



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년11월16일
(11) 등록번호 10-1798022
(24) 등록일자 2017년11월09일

(51) 국제특허분류(Int. Cl.)
G06F 21/12 (2013.01) G06F 21/31 (2013.01)
G06F 21/60 (2013.01) H04L 9/30 (2006.01)
(52) CPC특허분류
G06F 21/12 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2016-0064823
(22) 출원일자 2016년05월26일
심사청구일자 2016년05월26일
(56) 선행기술조사문헌
KR1020130026351 A
KR1020060030611 A
KR1020140058196 A
US8745394 B1

(73) 특허권자
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57, 132동 801호(어은동, 한빛아파트)
조제경
대전광역시 유성구 온천북로33번길 22-9, 304호(봉명동)
김상후
대전광역시 유성구 대학로81번길 38, 502호(궁동, 살롬하우스)
(74) 대리인
홍성욱, 심경식

전체 청구항 수 : 총 16 항

심사관 : 윤혜숙

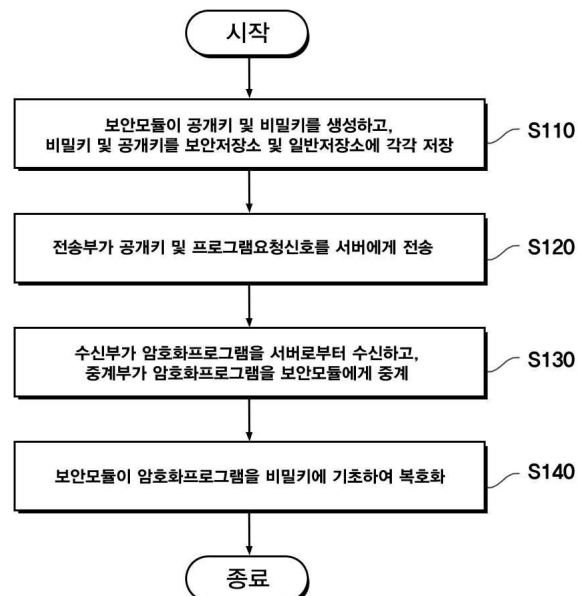
(54) 발명의 명칭 보안모듈을 이용한 프로그램의 실행 방법 및 장치

(57) 요약

보안모듈을 이용한 프로그램 실행 방법을 제공한다. 본 발명의 일 실시예에 따른 보안모듈을 이용한 프로그램 실행 방법은 클라이언트의 중앙처리장치(CPU)에 연결된 보안모듈(trusted platform module)을 이용하여 서버에 저장된 프로그램을 실행하는 방법에 있어서, 상기 보안모듈이 공개키 암호화 방법에 이용되는 공개키 및 비밀키를

(뒷면에 계속)

대표도 - 도1



생성하고, 상기 비밀키 및 상기 공개키를 상기 보안모듈 외부에서의 접근이 제한된 보안저장소 및 상기 보안모듈 외부에 위치한 일반저장소에 각각 저장하는 단계; 전송부가 상기 저장된 공개키 및 상기 프로그램의 전송을 요청하는 신호인 프로그램요청신호를 상기 서버에게 전송하는 단계; 수신부가 상기 전송된 프로그램요청신호에 대응하여 상기 공개키에 기초하여 암호화된 상기 프로그램인 암호화프로그램을 상기 서버로부터 수신하고, 중계부가 상기 암호화프로그램을 상기 보안모듈에게 중계하는 단계; 및 상기 보안모듈이 상기 암호화프로그램을 상기 비밀키에 기초하여 복호화하는 단계를 포함한다.

(52) CPC특허분류

G06F 21/602 (2013.01)

H04L 9/30 (2013.01)

G06F 2211/008 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 NRF2014M3C4A7030648

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 원천기술개발사업

연구과제명 미래 컴퓨팅 환경을 위한 암호와 기반 SW의 안전성 분석 및 대응기술 연구

기 여 율 1/1

주관기관 충남대학교 산학협력단

연구기간 2014.07.01 ~ 2019.06.30

명세서

청구범위

청구항 1

클라이언트의 중앙처리장치(CPU)에 연결된 보안모듈(trusted platform module)을 이용하여 서버에 저장된 프로그램을 실행하는 방법에 있어서,

상기 보안모듈이 공개키 암호화 방법에 이용되는 공개키 및 비밀키를 생성하고, 상기 비밀키 및 상기 공개키를 상기 보안모듈 외부에서의 접근이 제한된 보안저장소 및 상기 보안모듈 외부에 위치한 일반저장소에 각각 저장하는 단계;

상기 클라이언트에 포함된 전송부가 상기 저장된 공개키 및 상기 프로그램의 전송을 요청하는 신호인 프로그램 요청신호를 상기 서버에게 전송하는 단계;

상기 클라이언트에 포함된 수신부가 상기 전송된 프로그램요청신호에 대응하여 상기 공개키에 기초하여 암호화된 상기 프로그램인 암호화프로그램을 상기 서버로부터 수신하고, 상기 클라이언트에 포함된 중계부가 상기 암호화프로그램을 상기 보안모듈에게 중계하는 단계; 및

상기 보안모듈이 상기 암호화프로그램을 상기 비밀키에 기초하여 복호화하는 단계를 포함하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 방법.

청구항 2

제1항에 있어서,

상기 수신부가 상기 복호화된 프로그램을 상기 보안모듈로부터 수신하는 단계; 및

상기 클라이언트에 포함된 제어부가 상기 수신된 프로그램을 실행하는 단계;

를 더 포함하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 방법.

청구항 3

제1항에 있어서,

상기 프로그램요청신호를 상기 서버에게 전송하는 단계에서, 상기 전송부가 사용자를 식별하기 위한 수단인 사용자식별정보를 더 전송할 때,

상기 사용자식별정보는

상기 서버에 의한 식별 결과에 따라, 선택적으로 상기 프로그램요청신호에 대응하기 위하여 이용되는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 방법.

청구항 4

제1항에 있어서,

상기 보안모듈에게 중계하는 단계는

상기 수신부가 상기 프로그램을 실행하는데 필요한 데이터인 프로그램데이터를 더 수신하고, 상기 중계부가 상기 프로그램데이터를 더 중계하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 방법.

청구항 5

제4항에 있어서,

상기 프로그램데이터가 상기 공개키에 기초하여 암호화되었을 때,

상기 비밀키에 기초하여 복호화하는 단계는

상기 보안모듈이 상기 프로그램데이터를 더 복호화하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 방법.

청구항 6

제1항에 있어서,

상기 중앙처리장치 및 상기 보안모듈은

데스크탑컴퓨터, 노트북, 스마트폰, 태블릿 및 웨어러블기기 중 하나에 탑재된 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 방법.

청구항 7

제1항에 있어서,

상기 공개키 암호화 방법은

RSA 암호 시스템, 타원곡선(elliptic curve) 암호 시스템 및 이산로그(discrete logarithm) 암호 시스템 중 하나인 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 방법.

청구항 8

제1항에 있어서,

상기 보안모듈이 상기 암호화프로그램을 복호화한 시간 및 상기 암호화프로그램의 명칭 중 적어도 하나를 포함하는 프로그램복호화정보를 상기 공개키에 기초하여 암호화하여 상기 보안저장소에 저장하는 단계

를 더 포함하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 방법.

청구항 9

클라이언트에 탑재되고, 상기 클라이언트의 중앙처리장치에 연결된 보안모듈을 이용하여 서버에 저장된 프로그램을 실행하는 장치에 있어서,

공개키 암호화 방법에 이용되는 공개키 및 비밀키를 생성하고, 상기 비밀키 및 상기 공개키를 상기 보안모듈 외부에서의 접근이 제한된 보안저장소 및 상기 보안모듈 외부에 위치한 일반저장소에 각각 저장하는 보안모듈;

상기 저장된 공개키 및 상기 프로그램의 전송을 요청하는 신호인 프로그램요청신호를 상기 서버에게 전송하는 전송부;

상기 전송된 프로그램요청신호에 대응하여 상기 공개키에 기초하여 암호화된 상기 프로그램인 암호화프로그램을 상기 서버로부터 수신하는 수신부; 및

상기 암호화프로그램을 상기 보안모듈에게 중계하는 중계부

를 포함하고,

상기 보안모듈은

상기 암호화프로그램을 상기 비밀키에 기초하여 더 복호화하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 장치.

청구항 10

제9항에 있어서,

상기 수신부가 상기 복호화된 프로그램을 상기 보안모듈로부터 더 수신할 때,

상기 클라이언트의 중앙처리장치가 상기 수신된 프로그램을 실행하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 장치.

청구항 11

제9항에 있어서,

상기 전송부가 사용자를 식별하기 위한 수단인 사용자식별정보를 더 전송할 때,

상기 사용자식별정보는

상기 서버에 의한 식별 결과에 따라, 선택적으로 상기 프로그램요청신호에 대응하기 위하여 이용되는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 장치.

청구항 12

제9항에 있어서,

상기 수신부가 상기 프로그램을 실행하는데 필요한 데이터인 프로그램데이터를 더 수신하고, 상기 중계부가 상기 프로그램데이터를 더 중계하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 장치.

청구항 13

제12항에 있어서,

상기 프로그램데이터가 상기 공개키에 기초하여 암호화되었을 때,

상기 보안모듈은

상기 프로그램데이터를 더 복호화하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 장치.

청구항 14

제9항에 있어서,

상기 중앙처리장치 및 상기 보안모듈은

데스크탑컴퓨터, 노트북, 스마트폰, 태블릿 및 웨어러블기기 중 하나에 탑재된 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 장치.

청구항 15

제9항에 있어서,

상기 공개키 암호화 방법은

RSA 암호 시스템, 타원곡선(elliptic curve) 암호 시스템 및 이산로그(discrete logarithm) 암호 시스템 중 하나인 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 장치.

청구항 16

제9항에 있어서,

상기 보안모듈은

상기 암호화프로그램을 복호화한 시간 및 상기 암호화프로그램의 명칭 중 적어도 하나를 포함하는 프로그램복호화정보를 상기 공개키에 기초하여 암호화하여 상기 보안저장소에 더 저장하는 것을 특징으로 하는 보안모듈을 이용한 프로그램 실행 장치.

발명의 설명

기술 분야

[0001] 본 발명은 보안모듈을 이용하여 암호화 및 복호화하는 과정을 통해, 서버에 저장된 프로그램을 실행하는 방법 및 장치에 관한 것이다.

배경 기술

[0002] 중앙처리장치(CPU)의 발전으로 보안모듈(trusted platform module)을 보유하기 시작하였으며, 이를 통하여 데이

터의 암호화, 보안 상태의 프로그램 처리 등이 가능하기 시작했다. 또한, 보안모듈을 이용할 경우 공개키 암호화 알고리즘 등을 사용할 수 있으며, 프로그램의 실행파일을 암호화함으로써 프로그램을 보호하기 위한 기술로 활용될 수 있었다.

[0003] 그러나, 이와 같은 종래의 기술에서는 공개키 암호화 알고리즘의 비밀키가 보안모듈 외부에 위치한 일반저장소에 저장되어 잠재적인 보안상의 문제가 있었다. 또한, 암호화된 프로그램의 실행파일이 보안모듈을 통해 실행되어 프로그램의 실행 속도가 느려지는 문제가 있었다.

[0004] 이와 같은 문제를 해결하기 위하여, 비밀키를 보다 안전한 보안저장소에 분리하여 저장하고, 중앙처리장치(CPU)를 통해 프로그램을 실행하여 프로그램의 실행속도를 향상시키는 프로그램의 실행 방법 및 장치의 필요성이 대두되고 있다.

[0005] 관련 선행기술로는 한국등록특허 제10-1078841호(발명의 명칭: 신뢰 보안 모듈이 적용된 모바일 시스템 및 보안 모듈 운용 방법, 공개일자: 2010년 6월 14일)가 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 보안모듈이 생성한 공개키 암호화 알고리즘에 사용되는 비밀키를 보다 안전한 보안저장소에 분리하여 저장함으로써, 비밀키의 보안을 향상시킨 프로그램의 실행 방법 및 장치를 제공하고자 한다.

[0007] 또한, 본 발명은 서버에서 수신한 암호화된 프로그램을 비밀키와 보안모듈을 이용하여 복호화한 뒤, 중앙처리장치를 이용하여 실행함으로써, 프로그램의 실행속도를 향상시킨 프로그램의 실행 방법 및 장치를 제공하고자 한다.

과제의 해결 수단

[0008] 상기 목적을 달성하기 위해, 본 발명에서 제공하는 보안모듈을 이용한 프로그램 실행 방법은 클라이언트의 중앙처리장치(CPU)에 연결된 보안모듈(trusted platform module)을 이용하여 서버에 저장된 프로그램을 실행하는 방법에 있어서, 상기 보안모듈이 공개키 암호화 방법에 이용되는 공개키 및 비밀키를 생성하고, 상기 비밀키 및 상기 공개키를 상기 보안모듈 외부에서의 접근이 제한된 보안저장소 및 상기 보안모듈 외부에 위치한 일반저장소에 각각 저장하는 단계; 전송부가 상기 저장된 공개키 및 상기 프로그램의 전송을 요청하는 신호인 프로그램 요청신호를 상기 서버에게 전송하는 단계; 수신부가 상기 전송된 프로그램요청신호에 대응하여 상기 공개키에 기초하여 암호화된 상기 프로그램인 암호화프로그램을 상기 서버로부터 수신하고, 중계부가 상기 암호화프로그램을 상기 보안모듈에게 중계하는 단계; 및 상기 보안모듈이 상기 암호화프로그램을 상기 비밀키에 기초하여 복호화하는 단계;를 포함한다.

[0009] 바람직하게는, 상기 수신부가 상기 복호화된 프로그램을 상기 보안모듈로부터 수신하는 단계; 및 제어부가 상기 수신된 프로그램을 실행하는 단계;를 더 포함할 수 있다.

[0010] 바람직하게는, 상기 프로그램요청신호를 상기 서버에게 전송하는 단계가 사용자를 식별하기 위한 수단인 사용자 식별정보를 더 전송할 때, 상기 사용자식별정보는 상기 서버에 의한 식별 결과에 따라, 선택적으로 상기 프로그램요청신호에 대응하기 위하여 이용될 수 있다.

[0011] 바람직하게는, 상기 보안모듈에게 중계하는 단계는 상기 수신부가 상기 프로그램을 실행하는데 필요한 데이터인 프로그램데이터를 더 수신하고, 상기 중계부가 상기 프로그램데이터를 더 중계할 수 있다.

[0012] 바람직하게는, 상기 프로그램데이터가 상기 공개키에 기초하여 암호화되었을 때, 상기 비밀키에 기초하여 복호화하는 단계는 상기 보안모듈이 상기 프로그램데이터를 더 복호화할 수 있다.

[0013] 바람직하게는, 상기 중앙처리장치 및 상기 보안모듈은 데스크탑컴퓨터, 노트북, 스마트폰, 태블릿 및 웨어러블 기기 중 하나에 탑재될 수 있다.

[0014] 바람직하게는, 상기 공개키 암호화 방법은 RSA 암호 시스템, 타원곡선(elliptic curve) 암호 시스템 및 이산로그(discrete logarithm) 암호 시스템 중 하나일 수 있다.

[0015] 바람직하게는, 상기 보안모듈이 상기 암호화프로그램을 복호화한 시간 및 상기 암호화프로그램의 명칭 중 적어도 하나를 포함하는 프로그램복호화정보를 상기 공개키에 기초하여 암호화하여 상기 보안저장소에 저장하는 단

계를 더 포함할 수 있다.

- [0016] 또한, 상기 목적을 달성하기 위해, 본 발명에서 제공하는 보안모듈을 이용한 프로그램 실행 장치는 클라이언트의 중앙처리장치에 연결된 보안모듈을 이용하여 서버에 저장된 프로그램을 실행하는 장치에 있어서, 공개키 암호화 방법에 이용되는 공개키 및 비밀키를 생성하고, 상기 비밀키 및 상기 공개키를 상기 보안모듈 외부에서의 접근이 제한된 보안저장소 및 상기 보안모듈 외부에 위치한 일반저장소에 각각 저장하는 보안모듈; 상기 저장된 공개키 및 상기 프로그램의 전송을 요청하는 신호인 프로그램요청신호를 상기 서버에게 전송하는 전송부; 상기 전송된 프로그램요청신호에 대응하여 상기 공개키에 기초하여 암호화된 상기 프로그램인 암호화프로그램을 상기 서버로부터 수신하는 수신부; 및 상기 암호화프로그램을 상기 보안모듈에게 중계하는 중계부;를 포함하고, 상기 보안모듈은 상기 암호화프로그램을 상기 비밀키에 기초하여 더 복호화할 수 있다.
- [0017] 바람직하게는, 상기 수신부가 상기 복호화된 프로그램을 상기 보안모듈로부터 더 수신할 때, 상기 수신된 프로그램을 실행하는 제어부를 더 포함할 수 있다.
- [0018] 바람직하게는, 상기 전송부가 사용자를 식별하기 위한 수단인 사용자식별정보를 더 전송할 때, 상기 사용자식별정보는 상기 서버에 의한 식별 결과에 따라, 선택적으로 상기 프로그램요청신호에 대응하기 위하여 이용될 수 있다.
- [0019] 바람직하게는, 상기 수신부가 상기 프로그램을 실행하는데 필요한 데이터인 프로그램데이터를 더 수신하고, 상기 중계부가 상기 프로그램데이터를 더 중계할 수 있다.
- [0020] 바람직하게는, 상기 프로그램데이터가 상기 공개키에 기초하여 암호화되었을 때, 상기 보안모듈은 상기 프로그램데이터를 더 복호화할 수 있다.
- [0021] 바람직하게는, 상기 중앙처리장치 및 상기 보안모듈은 데스크탑컴퓨터, 노트북, 스마트폰, 태블릿 및 웨어러블 기기 중 하나에 탑재될 수 있다.
- [0022] 바람직하게는, 상기 공개키 암호화 방법은 RSA 암호 시스템, 타원곡선(elliptic curve) 암호 시스템 및 이산로그(discrete logarithm) 암호 시스템 중 하나일 수 있다.
- [0023] 바람직하게는, 상기 보안모듈은 상기 암호화프로그램을 복호화한 시간 및 상기 암호화프로그램의 명칭 중 적어도 하나를 포함하는 프로그램복호화정보를 상기 공개키에 기초하여 암호화하여 상기 보안저장소에 더 저장할 수 있다.

발명의 효과

- [0024] 본 발명은 보안모듈이 생성한 공개키 암호화 알고리즘에 사용되는 비밀키를 보안모듈 외부에서의 접근이 제한되어 보다 안전한 보안저장소에 분리하여 저장함으로써, 비밀키의 보안을 향상시키는 효과가 있다.
- [0025] 또한, 본 발명은 서버에서 수신한 암호화된 프로그램을 비밀키를 이용하여 복호화한 뒤, 중앙처리장치를 이용하여 실행함으로써, 프로그램의 실행속도를 향상시키는 효과가 있다.

도면의 간단한 설명

- [0026] 도 1은 본 발명의 일 실시예에 따른 보안모듈을 이용한 프로그램 실행 방법을 설명하기 위하여 도시한 흐름도이다.
- 도 2는 본 발명의 다른 실시예에 따른 보안모듈을 이용한 프로그램 실행 방법을 설명하기 위하여 도시한 흐름도이다.
- 도 3은 본 발명의 일 실시예에 따른 보안모듈을 이용한 프로그램 실행 장치를 설명하기 위하여 도시한 도면이다.
- 도 4는 본 발명의 다른 실시예에 따른 보안모듈을 이용한 프로그램 실행 장치를 설명하기 위하여 도시한 도면이다.
- 도 5는 본 발명의 다른 실시예에 따른 중앙처리장치, 보안모듈, 보안저장소 및 일반저장소의 관계를 설명하기 위하여 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0027] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 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.
- [0028] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 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.
- [0029] 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.
- [0030] 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.
- [0031] 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.
- [0032] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0033] 도 1은 본 발명의 일 실시예에 따른 보안모듈을 이용한 프로그램 실행 방법을 설명하기 위하여 도시한 흐름도이다.
- [0034] 보안모듈(310, trusted platform module)은 컴퓨팅 환경에서 데이터 보안을 향상시키기 위한 모듈로, 중앙처리장치(CPU)와 연결된 하드웨어 장치일 수 있다. 또한, 보안모듈(310)은 난수발생, 해쉬생성 및 암호화 키 생성 등을 담당하는 보안 프로세서와 필요한 데이터를 저장하기 위한 메모리영역을 포함할 수 있다.
- [0035] 단계 S110에서는, 보안모듈(310)이 공개키 암호화 방법에 이용되는 공개키 및 비밀키를 생성하고, 그 비밀키 및 공개키를 보안모듈(310) 외부에서의 접근이 제한된 보안저장소 및 보안모듈(310) 외부에 위치한 일반저장소에 각각 저장한다.
- [0036] 공개키 암호화 방법에는 암호화 및 복호화를 위하여 공개키와 비밀키가 존재하며, 공개키는 누구나 알 수 있지만 그 공개키에 대응되는 비밀키는 소유자만이 알 수 있다. 또한, 공개키를 이용하여 암호화된 데이터는 그 공개키에 대응되는 비밀키를 이용하여서만 복호화할 수 있다. 한편, 공개키 암호화 방법은 대칭키 암호 방법과 비교하여 비대칭 암호 방법으로 부르기도 하며, 대표적인 공개키 암호화 방법으로는 RSA(Rivest Shamir Adleman) 암호화 방법 등이 있다.
- [0037] 한편, 보안저장소는 보안이 요구되는 데이터를 저장하기 위한 저장 영역으로, 보안모듈(310)의 내부에 포함된 메모리영역일 수 있다. 보안저장소는 보안모듈(310) 외부에서의 접근이 제한되어 있기 때문에, 보안이 요구되는 데이터(예, 비밀키, 소프트웨어 라이선스 등)를 저장하기에 적합할 수 있다.
- [0038] 반면에, 일반저장소는 특별한 보안이 요구되지 않는 일반적인 컴퓨팅 환경에서 데이터를 저장하기 위한 저장 영역으로, 휘발성 메모리, 플래시 메모리, 하드디스크(HDD) 또는 솔리드스테이트디스크(SSD)등이 이에 해당할 수 있다. 또한, 일반저장소는 중앙처리장치 및 보안모듈 모두로부터 접근이 가능할 수 있다.
- [0039] 도 5를 참조하면, 중앙처리장치(510)와 보안모듈(310)이 연결되어 있을 때, 보안저장소(520)는 보안모듈(310)에서만 접근할 수 있고, 일반저장소(530)는 중앙처리장치(510) 및 보안모듈(310) 모두에서 접근할 수 있는 것을

볼 수 있다.

- [0040] 예컨대, 보안모듈(310)은 내부의 보안프로세서를 이용하여 RSA 암호화 방법에 따른 공개키와 비밀키를 각각 생성할 수 있다. 또한, 그 공개키와 비밀키에 대하여, 높은 수준의 보안이 요구되는 비밀키는 보안저장소에 저장하고, 높은 수준의 보안이 요구되지 않는 공개키는 일반저장소에 저장할 수 있다.
- [0041] 참고로, RSA 암호화 방법은 1977년 론 리베스트(Ron Rivest)와 아디 셰미르(Adi Shamir), 레오나르드 아델만(Leonard Adleman) 등 3명의 수학자에 의해 개발된 암호화 방법이다. 이 암호화 방법은 두 개의 큰 소수(보통 140자리 이상의 수)를 이용한다. 큰 소수들의 곱과 추가연산을 통해 하나는 공개키를 구성하고 다른 하나는 비밀키를 구성하는데, 사용되는 두 세트의 수 체계를 유도하는 복잡한 작업이 수반되는 것을 특징으로 한다.
- [0042] 단계 S120에서는, 전송부(320)가 저장된 공개키 및 프로그램의 전송을 요청하는 신호인 프로그램요청신호를 서버에게 전송한다.
- [0043] 서버는 프로그램을 저장하고 있으며, 유선 또는 무선으로 중앙처리장치와 연결되어 사용자의 요청에 따라 저장된 프로그램을 전송하는 역할을 수행한다. 이때, 프로그램은 사용 상에 보안이 요구되는 프로그램일 수 있다. 예컨대, 서버에 저장되는 프로그램은 외부로 노출되면 곤란해지는 국방상 또는 업무상의 중요 프로그램일 수 있다.
- [0044] 프로그램요청신호는 요청하는 프로그램의 명칭 정보 및 버전 정보 등을 포함하도록 생성할 수 있다.
- [0045] 또한, 동일한 공개키가 이미 서버에게 전송된 경우, 전송부(320)는 공개키를 제외하고 프로그램요청신호만을 전송할 수 있다. 이때, 서버는 프로그램요청신호를 전송하는 사용자에 대한 공개키를 저장하고 있다가 다른 식별 방법(전송부(320)의 IP주소, 아이디 및 패스워드 등)을 통해 식별하여 사용할 수 있다.
- [0046] 다른 실시예에서는, 전송부(320)가 사용자를 식별하기 위한 수단인 사용자식별정보를 더 전송할 때, 그 사용자식별정보는 서버에 의한 식별 결과에 따라, 선택적으로 프로그램요청신호에 대응하기 위하여 이용될 수 있다.
- [0047] 예컨대, 전송부(320)가 IP주소 또는 사용자의 아이디 및 패스워드를 사용자식별정보로 서버에게 더 전송할 수 있다. 그러면, 서버는 그 전송된 사용자식별정보를 사용자DB에서 검색하여, 그 사용자가 정당한 사용 권한을 가진 사용자인지 판단할 수 있다. 그 판단 결과에 따라, 선택적으로 프로그램요청신호에 대응하여 암호화프로그램을 전송할 수 있다. 즉, 정당한 사용 권한이 없는 사용자에게는 암호화프로그램을 전송하지 않을 수 있다.
- [0048] 단계 S130에서는, 수신부(330)가 그 전송된 프로그램요청신호에 대응하여 공개키에 기초하여 암호화된 프로그램인 암호화프로그램을 서버로부터 수신하고, 중계부(340)가 그 암호화프로그램을 보안모듈(310)에게 중계한다.
- [0049] 전송부(320)가 서버에게 공개키와 프로그램요청신호를 전송하면, 서버에서는 프로그램요청신호에 대응되는 프로그램이 전송된 공개키를 이용하여 암호화될 수 있다. 그리고, 그 암호화된 암호화프로그램이 서버로부터 수신부(330)에게 전송될 수 있다. 암호화프로그램은 비밀키를 가지지 않은 경우에는 복호화할 수 없기 때문에, 설사 비밀키가 없는 제3자가 이를 입수하더라도 복호화할 수 없어 상대적으로 안전할 수 있다.
- [0050] 예컨대, 수신부(330)는 전송된 프로그램요청신호에 대응되는 암호화프로그램을 서버로부터 수신하고, 이를 일반저장소에 저장할 수 있다. 그리고, 중계부(340)가 그 일반저장소에 저장된 암호화프로그램을 보안모듈(310)에게 중계할 수 있다.
- [0051] 다른 실시예에서는, 수신부(330)가 프로그램을 실행하는데 필요한 데이터인 프로그램데이터를 더 수신하고, 중계부(340)가 프로그램데이터를 더 중계할 수 있다.
- [0052] 프로그램데이터는 프로그램을 실행하기 위해서 요구되는 각종 리소스(사진, 동영상, 음악, 문서, 데이터베이스 등)를 포함할 수 있다. 여기서, 프로그램의 실행은 프로그램의 시작으로 한정되는 것이 아니며, 프로그램이 각종 기능을 수행하는 것을 포함하는 의미일 수 있다.
- [0053] 이때, 수신부(330)는 프로그램데이터를 프로그램과 함께 서버로부터 수신하고, 중계부(340)는 그 수신된 프로그램데이터를 보안모듈(310)에게 중계할 수 있다.
- [0054] 마지막으로 단계 S140에서는, 보안모듈(310)이 그 암호화프로그램을 비밀키에 기초하여 복호화한다.
- [0055] 비밀키는 보안모듈(310) 외부에서의 접근이 제한된 보안저장소에 저장되어 있으므로, 보안모듈(310)이 그 중계된 암호화프로그램을 그 비밀키를 이용하여 복호화할 수 있다. 다시 말하면, 보안모듈(310)의 외부에서는 비밀키를 확보할 수 없으므로, 그 중계된 암호화프로그램을 복호화할 수 없어서, 보안모듈(310)만이 복호화를 수행

할 수 있다.

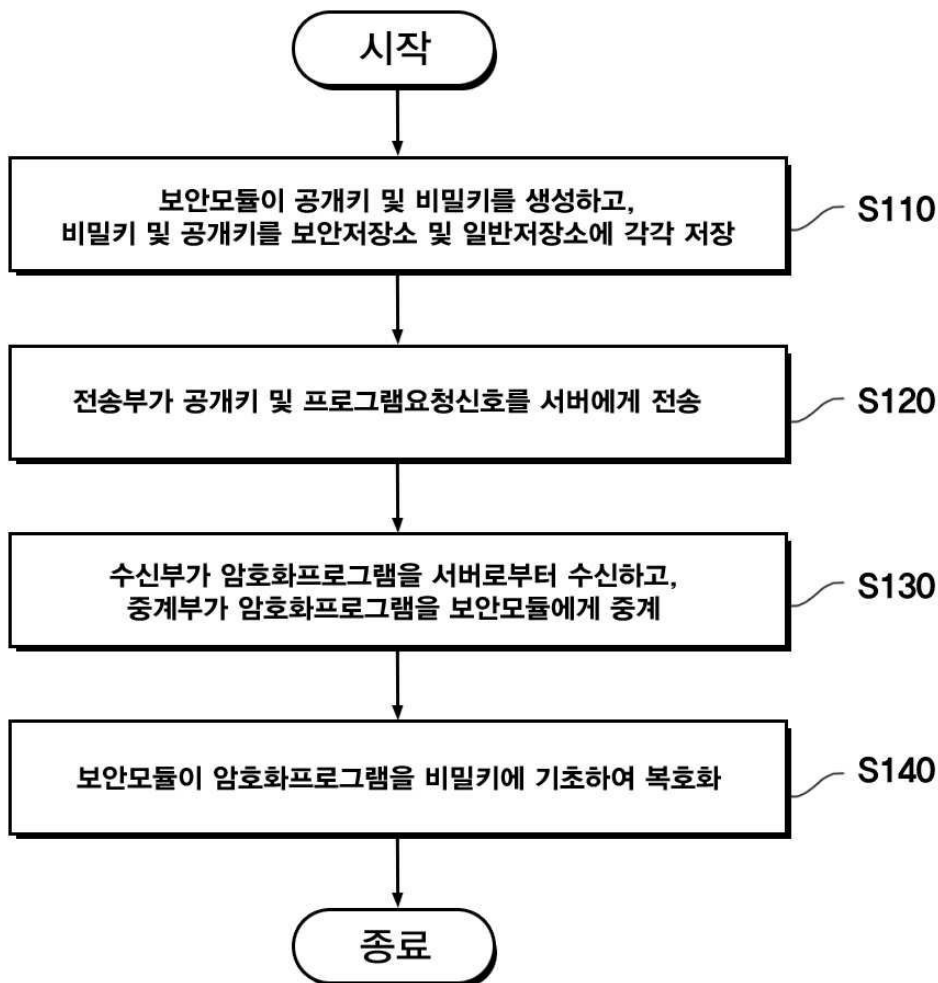
- [0056] 보안모듈(310)이 암호화프로그램을 복호화한 후에는, 그 복호화의 결과인 프로그램은 컴퓨팅 환경에서 실행될 수 있다. 예컨대, PC나 스마트폰 등에서 자유롭게 실행될 수 있다.
- [0057] 다른 실시예에서는, 프로그램데이터가 공개키에 기초하여 암호화되었을 때, 보안모듈(310)이 프로그램데이터를 더 복호화할 수 있다.
- [0058] 예컨대, 프로그램을 실행하기 위해서 필요한 프로그램데이터 역시 보안상의 이유로 암호화가 필요한 경우, 프로그램데이터 역시 서버에 의해 공개키에 기초하여 암호화된 채로 전송될 수 있다.
- [0059] 이때, 보안모듈(310)이 그 암호화된 프로그램데이터를 암호화프로그램과 마찬가지로 복호화하여 프로그램을 실행하기 위하여 이용할 수 있다.
- [0060] 또 다른 실시예에서는, 중앙처리장치 및 보안모듈(310)은 데스크탑컴퓨터, 노트북, 스마트폰, 태블릿 및 웨어러블기기 중 하나에 탑재될 수 있다.
- [0061] 예컨대, 스마트폰용 어플리케이션도 프로그램과 동일한 방법으로 실행될 수 있다. 즉, 본 발명의 프로그램은 PC에서 동작하는 프로그램으로 한정되는 것이 아니며, 스마트폰, 태블릿 및 웨어러블기기에서 동작하는 각종 어플리케이션에도 동일하게 적용될 수 있다.
- [0062] 또 다른 실시예에서는, 공개키 암호화 방법은 RSA 암호 시스템, 타원곡선(elliptic curve) 암호 시스템 및 이산로그(discrete logarithm) 암호 시스템 중 하나일 수 있다.
- [0063] 예컨대, 보안모듈(310)이 RSA 암호 시스템, 타원곡선 암호 시스템 및 이산로그 암호 시스템 중 전부 또는 일부를 지원할 수 있으며, 그 경우 지원되는 암호 시스템을 이용하여 프로그램을 암호화 및 복호화할 수 있다. 이때, 보안모듈(310)은 내부에 탑재된 보안 프로세서를 이용하여 그 지원되는 암호 시스템에 대응되는 공개키와 비밀키를 생성할 수 있다.
- [0064] 또 다른 실시예에서는, 보안모듈(310)이 암호화프로그램에 대한 복호화 정보인 프로그램복호화정보를 공개키에 기초하여 암호화하여 보안저장소에 저장할 수 있다.
- [0065] 예컨대, 보안모듈(310)은 암호화프로그램에 대한 복호화가 수행될 때마다, 그 암호화프로그램을 복호화한 시간 및 그 암호화프로그램의 명칭 중 적어도 하나를 포함하는 프로그램복호화정보를 로그(log)파일에 추가하여 보안저장소에 저장할 수 있다. 이때, 로그파일은 보안을 위하여 공개키로 암호화되어 저장될 수 있다.
- [0066] 이와 같이, 본 발명의 일 실시예에 따른 보안모듈(310)을 이용한 프로그램 실행 방법은 비밀키를 보안모듈(310) 외부에서의 접근이 제한되어 보다 안전한 보안저장소에 분리하여 저장함으로써, 비밀키의 보안을 향상시켜 결과적으로 실행되는 프로그램에 대한 보안을 향상시키는 효과가 있다.
- [0067] 도 2는 본 발명의 다른 실시예에 따른 보안모듈을 이용한 프로그램 실행 방법을 설명하기 위하여 도시한 흐름도이다.
- [0068] 단계 S210에서는, 보안모듈(310)이 공개키 암호화 방법에 이용되는 공개키 및 비밀키를 생성하고, 그 비밀키 및 공개키를 보안모듈(310) 외부에서의 접근이 제한된 보안저장소 및 보안모듈(310) 외부에 위치한 일반저장소에 각각 저장한다.
- [0069] 단계 S220에서는, 전송부(320)가 저장된 공개키 및 프로그램의 전송을 요청하는 신호인 프로그램요청신호를 서버에게 전송한다.
- [0070] 단계 S230에서는, 수신부(330)가 그 전송된 프로그램요청신호에 대응하여 공개키에 기초하여 암호화된 프로그램인 암호화프로그램을 서버로부터 수신하고, 중계부(340)가 그 암호화프로그램을 보안모듈(310)에게 중계한다.
- [0071] 단계 S240에서는, 보안모듈(310)이 그 암호화프로그램을 비밀키에 기초하여 복호화한다.
- [0072] 단계 S250에서는, 수신부(330)가 그 복호화된 프로그램을 보안모듈(310)로부터 수신한다.
- [0073] 예컨대, 보안모듈(310)의 내부에서 프로그램이 실행되는 경우, 보안모듈(310)의 성능이 중앙처리장치에 미치지 못하여 프로그램의 실행속도가 상대적으로 느려질 수 있다. 따라서, 중앙처리장치에서 프로그램을 실행하기 위한 목적으로 수신부가 보안모듈(310)로부터 그 복호화된 프로그램을 수신할 수 있다. 보안모듈(310)은 중앙처리장치와는 분리된 하드웨어장치일 수 있기 때문이다.

- [0074] 이때, 수신부(330)가 수신한 그 복호화된 프로그램은 일반저장소에 저장하지 않는 것이 바람직할 수 있다. 만일 일반저장소에 저장된다면, 실행중인 다른 프로그램으로부터의 접근이 가능할 수 있어, 만일 그 실행중인 다른 프로그램 중에 악성코드를 포함하고 있는 프로그램이 있는 경우 그 복호화된 프로그램이 노출될 수 있기 때문이다. 이 경우, 예컨대, 각 프로그램(또는 프로세스)별로 접근이 제한될 수 있는, 휘발성 메모리(예, RAM) 상에서 저장하는 것이 보안을 위하여 보다 바람직할 수 있다.
- [0075] 마지막으로 단계 S260에서는, 제어부(350)가 그 수신된 프로그램을 실행한다.
- [0076] 예컨대, 제어부(350)가 휘발성 메모리 상에 저장된 그 복호화된 프로그램을 호출하여, 실행할 수 있다. 이때, 중앙처리장치를 통해 그 복호화된 프로그램을 실행함으로써 인하여 프로그램의 실행속도가 보안모듈(310)을 통해 실행하는 경우에 비하여 상대적으로 향상될 수 있다.
- [0077] 또한, 제어부(350)는 보안모듈(310), 전송부(320), 수신부(330) 및 중계부(340) 등과 같은 다른 구성을 제어하여, 프로그램을 실행하도록 할 수 있다. 예컨대, 보안모듈(310)에게 신호를 전송하여 공개키와 비밀키를 생성할 수 있으며, 공개키와 프로그램요청신호를 전송부(320)에게 전달하여 서버에게 전송하도록 할 수 있다.
- [0078] 도 3은 본 발명의 일 실시예에 따른 보안모듈을 이용한 프로그램 실행 장치를 설명하기 위하여 도시한 도면이다.
- [0079] 도 3을 참조하면, 본 발명의 일 실시예에 따른 보안모듈을 이용한 프로그램 실행 장치(300)는 보안모듈(310), 전송부(320), 수신부(330) 및 중계부(340)를 포함한다. 한편, 보안모듈을 이용한 프로그램 실행 장치(300)는 데스크탑 컴퓨터, 노트북, 스마트폰, 태블릿 및 웨어러블기기 등에 탑재될 수 있다.
- [0080] 보안모듈(310)은 공개키 암호화 방법에 이용되는 공개키 및 비밀키를 생성하고, 그 비밀키 및 공개키를 보안모듈만 접근가능한 보안저장소 및 보안모듈 외부에 위치한 일반저장소에 각각 저장한다. 또한, 보안모듈(310)은 암호화프로그램을 비밀키에 기초하여 더 복호화할 수 있다.
- [0081] 다른 실시예에서는, 보안모듈(310)은 암호화프로그램을 복호화한 시간 및 암호화프로그램의 명칭 중 적어도 하나를 포함하는 프로그램복호화정보를 공개키에 기초하여 암호화하여 보안저장소에 더 저장할 수 있다.
- [0082] 전송부(320)는 저장된 공개키 및 프로그램의 전송을 요청하는 신호인 프로그램요청신호를 서버에게 전송한다.
- [0083] 다른 실시예에서는, 전송부(320)가 사용자를 식별하기 위한 수단인 사용자식별정보를 더 전송할 때, 사용자식별 정보는 서버에 의한 식별 결과에 따라, 선택적으로 프로그램요청신호에 대응하기 위하여 이용될 수 있다.
- [0084] 수신부(330)는 전송된 프로그램요청신호에 대응하여 공개키에 기초하여 암호화된 프로그램인 암호화프로그램을 서버로부터 수신한다.
- [0085] 중계부(340)는 수신된 암호화프로그램을 보안모듈에게 중계한다.
- [0086] 다른 실시예에서는, 수신부(330)가 프로그램을 실행하는데 필요한 데이터인 프로그램데이터를 더 수신하고, 중계부(340)가 그 프로그램데이터를 더 중계할 수 있다.
- [0087] 또 다른 실시예에서는, 그 프로그램데이터가 공개키에 기초하여 암호화되었을 때, 보안모듈(310)은 그 프로그램데이터를 더 복호화할 수 있다.
- [0088] 또 다른 실시예에서는, 중앙처리장치 및 보안모듈(310)은 데스크탑컴퓨터, 노트북, 스마트폰, 태블릿 및 웨어러블기기 중 하나에 탑재될 수 있다.
- [0089] 또 다른 실시예에서는, 공개키 암호화 방법은 RSA 암호 시스템, 타원곡선 암호 시스템 및 이산로그 암호 시스템 중 하나일 수 있다.
- [0090] 도 4는 본 발명의 다른 실시예에 따른 보안모듈을 이용한 프로그램 실행 장치를 설명하기 위하여 도시한 도면이다.
- [0091] 도 4를 참조하면, 본 발명의 일 실시예에 따른 보안모듈을 이용한 프로그램 실행 장치(300)는 보안모듈(310), 전송부(320), 수신부(330), 중계부(340) 및 제어부(350)를 포함한다.
- [0092] 보안모듈(310)은 공개키 암호화 방법에 이용되는 공개키 및 비밀키를 생성하고, 그 비밀키 및 공개키를 보안모듈만 접근가능한 보안저장소 및 보안모듈 외부에 위치한 일반저장소에 각각 저장한다.

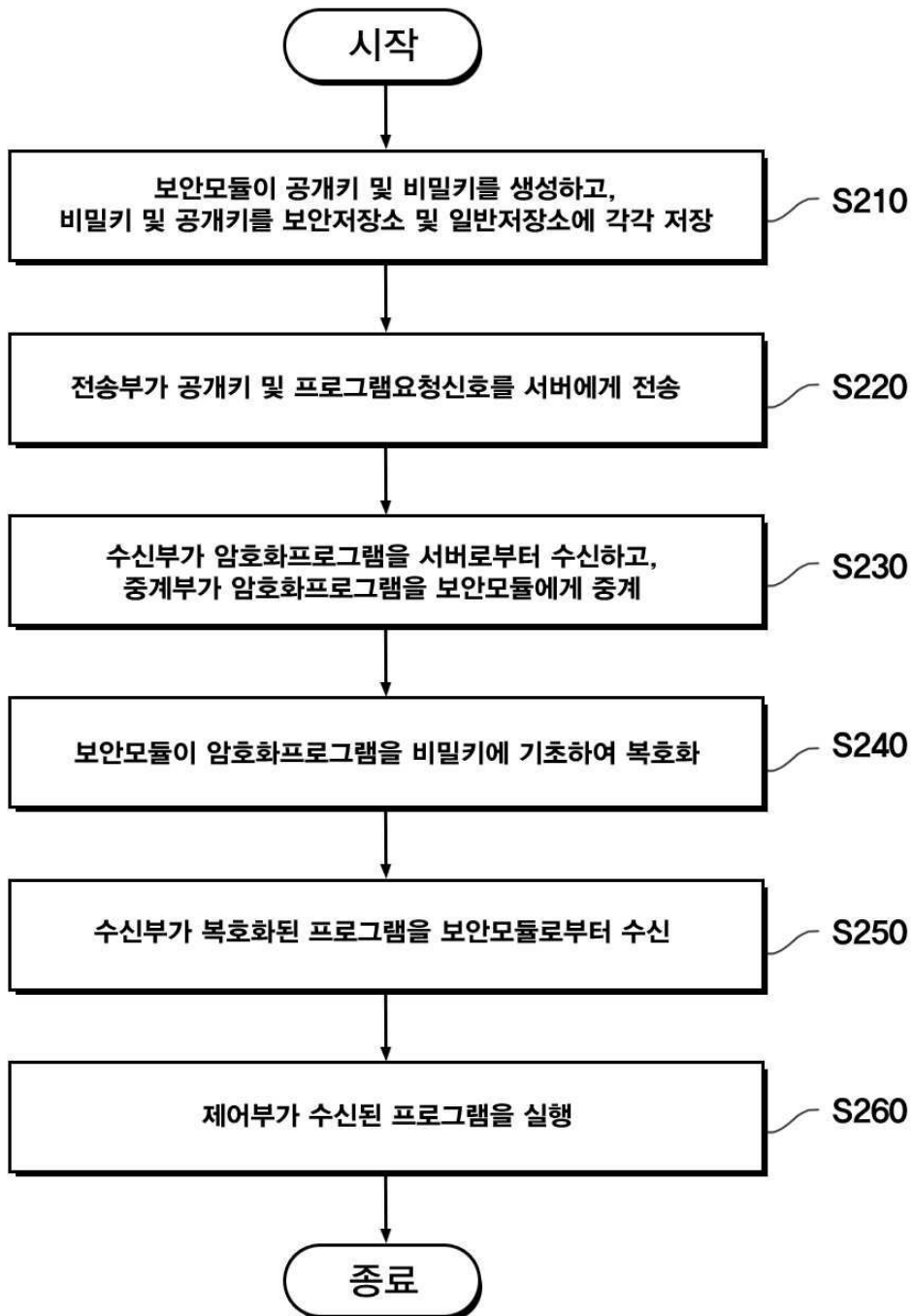
- [0093] 전송부(320)는 저장된 공개키 및 프로그램의 전송을 요청하는 신호인 프로그램요청신호를 서버에게 전송한다.
- [0094] 수신부(330)는 전송된 프로그램요청신호에 대응하여 공개키에 기초하여 암호화된 프로그램인 암호화프로그램을 서버로부터 수신한다. 중계부(340)는 수신된 암호화프로그램을 보안모듈에게 중계한다.
- [0095] 이때, 보안모듈(310)은 그 암호화프로그램을 비밀키에 기초하여 더 복호화하고, 수신부(330)는 그 복호화된 프로그램을 보안모듈로부터 더 수신한다.
- [0096] 마지막으로 제어부(350)는 그 수신된 프로그램을 실행한다.
- [0097] 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.
- [0098] 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등)를 포함한다.
- [0099] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

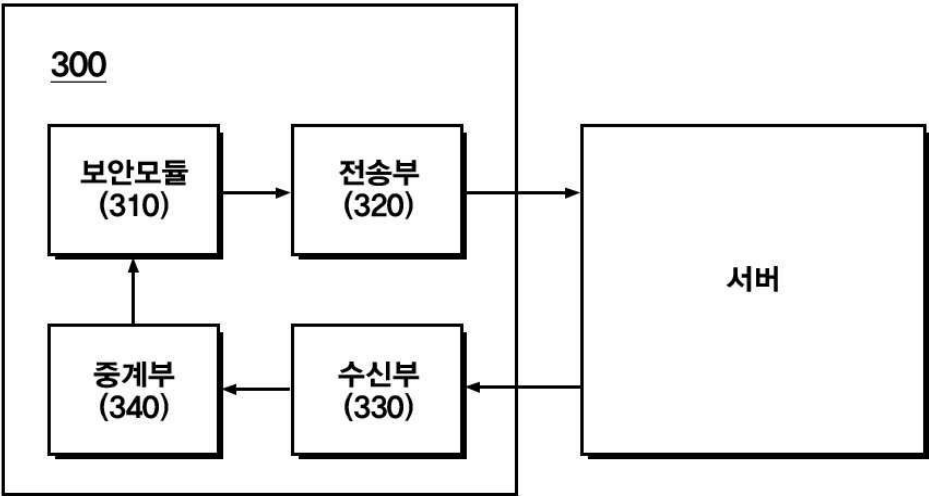
도면1



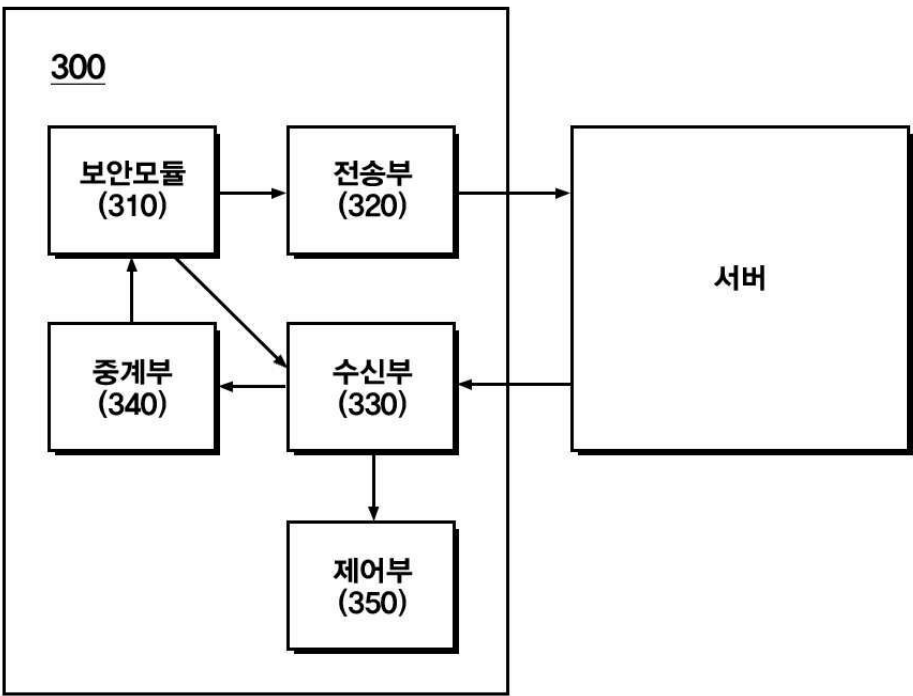
도면2



도면3



도면4



도면5

500

