기 사용자 정보를 사용자 데이터베이스

에 저장한다. 상기 사용자 단말을 통해 상기 보안 에이전트에 사용자 정보와 함께 사용자 단말 등록을 요청하면, 상기 보안 에이전트가 해당 사용자 정보를 전달받아 패스워드 기반 인증을 수행하고 사용자 인증에 성공하면 사용자 단말 정보를 사용자 데이터베이스에 추가하고, 사용자 등록 결과를 반환한다.

[0029] 단계(220)에서, 개방형 클라우드 플랫폼에 저장된 센싱 데이터 내 민감정보에 대한 열에 대해 상기 개방형 클라우드 플랫폼에 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고, 상기 개방형 클라우드 플랫폼에 저장하는 센싱 데이터 다운로드 단계를 수행한다.

[0030] 이때, 상기 개방형 클라우드 플랫폼에 센싱 데이터를 업로드하기 전에 해당 센싱 데이터에 대한 추가 데이터를 미리 등록된 기관들로부터 전달 받아 데이터 연계 및 민감정보에 대한 비식별화를 진행한다. 이후, 해당 기관들로부터 비식별화된 센싱 데이터를 민감정보를 포함한 열에 대한 정보와 함께 상기 개방형 클라우드 플랫폼에 업로드한다. 상기 개방형 클라우드 플랫폼 내 보안 에이전트는 업로드된 정보에 기초하여 민감정보를 포함한 열에 대해 해당 기관들의 위치정보를 이용하여 속성기반 암호화를 수행한다. 상기 보안 에이전트는 민감정보 데이터베이스에 해당 데이터를 업로드하고, 업로드에 관한 결과를 업로드를 요청한 기관에 전달한다.

[0031] 단계(230)에서, 사용자 단말을 통해 활용하고자 하는 센싱 데이터를 다운로드하는 센싱 데이터 다운로드 단계를 수행한다.

[0032] 이때, 사용자 단말을 통해 상기 개방형 클라우드 플랫폼에 로그인한 후, 다운로드를 원하는 센싱 데이터를 선택하고, 선택된 센싱 데이터를 개방형 클라우드 플랫폼에 요청한다. 개방형 클라우드 플랫폼 내 보안 에이전트는 해당 센싱 데이터를 민감정보 데이터베이스에서 검색하여 가져오고, 상기 보안 에이전트는 사용자 데이터베이스에서 다운로드를 요청한 사용자 정보를 가져온다. 이후, 가져온 사용자의 정보를 이용하여 센싱 데이터에 대해 속성기반 암호화를 한 번 더 수행하고, 데이터 내용 전체를 암호화하여 암호화된 센싱 데이터를 사용자 단말에게 반환한다.

[0033] 단계(240)에서, 상기 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계를 수행한다.

[0034] 이때, 사용자 단말을 통해 상기 개방형 클라우드 플랫폼에 로그인 및 인증을 수행한다. 상기 개방형 클라우드 플랫폼 내 보안 에이전트가 사용자의 실시간 위치정보와 사용자 정보를 이용하여 암호화된 센싱 데이터의 복호화를 시도하여 복호화에 성공하면, 해당 사용자 활동을 타임 스탬프와 함께 블록체인 네트워크의 분산원장에 기록하도록 개방형 클라우드 플랫폼 내 등록된 기관들에 요청한다.

[0035] 상기 블록체인 네트워크를 통해 해당 기관들에 대한 스마트 계약을 실행하여, 분산원장에 해당 사용자 활동을 기록하고, 상기 보안 에이전트에게 요청 결과를 반환한다.

[0036] 상기 보안 에이전트가 기록에 성공했음을 반환 받으면, 최종적으로 복호화된 데이터를 활용하도록 활용 페이지와 복호화된 데이터를 사용자 사용자 단말에게 전달한다.

[0037] 본 발명의 실시예에 따른 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용하는 단계는, 플랫폼 내 인증되지 않은 불법 사용자 탐지 단계(241) 및 플랫폼 내 인가되지 않은 불법 사용자 탐지 단계(242)를 포함한다.

[0038] 단계(241)에서, 센싱 데이터 활용을 위해 플랫폼에 사용자가 로그인하는 과정에서 발생하는 상기 개방형 클라우드 플랫폼 내 인증되지 않은 불법 사용자가 정당한 사용자의 아이디를 탈취하여 무작위 대입 공격을 수행하는 경우를 실시간으로 탐지한다.

[0039] 단계(242)에서, 센싱 데이터의 복호화를 수행하는 과정에서 발생하는 상기 개방형 클라우드 플랫폼에서 인가된 사용자가 다운로드한 센싱 데이터가 불법적으로 인가되지 않은 사용자에게 공유되어 활용을 시도하는 경우를 실시간으로 탐지한다.

[0041] 도 3은 본 발명의 일 실시예에 따른 사용자 등록 단계를 설명하기 위한 흐름도이다.

[0042] 본 발명의 실시예에 따른 사용자 등록 단계에서, 민감정보를 포함하는 개방형 클라우드 플랫폼(320)에 저장된 데이터를 활용하기 위해 지문 인증과 GPS 기능을 사용할 수 있는 기기(예를 들어, 스마트폰)(313)와 속성기반 암호화(Attribute-based encryption)의 속성으로 활용하기 위한 사용자 정보를 저장한다.

[0043] 사용자 단말(310)은 플랫폼(320)에 등록된 특정 기관에 소속된 연구원(311)이나 서비스 제공자들이 이용하는 단말이며 이들은 플랫폼(320) 내 회원가입 페이지에서 PC와 같은 클라이언트(312)를 이용하여 사용할 아이디, 패

스위드를 포함한 소속 정보, 직위 등을 입력(3-1)하고, 이를 보안 에이전트(321)에 전달한다(3-2). 플랫폼(320) 내 보안 에이전트(321)는 해당 정보를 전달받아 사용자 데이터베이스(322)에 저장하고(3-3), 사용자(311)에게 지문 인증에 사용할 기기(313) 등록을 요청한다(3-4). 사용자(311)는 자신의 기기(313) 내 애플리케이션을 통해 플랫폼(320)에 접속한 다음(3-5), 아이디 및 패스워드와 함께 해당 기기(313)의 등록을 요청한다(3-6). 보안 에이전트(321)는 해당 정보를 전달받아 패스워드 기반 인증을 수행하고 정상적으로 인증에 성공하면, 기기(313) 정보를 사용자 데이터베이스(322)에 추가하고(3-7), 결과를 반환하게 된다(3-8). 사용자 등록 단계 이후에는 사용자(311)는 언제든지 플랫폼(320)에 등록된 아이디와 패스워드를 이용해 로그인할 수 있고, 언제든지 자신에게 인가된 민감정보를 포함하는 센싱 데이터를 플랫폼(120)에 요청할 수 있다.

[0045] 도 4는 본 발명의 일 실시예에 따른 센싱 데이터 저장 단계를 설명하기 위한 흐름도이다.

[0046] 본 발명의 실시예에 따른 센싱 데이터 저장 단계에서, 센싱 데이터 내 민감정보에 대한 열에 대해 개방형 클라우드 플랫폼에 등록된 기관들의 위치정보를 이용하여 속성기반 암호화를 수행하고 개방형 클라우드 플랫폼에 저장한다.

[0047] 개방형 클라우드 플랫폼(410) 내 등록된 기관들은 플랫폼(410)에 센싱 데이터를 업로드하기 전에 해당 데이터에 대한 추가 데이터를 다른 기관들(421, 422)로부터 전달 받아(4-1, 4-2) 데이터 연계 및 민감정보에 대해 비식별화를 진행한다(4-3). 그런 다음, 해당 기관은 비식별화된 센싱 데이터를 민감정보를 포함한 열에 대한 정보와 함께 플랫폼에 업로드하고(4-4), 플랫폼 내 보안 에이전트(411)는 해당 정보를 토대로 민감정보를 포함한 열에 대해 기관들의 위치정보를 이용해 속성기반 암호화를 수행한다(4-5). 마지막으로, 보안 에이전트(411)는 민감정보 데이터베이스(412)에 해당 데이터를 업로드하고(4-6) 업로드에 관한 결과를 업로드를 요청한 기관에 전달한다(4-7). 이 단계는 플랫폼 내 저장된 민감정보를 포함한 센싱 데이터가 해커의 공격으로 데이터 유출이 발생하게 되더라도 해당 데이터에 대한 프라이버시를 보장하고 재식별을 방지하기 위함이다. 또한, 민감정보를 포함한 센싱 데이터가 소속된 기관 외에 다른 장소에 사용되는 것을 방지한다.

[0049] 도 5는 본 발명의 일 실시예에 따른 센싱 데이터 다운로드 단계를 설명하기 위한 흐름도이다.

[0050] 본 발명의 실시예에 따른 센싱 데이터 다운로드 단계에서, 사용자 단말을 통해 활용하고자 하는 센싱 데이터를 다운로드한다.

[0051] 사용자 단말(510) 이용하는 사용자(511)는 클라이언트(512)를 이용해 플랫폼에 로그인한 후, 다운로드를 원하는 센싱 데이터를 선택한다(5-1). 사용자(511)의 클라이언트(512)는 사용자가 요청한 데이터를 개방형 클라우드 플랫폼(520)에 요청하고(5-2), 개방형 클라우드 플랫폼(520) 내 보안 에이전트(521)는 해당 데이터를 민감정보 데이터베이스(522)에서 검색하여(5-3) 가져온다(5-4). 또한, 보안 에이전트(521)는 사용자 데이터베이스(523)에서 다운로드를 요청한(5-5) 사용자 정보(예를 들어, 직위, 소속 등)를 가져온다(5-6). 그 후, 보안 에이전트(521)는 가져온 사용자의 정보를 이용해 센싱 데이터에 대해 속성기반 암호화를 한 번 더 수행하여 데이터 내용 전체를 암호화한다(5-7). 보안 에이전트(521)는 암호화된 센싱 데이터를 클라이언트에게 반환해주고(5-8), 사용자는 클라이언트(512)를 통해 해당 데이터를 다운받아 소지할 수 있게 된다. 센싱 데이터 다운로드 단계는 분석한 센싱 데이터를 반출될 수 있도록 하여 인가된 사용자라면 지정된 환경에서 언제든지 추가 분석을 수행할 수 있도록 하고, 다른 연구자들과의 협업을 위한 데이터 추가 공유를 할 수 있도록 하기 위한 단계이다.

[0053] 도 6은 본 발명의 일 실시예에 따른 센싱 데이터 활용 단계를 설명하기 위한 흐름도이다.

[0054] 본 발명의 실시예에 따른 센싱 데이터 활용 단계에서, 개방형 클라우드 플랫폼에서 암호화된 민감정보를 포함하는 센싱 데이터를 사용자 단말을 통해 개방형 클라우드 플랫폼에서 활용한다.

[0055] 사용자 단말(610)을 이용하는 사용자(611)는 클라이언트(612)를 이용하여 개방형 클라우드 플랫폼(620)에 로그인을 시도하고(6-1), 로그인에 성공하면 암호화된 센싱 데이터를 클라이언트(612)를 이용해 개방형 클라우드 플랫폼(620)에 업로드한다(6-2). 개방형 클라우드 플랫폼(620) 내 보안 에이전트(621)는 사용자가 요청하면(6-3), 사용자의 정보(예를 들어, 직위, 소속, 기기 정보) 등을 사용자 데이터베이스(622)에서 가져온다(6-4). 가져온 기기 정보를 이용해 보안 에이전트(621)는 해당 사용자에게 지문 인증을 요청한다(6-5). 사용자(611)는 자신의 기기(613)를 이용해 지문 인증을 수행한다(6-6). 지문 인증에 성공하면, 해당 기기(613)는 전자서명과 함께 사용자의 실시간 위치정보를 보안 에이전트(621)에게 전달한다(6-7). 보안 에이전트(621)는 전달받은 서명을 검증하고, 올바르게 실시간 위치정보와 사용자 정보를 이용해 암호화된 센싱 데이터의 복호화를 시도한다(6-8). 복호화에 성공하면 보안 에이전트(621)는 해당 사용자 활동을 타임 스탬프와 함께 블록체인 네트워크(630)의 분산 원장(634)에 기록하도록 개방형 클라우드 플랫폼(620) 내 등록된 기관들(631, 632, 633)에 요청한다(6-9). 해당

기관들(631, 632, 633)은 스마트 계약(635)을 실행하여(6-10), 분산원장(634)에 해당 사용자 활동을 기록하고(6-11), 이를 반환하여(6-12), 보안 에이전트(621)에게 요청 결과를 반환한다(6-13). 보안 에이전트(621)는 기록에 성공했음을 반환 받으면, 최종적으로 복호화된 데이터를 활용할 수 있도록 활용 페이지와 데이터를 사용자에게 전달하고(614), 사용자는 활용 페이지에서 일정 시간 동안 민감정보를 포함한 센싱 데이터를 자유롭게 활용할 수 있다. 센싱 데이터 활용 단계에서 사용자가 로그인하거나 민감정보를 포함한 센싱 데이터를 복호화할 때, 보안 에이전트가 불법 사용자를 탐지하게 된다. 보안 에이전트가 불법 사용자를 탐지하는 과정은 도 7 내지 도 9를 참조하여 더욱 상세히 설명한다.

- [0057] 도 7은 본 발명의 일 실시예에 따른 플랫폼 내 인증되지 않은 불법 사용자 탐지 과정을 설명하기 위한 도면이다.
- [0058] 본 발명의 실시예에 따른 플랫폼 내 인증되지 않은 불법 사용자 탐지는 플랫폼 내 인증되지 않은 불법 사용자 중에서도 정당한 사용자의 아이디를 탈취하여 무작위 대입 공격을 수행하는 경우를 실시간으로 탐지하는 것이다. 제안하는 탐지 방법은 일반적으로 센싱 데이터 활용 단계에서 센싱 데이터를 활용을 위해 플랫폼에 사용자가 로그인할 때 발생한다.
- [0059] 도 7을 참조하면, 먼저 인증되지 않은 사용자(740)인 해커(741)는 개방형 클라우드 플랫폼(720) 내 정당한 사용자(711)의 아이디를 탈취한다(7-1).
- [0060] 해커(741)는 자신의 클라이언트(742)를 이용해 플랫폼(720)에 접속한 후에 탈취한 아이디와 무작위 패스워드를 입력한다(7-2).
- [0061] 해커의 클라이언트(742)는 입력 받은 아이디와 패스워드를 플랫폼(720) 내 보안 에이전트(721)에 전달한다(7-3).
- [0062] 보안 에이전트(721)는 사용자 데이터베이스(722)에 해당 사용자에 대한 기기(712) 정보 및 해시화된 패스워드를 요청한다(7-4).
- [0063] 사용자 데이터베이스(722)는 요청 받은 사용자의 기기 정보 및 해시화된 패스워드를 보안 에이전트(721)에 전달한다(7-5).
- [0064] 보안 에이전트(721)는 전달받은 해시화된 패스워드를 기반으로 사용자에 대한 패스워드 인증을 수행한다(7-6).
- [0065] 패스워드가 불일치하기 때문에 인증에 실패하게 되고, 보안 에이전트(721)는 등록된 기관들(731, 732, 733)이 해당 계정에 대한 로그인 실패 결과와 타임 스탬프를 분산원장(734)에 기록하도록 요청한다(7-7).
- [0066] 타임 스탬프와 함께 사용자의 활동 기록을 전달받은 기관들(731, 732, 733)은 블록체인 네트워크(730) 내 스마트 계약(735)을 실행한다(7-8).
- [0067] 스마트 계약(735)은 플랫폼(720) 내 사용자 활동을 분산원장(734)에 기록한다(7-9).
- [0068] 스마트 계약(735)은 기록 결과를 플랫폼(720)에 등록된 기관(731, 732, 733)에 반환한다(7-10).
- [0069] 사용자 활동 기록에 성공하면, 기관들(731, 732, 733)은 보안 에이전트(721)에 요청에 관한 결과를 반환한다(7-11).
- [0070] 플랫폼(720) 내 보안 에이전트(721)는 사용자 인증을 시도한 해커(741)에게 로그인에 실패했음을 전달한다(7-12).
- [0071] 상기 과정을 통해 로그인이 한 번 실패한 이후에도 해커가 두 번 이상 연속적으로 이러한 과정을 반복하게 되면, 분산원장(734)에 이러한 시도들이 계속 기록되게 되고 보안 에이전트(721)는 등록된 기록을 토대로 해당 아이디를 일시적으로 플랫폼(720)에서 차단한다(7-13).
- [0072] 보안 에이전트(721)는 해당 아이디의 기기 정보를 이용하여 등록된 기기(712)에 지문 인증을 요청하고, 해당 기기(712)를 통해 지문 인증이 성공하기 전까지 해당 아이디는 플랫폼(720)에서 사용할 수 없게 된다(7-14).
- [0073] 또한, 보안 에이전트(721)는 플랫폼(720)의 관리자에게 3번 이상 로그인을 실패한 기록이 존재함을 블록체인 네트워크(730) 내 기록과 함께 메일로 전달하여 관리자가 이를 분석하여 적절한 사후 조치를 할 수 있도록 한다.
- [0075] 도 8은 본 발명의 일 실시예에 따른 플랫폼 내에서 인가되지 않은 불법 사용자 탐지 과정을 설명하기 위한 도면

이다.

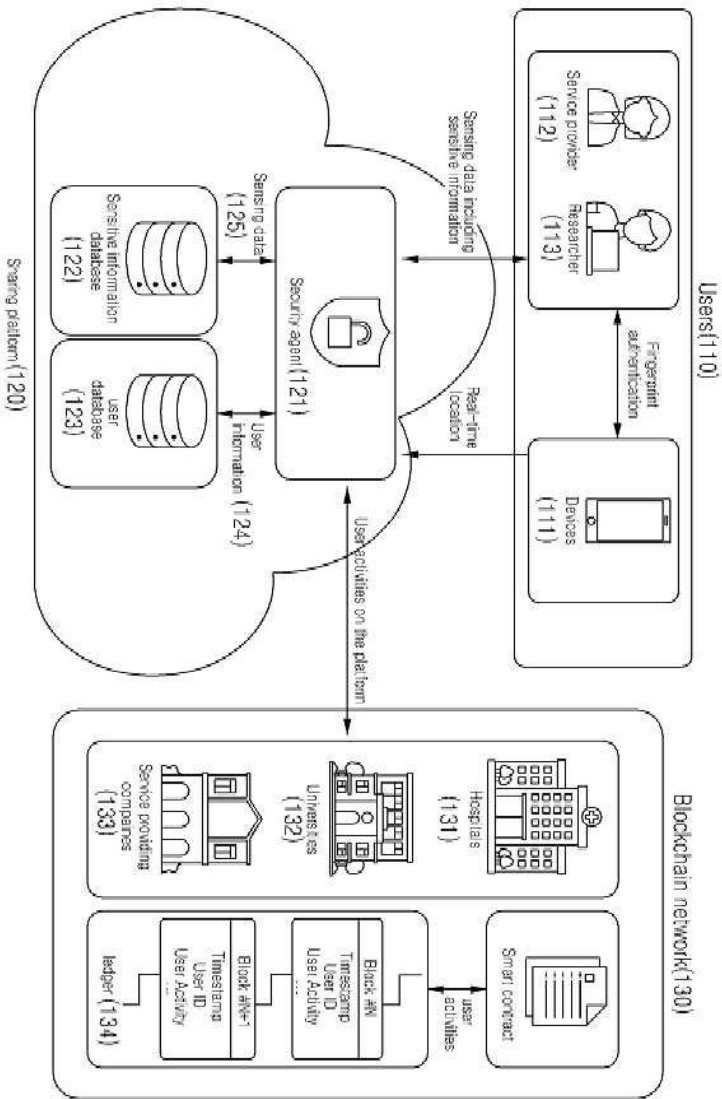
- [0076] 본 발명의 실시예에 따른 플랫폼 내에서 인가되지 않은 불법 사용자 탐지는 개방형 클라우드 플랫폼에서 인가된 사용자가 다운로드한 센싱 데이터가 불법적으로 인가되지 않은 사용자에게 공유되어 활용을 시도할 때, 이를 실시간으로 탐지하는 것이다. 플랫폼 내에서 인가되지 않은 불법 사용자 탐지는 센싱 데이터 활용 단계에서도 센싱 데이터의 복호화를 수행하는 과정에서 발생한다.
- [0077] 도 8을 참조하면, 먼저 불법 사용자(840)인 서비스 제공자(841)는 인가되지 않은 특정 센싱 데이터(812)를 사용자 단말(810)을 통해 인가된 사용자(811)로부터 불법적으로 공유받는다(8-1).
- [0078] 불법 사용자(841)는 자신의 아이디와 패스워드를 이용해 플랫폼(820)에 로그인하고 불법 공유 받은 센싱 데이터를 클라이언트(842)를 통해 플랫폼에 업로드한다(8-2).
- [0079] 해당 사용자의 클라이언트(842)는 사용자(811)가 업로드한 센싱 데이터를 보안 에이전트(821)에게 전달한다(8-3).
- [0080] 플랫폼(820) 내 보안 에이전트(821)는 해당 사용자(841)에 대한 기기(843) 정보를 포함한 사용자 정보를 사용자 데이터베이스(822)에 요청한다(8-4).
- [0081] 사용자 데이터베이스(822)는 보안 에이전트(821)에게 요청한 사용자 정보를 반환한다(8-5).
- [0082] 보안 에이전트(821)는 전달받은 기기 정보를 이용하여 해당 사용자의 기기(843)에 지문 인증을 요청한다(8-6).
- [0083] 인가되지 않은 사용자(841)는 자신의 기기(843)를 이용해 지문 인증을 수행한다(8-7).
- [0084] 지문 인증에 성공하면, 해당 기기(843)는 전자서명과 함께 실시간 속성 정보를 보안 에이전트(821)에게 전달한다(8-8).
- [0085] 보안 에이전트(821)는 전달받은 실시간 속성 정보와 사용자 정보를 이용해 업로드된 센싱 데이터의 복호화를 시도한다(8-9).
- [0086] 사용자 정보가 일치하지 않기 때문에 암호화된 센싱 데이터의 복호화가 실패하게 되고, 보안 에이전트(821)는 등록된 기관들이 해당 계정에 대한 복호화 실패 결과와 타임 스탬프를 분산원장(834)에 기록하도록 요청한다(8-10).
- [0087] 타임 스탬프와 함께 사용자의 활동 기록을 전달받은 기관들(831, 832, 833)은 블록체인 네트워크(830) 내 스마트 계약(835)을 실행한다(8-11).
- [0088] 스마트 계약(835)은 플랫폼(820) 내 사용자 활동을 분산원장(834)에 기록한다(8-12).
- [0089] 스마트 계약(835)은 기록 결과를 플랫폼(820)에 등록된 기관(831, 832, 833)에 반환한다(8-13).
- [0090] 사용자 활동 기록에 성공하면, 기관들(831, 832, 833)은 보안 에이전트(821)에 요청에 관한 결과를 반환한다(8-14).
- [0091] 보안 에이전트(821)는 센싱 데이터의 활용을 시도한 인가되지 않은 불법 사용자(841)에게 해당 데이터의 복호화에 실패했음을 전달한다(8-15).
- [0092] 복호화가 한 번 실패된 이후에도 인가되지 않은 사용자가 이러한 실패 과정을 연속적으로 한 번 더 반복하게 되면, 블록체인 네트워크(830)에 이러한 시도들이 계속 기록되게 되고 보안 에이전트(821)는 기록된 사용자 활동을 토대로 해당 아이디를 일시적으로 플랫폼에서 차단한다(8-16).
- [0093] 플랫폼 내에서 인가되지 않은 불법 사용자 탐지 과정 이후에 보안 에이전트(821)는 플랫폼(820)의 관리자에게 2번 이상 연속적으로 복호화에 실패한 기록이 존재함을 블록체인 네트워크(830) 내 해당 기록들과 함께 메일로 전달하게 되고, 플랫폼 관리자들은 해당 기록 분석을 통해 플랫폼 내에서 악의적인 시도 여부를 판단할 수 있도록 하여 사용자의 아이디 차단 해제와 같은 적절한 보안 조치를 수행할 수 있도록 한다.
- [0094] 이 밖에도, 본 프레임워크 내의 민감정보를 포함한 센싱 데이터를 공유하기 위한 플랫폼에서는 보안 에이전트에 의해 사용자의 모든 일련의 활동이 블록체인에 기록되기 때문에 두 가지 불법 사용자 탐지 외에도 다양한 보안 사고가 발생하였을 때 해당 기록을 토대로 적절한 사후 조치 및 관리를 수행할 수 있도록 하고 블록체인의 특징으로 인해 기록된 정보는 기본적으로 무결성을 보장하기 때문에 로그에 대한 신뢰성을 보장하고 부인방지 및 책임 추적성을 제공하게 된다.

- [0096] 도 9는 본 발명의 일 실시예에 따른 보안 에이전트의 의사코드 알고리즘을 나타내는 도면이다.
- [0097] 본 발명의 실시예에 따른 보안 에이전트는 민감정보를 포함하는 센싱 데이터를 위한 개방형 클라우드 플랫폼에 핵심 구성요소로, 플랫폼 내 센싱 데이터를 안전하게 보호 및 관리하고 블록체인 클라이언트로서 플랫폼과 블록체인이 적절히 상호작용할 수 있도록 한다.
- [0098] 도 9에 도시된 알고리즘1은 보안 에이전트가 사용자 인증 단계 및 데이터 활용 단계에서 불법 사용자를 탐지하기 위한 일부 알고리즘을 보여주며, 자세한 설명은 다음과 같다.
- [0099] 알고리즘 1에서 1~26행은 패스워드 기반 사용자 인증을 위한 프로시저이다.
- [0100] 이 프로시저는 패스워드 인증을 수행하기 전에 사용자 데이터베이스에서 사용자의 아이디 잠금 여부를 판단한다(3행).
- [0101] 만약 해당 아이디가 잠겼을 경우, 인증 단계에서 아이디 잠금이 수행된 것인지 아니면 활용 단계(즉, 복호화)에서 수행된 것인지 판단하고 이에 대한 적절한 조치를 수행한다(4~11행).
- [0102] 아이디가 잠기지 않았을 때는 사용자 인증을 수행하고, 이 과정에서 인증에 실패하면 해당 아이디의 마지막 2번의 사용자 로그인 활동 기록이 실패였는지를 블록체인에서 조회한다(18행).
- [0103] 조회한 마지막 2번의 사용자 활동 기록이 연속적으로 실패한 것이 아니라면 해당 사용자에 대한 로그인 실패 기록을 블록체인에 기록하고, 연속적으로 두 번 로그인이 실패되었다면 해당 사용자를 일시적으로 플랫폼에서 차단하고 플랫폼 관리자에게 해당 사실을 알리게 된다(19~24행).
- [0104] 알고리즘 1에서 27~51행은 민감정보를 포함하는 센싱 데이터 활용을 위한 프로시저이다.
- [0105] 이 프로시저는 암호화된 센싱 데이터가 업로드되면 해당 사용자의 기기에 지문 인증을 요청하고, 지문 인증에 성공하면 실시간 위치정보와 사용자 정보를 이용해 데이터의 복호화를 시도한다(28~37행).
- [0106] 만약 복호화에 실패할 경우, 블록체인에서 해당 사용자의 플랫폼 내 마지막 활용에 관한 활동이 실패였는지의 여부를 확인한다(38~39행).
- [0107] 마지막 활용에 대한 활동이 실패였을 경우, 해당 사용자를 일시적으로 차단하고 플랫폼 관리자에게 이에 대해 전달하며 마지막 활동이 실패가 아닌 경우에는 블록체인에 현재 실패된 활용 활동을 기록한다(40~47행).
- [0109] 본 발명의 실시예에 따른 실험은 분산원장에 데이터를 읽거나 쓰는 과정에 대한 성능을 측정한다. 특히, 주요한 성능 중에서도 평균 지연율(Average Transaction Latency) 및 처리량(Throughput)을 하이퍼레저 캘리퍼(Hyperledger Caliper)를 이용하여 측정한다. 블록체인 네트워크는 1Peer with 10org, 1Peer with 20org, 2Peer with 20org로 구성하여 각각의 네트워크에 대한 성능을 측정하며 자세한 설명은 다음과 같다.
- [0110] 본 발명의 실시예에 따른 플랫폼 내 사용자 활동 기록에서, 사용자가 플랫폼에 로그인하거나 플랫폼 내에서 센싱 데이터를 활용할 때, 허가형 블록체인 내 분산원장에 해당 작업에 대한 성공 및 실패 여부를 기록하게 된다. 이러한 작업을 가정하기 위해 각 라운드(Round)에서 100, 150, 200, 250, 300TPS (Transactions Per Second) 비율로 플랫폼 내 사용자 활동을 기록하는 1,000개의 트랜잭션(Transactions)을 5라운드 수행한다.
- [0111] 본 발명의 실시예에 따른 플랫폼 내 사용자 활동 조회에서, 비인증된 사용자 또는 비인가된 사용자를 탐지하기 위해 분산원장에서 플랫폼 내 사용자의 이전 활동들을 읽는 과정이 존재한다. 이를 가정하기 위해 100개의 사용자 활동을 임의로 기록한 다음, 해당 사용자 활동을 모두 조회하는 1,000개의 트랜잭션을 각 라운드(Round)에서 100, 150, 200, 250, 300TPS 비율로 5라운드 수행한다. 도 10 및 도 11을 참조하면, 네트워크 구성 별로 읽기/쓰기에 대한 평균 지연율과 처리량을 나타내었다.
- [0113] 도 10은 본 발명의 일 실시예에 따른 블록체인 네트워크 구성에 따른 평균 지연율을 나타내는 그래프이다.
- [0114] 도 11은 본 발명의 일 실시예에 따른 블록체인 네트워크 구성에 따른 처리량을 나타내는 그래프이다.
- [0115] 도 10(a) 및 도 11(a)는 플랫폼 내 사용자 활동을 분산원장에 기록할 때의 평균 지연율과 처리량을 보여준다. 1Peer with 10org 네트워크에서 300TPS 비율에 대한 평균 지연율은 약 3초 미만으로 300TPS에서 다른 네트워크에 비해 평균 지연율이 낮다. 반대로, 처리량의 경우에는 300TPS에서 약 150TPS로 다른 네트워크에 비해 높은 처리량을 보여준다. 또한, 실험 설정에서 가장 복잡한 네트워크 구성인 2Peer with 20org에서 300TPS 비율에 대한 평균 지연율과 처리량은 각각 약 5초 및 약 100TPS이다.

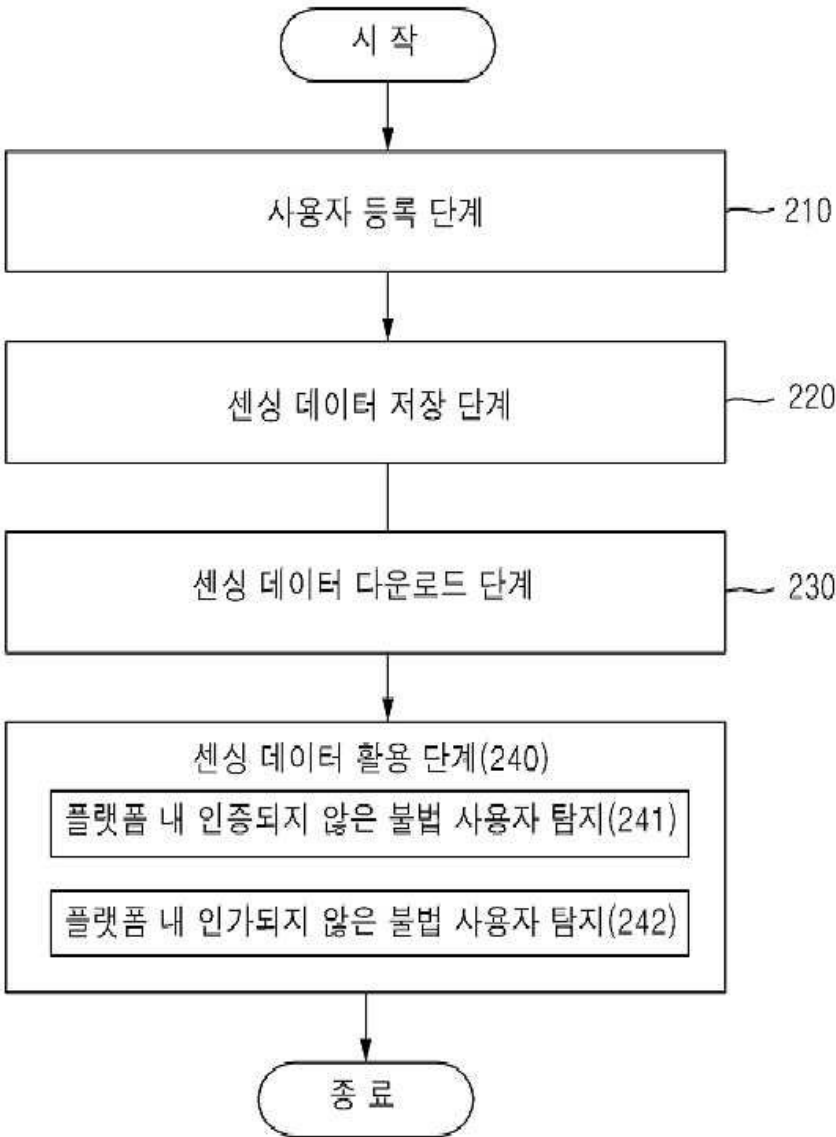
- [0116] 도 10(b) 및 도 11(b)는 플랫폼 내 사용자 활동을 분산원장에 조회할 때의 평균 지연율과 처리량을 보여준다. 1Peer with 10Org 네트워크에서 300TPS 비율에 대한 평균 지연율과 처리량은 각각 약 14초 및 약 63TPS이며, 실험 설정에서 가장 복잡한 네트워크 구성인 2Peer with 20Org에서 300TPS 비율에 대한 평균 지연율과 처리량은 각각 약 19초 및 47TPS를 보여준다.
- [0118] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0119] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0120] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.
- [0121] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.
- [0122] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

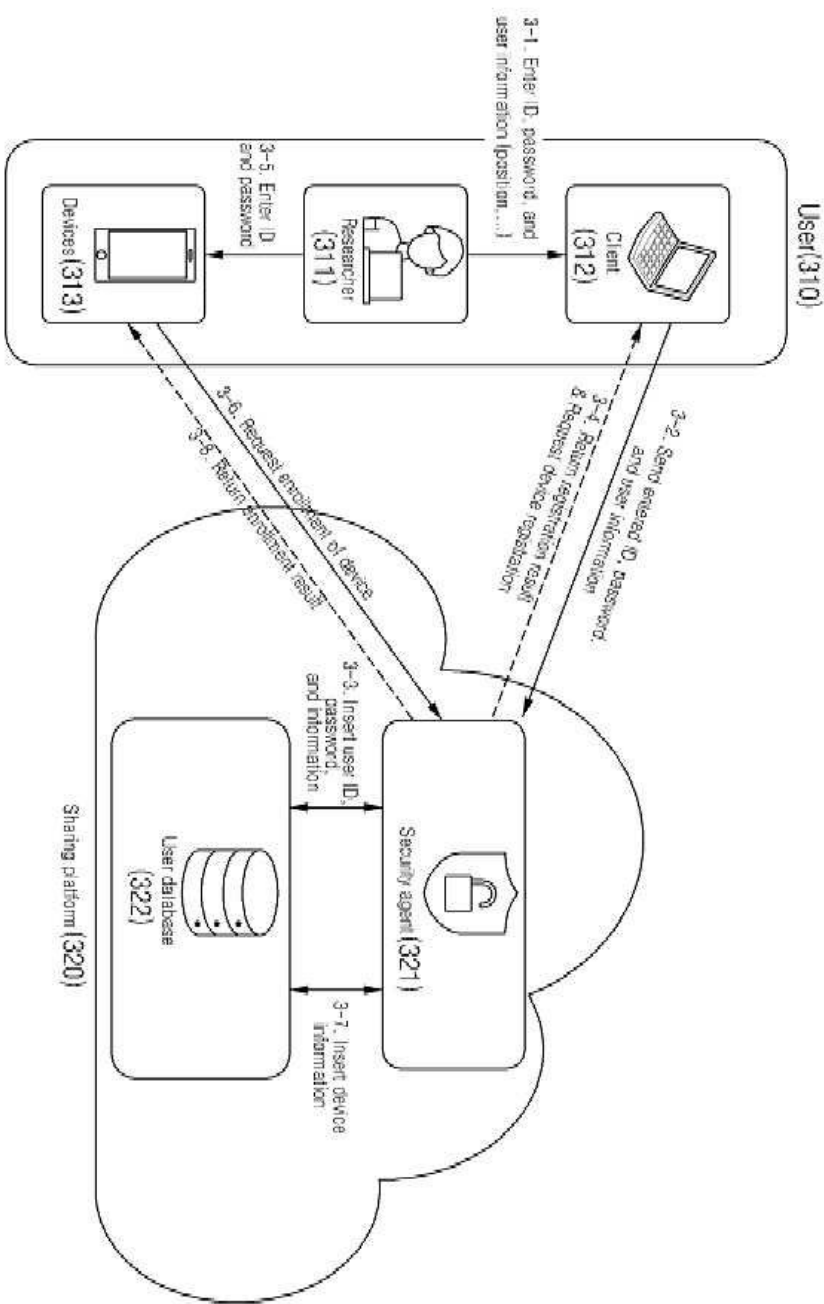
도면1



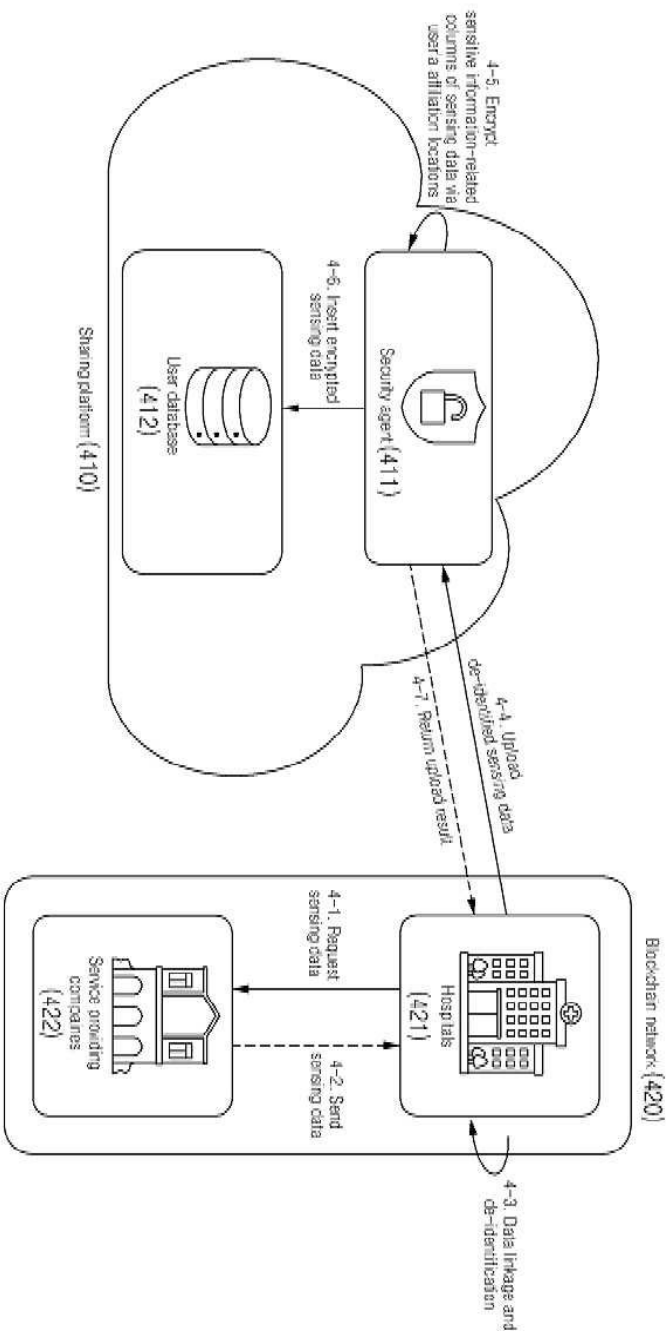
도면2



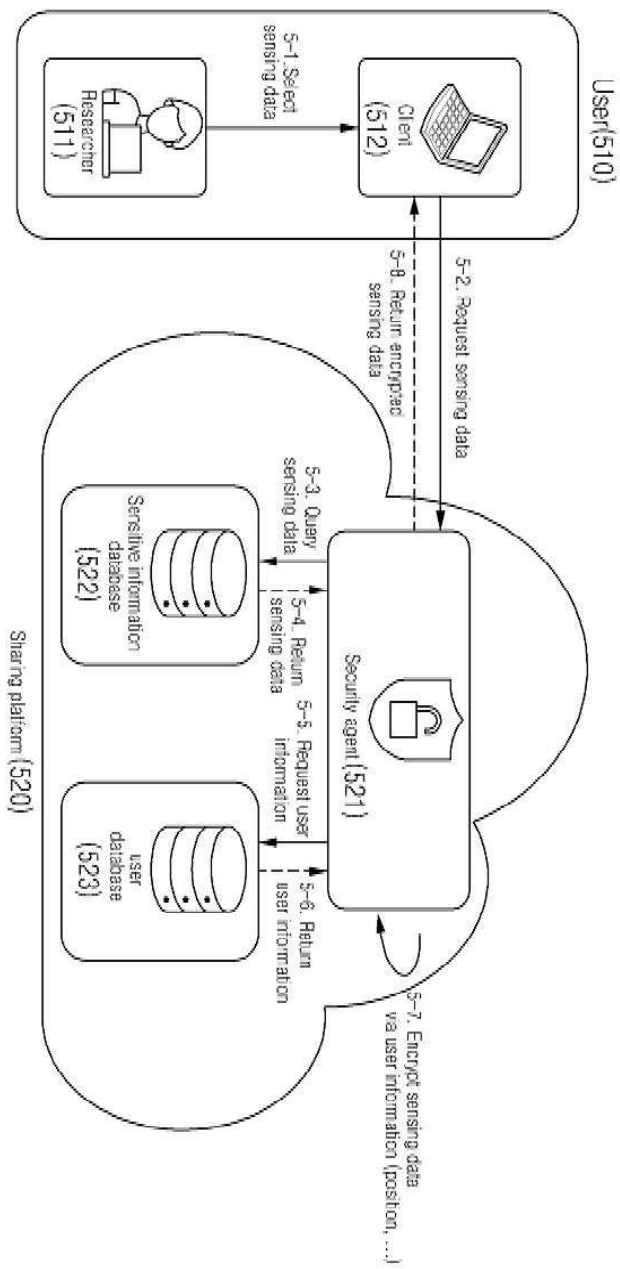
도면3



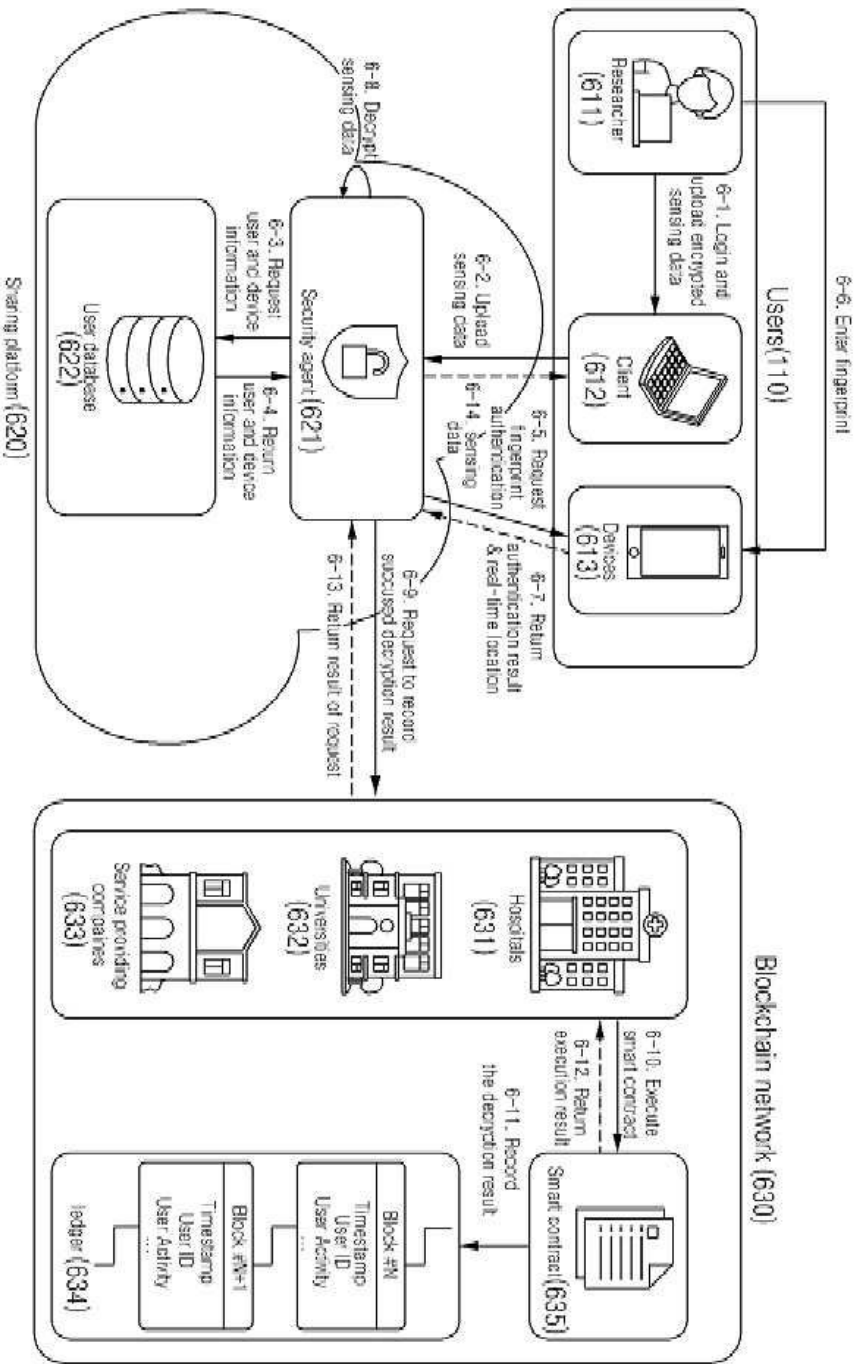
도면4



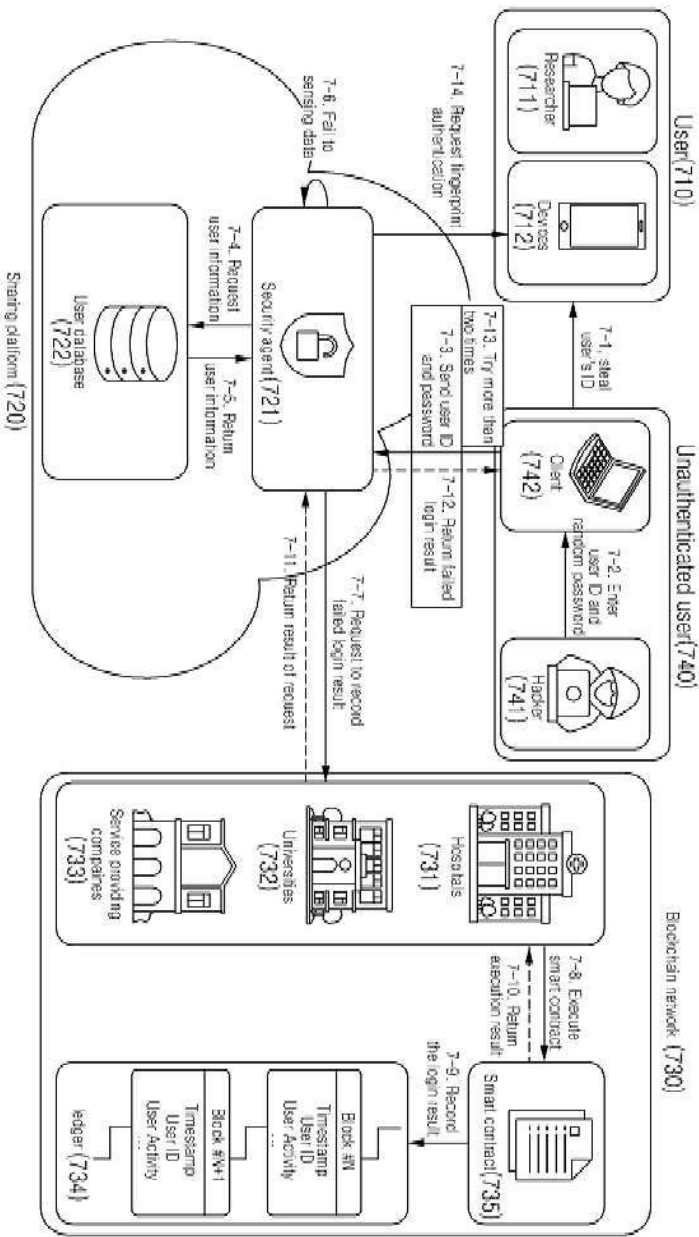
도면5



도면6



도면7



도면9

Algorithm 1. Pseudo-code of the security agent

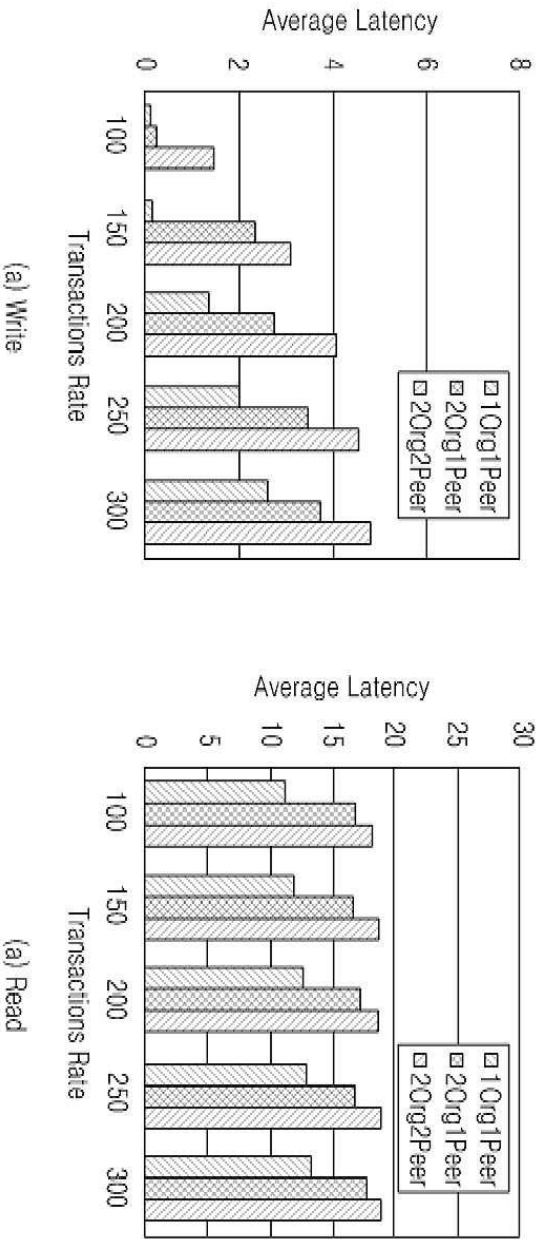
Input: enc_sensing_data, user_id, user_password, user_attributes (e.g., position, department, etc.), user_device_id

```

1:  procedure authentication (user_id, user_password, user_device_id):
2:      /* block_point is where the user is blocked. */
3:      Query block_point to the user database using user_id;
4:      if block_point is "login" then
5:          Request fingerprint authentication to the user device;
6:          Send e-mail about login try with a timestamp to the platform admin;
7:          return loginPage ();
8:      else if block_point is "utilization" then
9:          Send e-mail about decryption try with a timestamp to the platform admin;
10:         Print "Contract to the platform admin. Your ID is lock !";
11:         return loginPage ();
12:      else
13:          Authenticate the user using user_id and user_password;
14:          if authentication is successful then
15:              Record succussed login activity with a timestamp to blockchain network;
16:              return mainPage ("authenticated user");
17:          else
18:              Request last activity about login to blockchain network with user_id;
19:              if more than two last login activity is failed then
20:                  Update block_point to "login" in user database using user_id;
21:                  Block the user and then send e-mail about failed login results with a timestamp to the platform admin;
22:              end if
23:              Record failed login activity with a timestamp to blockchain network;
24:              return loginPage ();
25:          end if
26:      end procedure
27:  procedure utilization (enc_sensing_data, user_attributes, user_device_id):
28:      fingerprintAuth (user_device_id);
29:      if fingerprint authentication is failed then
30:          Print "fingerprint authentication is failed...";
31:          return user_uploadPage ();
32:      end if
33:      Add real_time_location into user_attributes;
34:      Create policy using user_attributes;
35:      for each row in enc_sensing_data do
36:          Decrypt row using policy;
37:      end for
38:      if decryption is failed then
39:          Request last activity about utilization to blockchain network with user_id;
40:          if last utilization activity is failed then
41:              Update block_point to "utilization" in user database using user_id;
42:              Block the user and then send e-mail about failed decryption results with timestamp to the platform admin;
43:              Print "Contract to the platform admin. Your ID is lock !";
44:              return loginPage ();
45:          end if
46:          Record failed decryption activity with a timestamp to blockchain network;
47:          return user_uploadPage ();
48:      end if
49:      Record succussed decryption activity with a timestamp to blockchain network;
50:      return viewPage (decrypted_sensing_data);
51:  end procedure

```

도면10



도면11

