(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0103833
(43) 공개일자 2025년07월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
H04L 9/3247 (2013.01)
(21) 출원번호 10-2023-0193924
(22) 출원일자 2023년12월28일
심사청구일자 2023년12월28일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
국민대학교산학협력단
서울특별시 성북구 정릉로 77 (정릉동, 국민대학교)
한양대학교 산학협력단
서울특별시 성동구 왕십리로 222(행당동, 한양대학교내)
(72) 발명자
이중희
서울특별시 성북구 길음로9길 50, 907동 202호
권용희
대구광역시 달성군 유가읍 테크노대로5길 57, 203동 1204호
(뒷면에 계속)
(74) 대리인
김준석, 박민욱

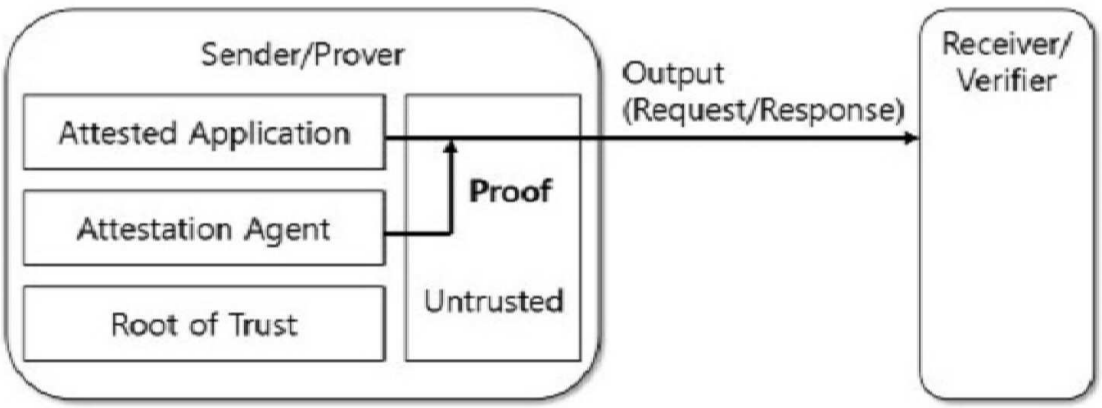
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **인증 증명 장치 및 그 방법**

(57) 요 약

본 발명의 일 기술적 측면에 따른 인증 증명 장치 및 방법에 관한 것으로, 증명 모듈이 기 수신된 요청 데이터의 해시값을 측정하는 단계; 상기 증명 모듈이 상기 요청 데이터에 대한 응답 데이터를 생성하는 단계; 상기 증명 모듈이 상기 응답 데이터의 해시값을 측정하는 단계; 및 상기 증명 모듈이 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 기초로 증명값을 생성하는 단계;를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/3263 (2013.01)
(72) 발명자
허승민
서울특별시 양천구 목동남로4길 80, 103동 1302호
오현옥
서울특별시 송파구 올림픽로 435, 211동 803호
김지혜
서울특별시 중구 마른내로 72, 1011호 (인현동2가)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711193772
과제번호 2021-0-00528-003
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보보호핵심원천기술개발(R&D)
연구과제명 하드웨어 중심 신뢰계산기반과 분산 데이터보호박스를 위한 표준 프로토콜 개발
기 여 율 60/100
과제수행기관명 고려대학교산학협력단
연구기간 2023.01.01 ~ 2023.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711193835
과제번호 2021-0-00727-003
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보보호핵심원천기술개발(R&D)
연구과제명 간결한 비대화형 연산 증명 시스템(SNARK)을 위한 암호 원천 기술 개발
기 여 율 20/100
과제수행기관명 한양대학교산학협력단
연구기간 2023.01.01 ~ 2023.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711194271
과제번호 2021-0-00518-003
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 데이터경제를위한블록체인기술개발
연구과제명 블록체인 데이터 암호화 기반의 프라이버시 보호 기술개발
기 여 율 20/100
과제수행기관명 한양대학교산학협력단
연구기간 2023.01.01 ~ 2023.12.31

명 세 서

청구범위

청구항 1

증명 모듈이 기 수신된 요청 데이터의 해시값을 측정하는 단계;

상기 증명 모듈이 상기 요청 데이터에 대한 응답 데이터를 생성하는 단계;

상기 증명 모듈이 상기 응답 데이터의 해시값을 측정하는 단계; 및

상기 증명 모듈이 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 기초로 증명값을 생성하는 단계;

를 포함하는 인증 증명 방법.

청구항 2

제1항에 있어서,

상기 요청 데이터는,

검증 모듈에서 입력받아 신뢰하지 않은 어플리케이션을 통해 상기 증명 모듈로 전송되는 데이터이고, 상기 신뢰하지 않은 어플리케이션의 공격이 있는 경우에 오류가 발생된 데이터가 상기 증명 모듈로 전송되는 것을 특징으로 하는 인증 증명 방법.

청구항 3

제1항에 있어서,

상기 증명 모듈이 인증된 어플리케이션에 대한 초기 상태의 해시값을 측정하는 단계;를 더 포함하고,

상기 증명값을 생성하는 단계는,

상기 요청 데이터의 해시값, 상기 응답 데이터의 해시값, 상기 초기 상태의 해시값 및 개인키를 이용하여 상기 증명값을 생성하는 단계;를 더 포함하는 것을 특징으로 하는 인증 증명 방법.

청구항 4

제3항에 있어서,

상기 요청 데이터의 해시값, 상기 응답 데이터의 해시값, 상기 초기 상태의 해시값 및 개인키를 이용하여 상기 증명값을 생성하는 단계는,

디지털서명 함수를 이용하여 다음의 수학식을 통해 상기 증명값을 생성하는 단계;를 포함하는 것을 특징으로 하는 인증 증명 방법;

$$\pi = SIG(H(x^P)\|H(s_0^P)\|H(y^P), Ks)$$

여기서, π는 상기 증명값이고, Ks는 상기 개인키이며, SIG는 상기 개인키(Ks)로 디지털 서명을 생성하는 체계이고, $H(x^P)$는 상기 요청 데이터의 해시값이며, $H(s_0^R)$는 상기 인증된 어플리케이션에 대한 초기 상태의 해시값이고, $H(y^P)$는 상기 응답 데이터의 해시값을 나타낸다.

청구항 5

제1항에 있어서,

상기 증명 모듈이 상기 응답 데이터 및 상기 증명값을 검증 모듈에 전송하는 단계;

상기 검증 모듈이 참조 무결성 측정값을 수신하는 단계;

상기 검증 모듈이 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 연산하는 단계; 및

상기 증명값과, 상기 참조 무결성 측정값, 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값이 동일한지 여부를 통해 상기 증명값을 검증하는 단계;를 포함하는 것을 특징으로 하는 인증 증명 방법.

청구항 6

제5항에 있어서,

상기 응답 데이터는,

상기 증명 모듈에서 생성되어 신뢰하지 않은 어플리케이션을 통해 상기 검증 모듈로 전송되는 데이터이고, 상기 신뢰하지 않은 어플리케이션의 공격이 있는 경우에 오류가 발생된 데이터가 상기 검증 모듈로 전송되는 것을 특징으로 하는 인증 증명 방법.

청구항 7

제5항에 있어서,

상기 증명값을 검증하는 단계는,

상기 증명값에 포함된 요청 데이터의 해시값과 상기 연산된 요청 데이터의 해시값이 동일한지 여부를 검증하는 단계;

상기 증명값에 포함된 응답 데이터의 해시값과 상기 연산된 응답 데이터의 해시값이 동일한지 여부를 검증하는 단계; 및

상기 증명값에 포함된 초기 상태의 해시값과 상기 참조 무결성 측정값이 동일한지 여부를 검증하는 단계;를 포함하는 것을 특징으로 하는 인증 증명 방법.

청구항 8

제7항에 있어서,

상기 증명값을 검증하는 단계는,

공개키를 이용하여 상기 증명값의 유효성을 검증하는 단계;를 더 포함하는 것을 특징으로 하는 인증 증명 방법.

청구항 9

기 수신된 요청 데이터의 해시값을 측정하고, 응답 데이터의 해시값을 측정하며, 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 기초로 증명값을 생성하는 인증 에이전트와, 상기 요청 데이터에 대한 상기 응답 데이터를 생성하는 인증된 어플리케이션을 포함하는 증명 모듈;

을 포함하는 인증 증명 장치.

청구항 10

제9항에 있어서,

상기 요청 데이터는,

검증 모듈에서 입력받아 신뢰하지 않은 어플리케이션을 통해 상기 증명 모듈로 전송되는 데이터이고, 상기 신뢰하지 않은 어플리케이션의 공격이 있는 경우에 오류가 발생된 데이터가 상기 증명 모듈로 전송되는 것을 특징으로 하는 인증 증명 장치.

청구항 11

제9항에 있어서,

상기 인증 에이전트는,

상기 인증된 어플리케이션에 대한 초기 상태의 해시값을 측정하고, 상기 요청 데이터의 해시값, 상기 응답 데이터의 해시값, 상기 초기 상태의 해시값 및 개인키를 이용하여 상기 증명값을 생성하는 것을 특징으로 하는 인증

증명 장치.

청구항 12

제11항에 있어서,

상기 인증 에이전트는,

디지털서명 함수를 이용하여 다음의 수학식을 통해 상기 증명값을 생성하는 것을 특징으로 하는 인증 증명 장치;

$$\pi = SIG(H(x^P) \| H(s_0^P) \| H(y^P), Ks)$$

여기서, π는 상기 증명값이고, Ks는 상기 개인키이며, SIG는 상기 개인키(Ks)로 디지털 서명을 생성하는 체계이고, $H(x^P)$는 상기 요청 데이터의 해시값이며, $H(s_0^R)$는 상기 인증된 어플리케이션에 대한 초기 상태의 해시값이고, $H(y^P)$는 상기 응답 데이터의 해시값을 나타낸다.

청구항 13

제9항에 있어서,

상기 인증 에이전트는,

상기 응답 데이터 및 상기 증명값을 검증 모듈에 전송하며,

참조 무결성 측정값을 수신하고, 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 연산하며, 상기 증명값과, 상기 참조 무결성 측정값, 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값이 동일한지 여부를 통해 상기 증명값을 검증하는 검증부를 포함하는 검증 모듈;을 더 포함하는 것을 특징으로 하는 인증 증명 장치.

청구항 14

제13항에 있어서,

상기 응답 데이터는,

상기 증명 모듈에서 생성되어 신뢰하지 않은 어플리케이션을 통해 상기 검증 모듈로 전송되는 데이터이고, 상기 신뢰하지 않은 어플리케이션의 공격이 있는 경우에 오류가 발생된 데이터가 상기 검증 모듈로 전송되는 것을 특징으로 하는 인증 증명 장치.

청구항 15

제13항에 있어서,

상기 검증부는,

상기 증명값에 포함된 요청 데이터의 해시값과 상기 연산된 요청 데이터의 해시값이 동일한지 여부를 검증하고, 상기 증명값에 포함된 응답 데이터의 해시값과 상기 연산된 응답 데이터의 해시값이 동일한지 여부를 검증하며, 상기 증명값에 포함된 초기 상태의 해시값과 상기 참조 무결성 측정값이 동일한지 여부를 검증하는 것을 특징으로 하는 인증 증명 장치.

청구항 16

제15항에 있어서,

상기 검증부는,

공개키를 이용하여 상기 증명값의 유효성을 검증하는 것을 특징으로 하는 인증 증명 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 인증 증명 장치 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 네트워크 및 통신 기술의 박전으로 네트워크를 통해 원격으로 리소스에 접근할 수 있다.

[0003] 원격 액세스를 위해서 요청자가 액세스할 권한이 있는지를 확인하는 승인이 필요하며, 대부분의 원격 액세스용 종래의 승인 및 인증 메커니즘은 비밀 정보를 기반으로 한다.

[0004] 일반적으로, 인증은 사람 또는 기기가 목적에 접근 가능한지 확인하는 절차로, 사람의 경우에는 패스워드 등과 같은 비밀 정보, 신분증 등과 같은 실물 정보, 외모 또는 움직임 등의 모습을 통해 인증할 수 있다.

[0005] 그러나, 기기를 인증할 경우에는 사람과 달리 비밀 정보를 이용하는 방법밖에 활용할 수 없다는 문제가 있다.

[0006] 그리고, 증명(Attestation)는 소프트웨어의 무결성을 확인하는 방법으로, 일반적으로 소프트웨어의 코드에 대한 해시값 값을 계산하여 원래 해시값 값과 같은지 비교하는 방법으로 소프트웨어가 조작되었는지 확인할 수 있다.

[0007] 다만, 하나의 비밀을 기반으로 한 승인만으로는 보안 중요 애플리케이션은 정보 누출의 위험이 있는 문제가 있다.

[0008] 이러한 이유로, 다중 모달 승인이 종종 사용되며, 이는 요청자를 확인하기 위한 추가 방법이 필요하다.

[0009] 그러나, 이러한 방법들도 여전히 비밀을 기반으로 하고 있으며, 다중 모달 승인을 기계 간 통신에 적용하기 쉽지 않다는 문제가 있다.

[0010] 또한, 이러한 승인 메커니즘은 엔드 포인트(End-Point) 소프트웨어가 안전하다가 가정하나, 엔드 포인트가 손상된 경우에 비밀을 훔치거나 가짜 명령을 주입하거나 민감한 정보를 유출할 수 있는 문제가 있다.

선행기술문헌

특허문헌

[0011] (특허문헌 0001) 대한민국 공개특허공보 제10-2017-0129866호("블록 체인을 사용하여 디바이스 무결성의 자동화된 입증", 공개일자: 2017.11.27)

발명의 내용

해결하려는 과제

[0012] 본 발명은 요청 데이터의 해시값 및 응답 데이터의 해시값을 이용하여 증명값을 생성하여 검증하는 인증 증명 장치 및 그 방법을 제공하고자 한다.

과제의 해결 수단

[0013] 상술한 과제를 해결하기 위하여 인증 증명 장치 및 그 방법이 제공된다.

[0014] 인증 증명 방법은 증명 모듈이 기 수신된 요청 데이터의 해시값을 측정하는 단계; 상기 증명 모듈이 상기 요청 데이터에 대한 응답 데이터를 생성하는 단계; 상기 증명 모듈이 상기 응답 데이터의 해시값을 측정하는 단계; 및 상기 증명 모듈이 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 기초로 증명값을 생성하는 단계;를 포함한다.

[0015] 일 실시예에서, 상기 요청 데이터는, 검증 모듈에서 입력받아 신뢰하지 않은 어플리케이션을 통해 상기 증명 모듈로 전송되는 데이터이고, 상기 신뢰하지 않은 어플리케이션의 공격이 있는 경우에 오류가 발생된 데이터가 상기 증명 모듈로 전송되는 것을 특징으로 할 수 있다.

[0016] 일 실시예에서, 상기 증명 모듈이 인증된 어플리케이션에 대한 초기 상태의 해시값을 측정하는 단계;를 더 포함하고, 상기 증명값을 생성하는 단계는, 상기 요청 데이터의 해시값, 상기 응답 데이터의 해시값 및 상기 초기

상태의 해시값 및 개인키를 이용하여 상기 증명값을 생성하는 단계;를 더 포함하는 것을 특징으로 할 수 있다.

[0017] 일 실시예에서, 상기 요청 데이터의 해시값, 상기 응답 데이터의 해시값, 상기 초기 상태의 해시값 및 개인키를 이용하여 상기 증명값을 생성하는 단계는, 디지털서명 함수를 이용하여 다음의 수학식을 통해 상기 증명값을 생성하는 단계;를 포함하는 것을 특징으로 할 수 있다.

[0018] $$\pi = SIG(H(x^P)\|H(s_0^P)\|H(y^P), Ks)$$

[0019] 여기서, π는 상기 증명값이고, Ks는 상기 개인키이며, SIG는 상기 개인키(Ks)로 디지털 서명을 생성하는 체계이고, $H(x^P)$는 상기 요청 데이터의 해시값이며, $H(s_0^R)$는 상기 인증된 어플리케이션에 대한 초기 상태의 해시값이고, $H(y^P)$는 상기 응답 데이터의 해시값을 나타낸다.

[0020] 일 실시예에서, 상기 증명 모듈이 상기 응답 데이터 및 상기 증명값을 검증 모듈에 전송하는 단계; 상기 검증 모듈이 참조 무결성 측정값을 수신하는 단계; 상기 검증 모듈이 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 연산하는 단계; 및 상기 증명값과, 상기 참조 무결성 측정값, 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값이 동일한지 여부를 통해 상기 증명값을 검증하는 단계;를 포함하는 것을 특징으로 할 수 있다.

[0021] 일 실시예에서, 상기 응답 데이터는, 상기 증명 모듈에서 생성되어 신뢰하지 않은 어플리케이션을 통해 상기 검증 모듈로 전송되는 데이터이고, 상기 신뢰하지 않은 어플리케이션의 공격이 있는 경우에 오류가 발생된 데이터가 상기 검증 모듈로 전송되는 것을 특징으로 할 수 있다.

[0022] 일 실시예에서, 상기 증명값을 검증하는 단계는, 상기 증명값에 포함된 요청 데이터의 해시값과 상기 연산된 요청 데이터의 해시값이 동일한지 여부를 검증하는 단계; 상기 증명값에 포함된 응답 데이터의 해시값과 상기 연산된 응답 데이터의 해시값이 동일한지 여부를 검증하는 단계; 및 상기 증명값에 포함된 초기 상태의 해시값과 상기 참조 무결성 측정값이 동일한지 여부를 검증하는 단계;를 포함하는 것을 특징으로 할 수 있다.

[0023] 일 실시예에서, 상기 증명값을 검증하는 단계는, 공개키를 이용하여 상기 증명값의 유효성을 검증하는 단계;를 더 포함하는 것을 특징으로 할 수 있다.

[0024] 인증 증명 장치는, 기 수신된 요청 데이터의 해시값을 측정하고, 상기 증명 모듈이 응답 데이터의 해시값을 측정하며, 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 기초로 증명값을 생성하는 인증 에이전트와, 상기 요청 데이터에 대한 상기 응답 데이터를 생성하는 인증된 어플리케이션을 포함하는 증명 모듈;을 포함한다.

[0025] 일 실시예에서, 상기 요청 데이터는, 검증 모듈에서 입력받아 신뢰하지 않은 어플리케이션을 통해 상기 증명 모듈로 전송되는 데이터이고, 상기 신뢰하지 않은 어플리케이션의 공격이 있는 경우에 오류가 발생된 데이터가 상기 증명 모듈로 전송되는 것을 특징으로 할 수 있다.

[0026] 일 실시예에서, 상기 인증 에이전트는, 상기 인증된 어플리케이션에 대한 초기 상태의 해시값을 측정하고, 상기 요청 데이터의 해시값, 상기 응답 데이터의 해시값, 상기 초기 상태의 해시값 및 개인키를 이용하여 상기 증명값을 생성하는 것을 특징으로 할 수 있다.

[0027] 일 실시예에서, 상기 인증 에이전트는, 디지털서명 함수를 이용하여 다음의 수학식을 통해 상기 증명값을 생성하는 것을 특징으로 할 수 있다.

[0028] $$\pi = SIG(H(x^P)\|H(s_0^P)\|H(y^P), Ks)$$

[0029] 여기서, π는 상기 증명값이고, Ks는 상기 개인키이며, SIG는 상기 개인키(Ks)로 디지털 서명을 생성하는 체계이고, $H(x^P)$는 상기 요청 데이터의 해시값이며, $H(s_0^R)$는 상기 인증된 어플리케이션에 대한 초기 상태의 해시값이고, $H(y^P)$는 상기 응답 데이터의 해시값을 나타낸다.

[0030] 일 실시예에서, 상기 인증 에이전트는, 상기 응답 데이터 및 상기 증명값을 검증 모듈에 전송하며, 참조 무결성 측정값을 수신하고, 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값을 연산하며, 상기 증명값과, 상기 참조 무결성 측정값, 상기 요청 데이터의 해시값 및 상기 응답 데이터의 해시값이 동일한지 여부를 통해 상

기 증명값을 검증하는 검증부를 포함하는 검증 모듈;을 더 포함하는 것을 특징으로 할 수 있다.

[0031] 일 실시예에서, 상기 응답 데이터는, 상기 증명 모듈에서 생성되어 신뢰하지 않은 어플리케이션을 통해 상기 검증 모듈로 전송되는 데이터이고, 상기 신뢰하지 않은 어플리케이션의 공격이 있는 경우에 오류가 발생된 데이터가 상기 검증 모듈로 전송되는 것을 특징으로 할 수 있다.

[0032] 일 실시예에서, 상기 검증부는, 상기 증명값에 포함된 요청 데이터의 해시값과 상기 연산된 요청 데이터의 해시값이 동일한지 여부를 검증하고, 상기 증명값에 포함된 응답 데이터의 해시값과 상기 연산된 응답 데이터의 해시값이 동일한지 여부를 검증하며, 상기 증명값에 포함된 초기 상태의 해시값과 상기 참조 무결성 측정값이 동일한지 여부를 검증하는 것을 특징으로 할 수 있다.

[0033] 일 실시예에서, 상기 검증부는, 공개키를 이용하여 상기 증명값의 유효성을 검증하는 것을 특징으로 할 수 있다.

발명의 효과

[0034] 본 발명의 일 실시형태에 따르면, 증명(Attestation)을 이용하여 종래의 비밀 기반 인증에 추가적인 인증 방법을 도입함으로써, 기밀이 유출되더라도 증명을 통과할 수 없다.

도면의 간단한 설명

[0035] 도 1은 본 발명의 일 실시예에 따른 인증 증명 장치를 설명하기 위한 블록도이다.

도 2는 본 발명의 일 실시예에 따른 인증 증명 장치를 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 증명 모듈 및 검증 모듈의 관점에서 입력, 출력 및 예상 실행을 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 인증 증명 방법을 설명하기 위한 순서도이다.

도 5는 본 발명의 일 실시예에 따른 서버 환경에서의 인증 증명 방법을 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 모바일 장치에서의 인증 증명 방법을 설명하기 위한 순서도이다.

도 7은 본 발명의 일 실시예에 따른 모바일 장치에서의 인증 증명 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0036] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[0037] 본 명세서에서 사용되는 용어에 대해 간략히 설명하고, 본 발명에 대해 구체적으로 설명하기로 한다.

[0038] 본 발명에서 사용되는 용어는 본 발명에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 발명에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 발명의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0039] 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 있음을 의미한다. 또한, 명세서에서 사용되는 "부", "모듈", "유닛" 등의 용어는 적어도 하나의 기능 또는 동작을 처리하는 단위를 의미하며, 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소, 또는 소프트웨어와 하드웨어의 결합으로 구현될 수 있다. 그렇지만 "부", "모듈", "유닛" 등의 용어가 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. "부", "모듈", "유닛" 등은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 ""부", "모듈", "유닛" 등의 용어는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들,

속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다.

[0040] 아래에서는 첨부한 도면을 참고하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략한다.

[0041] "제1", "제2" 등과 같이 서수를 포함하는 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 구성 요소들은 용어들에 의해 한정되지는 않는다. 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 항목들의 조합 또는 복수의 관련된 항목들 중의 어느 하나의 항목을 포함한다.

[0043] 이하, 도면을 참조하여 본 발명의 일 실시예에 따른 인증 증명 장치를 설명하도록 한다.

[0044] 도 1은 본 발명의 일 실시예에 따른 인증 증명 장치의 구성을 설명하기 위한 블록도이고, 도 2는 본 발명의 일 실시예에 따른 인증 증명 장치를 설명하기 위한 도면이다.

[0045] 도 1 및 도 2에서 도시한 바와 같이, 인증 증명 장치(1)는 검증 모듈(Receiver/Verifier)(100), 증명 모듈(Sender/Prover)(200), 저장부(300) 및 통신부(400)를 포함한다.

[0046] 인증 증명 장치(1)는 요청 데이터 및 응답 데이터 각각의 해시값을 이용하여 증명값을 생성하여 비밀 기반의 인증을 수행할 수 있다.

[0047] 이로 인해, 검증 모듈(100)은 증명 모듈(200)에 포함된 어플리케이션(210)이 올바르게 실행 중인지 여부를 판단할 수 있다.

[0048] 통신부(400)는 검증 모듈(100), 증명 모듈(200) 및 저장부(300)가 서로 데이터를 송수신할 수 있도록 할 수 있다.

[0049] 통신부(400)는 유무선 통신망을 모두 포함한다. 가령 통신부(400)로서 유무선 인터넷망이 이용되거나 연동될 수 있다. 여기서, 유선망은 케이블망이나 공중 전화망(PSTN)과 같은 인터넷망을 포함하는 것이고, 무선 통신망은 CDMA, WCDMA, GSM, EPC(Evolved Packet Core), LTE(Long Term Evolution), 와이브로(Wibro) 망, 5G 통신망 등을 포함하는 의미이다. 물론 본 발명의 실시예에 따른 통신부(400)은 이에 한정되는 것이 아니며, 향후 구현될 차세대 이동통신 시스템의 접속망으로서 가령 클라우드 컴퓨팅 환경하의 클라우드 컴퓨팅망, 5G망 등에 사용될 수 있다. 가령, 통신부(400)가 유선 통신망인 경우 통신부(400) 내의 액세스포인트는 전화국의 교환국 등에 접속할 수 있지만, 무선 통신망인 경우에는 통신사에서 운용하는 SGSN 또는 GGSN(Gateway GPRS Support Node)에 접속하여 데이터를 처리하거나, BTS(Base Station Transmission), NodeB, e-NodeB 등의 다양한 중계기에 접속하여 데이터를 처리할 수 있다.

[0050] 검증 모듈(100)은 입력부(110), 검증부(120)를 포함할 수 있다.

[0051] 입력부(110)는 사용자로부터 요청 데이터를 입력받는다.

[0052] 여기서, 요청 데이터는 어플리케이션에 대한 권한 데이터뿐 아니라, 모든 종류의 입력 데이터(y=F(x)에서의 x)일 수 있다.

[0053] 입력부(110)는 기 입력된 요청 데이터를 증명 모듈(200)에 전송할 수 있다.

[0054] 검증부(120)는 증명 모듈(200)로부터 전송된 응답 데이터를 수신한다.

[0055] 여기서, 응답 데이터는 증명 모듈(200)에서 생성되어 신뢰하지 않은 어플리케이션(Trusted)을 통해 검증 모듈(100)로 전송되고, 신뢰하지 않은 어플리케이션(Trusted) 또는 네트워크에서의 중간자 공격이 있는 경우에 오류가 발생된 데이터가 검증 모듈(100)로 전송될 수 있다.

[0056] 즉, 증명 모듈(200)에서 생성된 응답 데이터와 검증 모듈(100)에서 수신한 응답 데이터가 서로 다를 수 있다.

[0057] 검증부(120)는 참조 무결성 측정값을 수신한다.

[0058] 검증부(120)는 기 입력받은 요청 데이터의 해시값 및 증명 모듈(200)로부터 수신한 응답 데이터의 해시값을 연

산한다.

[0059] 검증부(120)는 기 입력받은 요청 데이터의 해시값 및 증명 모듈(200)로부터 수신한 응답 데이터의 해시값을 이용하여 증명값을 검증할 수 있다.

[0060] 검증부(120)는 수신한 증명값과, 참조 무결성 측정값, 기 입력받은 요청 데이터의 해시값 및 증명 모듈(200)로부터 수신한 응답 데이터의 해시값이 동일한지 여부를 통해 증명값을 검증한다.

[0061] 검증부(120)는 증명값에 포함된 요청 데이터의 해시값과 연산된 요청 데이터의 해시값이 동일한지 여부를 검증할 수 있다.

[0062] 검증부(120)는 증명값에 포함된 응답 데이터의 해시값과 연산된 요청 데이터의 해시값이 동일한지 여부를 검증할 수 있다.

[0063] 검증부(120)는 증명값에 포함된 초기 상태의 해시값과 참조 무결성 측정값이 동일한지 여부를 검증할 수 있다.

[0064] 여기서, 검증부(120)는 출력을 수락해야 하는지 여부를 나타내는 VERIFY 함수를 이용할 수 있다.

[0065] 검증부(120)는 VERIFY 함수가 1을 반환하는 경우 출력을 수락한다.

[0066] 증명 모듈(200)은 인증 에이전트(Attestation Agent)(210) 및 인증된 어플리케이션(Attested Application)(220)을 포함한다.

[0067] 증명 모듈(200)은 신뢰의 뿌리(Root of Trust) 및 신뢰하지 않은 어플리케이션(Untrusted)을 더 포함할 수 있다.

[0068] 여기서, 신뢰의 뿌리는 증명의 보안 속성을 보장하는 모듈로, 저장된 비밀은 노출될 수 없다고 가정할 수 있다.

[0069] 또한, 신뢰하지 않은 어플리케이션(Untrusted)은 요청 데이터 및 응답 데이터를 공격할 수 있는 공격자를 나타낸다.

[0070] 인증 에이전트(210)는 검증 모듈(100)로부터 전송된 요청 데이터를 수신한다.

[0071] 여기서, 도 2에서 도시한 바와 같이, 요청 데이터는 검증 모듈(100)에서 입력받아 신뢰하지 않은 어플리케이션(Untrusted)을 통해 증명 모듈(200)로 전송되는 데이터로, 신뢰하지 않은 어플리케이션(Untrusted)의 공격이 있는 경우에 오류가 발생된 데이터가 증명 모듈(200)로 전송될 수 있다.

[0072] 즉, 검증 모듈(100)에서 입력받은 요청 데이터는 증명 모듈(200)에서 수신된 요청 데이터와 서로 다를 수 있다.

[0073] 인증 에이전트(210)는 인증된 어플리케이션(220)에 대한 초기 상태의 해시값을 측정한다.

[0074] 인증 에이전트(210)는 제2 요청 데이터의 해시값을 측정한다.

[0075] 인증 에이전트(210)는 제2 요청 데이터를 인증된 어플리케이션(220)에 전송할 수 있다.

[0076] 인증 에이전트(210)는 기 생성된 제1 응답 데이터의 해시값을 측정한다.

[0077] 인증 에이전트(210)는 요청 데이터의 해시값, 응답 데이터의 해시값, 초기 상태의 해시값 및 개인키를 이용하여 증명값을 생성할 수 있다.

[0078] 인증 에이전트(210)는 디지털 서명 함수를 이용하여 증명값을 생성할 수 있다.

[0079] 여기서, 인증 에이전트(210)는 신뢰의 뿌리(Root of Trust)의 일부이거나 별도의 엔터티(Entity)일 수 있다.

[0080] 인증된 어플리케이션(220)은 요청 데이터에 대한 응답 데이터를 생성한다.

[0081] 인증된 어플리케이션(220)은 생성된 응답 데이터를 검증 모듈(100)에 전송할 수 있다.

[0082] 저장부(300)는 요청 데이터, 응답 데이터 및 증명값을 저장할 수 있다.

[0083] 저장부(300)에 저장된 프로그램은, 프로그래머 등의 설계자에 의해 직접 작성 또는 수정된 후 저장부(300)에 저장된 것일 수도 있고, 다른 물리적 기록 매체(외장 메모리 장치나 콤팩트 디스크(CD) 등)으로부터 전달받아 저장된 것일 수도 있으며, 및/또는 유무선 통신 네트워크를 통해 접속 가능한 전자 소프트웨어 유통망을 통하여 획득 또는 갱신된 것일 수도 있다.

[0084] 저장부(300)는, 주기억장치 및 보조기억장치 중 적어도 하나를 포함할 수 있다. 주기억장치는 예를 들어, 롬

(ROM) 및/또는 램(RAM)과 같은 반도체 저장 매체를 이용하여 구현된 것일 수 있고, 보조기억장치는, 플래시 메모리 장치(솔리드 스테이트 드라이브(SSD, Solid State Drive) 등), SD(Secure Digital) 카드, 하드 디스크 드라이브(HDD, Hard Disc Drive), 콤팩트 디스크, 디브이디(DVD) 또는 레이저 디스크 등과 같이 데이터를 영구적 또는 반영구적으로 저장 가능한 장치를 기반으로 구현될 수 있다.

[0086] 이하, 도면을 참고하여 본 발명의 일 실시예에 따른 증명 모듈 및 검증 모듈의 관점에서 입력, 출력 및 예상 실행을 설명하도록 한다.

[0087] 도 3은 본 발명의 일 실시예에 따른 증명 모듈 및 검증 모듈의 관점에서 입력, 출력 및 예상 실행을 설명하기 위한 도면이다.

[0088] 도 3에서 도시한 바와 같이, 검증 모듈(100)의 관점에서, 입력부(110)는 사용자로부터 요청 데이터(x^V)를 입력받을 수 있다.

[0089] 입력부(110)는 기 입력받은 요청 데이터(x^V)를 어플리케이션(Trusted)을 통해 증명 모듈(200)에 전송할 수 있다.

[0090] 여기서, 요청 데이터(x^V)는 신뢰하지 않은 어플리케이션(Trusted) 또는 네트워크에서의 중간자 공격이 있는 경우에 오류가 발생된 데이터(x^P)가 증명 모듈(200)로 전송될 수 있다.

[0091] 인증 에이전트(210)는 신뢰하지 않은 어플리케이션(Trusted)를 통해 전송된 요청 데이터(x^P)를 수신할 수 있다.

[0092] 여기서, 증명 모듈(200)에서 수신된 요청 데이터(x^P)는 신뢰하지 않은 어플리케이션(Trusted) 또는 네트워크에서의 중간자 공격으로 인해 입력부(110)에서 입력받은 요청 데이터(x^P)와 다를 수 있다.

[0093] 증명 모듈(200)은 실제 기계(real machine, f^R)에서 요청 데이터(x^P)를 이용하여 인증된 어플리케이션(220)을 실행할 수 있다.

[0094] 인증된 어플리케이션(220)는 요청 데이터(x^P)에 대한 응답 데이터(y^P)를 생성할 수 있다.

[0095] 인증된 어플리케이션(220)은 y=F(x)에 대응하여 요청 데이터(x)에 대한 응답 데이터(y)를 생성할 수 있다.

[0096] 여기서, F는 사용자가 정의한 알고리즘 또는 기능을 나타낸다.

[0097] 예를 들어, 요청 데이터는 웹서버에 요청한 URL일 수 있고, 응답 데이터는 요청한 URL의 HTML일 수 있으며, F는 요청받은 URL에 대한 HTML을 생성하는 알고리즘일 수 있다.

[0098] 인증된 어플리케이션(220)는 인증 에이전트(210)에 응답 데이터(y^P)를 전송하고, 인증 에이전트(210)는 신뢰하지 않은 어플리케이션(Trusted)를 통해 응답 데이터(y^P)를 검증 모듈(100)에 전송할 수 있다.

[0099] 여기서, 인증된 어플리케이션(220)에서 생성된 응답 데이터(y^P)는 신뢰하지 않은 어플리케이션(Trusted) 또는 네트워크에서의 중간자 공격이 있는 경우에 오류가 발생된 데이터(y^V)가 검증 모듈(100)로 전송될 수 있다.

[0100] 검증부(120)는 신뢰하지 않은 어플리케이션을 통해 전송되는 응답 데이터(y^V)를 수신할 수 있다.

[0101] 검증부(120)는 응답 데이터(y^V)가 이상적인 기계(ideal machine, f^I)에서 요청 데이터(x^V)로 실행 중인 어플리케이션의 결과와 동일할 것으로 판단할 수 있다.

[0102] 더욱 자세하게는, 증명 모듈(200)에 포함된 신뢰의 뿌리는 다음의 수학식 1을 보장할 수 있다.

수학식 1

[0103] $$y^{P} = f^{R}(x^{P})$$

[0104] 여기서, y^{P}는 인증된 어플리케이션에서 생성된 응답 데이터고, f^{R}는 실제 기계이며, x^{P}는 검증 모듈로부터 수신한 요청 데이터를 나타낸다.

[0105] 실제 기계(f^{R})에서 실행 중인 인증된 어플리케이션(220)의 초기 상태가 이상적인 기계(f^{I})에서 실행 중인 어플리케이션의 초기 상태와 동일하다면, 신뢰의 뿌리는 다음의 수학식 2를 보장할 수 있다.

수학식 2

[0106] $$f^{R} = f^{I}$$

[0107] 여기서, f^{R}는 실제 기계이고, f^{I}는 이상적인 기계를 나타낸다.

[0108] 구체적으로, 실제 기계(f^{R})의 실행 추적은 (s^{R}_{i}, s^{R}_{i}+1, ..., s^{R}_{0})로 나타낼 수 있고, 이상적인 기계(f^{I})의 실행 추적은 (s^{I}_{i}, s^{I}_{i}+1, ..., s^{I}_{0})로 나타낼 수 있다.

[0109] 여기서, s^{R}_{i}은 증명 모듈에서 요청 데이터가 수신된 상태이고, s^{R}_{0}은 응답 데이터가 생성된 상태를 나타낸다.

[0110] 인증된 어플리케이션(220)의 예상 실행은 (s^{R}_{i}, s^{R}_{i}+1, ..., s^{R}_{0})가 (s^{I}_{i}, s^{I}_{i}+1, ..., s^{I}_{0})와 동일하고, 요청 데이터는 s^{R}_{i}의 일부이며, 응답 데이터는 s^{R}_{0}의 일부일 경우, 인증된 어플리케이션(220)은 이상적인 기계(f^{I})에서의 예상 실행과 동일하게 수행될 수 있다.

[0111] 다시 말해, s^{R}_{i}가 s^{I}_{i}과 동일한 경우, 신뢰의 뿌리는 f^{R}은 f^{I}와 동일하고, (s^{R}_{i}, s^{R}_{i}+1, ..., s^{R}_{0})가 (s^{I}_{i}, s^{I}_{i}+1, ..., s^{I}_{0})과 동일임을 보장할 수 있다.

[0112] 따라서, 검증부(120)는 다음의 수학식 3과 같이 증명 모듈(200)로부터 수신한 응답 데이터(y^{V})가 이상적인 기계(f^{I})에서 사용자로부터 입력받은 요청 데이터(x^{V})로 실행 중인 어플리케이션의 결과와 동일할 것으로 판단하므로, 인증된 어플리케이션(220)에서 생성된 응답 데이터와 증명 모듈(200)로부터 수신한 응답 데이터가 동일한 경우(y^{P}=y^{V}), 인증된 어플리케이션(220)에 대한 초기 상태의 해시값과 참조 무결성 측정값이 동일한 경우(s^{R}_{i}=s^{I}_{i}), 사용자로부터 입력받은 요청 데이터와 검증 모듈(100)로부터 수신한 요청 데이터가 동일한 경우(x^{V}=x^{P})를 통해 검증할 수 있다.

수학식 3

[0113] $$y^{V} = f^{I}(x^{V})$$

[0114] 여기서, y^{V}는 증명 모듈로부터 수신한 응답 데이터고, f^{I}는 이상적인 기계이며, x^{V}는 사용자로부터 입력받은 요청 데이터를 나타낸다.

[0115] 검증부(120)는 어테이션 알고리즘(Attestation Algorithm)을 이용하여 출력 데이터를 검증할 수 있다.

[0116] 여기서, 어테이션 알고리즘은 출력을 수락해야 하는지 여부를 나타내는 VERIFY 함수를 이용할 수 있다.

[0117] 즉, 어테이션 알고리즘은 출력 데이터와 함께 전송받은 증명을 확인하여 증명이 맞는 경우에 출력 데이터를 신뢰하여 출력을 수락할 수 있다.

[0118] 검증부(120)는 인증된 어플리케이션(220)에서 생성된 응답 데이터와 증명 모듈(200)로부터 수신한 응답 데이터가 동일한 경우($y^P=y^V$), 인증된 어플리케이션(220)에 대한 초기 상태의 해시값과 참조 무결성 측정값이 동일한 경우($s^R_i=s^I_i$), 사용자로부터 입력받은 요청 데이터와 검증 모듈(100)로부터 수신한 요청 데이터가 동일한 경우($x^V=x^P$)일때, VERIFY 함수 값으로 1을 출력한다.

[0119] 또한, 검증부(120)는 인증된 어플리케이션(220)에서 생성된 응답 데이터와 증명 모듈(200)로부터 수신한 응답 데이터가 상이한 경우($y^P \neq y^V$), 인증된 어플리케이션(220)에 대한 초기 상태의 해시값과 참조 무결성 측정값이 상이한 경우($s^R_i \neq s^I_i$), 사용자로부터 입력받은 요청 데이터와 검증 모듈(100)로부터 수신한 요청 데이터가 상이한 경우($x^V \neq x^P$)일 때, VERIFY 함수 값으로 0을 출력할 수 있다.

[0120] 즉, 검증부(120)는 인증된 어플리케이션(220)에서 생성된 응답 데이터의 해시값과 증명 모듈(200)로부터 수신한 응답 데이터의 해시값이 동일한 경우, 인증된 어플리케이션(200)에 대한 초기 상태의 해시값과 참조 무결성 측정값이 동일한 경우, 사용자로부터 입력받은 요청 데이터의 해시값과 검증 모듈(100)로부터 수신한 요청 데이터의 해시값이 동일한 경우를 검증할 수 있다.

[0121] 이와 같은 방법으로, 검증부(120)는 증명값을 검증할 수 있다.

[0123] 이하, 도면을 참조하여 본 발명의 일 실시예에 따른 인증 증명 방법을 설명하도록 한다.

[0124] 도 4는 본 발명의 일 실시예에 따른 인증 증명 방법을 설명하기 위한 순서도이고, 도 5는 본 발명의 일 실시예에 따른 서버 환경에서의 인증 증명 방법을 설명하기 위한 도면이다.

[0125] 본 발명의 일 실시예에서는 에이전트(220)가 하이퍼바이저(Hypervisor)에 포함되어 구성될 수 있고, 하이퍼바이저(Hypervisor)는 신뢰의 뿌리(Root of Trust)로 작동될 수 있다.

[0126] 여기서, 하이퍼바이저(Hypervisor)(신뢰의 뿌리(Root of Trust))는 신뢰할 수 있는 것으로 가정한다.

[0127] 그리고, 증명 모듈(200)은 DMZ에 배치되어 내부 안전 영역(Secure Zone)의 데이터베이스(Database) 서버와 같은 내부 서버(Internal Server)에 연결될 수 있다.

[0128] 하이버파이저는 인증된 어플리케이션(220)을 위한 가상 머신을 호출하고, 인증된 어플리케이션(200)을 초기 상태(모든 비트가 0인 상태)로 초기화할 수 있다.

[0129] 하이퍼바이저는 인증 에이전트(210) 및 인증된 어플리케이션(220)을 로드하고, 인증 에이전트(210)는 인증된 어플리케이션(220)에 대한 초기 상태의 해시값($H(s^R_0)$)를 측정할 수 있다(S110).

[0130] 인증된 어플리케이션(220)이 초기화되면, 가상 머신은 일시 중단될 수 있다.

[0131] 입력부(110)는 사용자로부터 요청 데이터를 입력받는다(S120).

[0132] 신뢰하지 않은 어플리케이션(Untrusted application)은 서비스 포트(Service Port)에서 요청 데이터를 수신 대기할 수 있다.

[0133] 신뢰하지 않은 어플리케이션에서 요청 데이터가 수락되면, 입력부(110)는 요청 데이터를 인증 에이전트(210)로 전송할 수 있다.

[0134] 입력부(110)는 요청 데이터를 신뢰하지 않은 어플리케이션(Trusted)를 통해 인증 에이전트(210)로 전송할 수 있다.

[0135] 인증 에이전트(210)는 신뢰하지 않은 어플리케이션(Trusted)를 통해 요청 데이터(x^P)를 수신할 수 있다.

[0136] 여기서, 요청 데이터(x^P)는 신뢰하지 않은 어플리케이션(Trusted) 또는 네트워크에서의 중간자 공격으로 인해 오류가 발생된 데이터일 수 있다.

[0137] 인증 에이전트(210)는 요청 데이터의 해시값($H(x^P)$)를 측정한다(S130).

[0138] 이때, 하이퍼바이저는 가상 머신을 재개하고, 인증 에이전트(210)는 요청 데이터(x^P)를 인증된 어플리케이션(220)에 전송할 수 있다.

[0139] 인증된 어플리케이션(220)은 요청 데이터를 처리하는 동안 직접 내부 서버와 통신할 수 있다.

[0140] 인증된 어플리케이션(220)은 요청 데이터 처리를 완료하고, 요청 데이터에 대한 응답 데이터(y^P)를 생성한다(S140).

[0141] 인증된 어플리케이션(220)은 응답 데이터(y^P)를 인증 에이전트(210)로 전송할 수 있다.

[0142] 이때, 하이퍼바이저는 가상 머신을 중지할 수 있다.

[0143] 인증 에이전트(210)는 응답 데이터의 해시값($H(y^P)$)를 측정한다(S150).

[0144] 인증 에이전트(210)는 요청 데이터의 해시값($H(x^P)$) 및 응답 데이터의 해시값($H(y^P)$)를 기초로 증명값을 생성할 수 있다(S160).

[0145] 구체적으로, 인증 에이전트(210)는 요청 데이터의 해시값($H(x^P)$), 응답 데이터의 해시값($H(y^P)$), 인증된 어플리케이션(220)에 대한 초기 상태의 해시값($H(s^R_0)$), 개인키(Ks)를 기초로 증명값을 생성할 수 있다.

[0146] 인증 에이전트(210)는 디지털 서명 함수를 이용하여 요청 데이터의 해시값($H(x^P)$), 응답 데이터의 해시값($H(y^P)$), 인증된 어플리케이션(220)에 대한 초기 상태의 해시값($H(s^R_0)$) 및 개인키를 기초로 증명값을 생성할 수 있다.

[0147] 여기서, 개인키는 증명 모듈(200)에서 미리 저장될 수 있다.

[0148] 인증 에이전트(210)는 증명값을 다음의 수학식 4와 같이 생성할 수 있다.

수학식 4

[0149] $$\pi = SIG(H(x^P)\|H(s_0^P)\|H(y^P), Ks)$$

[0150] 여기서, π는 증명값이고, Ks는 개인키이며, SIG는 개인키(Ks)로 디지털 서명을 생성하는 체계이고, $H(x^P)$는 요청 데이터의 해시값이며, $H(s^R_0)$는 인증된 어플리케이션에 대한 초기 상태의 해시값이고, $H(y^P)$는 응답 데이터의 해시값이며, $\|$는 concatenation을 나타낸다.

[0151] 인증 에이전트(210)는 생성된 증명값(π)과 응답 데이터(y^P)를 신뢰하지 않은 어플리케이션으로 전송할 수 있다.

[0152] 신뢰하지 않은 어플리케이션은 응답 데이터(y^P), 증명값(π), 참조 무결성 측정값($H(s^I_0)$), 증명 모듈(200)의 공개키(Kp) 및 인증서를 검증 모듈(100)에 제공할 수 있다.

[0153] 여기서, 참조 무결성 측정값($H(s^I_0)$)은 인증 에이전트(210)에서 미리 저장될 수 있다.

[0154] 검증부(120)는 신뢰하지 않은 어플리케이션을 통해 전송된 응답 데이터를 수신할 수 있다(S160).

[0155] 검증부(120)는 응답 데이터(y^V), 증명값(π), 참조 무결성 측정값($H(s^I_0)$), 증명 모듈(200)의 공개키(Kp) 및 인증

서를 수신할 수 있다.

[0156] 여기서, 참조 무결성 측정값($H(s^I_0)$)은 신뢰할 수 있는 권한(Trusted Authority, TA)에 등록되어 있으며, 인증서는 참조 무결성 측정값($H(s^I_0)$) 및 증명 모듈(200)의 공개키(Kp)를 확인하여 발급한 신뢰할 수 있는 권한(TA)를 통해 획득할 수 있다.

[0157] 신뢰할 수 있는 권한(TA)는 인증 에이전트(210)에서 미리 저장된 정보이고, 인증 에이전트(210)의 공개키(Kp)에 대한 인증서는 신뢰할 수 있는 권한(TA)를 통해 획득할 수 있다.

[0158] 또한, 프로토 타입(Prototype)에서는 참조 무결성을 측정하기 위해 안전한 해시값을 사용하고, 참조 무결성은 다른 방식으로 측정될 수 있다.

[0159] 예를 들어, 참조 무결성을 측정하기 위해 메모리의 무작위 순회의 다이제스트(Digest) 방법을 이용하여 측정될 수 있다.

[0160] 검증부(120)는 제2 응답 데이터(y^P), 증명값(π), 참조 무결성 측정값($H(s^I_0)$), 공개키(Kp) 및 인증서를 수신하면, TA로부터 폐기 목록을 획득하여 증명 모듈(200)이 목록에 있는지 여부를 판단할 수 있다.

[0161] 검증부(120)는 등록된 증명 모듈들의 공개키 목록에서 해당 증명 모듈(200)이 있는지 여부를 판단할 수 있다.

[0162] 검증부(120)는 인증서로 참조 무결성 측정값($H(s^I_0)$) 및 공개키(Kp)에 대한 유효성 검사를 수행할 수 있다.

[0163] 검증부(120)는 입력부(110)로부터 입력받은 요청 데이터(x^V)의 해시값, 증명 모듈(200)로부터 수신한 응답 데이터(y^V)의 해시값을 연산한다(S170).

[0164] 검증부(120)는 요청 데이터(x^V)의 해시값, 응답 데이터(y^V)의 해시값 및 참조 무결성 측정값을 기초로 증명값(π) 검증을 수행한다(S180).

[0165] 검증부(120)는 증명값에 포함된 요청 데이터의 해시값과 연산된 요청 데이터의 해시값이 동일한지 여부를 검증할 수 있다.

[0166] 검증부(120)는 증명값에 포함된 응답 데이터의 해시값과 연산된 응답 데이터의 해시값이 동일한지 여부를 검증할 수 있다.

[0167] 검증부(120)는 증명값에 포함된 초기 상태의 해시값과 참조 무결성 측정값이 동일한지 여부를 검증할 수 있다.

[0168] 검증부(120)는 요청 데이터의 해시값($H(x^V)$)과 요청 데이터의 해시값($H(x^P)$)이 동일한 경우, 응답 데이터의 해시값($H(y^V)$)과 응답 데이터의 해시값($H(y^P)$)이 동일한 경우, 인증된 어플리케이션(220)에 대한 초기 상태의 해시값($H(s^R_0)$)과 참조 무결성 측정값($H(s^I_0)$)이 동일한한 경우인지를 통해 증명값을 검증할 수 있다.

[0169] 즉, 검증부(120)는 $H(x^P)||H(s^R_0)||H(y^P)$가 $H(x^V)||H(s^I_0)||H(y^V)$와 동일한 경우에만 1을 반환할 수 있다.

[0170] 검증부(120)는 VERIFY 함수를 통해 공개 키(Kp)를 이용하여 증명값의 유효성을 검증할 수 있다.

[0171] 검증부(120)는 VERIFTY 함수가 1을 반환하면 출력을 수락한다.

[0172] 즉, 검증 모듈(100)은 요청 데이터와 응답 데이터에 증명값을 포함하여 검증함으로써 증명 모듈(200)이 손상되었는지 여부를 구별할 수 있도록 한다.

[0174] 이하, 도면을 참고하여 본 발명의 일 실시예에 따른 모바일 장치에서의 인증 증명 방법을 설명하도록 한다.

[0175] 도 6은 본 발명의 일 실시예에 따른 모바일 장치에서의 인증 증명 방법을 설명하기 위한 순서도이고, 도 7은 본 발명의 일 실시예에 따른 모바일 장치에서의 인증 증명 방법을 설명하기 위한 도면이다.

[0176] 모바일 장치가 부팅될 때, 하드웨어는 인증된 어플리케이션, 신뢰할 수 있는 어플리케이션 및 보안 모니터의 초

기 상태의 해시값($H(s^R_0)$)를 측정한다(S210).

[0177] 모바일 장치는 초기 해시값을 계산하는 하드웨어가 포함되어 있고, 하드웨어는 Application processor와 같은 칩에 포함되어 있는 모듈일 수 있다.

[0178] 입력부(110)는 사용자로부터 요청 데이터(x^V)를 입력받는다(S220).

[0179] 입력부(110)는 요청 데이터(x^V)를 증명 모듈(200)로 전송할 수 있다.

[0180] 신뢰하지 않은 어플리케이션(Trusted)는 서비스 포트에서 수신 대기할 수 있다.

[0181] 인증 에이전트(210)는 신뢰하지 않은 어플리케이션(Trusted)를 통해 요청 데이터(x^P)를 수신할 수 있다.

[0182] 여기서, 증명 모듈(200)에서 수신된 요청 데이터(x^P)는 신뢰하지 않은 어플리케이션(Trusted) 또는 네트워크에서의 중간자 공격으로 인해 입력부(110)에서 입력받은 요청 데이터(x^P)와 다를 수 있다.

[0183] 요청 데이터가 수락되면, 보안 모니터의 인증 에이전트(210)는 요청 데이터의 해시값($H(x^P)$)를 측정한다(S230).

[0184] 인증 에이전트(210)는 요청 데이터(x^P)를 인증된 어플리케이션(220)으로 전송할 수 있다.

[0185] 인증된 어플리케이션(220)이 요청 데이터 처리를 완료하면, 응답 데이터(y^P)를 생성한다(S240).

[0186] 인증된 어플리케이션(220)은 응답 데이터(y^P)를 인증 에이전트(210)로 전송할 수 있다.

[0187] 인증 에이전트(210)는 응답 데이터의 해시값($H(y^P)$)를 측정한다(S250).

[0188] 인증 에이전트(210)는 요청 데이터의 해시값($H(x^P)$), 응답 데이터의 해시값($H(y^P)$) 및 보안 모니터의 초기 상태의 해시값을 기초로 증명값을 생성한다(S260).

[0189] 인증 에이전트(210)는 증명값을 상기 수학식 4와 같이 생성할 수 있다.

[0190] 인증 에이전트(210)는 응답 데이터의 해시값($H(y^P)$) 및 증명값(π)을 신뢰하지 않은 어플리케이션(Untrusted)에 전송할 수 있다.

[0191] 신뢰하지 않은 어플리케이션(Untrusted)는 응답 데이터(y^P), 증명값(π), 참조 무결성 측정값($H(s^I_0)$), 증명 모듈(200)의 공개키(Kp) 및 인증서를 검증 모듈(100)에 제공할 수 있다.

[0192] 검증 모듈(100)에서 증명값을 검증하는 방법은 도 4의 S170 및 S180 단계와 동일하게 진행되며, 중복된 내용은 생략한다.

[0194] 이상에서 설명한 바와 같이, 본 발명에 따르면, 증명(Attestation)을 이용하여 종래의 비밀 기반 인증에 추가적인 인증 방법을 도입함으로써, 기밀이 유출되더라도 증명을 통과할 수 없다.

[0196] 본원 발명의 실시예들과 관련된 기술 분야에서 통상의 지식을 가진 자는 상기 기재의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로, 개시된 방법들은 한정적인 관점이 아닌 설명적 관점에서 고려되어야 한다. 본 발명의 범위는 발명의 상세한 설명이 아닌 특허청구 범위에 나타나며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0198] 1: 인증 증명 장치

100: 검증 모듈

110: 입력부　　120: 검증부

200: 증명 모듈

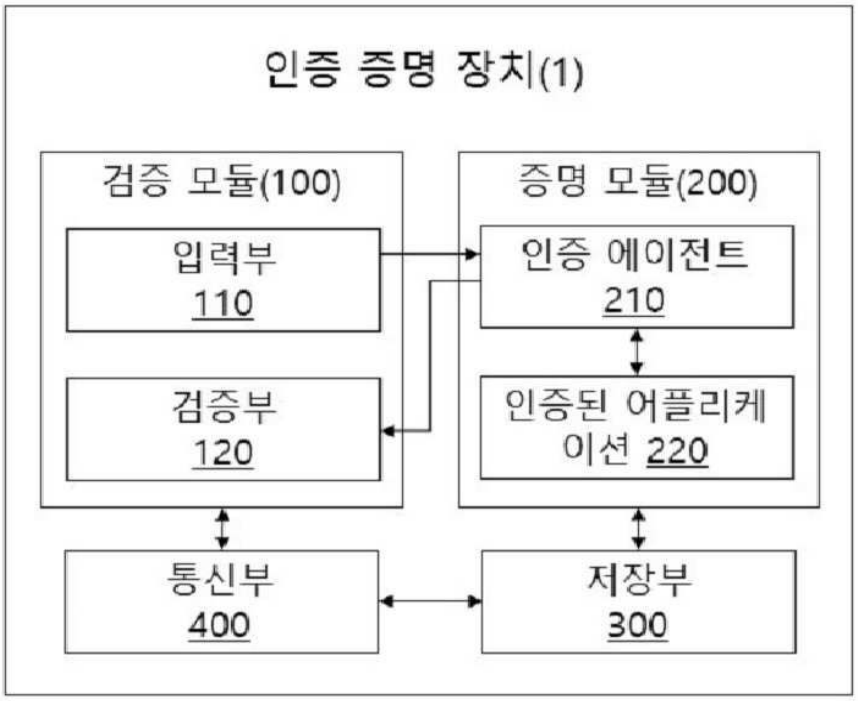
210: 인증 에이전트　220: 인증된 어플리케이션

300: 저장부

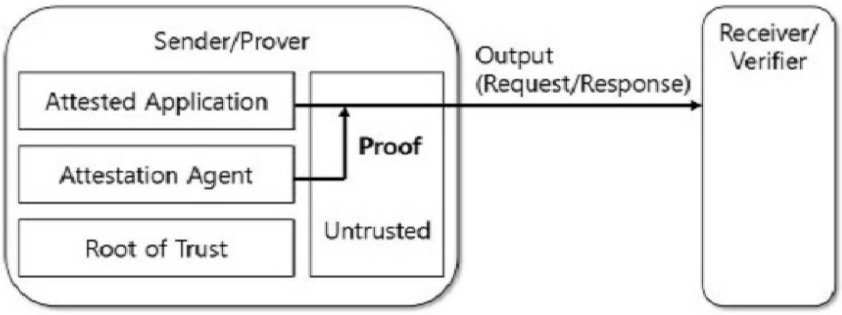
400: 통신부

도면

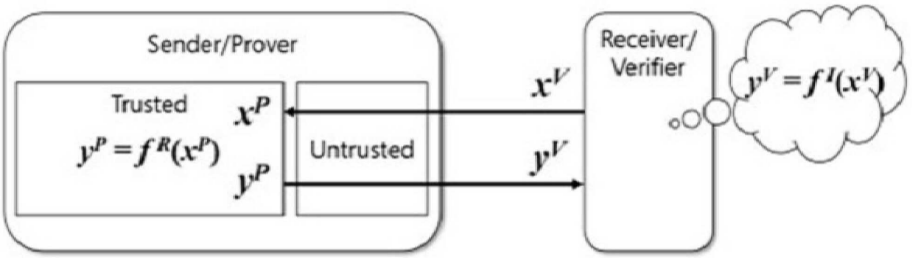
도면1



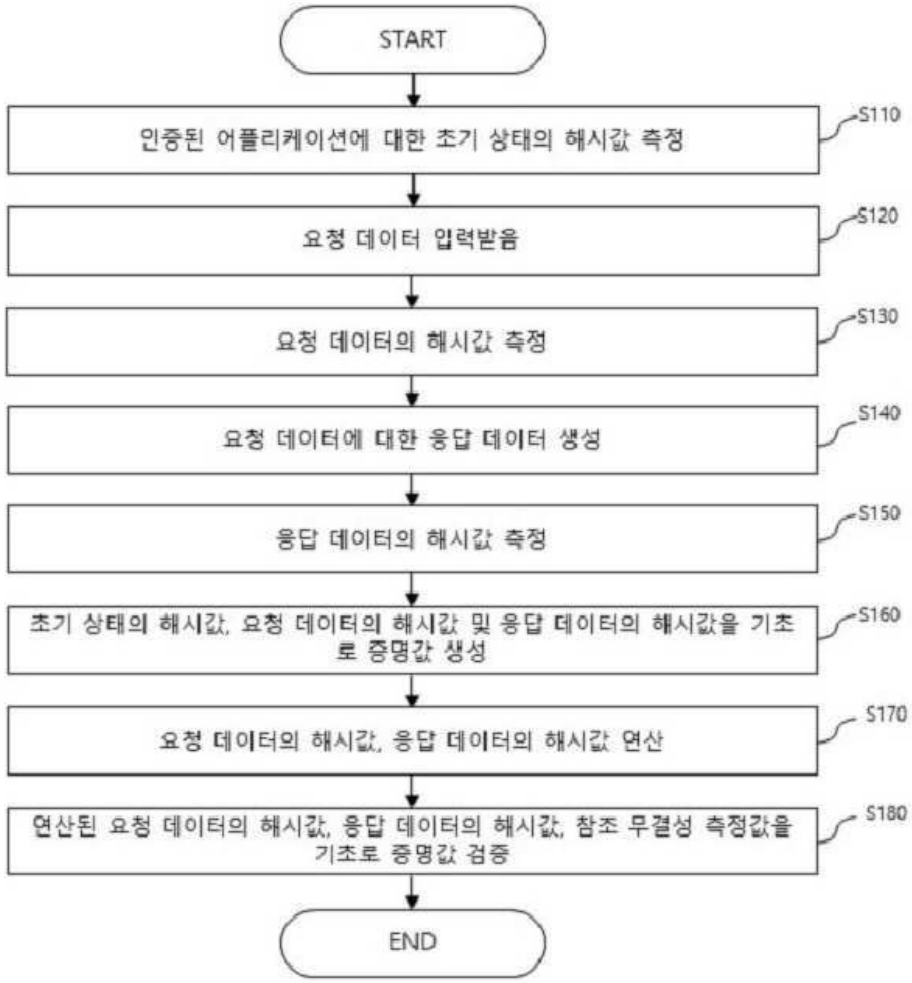
도면2



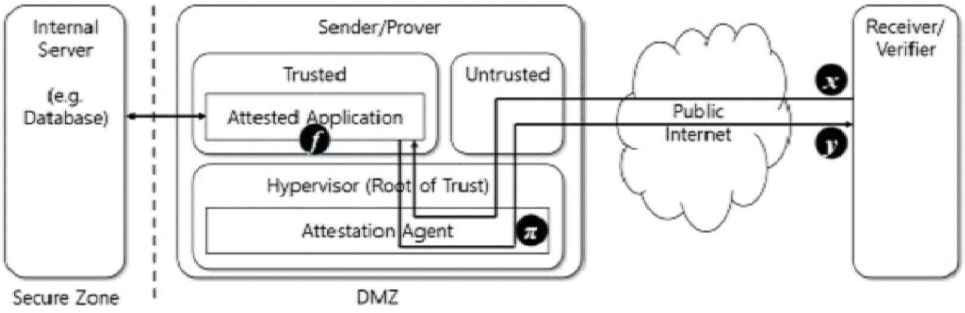
도면3


Sender/Prover
Trusted
$y^P = f^R(x^P)$
x^P
y^P
Untrusted
x^V
y^V
Receiver/
Verifier
$y^V = f^I(x^V)$

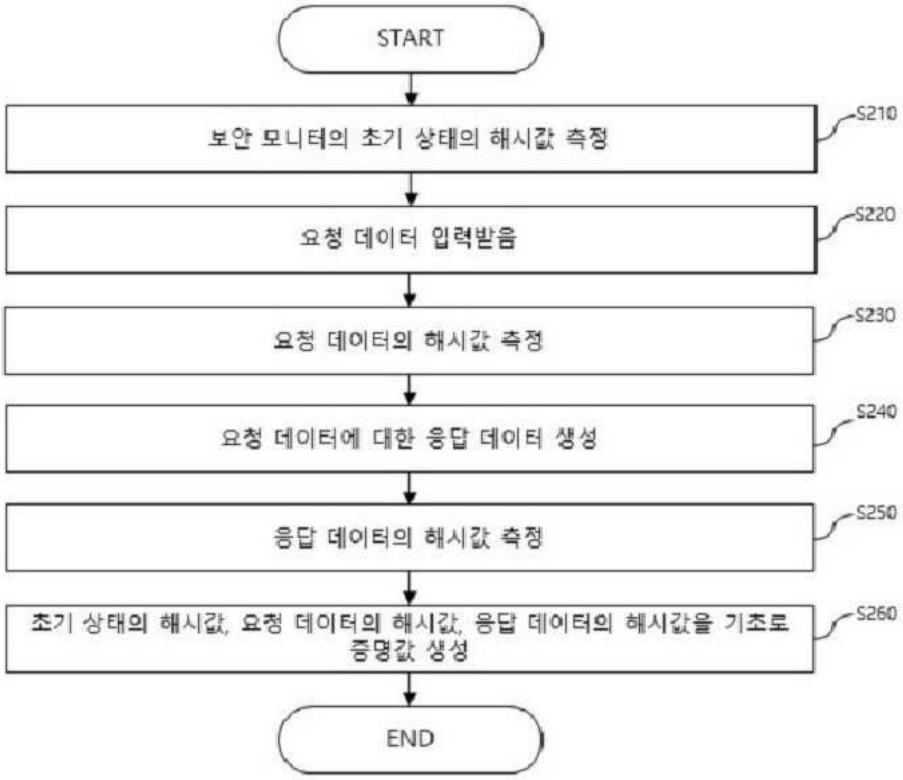
도면4


START
인증된 어플리케이션에 대한 초기 상태의 해시값 측정
S110
요청 데이터 입력받음
S120
요청 데이터의 해시값 측정
S130
요청 데이터에 대한 응답 데이터 생성
S140
응답 데이터의 해시값 측정
S150
초기 상태의 해시값, 요청 데이터의 해시값 및 응답 데이터의 해시값을 기초로 증명값 생성
S160
요청 데이터의 해시값, 응답 데이터의 해시값 연산
S170
연산된 요청 데이터의 해시값, 응답 데이터의 해시값, 참조 무결성 측정값을 기초로 증명값 검증
S180
END

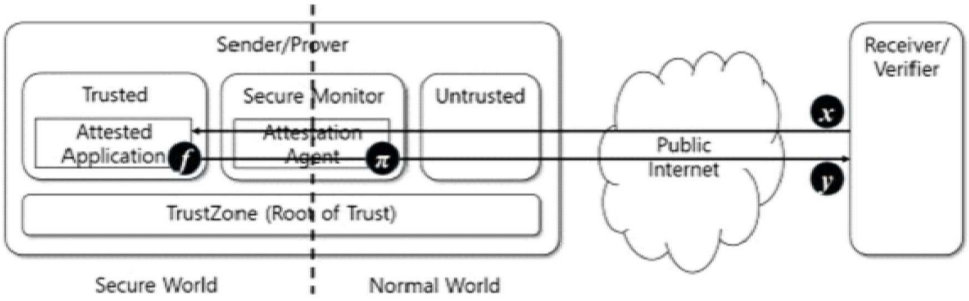
도면5


Internal Server
(e.g. Database)
Sender/Prover
Trusted
Attested Application
Untrusted
Hypervisor (Root of Trust)
Attestation Agent
Public Internet
Receiver/ Verifier
Secure Zone
DMZ

도면6


START
보안 모니터의 초기 상태의 해시값 측정
S210
요청 데이터 입력받음
S220
요청 데이터의 해시값 측정
S230
요청 데이터에 대한 응답 데이터 생성
S240
응답 데이터의 해시값 측정
S250
초기 상태의 해시값, 요청 데이터의 해시값, 응답 데이터의 해시값을 기초로 증명값 생성
S260
END

도면7


Sender/Prover
Trusted
Attested Application
Secure Monitor
Attestation Agent
Untrusted
TrustZone (Root of Trust)
Public Internet
Receiver/ Verifier
Secure World
Normal World