(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년04월18일
(11) 등록번호 10-2522981
(24) 등록일자 2023년04월13일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06Q 50/30* (2012.01)
H04L 51/00 (2022.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 63/0876 (2013.01)
G06Q 50/30 (2015.01)
(21) 출원번호 10-2021-0152232
(22) 출원일자 2021년11월08일
심사청구일자 2021년11월08일
(65) 공개번호 10-2022-0066842
(43) 공개일자 2022년05월24일
(30) 우선권주장
1020200153185 2020년11월16일 대한민국(KR)
(56) 선행기술조사문헌
KR1020170024777 A
JP2020526806 A
KR102003272 B1
KR102054581 B1

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
황제영
경상북도 포항시
(뒷면에 계속)
(74) 대리인
특허법인이상

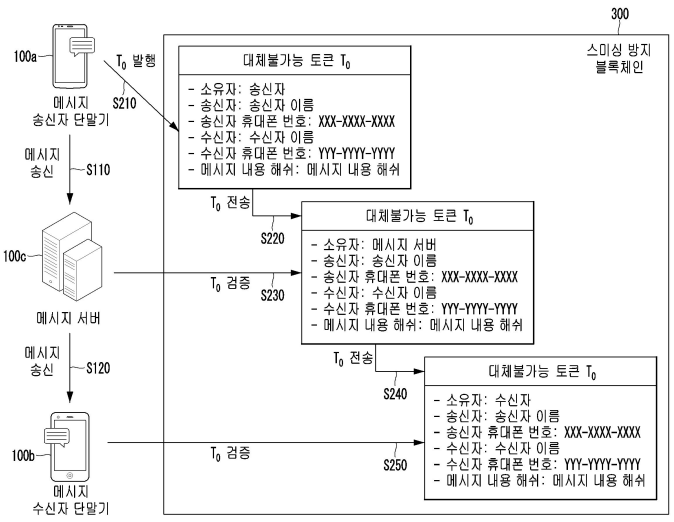
전체 청구항 수 : 총 20 항 심사관 : 천대식

(54) 발명의 명칭 **블록체인 기반 스미싱 방지 방법 및 장치**

(57) 요 약

본 발명의 블록체인 기반 스미싱 방지 시스템은, 메시지 관련 정보를 트랜잭션으로 생성하는 메시지 송신자 단말기, 송신 메시지 및 수신 메시지를 중계하는 메시지 서버, 메시지 송신자가 송신한 메시지를 최종 수신하는 메시지 수신자 단말기 및 허가형 블록체인으로 구성되는 스미싱 방지 블록체인과, 메시지 송·수신자의 트랜잭션 전송을 중계하는 적어도 하나의 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)를 포함하는 블록체인 기반 스미싱 방지 장치를 포함한다.

대 표 도



(52) CPC특허분류
H04L 51/23 (2022.05)
H04L 63/1441 (2013.01)
H04L 9/3213 (2013.01)
H04L 9/50 (2022.05)

(72) 발명자
노용두
대전광역시 유성구 봉산로 39, 203동 907호

홍상원
서울특별시 노원구 석계로 49, 111동 405호

이 발명을 지원한 국가연구개발사업
과제고유번호 1711125876
과제번호 2020-0-00936-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 블록체인융합기술개발(R&D)
연구과제명 5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율 30/100
과제수행기관명 포항공과대학교 산학협력단
연구기간 2021.01.01 ~ 2021.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711193875
과제번호 2021-0-00484-003
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 데이터경제를위한블록체인기술개발(R&D)
연구과제명 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발
기 여 율 30/100
과제수행기관명 포항공과대학교 산학협력단
연구기간 2023.01.01 ~ 2023.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711193306
과제번호 2018-0-01441-006
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보통신방송혁신인재양성
연구과제명 크로스 도메인 호환성을 위한 블록체인 플랫폼 및 비즈모델 개발
기 여 율 40/100
과제수행기관명 포항공과대학교 산학협력단
연구기간 2023.01.01 ~ 2023.12.31

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

메시지 관련 정보를 트랜잭션으로 생성하는 메시지 송신자 단말기;

송신 메시지 및 수신 메시지를 중계하는 메시지 서버;

메시지 송신자가 송신한 메시지를 최종 수신하는 메시지 수신자 단말기; 및

허가형 블록체인으로 구성되는 스미싱 방지 블록체인과, 메시지 송·수신자의 트랜잭션 전송을 중계하는 적어도 하나의 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)를 포함하는 블록체인 기반 스미싱 방지 장치; 를 포함하는,

블록체인 기반 스미싱 방지 시스템.

청구항 2

허가형 블록체인으로 구성되는 스미싱 방지 블록체인;

메시지 송·수신자의 트랜잭션 전송을 중계하는 적어도 하나의 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK);

프로세서(processor); 및

프로세서를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory); 를 포함하되,

적어도 하나의 명령은 상기 프로세서가:

문자 메시지 서비스 사용자의 신원 정보를 블록체인을 통해 관리하는 단계;

송신 메시지 관련 정보를 블록체인에 기록하는 단계; 및

메시지 서버가 송신자로부터 블록체인에 기록한 정보를 이용하여 송신자 신원 정보를 검증하고 택배 및 공공기관 사칭에 의한 스미싱을 차단한 메시지만 메시지 수신자에게 중계하는 단계; 를 수행하도록 구성되는,

블록체인 기반 스미싱 방지 장치.

청구항 3

청구항 2에 있어서, 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)는,

스미싱 방지 블록체인 상에 메시지 내용을 기반으로 하는 스미싱 방지 토큰을 발행하는 트랜잭션을 생성하는 토큰 발행부;

스미싱 방지 블록체인 상에서 스미싱 방지 토큰을 다른 사용자에게 전송하는 기능을 담당하는 토큰 전송부;

대체불가능 토큰을 발행한 사용자의 신원을 인증하는 기능을 담당하는 토큰 속성 검증부; 및

스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)가 스미싱 방지 블록체인으로부터 이벤트를 받으면, 호출한 주체에게 알림을 보내는 기능을 하는 이벤트부; 를 포함하는,

블록체인 기반 스미싱 방지 장치.

청구항 4

청구항 3에 있어서, 이벤트부가 전달하는 이벤트는,

메시지 송신자 단말기가 토큰 발행부를 통해 스미싱 방지 토큰 발행을 요청한 후, 스미싱 방지 블록체인 상에 토큰 생성이 완료되는 경우, 이벤트부는 토큰 발행 완료 사실을 메시지 송신자 단말기에게 이벤트로 알리고,

토큰의 소유자가 토큰 전송부를 통해 스미싱 방지 토큰을 다른 사용자에게 전송을 요청한 후, 스미싱 방지 블록

체인 상에서 전송이 완료되는 경우, 이벤트부는 성공적인 소유권 양도 완료 사실을 토큰 전송부 호출자에게 이벤트로 알리는,

블록체인 기반 스미싱 방지 장치.

청구항 5

청구항 3에 있어서, 토큰 발행부는,

메시지 송신자 단말기가 토큰 발행부를 통해 블록체인 트랜잭션을 생성하여 스미싱 방지 블록체인 상에 스미싱 방지 토큰을 발행하는,

블록체인 기반 스미싱 방지 장치.

청구항 6

청구항 3에 있어서, 토큰 전송부는,

스미싱 방지 토큰의 소유자가 토큰 전송부를 통해 스미싱 방지 토큰의 소유권을 다른 사용자에게 양도하는 블록체인 트랜잭션을 생성하고,

토큰 전송부 호출이 완료되면 토큰의 소유자가 변경되는,

블록체인 기반 스미싱 방지 장치.

청구항 7

청구항 3에 있어서, 토큰 속성 검증부는,

대체불가능 토큰 수신자는 토큰 속성 검증부를 호출하여 송신자가 발행한 대체불가능 토큰에 기록된 송신자 이름과 휴대폰 번호를 확인하며,

송신자 이름 및 휴대폰 번호와 대응되는 사용자 정보 및 공개키가 택배사 혹은 공공기관 관계자의 사용자 정보 및 공개키와의 일치 여부를 비교함으로써, 송신자 당사자 인증을 수행하는,

블록체인 기반 스미싱 방지 장치.

청구항 8

제 5항에 있어서, 스미싱 방지 토큰은,

메시지 내용 정보를 블록체인 상에 기록하기 위한 대체불가능 토큰(Non-fungible token)으로,

표준 속성과 온체인(on-chain) 및 오프체인(off-chain) 확장 속성으로 구성되고,

표준 속성은 토큰 ID 속성, 토큰 타입 속성, 소유자 속성, 피승인자 속성으로 구성되고,

온체인 확장 속성은 표준 속성의 토큰 타입에 따라 하위 속성이 다르게 정의되고,

오프체인 확장 속성은 대체불가능 토큰을 표현할 때 오프체인 데이터가 필요한 경우 오프체인 저장소를 연결하기 위해 오프체인 저장소 경로를 저장하는 경로 속성과 오프체인 저장소의 데이터들로 구성된 머클 트리(merkle tree)의 머클 루트(merkle root)를 저장하는 해시 속성이 하위 속성으로 구성되는,

블록체인 기반 스미싱 방지 장치.

청구항 9

제 5항에 있어서, 스미싱 방지 토큰은,

온체인 확장 속성을 정의하는 스미싱 방지 토큰 타입으로,

송·수신자 이름, 송·수신자 휴대폰 번호, 및 메시지 내용 해쉬 속성으로 구성되고,

메시지를 송신하는 메시지 송신자 이름과 휴대폰 번호 정보와 해당 메시지를 수신하는 수신자 이름과 휴대폰 번호 정보를 각각 저장하는 송신자 이름, 송신자 휴대폰 번호 및 수신자 이름, 수신자 휴대폰 번호 속성을 온체인

확장 속성의 하위 속성으로 정의되고,

송신 메시지 내용의 무결성을 증명하기 위한 메시지 내용 해쉬 속성을 온체인 확장 속성의 하위 속성으로 정의하여 대체불가능 토큰으로 블록체인 상에 표현되는,

블록체인 기반 스미싱 방지 장치.

청구항 10

메시지 관련 정보를 블록체인 상에 기록하는 블록체인 기반 스미싱 방지 방법에 있어서,

문자 메시지 서비스 사용자의 신원 정보를 블록체인을 통해 관리하는 단계;

송신 메시지 관련 정보를 블록체인에 기록하는 단계; 및

메시지 서버가 송신자로부터 블록체인에 기록한 정보를 이용하여 송신자 신원 정보를 검증하고 택배 및 공공기관 사칭에 의한 스미싱을 차단한 메시지만 메시지 수신자에게 중계하는 단계; 를 포함하는,

블록체인 기반 스미싱 방지 방법.

청구항 11

제 10항에 있어서, 상기 방법은,

메시지 송신자가 송신하려는 메시지와 관련된 메시지 송·수신자 이름과 휴대폰 번호, 그리고 메시지 내용 해쉬 정보를 포함하여 대체불가능 토큰을 발행하는 단계; 를 더 포함하는,

블록체인 기반 스미싱 방지 방법.

청구항 12

제 10항에 있어서, 상기 방법은,

메시지 송신자가 발행된 대체불가능 토큰을 메시지 서버에게 전송하는 단계; 를 더 포함하는,

블록체인 기반 스미싱 방지 방법.

청구항 13

제 10항에 있어서, 상기 방법은,

메시지 송신자가 발행한 대체불가능 토큰 관련 정보와 송신 메시지 내용을 메시지 서버에게 전송하는 단계; 를 더 포함하는,

블록체인 기반 스미싱 방지 방법.

청구항 14

제 10항에 있어서, 상기 방법은,

메시지 서버가 대체불가능 토큰에 기록된 메시지 송신자 이름과 휴대폰 번호 속성을 이용하여 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는 단계; 를 더 포함하는,

블록체인 기반 스미싱 방지 방법.

청구항 15

제 10항에 있어서, 상기 방법은,

송신자 신원 및 메시지 내용의 무결성이 성공적으로 검증되는 경우에만, 메시지 서버가 메시지 수신자에게 대체불가능 토큰을 전송하는 단계; 를 더 포함하는,

블록체인 기반 스미싱 방지 방법.

청구항 16

제 10항에 있어서, 상기 방법은,

메시지 서버가 메시지 수신자에게 대체불가능 토큰 관련 정보와 송신 메시지 내용을 송신하는 단계; 를 더 포함하는,

블록체인 기반 스미싱 방지 방법.

청구항 17

제 10항에 있어서, 상기 방법은,

메시지 수신자가 대체불가능 토큰에 기록된 수신자 이름과 휴대폰 번호를 통해 수신자 본인과 일치하다는 것을 검증하는 단계; 를 더 포함하는,

블록체인 기반 스미싱 방지 방법.

청구항 18

제 10항에 있어서, 상기 방법은,

메시지 관련 정보를 블록체인 상에 기록하기 위한 방법 중 대체불가능 토큰(Non-fungible token)으로 표현하고,

대체불가능 토큰(Non-fungible token)은 스미싱 방지 토큰 속성으로 표현된 데이터 구조를 가지고,

스미싱 방지 토큰 속성은 표준 속성으로서 토큰 식별자(id), 토큰 타입(type), 소유자(owner), 운영자(operator), 및 피승인자(approvee) 속성을 가지며, 온체인 확장 속성(xattr)의 하위 속성으로 송·수신자의 이름, 휴대폰 번호 속성을 포함하고, 송신자가 송신하는 스미싱 방지 메시지 내용의 무결성을 검증하기 위한 메시지 내용 해쉬 속성을 가지는,

블록체인 기반 스미싱 방지 방법.

청구항 19

청구항 10 내지 청구항 18 중 어느 한 항의 블록체인 기반 스미싱 방지 방법을 구현하기 위한 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램.

청구항 20

청구항 10 내지 청구항 18 중 어느 한 항의 블록체인 기반 스미싱 방지 방법 의 프로그램을 구현하기 위한 컴퓨터 판독 가능한 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 메시지를 송신한 상대방의 신원을 블록체인을 통해 인증함으로써, 택배 및 공공기관 사칭 등에 의한 스미싱 공격 문제를 해결하기 위한 것으로, 송신자의 메시지 정보와 대응하는 블록체인 상의 대체불가능 토큰(Non-fungible token) 검증 여부를 통해 사용자 인증을 수행하는 기술에 관한 것이다.

배 경 기 술

[0002] 피싱(Phishing)이란 개인정보(Private data)와 낚는다(Fishing)의 합성어로, 전화, 메시지 및 문자 메시지 등을 토대로 이용자의 개인정보를 불법적으로 획득하여 금전적 피해를 입히는 사기수법이다. 스미싱의 대표적인 유형은 보이스 피싱, 스미싱(Smishing), 메신저 피싱 등이 있다. 특히, 스미싱은 문자 메시지(SMS)와 피싱(Phishing)의 합성어로, 스미싱 공격자는 악성 앱 주소가 포함된 문자(SMS)를 불특정 다수에게 송신하며, 수신자가 악성 앱 주소 클릭 및 악성 앱을 설치하도록 유도하여 수신자의 금융 및 개인정보 등을 탈취하는 공격 수법이다. 이때, 스미싱 공격자는 택배 사칭, 공공기관 사칭 및 지인 사칭 등 다양한 방식으로 피해자에게 접근하며 악성 앱 주소 클릭을 유도한다. 스미싱은 오래전부터 잘 알려진 공격 방식임에도 불구하고, 피해자의 심리를 이용한 범죄 행위이기 때문에 현재에도 끊임없이 발생하고 있다. 본 발명에서는 스미싱 공격에 대한 대응 방법

을 서술한다.

[0003] 일반적으로 온라인 상 정보 전달을 위해 사용자는 이메일, 문자 메시지, 혹은 메시지 서비스 등을 이용한다. 특히, 문자 메시지 서비스는 송신자가 수신자의 핸드폰 번호만 알면 정보를 쉽게 전달할 수 있으므로, 주변 지인과 비형식적인 대화 수단으로 많이 사용될 뿐 아니라 또한 택배사 혹은 공공기관 등에서 알림 서비스로도 주로 사용되는 정보 전달 수단이다.

[0004] 문자 메시지 서비스는 접근성이 매우 낮기 때문에 송·수신자 간 정보 교환이 매우 용이하다는 장점이 있는 반면, 어느 사용자라도 수신자의 핸드폰 번호만 알면 메시지를 송신할 수 있다는 점과, 메시지 송·수신 시 사용자 인증 절차를 전혀 수행하지 않는다는 점은 주변 지인, 택배 및 공공기관 사칭 등에 의한 공격에 취약하다는 문제점을 가진다. 따라서, 스미싱 공격자는 불특정 다수에게 악성 앱 주소가 포함된 문자 메시지를 송신하며, 수신자의 악성 앱 설치를 교묘하게 유도하여 소액결제 및 개인정보 탈취 등을 시도한다. 송신자의 신원 인증을 수행하지 않기 때문에 수신자는 송신자가 실제 택배사, 공공기관 등 실제 관계자인지 혹은 스미싱 공격자인지 여부를 알 수 없으므로, 송신 메시지에 포함된 인터넷 주소가 올바른 주소인지 악성 앱 주소인지 여부를 판별하기 어렵다. 이러한 스미싱 공격은 피해자의 심리를 이용하는 수법이므로 현재에도 피해 사례가 끊임없이 발생하고 있다.

[0005] 문자 메시지 서비스는 접근성이 매우 낮기에 온라인 상 주변 지인과 비형식적인 대화 수단으로 사용될 뿐 아니라 사용자 간 간단한 정보 전달을 위해서도 필수적인 서비스로 사용된다. 그러나 상기 서비스는 사용자 신원 인증을 전혀 수행하지 않기 때문에, 송신자가 인터넷 주소를 포함한 메시지를 송신하였을 경우, 수신자는 해당 주소가 올바른 주소인지 악성 앱 주소인지 여부를 판별하는 것이 어렵다는 문제점을 가지고 있다.

[0006] 스미싱 공격자는 상술한 문제점을 기반으로 스미싱 대상자의 심리를 이용하여 접근하며, 택배 사칭, 공공기관 사칭 및 지인 사칭 등 다양한 방식으로 공격을 시도한다. 특히, 택배 사칭 스미싱은 현재 스미싱 피해 사례 중 상당 부분을 차지할 만큼 수신자에게 있어 각별한 주의가 요구되는 공격 행위이다. 택배 서비스는 현대 사회에서 주로 이용되는 서비스이며, 이를 이용하는 사용자들은 일반적으로 택배사 관계자로부터 배송 관련 메시지를 기다리게 되므로, 택배 사칭 스미싱 공격에 항상 노출될 수 밖에 없는 실정이다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 특허출원 제 10-2020-0045447 호

발명의 내용

해결하려는 과제

[0008] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 택배 혹은 공공기관 사칭 스미싱 공격을 대응하기 위한 것으로서, 문자 메시지 서비스에서 메시지를 송신한 상대방의 신원 인증을 블록체인 기술을 활용하여 제공받는, 블록체인 기반 스미싱 방지 방법 및 장치를 제공하는 것이다.

과제의 해결 수단

[0009] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 블록체인 기반 스미싱 방지 시스템은, 메시지 관련 정보를 트랜잭션으로 생성하는 메시지 송신자 단말기; 송신 메시지 및 수신 메시지를 중계하는 메시지 서버; 메시지 송신자가 송신한 메시지를 최종 수신하는 메시지 수신자 단말기; 및 허가형 블록체인으로 구성되는 스미싱 방지 블록체인과, 메시지 송·수신자의 트랜잭션 전송을 중계하는 적어도 하나의 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)를 포함하는 블록체인 기반 스미싱 방지 장치; 를 포함할 수 있다.

[0010] 본 발명의 다른 목적을 달성하기 위한 본 발명의 일 실시예에 따른 블록체인 기반 스미싱 방지 장치는, 허가형 블록체인으로 구성되는 스미싱 방지 블록체인; 메시지 송·수신자의 트랜잭션 전송을 중계하는 적어도 하나의 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK); 프로세서(processor); 및 프로세서를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory); 를 포함하되, 적어도 하나의 명령은 상기 프로세서가: 문자 메시지 서비스 사용자의 신원 정보를 블록체인을 통해 관리하는 단계; 송신 메시지 관련 정보를 블록

체인에 기록하는 단계; 및 메시지 서버가 송신자로부터 블록체인에 기록한 정보를 이용하여 송신자 신원 정보를 검증하고 택배 및 공공기관 사칭에 의한 스미싱을 차단한 메시지만 메시지 수신자에게 중계하는 단계; 를 수행하도록 구성될 수 있다.

[0011] 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)는, 스미싱 방지 블록체인 상에 메시지 내용을 기반으로 하는 스미싱 방지 토큰을 발행하는 트랜잭션을 생성하는 토큰 발행부; 스미싱 방지 블록체인 상에서 스미싱 방지 토큰을 다른 사용자에게 전송하는 기능을 담당하는 토큰 전송부; 대체불가능 토큰을 발행한 사용자의 신원을 인증하는 기능을 담당하는 토큰 속성 검증부; 및 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)가 스미싱 방지 블록체인으로부터 이벤트를 받으면, 호출한 주체에게 알림을 보내는 기능을 하는 이벤트부; 를 포함할 수 있다.

[0012] 이벤트부가 전달하는 이벤트는, 메시지 송신자 단말기가 토큰 발행부를 통해 스미싱 방지 토큰 발행을 요청한 후, 스미싱 방지 블록체인 상에 토큰 생성이 완료되는 경우, 이벤트부는 토큰 발행 완료 사실을 메시지 송신자 단말기에게 이벤트로 알리고, 토큰의 소유자가 토큰 전송부를 통해 스미싱 방지 토큰을 다른 사용자에게 전송을 요청한 후, 스미싱 방지 블록체인 상에서 전송이 완료되는 경우, 이벤트부는 성공적인 소유권 양도 완료 사실을 토큰 전송부 호출자에게 이벤트로 알릴 수 있다.

[0013] 토큰 발행부는, 메시지 송신자 단말기가 토큰 발행부를 통해 블록체인 트랜잭션을 생성하여 스미싱 방지 블록체인 상에 스미싱 방지 토큰을 발행할 수 있다.

[0014] 토큰 전송부는, 스미싱 방지 토큰의 소유자가 토큰 전송부를 통해 스미싱 방지 토큰의 소유권을 다른 사용자에게 양도하는 블록체인 트랜잭션을 생성하고, 토큰 전송부 호출이 완료되면 토큰의 소유자가 변경될 수 있다.

[0015] 토큰 속성 검증부는, 대체불가능 토큰 수신자는 토큰 속성 검증부를 호출하여 송신자가 발행한 대체불가능 토큰에 기록된 송신자 이름과 휴대폰 번호를 확인하며, 송신자 이름 및 휴대폰 번호와 대응되는 사용자 정보 및 공개키가 택배사 혹은 공공기관 관계자의 사용자 정보 및 공개키와의 일치 여부를 비교함으로써, 송신자 당사자 인증을 수행할 수 있다.

[0016] 스미싱 방지 토큰은, 메시지 내용 정보를 블록체인 상에 기록하기 위한 대체불가능 토큰(Non-fungible token)으로, 표준 속성과 온체인(on-chain) 및 오프체인(off-chain) 확장 속성으로 구성될 수 있고, 표준 속성은 토큰 ID 속성, 토큰 타입 속성, 소유자 속성, 피승인자 속성으로 구성될 수 있고, 온체인 확장 속성은 표준 속성의 토큰 타입에 따라 하위 속성을 다르게 정의될 수 있고, 오프체인 확장 속성은 대체불가능 토큰을 표현할 때 오프체인 데이터가 필요한 경우 오프체인 저장소를 연결하기 위해 오프체인 저장소 경로를 저장하는 경로 속성과 오프체인 저장소의 데이터들로 구성된 머클 트리(merkle tree)의 머클 루트(merkle root)를 저장하는 해시 속성이 하위 속성으로 구성될 수 있다.

[0017] 스미싱 방지 토큰은, 온체인 확장 속성을 정의하는 스미싱 방지 토큰 타입으로, 송·수신자 이름, 송·수신자 휴대폰 번호, 및 메시지 내용 해쉬 속성으로 구성될 수 있고, 메시지를 송신하는 메시지 송신자 이름과 휴대폰 번호 정보와 해당 메시지를 수신하는 수신자 이름과 휴대폰 번호 정보를 각각 저장하는 송신자 이름, 송신자 휴대폰 번호 및 수신자 이름, 수신자 휴대폰 번호 속성을 온체인 확장 속성의 하위 속성으로 정의될 수 있고, 송신 메시지 내용의 무결성을 증명하기 위한 메시지 내용 해쉬 속성을 온체인 확장 속성의 하위 속성으로 정의되어 대체불가능 토큰으로 블록체인 상에 표현될 수 있다.

[0018] 본 발명의 또 다른 목적을 달성하기 위한 일 실시예에 따른 블록체인 기반 스미싱 방지 방법은, 메시지 관련 정보를 블록체인 상에 기록하는 블록체인 기반 스미싱 방지 방법에 있어서, 문자 메시지 서비스 사용자의 신원 정보를 블록체인을 통해 관리하는 단계; 송신 메시지 관련 정보를 블록체인에 기록하는 단계; 및 메시지 서버가 송신자로부터 블록체인에 기록한 정보를 이용하여 송신자 신원 정보를 검증하고 택배 및 공공기관 사칭에 의한 스미싱을 차단한 메시지만 메시지 수신자에게 중계하는 단계; 를 포함할 수 있다.

[0019] 상기 방법은, 메시지 송신자가 송신하려는 메시지와 관련된 메시지 송·수신자 이름과 휴대폰 번호, 그리고 메시지 내용 해쉬 정보를 포함하여 대체불가능 토큰을 발행하는 단계; 를 더 포함할 수 있다.

[0020] 상기 방법은, 메시지 송신자가 발행된 대체불가능 토큰을 메시지 서버에게 전송하는 단계; 를 더 포함할 수 있다.

[0021] 상기 방법은, 메시지 송신자가 발행한 대체불가능 토큰 관련 정보와 송신 메시지 내용을 메시지 서버에게 전송하는 단계; 를 더 포함할 수 있다.

[0022] 상기 방법은, 메시지 서버가 대체불가능 토큰에 기록된 메시지 송신자 이름과 휴대폰 번호 속성을 이용하여 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는 단계; 를 더 포함할 수 있다.

[0023] 상기 방법은, 송신자 신원 및 메시지 내용의 무결성이 성공적으로 검증되는 경우에만, 메시지 서버가 메시지 수신자에게 대체불가능 토큰을 전송하는 단계; 를 더 포함할 수 있다.

[0024] 상기 방법은, 메시지 서버가 메시지 수신자에게 대체불가능 토큰 관련 정보와 송신 메시지 내용을 송신하는 단계; 를 더 포함할 수 있다.

[0025] 상기 방법은, 메시지 수신자가 대체불가능 토큰에 기록된 수신자 이름과 휴대폰 번호를 통해 수신자 본인과 일치하다는 것을 검증하는 단계; 를 더 포함할 수 있다.

[0026] 상기 방법은, 메시지 관련 정보를 블록체인 상에 기록하기 위한 방법 중 대체불가능 토큰(Non-fungible token)으로 표현하고, 대체불가능 토큰(Non-fungible token)은 스미싱 방지 토큰 속성으로 표현된 데이터 구조를 가지고, 스미싱 방지 토큰 속성은 표준 속성으로서 토큰 식별자(id), 토큰 타입(type), 소유자(owner), 운영자(operator), 및 피승인자(approvee) 속성을 가지며, 온체인 확장 속성(xattr)의 하위 속성으로 송·수신자의 이름, 휴대폰 번호 속성을 포함하고, 송신자가 송신하는 스미싱 방지 메시지 내용의 무결성을 검증하기 위한 메시지 내용 해쉬 속성을 가질 수 있다.

[0027] 전술한 항 중 어느 한 항의 블록체인 기반 스미싱 방지 방법을 구현하기 위한 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램일 수 있다.

[0028] 전술한 항 중 어느 한 항의 블록체인 기반 스미싱 방지 방법 의 프로그램을 구현하기 위한 컴퓨터 판독 가능한 기록매체일 수 있다.

발명의 효과

[0029] 본 발명은 온라인 상 정보 전달 수단 중 문자 메시지 서비스에 사용자 인증 절차를 제공하기 위한 블록체인 기술을 적용함으로써, 사용자 신원 사칭 여부를 판별하여 택배 및 공공기관 사칭 등에 의한 스미싱을 방지하는 효과가 있다.

[0030] 메시지 송신자가 실제 택배사 혹은 공공기관 관계자일 경우, 메시지 송신자는 먼저 블록체인 상 대체불가능 토큰을 발행하고 메시지 서버에게 대체불가능 토큰 정보를 제공함으로써 사용자 인증에 대한 증빙을 제공할 수 있다.

[0031] 메시지 서버는 송신자가 발행 및 전송한 대체불가능 토큰을 통해 송신자가 택배사 혹은 공공기관에 소속된 사용자임이 분명하다는 사용자 인증이 확인되고 메시지 내용의 무결성이 검증 완료되면, 수신자에게 대체불가능 토큰 및 메시지를 송신한다. 반면, 사용자 인증 혹은 메시지 내용 무결성 검증을 실패할 경우, 송신자를 스미싱 공격자로 판단하는 것이 가능해진다.

[0032] 따라서, 메시지 서버는 송신자의 신원 인증을 블록체인을 통해 검증함으로써, 스미싱 행위를 판별할 수 있으며, 이를 통해 메시지 수신자에게 스미싱 행위를 차단한 문자 메시지들만 중계하는 것이 가능해진다.

도면의 간단한 설명

[0033] 도 1은 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 방법 및 장치를 포함한 시스템의 구성을 보여주는 도면이다.

도 2는 본 발명의 블록체인을 활용하는 한 가지 예로서, 메시지 관련 정보를 대체불가능 토큰으로 표현할 경우, 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)의 구성을 보여주는 도면이다.

도 3은 본 발명의 블록체인 활용의 한 가지 예로서, 송·수신하는 메시지에 대해 사용자 인증, 무결성 검증 특성을 제공하기 위해 메시지 관련 정보를 대체불가능 토큰으로 표현한 데이터 구조를 보여주는 도면이다.

도 4는 본 발명의 블록체인을 활용하는 한 가지 예로서, 메시지 관련 정보를 대체불가능 토큰으로 표현할 경우, 블록체인 기반 스미싱 방지 방법 및 장치를 활용한 메시지 시스템 구성의 전체적인 진행 과정을 보여주는 도면이다.

도 5는 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 장치의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0034] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하여 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0035] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는 데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. "및/또는"이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0036] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0037] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0038] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0040] 본 발명에서 개시되는 피어 투 피어(Peer-to-Peer) 네트워크를 기반으로 하는 블록체인(Blockchain)은 모든 참여 노드(Node)들이 합의 알고리즘을 통해 동일한 순서의 트랜잭션 집합을 보유하도록 하여 트랜잭션 데이터의 투명성과 무결성을 지원하는 기술이다. 참여 노드 간 합의 알고리즘 수행 시, 새로 생성되는 블록은 이전 블록의 해시(Hash)값과 트랜잭션 집합을 포함한다. 따라서, 모든 참여 노드는 블록 해시 값으로 연결된 동일한 블록체인 데이터 구조를 유지 관리한다. 특정 노드가 임의로 블록체인 데이터 조작을 시도하더라도, 조작된 데이터는 노드 간 합의를 수행하지 않았기 때문에 블록체인에 반영되지 않는다. 이처럼 블록체인은 모든 참여 노드가 동일하게 보유하는 데이터 구조의 무결성 및 투명성을 지원하는 기술이다.

[0041] 블록체인은 비허가형 블록체인(Permissionless Blockchain)과 허가형 블록체인(Permissioned Blockchain)으로 구분된다. 비허가형 블록체인에서 사용자 및 노드는 아무런 제약 없이 블록체인 네트워크에 참여 가능하며 허가형 블록체인은 허가된 사용자 및 노드들만 블록체인 네트워크에 참여할 수 있는, 비즈니스 환경에서 활용하기에 적합한 블록체인이다.

[0042] 블록체인 상에서 실행되는 프로그램인 스마트 컨트랙트(Smart Contract)에 비즈니스 로직을 구성하여 분산 애플리케이션(Distributed Application: dApp)을 개발 및 운영할 수 있다. 스마트 컨트랙트는 제3자의 개입 없이 각 요청을 비즈니스 로직에 따라 자동으로 실행한다는 장점을 갖고 있다. 대표적인 dApp으로 토큰(Token)이 있다.

[0043] 토큰은 디지털 자산(Digital Asset)을 블록체인 상에 표현한 것이다. 블록체인에 디지털 자산을 토큰화하면 디지털 자산의 소유권 증명, 투명성 보장, 유동성 향상 등의 장점을 확보할 수 있다. 토큰은 대체가능 토큰(Fungible Token)과 대체불가능 토큰(Non-Fungible Token)으로 구분된다. 대체가능 토큰은 쪼개질 수 있는 디지털 자산을 표현한 토큰이고, 대체불가능 토큰은 쪼개질 수 없는 디지털 자산을 표현한 토큰이다.

[0045] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를

사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0047] 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 시스템은 메시지 송신자의 신원 인증을 수행하기 위하여 블록체인을 활용한다.

[0048] 본 발명은 사용자의 신원 인증을 제공하기 위한 정보 등을 블록체인 네트워크상에 유지 관리하는 다양한 방법을 포함하고 있으며, 하나의 구체적인 일례로 송신자의 메시지 내용과 대응되는 대체불가능 토큰을 블록체인에서 유지 관리하는 방법을 서술한다.

[0049] 송신자는 자신의 서명 정보를 기반으로 대체불가능 토큰을 발행하며, 해당 대체불가능 토큰은 송·수신 대상자 이름, 송신자와 수신자의 휴대폰 번호, 그리고 메시지 내용 무결성 검증을 위한 메시지 내용 해쉬 정보를 포함하기 때문에, 송신자 신원 및 메시지 내용 무결성 검증 방법을 용이하게 제공할 수 있다. 따라서, 송신자는 대체불가능 토큰을 발행하고 제공함으로써, 자신이 스미싱 공격자가 아니라는 확실한 증빙을 제공하는 것이 가능해진다.

[0050] 대체불가능 토큰 속성으로는 토큰 고유 식별 id 속성, 토큰 발행 주체인 소유자 속성, 메시지 송·수신자 이름, 송신자 휴대폰 번호 및 수신자 휴대폰 번호 속성, 그리고 메시지 내용 무결성 검증을 위한 메시지 내용 해쉬 속성 등으로 정의하며, 토큰 속성은 필요시 다양하게 추가 및 정의할 수 있다.

[0051] 사용자가 문자 메시지를 송신할 때 과정은 다음과 같다. 모든 사용자는 PKI(Public Key Infrastructure) 기반한 공개키, 비밀키 쌍을 가지고 있으며, 따라서 모든 사용자는 블록체인 트랜잭션을 생성할 수 있다고 가정한다.

[0052] 첫째. 송신자는 문자 메시지 내용을 작성 및 송신한다.

[0053] 둘째. 송신자는 방금 전송한 메시지 내용을 기반으로 블록체인 상에 대체불가능 토큰을 발행하며, 토큰 속성으로는 토큰 아이디(id), 소유자, 송·수신자 이름, 송·수신자 휴대폰 번호 및 메시지 내용 해쉬 정보 등을 포함한다. 이때, 토큰을 발행하기 위한 트랜잭션 정보에 메시지 송신자의 서명 정보가 포함되며, 따라서 발행된 토큰의 소유자는 메시지 송신자가 된다.

[0054] 셋째. 송신자는 블록체인 상 초기화한 대체불가능 토큰을 메시지 서버에게 전송하여 토큰의 소유자를 메시지 서버로 변경한다.

[0055] 넷째. 송신자는 대체불가능 토큰 관련 정보와 메시지 내용을 메시지 서버로 송신한다.

[0056] 다섯째. 메시지 서버는 수신한 대체불가능 토큰 정보를 기반으로 블록체인 상 대체불가능 토큰을 검증하며, 이를 통해 송신자의 신원 인증을 수행한다. 예를 들어, 택배 사칭 스미싱 공격자는 실제 택배사 관계자의 서명 정보를 기반으로 대체불가능 토큰을 발행해야 한다. 그러나 택배 사칭 스미싱 공격자는 실제 택배사 관계자의 서명 정보를 알 수 없으므로, 택배사 관계자를 사칭하기 위한 대체불가능 토큰을 발행할 수 없다. 따라서, 메시지 서버는 송신자가 발행한 대체불가능 토큰에 기록된 송신자 이름과 휴대폰 번호를 확인함으로써, 송신자가 실제 택배사 관계자인지 스미싱 공격자인지 여부를 판별할 수 있다.

[0057] 메시지 서버가 송신자 신원을 검증 완료하면, 메시지 내용의 무결성을 검증한다. 메시지 서버가 수신한 메시지 내용을 해싱한 값이 대체불가능 토큰에 기록된 메시지 내용 해쉬 값과 일치하는지를 비교함으로써, 메시지 내용이 무결한지 검증할 수 있다. 이때, 메시지 서버가 송신자 신원 및 메시지 내용의 무결성 검증을 실패한다면 수신자에게 대체불가능 토큰 및 메시지를 송신하지 않는다.

[0058] 여섯째. 송신자의 신원 및 메시지 내용의 무결성이 블록체인 상 대체불가능 토큰을 통해 검증 완료되면, 메시지 서버는 수신자에게 대체불가능 토큰을 전송하여 소유자를 변경한다.

[0059] 일곱째. 메시지 서버는 대체불가능 토큰 관련 정보와 메시지를 메시지 수신자에게 송신한다.

[0060] 여덟째. 메시지 수신자는 대체불가능 토큰 속성을 통해 수신자 이름과 휴대폰 번호가 자신의 정보와 일치하는지를 확인한다. 정보가 일치하다면 수신자는 메시지 내용을 확인한다.

[0062] 도 1은 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 방법 및 장치(400)를 포함한 시스템 구성을 보여주는 도면이다.

[0063] 도 1을 참조하면, 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 시스템은, 택배사 혹은 공공기관 관계자의 신원을 미리 인증하고 서비스를 제공하기 위해서 스미싱 방지 블록체인(300)을 허가형 블록체인으로 구성한다.

[0064] 본 발명의 일 실시 예에 따른 블록체인 기반 스미싱 방지 시스템은, 사용자의 메시지를 송신하는 메시지 송신자

단말기(100a)와 메시지 송신자 단말기가 송신한 메시지를 중계하는 메시지 서버(100c), 메시지 송신자 단말기(100a)가 송신한 메시지를 최종 수신하는 메시지 수신자 단말기(100b), 허가형 블록체인으로 구성되는 스미싱 방지 블록체인(300)과, 메시지 송·수신자 단말기의 트랜잭션 전송을 중계하는 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)(200)를 포함한다.

[0065] 메시지 송신자 단말기(100a)는 일반적인 메시지와 스미싱 방지 메시지 중 선택하여 송신할 수 있다. 일반적인 메시지 송신을 선택하는 경우 기존 문자 메시지 서비스와 동일하게 메시지 서버(100c)를 통해 전송하며, 스미싱 방지 메시지 송신을 선택할 경우에는 메시지 서버(100c)를 통해 메시지를 전송하고 추가적으로 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)(200)와 연동되어 스미싱 방지 블록체인(300)에 스미싱 방지를 위한 블록체인 트랜잭션을 생성하도록 동작한다.

[0067] 도 2는 본 발명의 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)(200)의 구성을 보여주는 도면이다.

[0068] 도 2를 참조하면, 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)(200)는 토큰 발행부(510), 토큰 전송부(520), 토큰 속성 검증부(530) 및 이벤트 부(540)를 포함한다.

[0069] 토큰 발행부(510)는 스미싱 방지 블록체인(300) 상에 메시지 내용을 기반으로 하는 스미싱 방지 토큰을 발행하는 트랜잭션을 생성한다. 보다 구체적으로는, 메시지 송신자 단말기(100a)가 토큰 발행부(510)를 통해 블록체인 트랜잭션을 생성하여 스미싱 방지 블록체인(300) 상에 스미싱 방지 토큰을 발행한다. 스미싱 방지 토큰 속성은 도 3에서 서술한다. 참고로, 토큰 소유자는 토큰을 발행한 주체가 된다.

[0070] 토큰 전송부(520)는 스미싱 방지 블록체인(300) 상에서 스미싱 방지 토큰을 다른 사용자에게 전송하는 기능을 담당한다. 보다 구체적으로는, 스미싱 방지 토큰의 소유자가 토큰 전송부(520)를 통해 스미싱 방지 토큰의 소유권을 다른 사용자에게 양도하는 블록체인 트랜잭션을 생성한다. 즉, 토큰 전송부(520) 호출이 완료되면 토큰의 소유자가 변경된다. 토큰 전송부(520) 호출 권한은 토큰 소유자만 가능하다.

[0071] 토큰 속성 검증부(530)는 대체불가능 토큰을 발행한 사용자의 신원을 인증하는 기능을 담당한다. 즉, 대체불가능 토큰을 발행한 사용자가 실제 택배사 혹은 공공기관 관계자인지 혹은 스미싱 공격자인지에 대한 판단 기준을 제공하는 기능을 한다. 모든 사용자는 사용자 신원을 검증 받은 후 스미싱 방지 블록체인에 등록되므로, 자신의 사용자 정보와 관련된 서명 정보를 기반으로 하는 트랜잭션만 생성 가능하다. 따라서, 대체불가능 토큰 수신자는 토큰 속성 검증부(530)를 호출하여 송신자가 발행한 대체불가능 토큰에 기록된 송신자 이름과 휴대폰 번호를 확인하며, 송신자 이름 및 휴대폰 번호와 대응되는 사용자 정보 및 공개키가 택배사 혹은 공공기관 관계자의 사용자 정보 및 공개키와의 일치 여부를 비교함으로써, 송신자 당사자 인증을 수행할 수 있다. 추가적으로, 토큰 속성에는 메시지 내용에 대한 해쉬 정보를 저장하고 있으므로, 이를 통해 수신된 메시지의 무결성을 검증하는 과정도 진행할 수 있다. 메시지 서버는 송신자 신원과 메시지의 무결성이 실패할 경우, 메시지 중계 작업을 더 이상 진행하지 않는다.

[0072] 이벤트부(540)는 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)(200)가 스미싱 방지 블록체인(300)으로부터 이벤트를 받으면, 호출한 주체에게 알림을 보내는 기능을 한다. 토큰 발행부(510), 토큰 전송부(520)가 호출된 후 스미싱 방지 토큰에 대한 동작 결과가 스미싱 방지 블록체인(300)에 최종적으로 커밋(commit)되면 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)(200)는 이벤트부 (540)를 통해 스미싱 방지 블록체인(300) 이벤트를 받게 된다.

[0073] 본 발명에서 이벤트부(540)가 전달하는 이벤트들은 다음과 같다. 메시지 송신자 단말기(100a)가 토큰 발행부(510)를 통해 스미싱 방지 토큰 발행을 요청한 후, 스미싱 방지 블록체인(300) 상에 토큰 생성이 완료되는 경우, 이벤트부(540)는 토큰 발행 완료 사실을 메시지 송신자 단말기(100a)에게 이벤트로 알린다. 또한, 토큰의 소유자가 토큰 전송부(520)를 통해 스미싱 방지 토큰을 다른 사용자에게 전송을 요청한 후, 스미싱 방지 블록체인(300) 상에서 전송이 완료되는 경우, 이벤트부(540)는 성공적인 소유권 양도 완료 사실을 토큰 전송부(520) 호출자에게 이벤트로 알린다.

[0075] 도 3은 본 발명의 블록체인을 활용하는 예시 중 하나로서, 스미싱 방지 토큰 속성 구조를 대체불가능 토큰으로 표현한 데이터 구조를 보여주는 도면이다.

[0076] 도 3을 참조하면, 스미싱 방지 토큰은 표준 속성으로서 토큰 식별자(id), 토큰 타입(type), 소유자(owner), 운영자(operator), 및 피승인자(approvee) 속성을 가지며, 온체인 확장 속성(xattr)의 하위 속성으로 송·수신자의 이름, 휴대폰 번호 속성을 포함한다. 또한 송신자가 송신하는 스미싱 방지 메시지 내용의 무결성을 검증하기

위한 메시지 내용 해쉬 속성을 가진다.

[0078] 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 방법은, 메시지 관련 정보를 블록체인 상에 기록하기 위한 방법 중 대체불가능 토큰(Non-fungible token)으로 표현하는 블록체인 기반 스미싱 방지 방법에 있어서, 문자 메시지 서비스 사용자의 신원 정보를 블록체인을 통해 관리하는 단계; 송신 메시지 관련 정보를 블록체인에 기록하는 단계; 및 메시지 서버가 송신자로부터 블록체인에 기록한 정보를 이용하여 송신자 신원 정보를 검증하고 택배 및 공공기관 사칭에 의한 스미싱을 차단한 메시지만 메시지 수신자에게 중계하는 단계; 를 포함한다.

[0079] 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 방법은, 메시지 송신자가 송신하려는 메시지와 관련된 메시지 송·수신자 이름과 휴대폰 번호, 그리고 메시지 내용 해쉬 정보를 포함하여 대체불가능 토큰을 발행하는 단계; 메시지 송신자가 발행된 대체불가능 토큰을 메시지 서버에게 전송하는 단계; 메시지 송신자가 발행한 대체불가능 토큰 관련 정보와 송신 메시지 내용을 메시지 서버에게 전송하는 단계; 메시지 서버가 대체불가능 토큰에 기록된 메시지 송신자 이름과 휴대폰 번호 속성을 이용하여 메시지 송신자의 신원을 검증하고, 메시지 내용 해쉬 정보를 이용하여 송신 메시지 내용의 무결성을 검증하는 단계; 송신자 신원 및 메시지 내용의 무결성이 성공적으로 검증되는 경우에만, 메시지 서버가 메시지 수신자에게 대체불가능 토큰을 전송하는 단계; 메시지 서버가 메시지 수신자에게 대체불가능 토큰 관련 정보와 송신 메시지 내용을 송신하는 단계; 및 메시지 수신자가 대체불가능 토큰에 기록된 수신자 이름과 휴대폰 번호를 통해 수신자 본인과 일치하다는 것을 검증하는 단계; 를 포함한다.

[0080] 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 장치(400)를 이용한 블록체인 기반 스미싱 방지 방법의 세부적인 작동을 도 4를 참조하여 설명한다.

[0082] 도 4는 블록체인을 활용하는 한 가지 예로서, 메시지 관련 정보를 대체불가능 토큰으로 표현할 경우, 블록체인 기반 스미싱 방지 방법 및 장치를 활용한 메시지 시스템 구성의 전체적인 진행 과정을 보여주는 도면이다.

[0083] 도 4를 참조하면, 메시지 송·수신자 단말기(100a~100b)는 모두 스미싱 방지 블록체인(300)에 등록된 사용자이며, 등록 시 사용자 신원을 인증받는다. 인증 받은 각 사용자는 사용자 정보와 대응되는 PKI 기반 공개키와 비밀키를 발급 받는다. 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)(200)는 허가된 사용자들만 스미싱 방지 블록체인(300)을 접근할 수 있도록 제어하기 위해 사용자들의 정보 및 해당 정보와 대응되는 공개키를 저장한다. 따라서, 각 사용자는 스미싱 방지 소프트웨어 개발 키트(Software Development Kit, SDK)(200)가 관리하는 사용자 별 공개키를 이용하여, 블록체인 상 대체불가능 토큰을 통한 사용자 인증을 수행할 수 있다.

[0084] 메시지 송신자 단말기(100a)가 스미싱 방지 메시지를 송신하고자 한다면, 메시지 내용을 기입한 뒤 스미싱 방지 메시지를 송신한다. 메시지 송신자 단말기(100a)의 메시지 송신 과정은 우선 토큰 발행부(510)를 호출한다.

[0085] 메시지 송신자 단말기(100a)가 호출한 토큰 발행부(510)는 스미싱 방지 블록체인(300) 상에 스미싱 방지 메시지 기반의 스미싱 방지 토큰(토큰의 id는 T0)을 발행한다(S210). 발행된 토큰 T0는 확장 속성의 하위 속성으로 메시지 송·수신자 이름, 휴대폰 번호 및 메시지 내용 해쉬 정보를 포함한다.

[0086] 이벤트부(540)는 메시지 송신자 단말기(100a)에게 토큰 T0의 성공적인 발행 완료 사실을 알리며, 메시지 송신자 단말기(100a)는 토큰 전송부(520)를 호출하여 메시지 서버(100c)에게 토큰 T0를 전송한다(S220). 토큰 T0의 소유권이 메시지 서버(100c)에게 성공적으로 양도되면, 이벤트부(540)는 메시지 송신자 단말기(100a)에게 성공적인 양도 완료 사실을 알린다.

[0087] 이벤트부(540)로부터 성공적인 알림을 받은 메시지 송신자 단말기(100a)는 스미싱 방지 메시지(T0 및 송신 메시지 내용)를 메시지 서버(100c)로 송신한다(S110).

[0088] 메시지를 수신한 메시지 서버(100c)는 메시지 송신자의 신원을 검증하기 위해 토큰 속성 검증부(530)를 호출한다(S230). 송신자는 오로지 자신의 서명 정보를 기반으로 하는 대체불가능 토큰만 발행할 수 있으므로, 메시지 서버는 대체불가능 토큰 상 기록된 송신자 이름과 휴대폰 번호를 확인하여 택배사 혹은 공공기관 등 미리 신원을 검증 받은 관계자의 사용자 정보와 일치하는지 여부를 비교함으로써 송신자 신원을 검증할 수 있다. 송신자 신원 검증이 성공적으로 완료되면, 메시지 서버(100c)는 메시지 내용의 무결성을 검증한다. 메시지 내용 무결성은 메시지 내용을 해싱한 값과 대체불가능 토큰에 기록된 메시지 내용 해쉬 값을 비교함으로써 검증할 수 있다. 이때, 사용자 신원 및 메시지 내용 무결성 검증 중 하나라도 실패하는 경우, 메시지 서버(100c)는 메시지 중계 작업을 더 이상 진행하지 않는다.

[0089] 사용자 신원 및 메시지 내용 무결성 검증이 성공적으로 완료되면, 메시지 서버(100c)는 메시지 수신자 단말기(100b)에게 대체불가능 토큰을 전송한다(S240).

[0090] 대체불가능 토큰 전송이 성공적으로 완료되어, 메시지 서버(100c)가 해당 사실을 이벤트로 받으면 스미싱 방지 메시지를 메시지 수신자 단말기(100b)에게 송신한다(S120). 마지막으로, 메시지 수신자 단말기(100b)는 송신 메시지를 확인하기 위해 토큰 속성 검증부(530)를 호출한다(S250). 메시지 수신자 단말기(100b)는 송신자가 자신에게 송신한 메시지라는 것을 확인하기 위해 송·수신자 이름과 휴대폰 번호를 확인한다. 수신자 이름과 휴대폰 번호가 자신의 정보와 일치하다면, 메시지 내용을 확인한다.

[0092] 이와 같이, 본 발명에 따르면 일반적인 메시지 서비스의 사용자 인증 부재에 따른 스미싱 공격을 블록체인 기술을 적용하여 해결할 수 있으며, 구체적인 실시 예로 대체불가능 토큰을 모델링하여 사용자 인증을 수행함으로써 스미싱 공격을 차단할 수 있음을 확인하였다.

[0093] 메시지 서버는 대체불가능 토큰을 통해 송신자의 사용자 인증 및 메시지 내용 무결성이 검증되면 송신자를 실제 신원 검증 완료된 택배사 혹은 공공기관 관계자라고 판단할 수 있으며, 반대로 송신자의 사용자 인증 및 메시지 내용 무결성 검증이 실패하는 경우, 송신자를 스미싱 공격자로 판단하는 것이 가능해진다.

[0094] 따라서, 송신자가 스미싱 공격자인지 아닌지 여부에 대한 사용자 인증을 블록체인을 통해 객관적인 방법으로 수행할 수 있으므로, 메시지 서버는 메시지 수신자에게 스미싱 공격을 차단한 정상적인 메시지만 중계하는 것이 가능해진다.

[0096] 도 5는 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 장치(400)의 구성도이다.

[0097] 도 5를 참조하면, 본 발명의 일 실시예의 블록체인 기반 스미싱 방지 장치(400)는, 프로세서(410), 메모리(420), 송수신 장치(transceiver, 430), 입력 인터페이스 장치(440), 출력 인터페이스 장치(450), 저장 장치(460) 및 버스(bus)(470)를 포함하여 구성될 수 있다.

[0098] 본 발명의 블록체인 기반 스미싱 방지 장치(400)는, 프로세서(processor)(410) 및 프로세서(410)를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory)(420)를 포함하되, 적어도 하나의 명령은 상기 프로세서(410)가, 문자 메시지 서비스 사용자의 신원 정보를 블록체인을 통해 관리하는 단계, 송신 메시지 관련 정보를 블록체인에 기록하는 단계, 및 메시지 서버가 송신자로부터 블록체인에 기록한 정보를 이용하여 송신자 신원 정보를 검증하고 택배 및 공공기관 사칭에 의한 스미싱을 차단한 메시지만 메시지 수신자에게 중계하는 단계를 수행하도록 구성된다.

[0099] 프로세서(410)는 중앙 처리 장치(central processing unit, CPU), 그래픽 처리 장치(graphics processing unit, GPU), 또는 본 발명의 실시예들에 따른 방법들이 수행되는 전용의 프로세서를 의미할 수 있다.

[0100] 메모리(420) 및 저장 장치(460) 각각은 휘발성 저장 매체 및 비휘발성 저장 매체 중에서 적어도 하나로 구성될 수 있다. 예를 들어, 메모리(420)는 읽기 전용 메모리(read only memory, ROM) 및 랜덤 액세스 메모리(random access memory, RAM) 중에서 적어도 하나로 구성될 수 있다.

[0101] 또한, 블록체인 기반 스미싱 방지 장치(400)는 무선 네트워크를 통해 통신을 수행하는 송수신 장치(transceiver)(430)를 포함할 수 있다.

[0102] 또한, 블록체인 기반 스미싱 방지 장치(100)는 입력 인터페이스 장치(440), 출력 인터페이스 장치(450), 저장 장치(460) 등을 더 포함할 수 있다.

[0103] 또한, 블록체인 기반 스미싱 방지 장치(400)에 포함된 각각의 구성 요소들은 버스(bus)(470)에 의해 연결되어 서로 통신을 수행할 수 있다.

[0104] 본 발명의 블록체인 기반 스미싱 방지 장치(400)의 예를 들면, 통신 가능한 데스크탑 컴퓨터(desktop computer), 랩탑 컴퓨터(laptop computer), 노트북(notebook), 스마트폰(smart phone), 태블릿 PC(tablet PC), 모바일폰(mobile phone), 스마트 워치(smart watch), 스마트 글래스(smart glass), e-book 리더기, PMP(portable multimedia player), 휴대용 게임기, 네비게이션(navigation) 장치, 디지털 카메라(digital camera), DMB(digital multimedia broadcasting) 재생기, 디지털 음성 녹음기(digital audio recorder), 디지털 음성 재생기(digital audio player), 디지털 동영상 녹화기(digital video recorder), 디지털 동영상 재생기(digital video player), PDA(Personal Digital Assistant) 등일 수 있다.

[0106] 본 발명은 온라인 상 정보 전달 수단 중 문자 메시지 서비스에 사용자 인증 절차를 제공하기 위한 블록체인 기

술을 적용함으로써, 사용자 신원 사칭 여부를 판별하여 택배 및 공공기관 사칭 등에 의한 스미싱을 방지하는 효과가 있다.

[0107] 메시지 송신자가 실제 택배사 혹은 공공기관 관계자일 경우, 메시지 송신자는 먼저 블록체인 상 대체불가능 토큰을 발행하고 메시지 서버에게 대체불가능 토큰 정보를 제공함으로써 사용자 인증에 대한 증빙을 제공할 수 있다.

[0108] 메시지 서버는 송신자가 발행 및 전송한 대체불가능 토큰을 통해 송신자가 택배사 혹은 공공기관에 소속된 사용자임이 분명하다는 사용자 인증이 확인되고 메시지 내용의 무결성이 검증 완료되면, 수신자에게 대체불가능 토큰 및 메시지를 송신한다. 반면, 사용자 인증 혹은 메시지 내용 무결성 검증을 실패할 경우, 송신자를 스미싱 공격자로 판단하는 것이 가능해진다.

[0109] 따라서, 메시지 서버는 송신자의 신원 인증을 블록체인을 통해 검증함으로써, 스미싱 행위를 판별할 수 있으며, 이를 통해 메시지 수신자에게 스미싱 행위를 차단한 문자 메시지들만 중계하는 것이 가능해진다.

[0111] 본 발명의 실시예에 따른 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0112] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

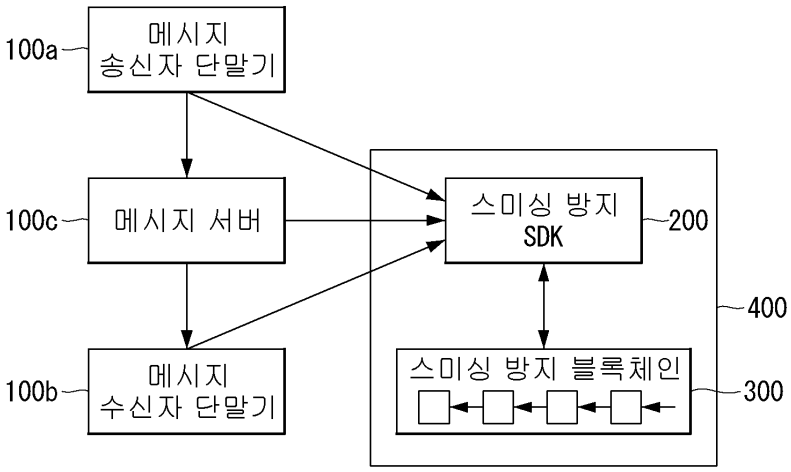
[0113] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0114] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

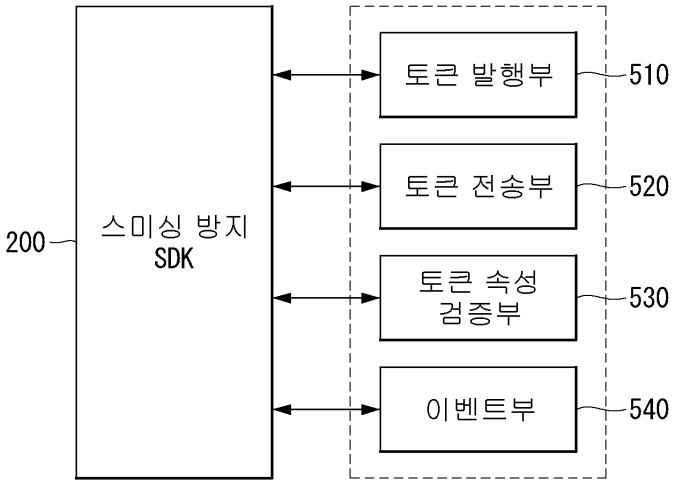
[0115] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

도면1



도면2

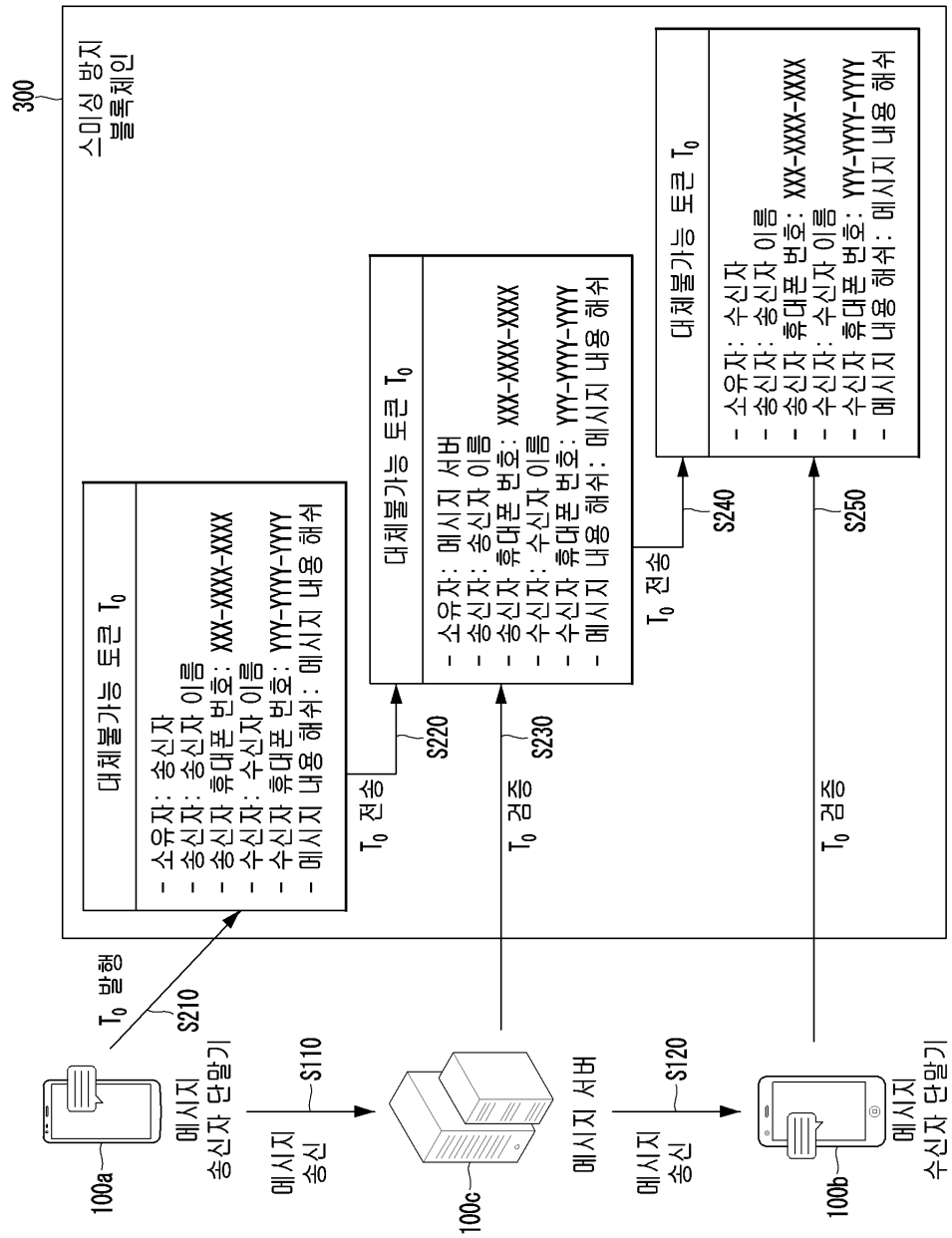


도면3

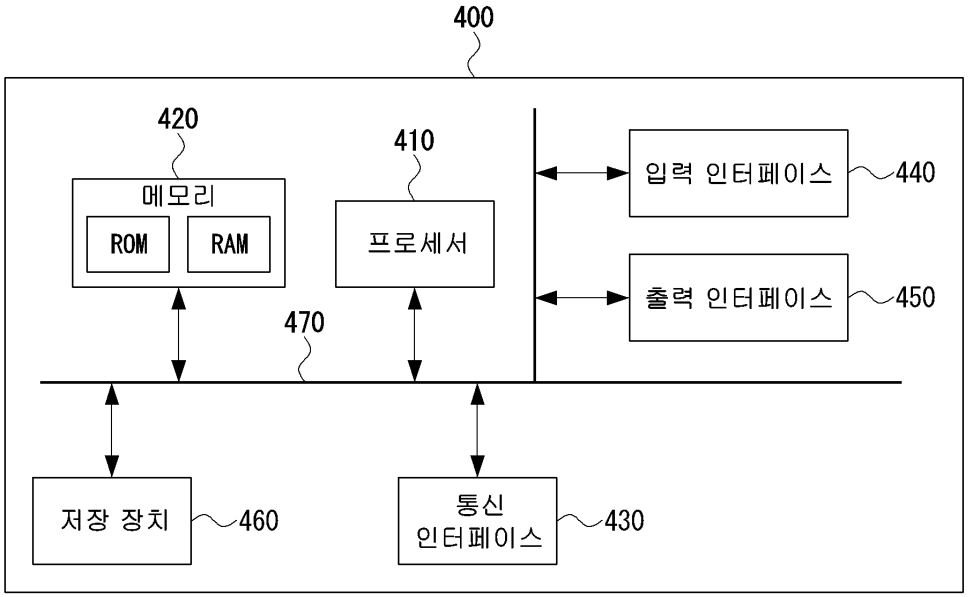
표준 속성	확장 속성

- id
- type(Anti-Smishing)
- owner
- operator
- approvee
	- xattr:{
	- 송신자:
	- 송신자 휴대폰 번호:
	- 수신자:
	- 수신자 휴대폰 번호:
	- 메시지 내용 해쉬:
	}
	- url:{
	- 오프체인 저장소 경로:
	- 해시:
	}

도면4


300
스미싱 방지
블록체인
대체불가능 토큰 T_0
- 소유자: 송신자
- 송신자: 송신자 이름
- 송신자 휴대폰 번호: XXX-XXXX-XXXX
- 수신자: 수신자 이름
- 수신자 휴대폰 번호: YYY-YYYY-YYYY
- 메시지 내용 해쉬: 메시지 내용 해쉬
T_0 발행
S210
T_0 전송
S220
대체불가능 토큰 T_0
- 소유자: 메시지 서버
- 송신자: 송신자 이름
- 송신자 휴대폰 번호: XXX-XXXX-XXXX
- 수신자: 수신자 이름
- 수신자 휴대폰 번호: YYY-YYYY-YYYY
- 메시지 내용 해쉬: 메시지 내용 해쉬
T_0 검증
S230
T_0 전송
S240
대체불가능 토큰 T_0
- 소유자: 수신자
- 송신자: 송신자 이름
- 송신자 휴대폰 번호: XXX-XXXX-XXXX
- 수신자: 수신자 이름
- 수신자 휴대폰 번호: YYY-YYYY-YYYY
- 메시지 내용 해쉬: 메시지 내용 해쉬
T_0 검증
S250
100a
메시지
송신자 단말기
S110
메시지
송신
100c
메시지 서버
S120
메시지
송신
100b
메시지
수신자 단말기

도면5


400
420
메모리
ROM
RAM
410
프로세서
입력 인터페이스
440
출력 인터페이스
450
470
저장 장치
460
통신
인터페이스
430