(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0032945
(43) 공개일자 2020년03월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04L 9/06 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/3234 (2013.01)
H04L 63/0272 (2013.01)
(21) 출원번호 10-2018-0112220
(22) 출원일자 2018년09월19일
심사청구일자 2018년11월09일

(71) 출원인
시큐리티플랫폼 주식회사
서울특별시 강남구 테헤란로 625 ,16층1610호(삼성동,덕명빌딩)
(72) 발명자
김경모
서울특별시 은평구 진관3로 15-45, 1015-1010 (진관동, 은평뉴타운 구파발)
강호관
서울특별시 강동구 상암로 251, 902동 1206호 (명일동, 고덕주공아파트)
(74) 대리인
특허법인아이피매그나

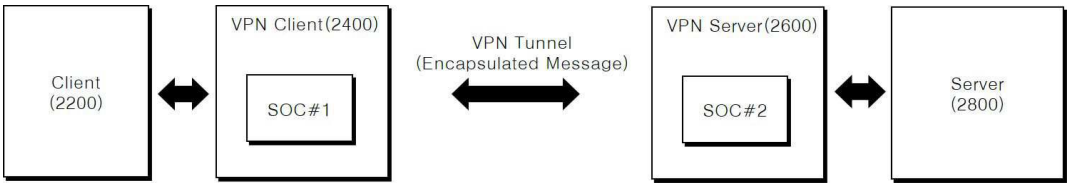
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **가상사설망 기능을 수행하기 위한 시스템 온 칩 및 이를 포함하는 시스템**

(57) 요 약

개시된 일 실시 예에 따른 시스템 온 칩은, TLS(Transport Layer Security) 방식에 기반하여 메시지 암호화 동작을 수행할 수 있다. 시스템 온 칩은, 메시지 암호화 동작을 위해 사용되는 키를 교환하고 통신을 수행할 주체에 대한 인증을 수행하기 위한 인증부, 키를 이용하여 메시지를 암호화하거나 암호화된 메시지를 복호화하는 기능, 키를 암호화하거나 암호화된 키를 복호화하는 기능을 수행하기 위한 AES 엔진 코어, 및 RTOS(Real Time Operating System) 및 메시지 암호화 동작을 수행하기 위한 펌웨어에 기반하여 AES(Advanced Encryption Standard) 엔진 코어 및 인증부를 제어하기 위한 제어부를 포함할 수 있다.

대 표 도 - 도2



(52) CPC특허분류
H04L 63/029 (2013.01)
H04L 63/166 (2013.01)
H04L 9/0631 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/302 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1415161309
부처명 산업통상자원부
연구관리전문기관 한국산업기술진흥원
연구사업명 사업화연계기술개발(R&D)
연구과제명 IoT 기기의 가상사설망 구축을 위한 VPN on Chip 솔루션
기 여 율 1/1
주관기관 시큐리티플랫폼 주식회사
연구기간 2018.04.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

TLS(Transport Layer Security) 기반 메시지 암호화 동작을 수행하기 위한 시스템 온 칩에 있어서,

상기 메시지 암호화 동작을 위해 사용되는 키를 교환하고 통신을 수행할 주체에 대한 인증을 수행하기 위한 인증부;

키를 이용하여 메시지를 암호화하거나 암호화된 상기 메시지를 복호화하는 기능, 상기 키를 암호화하거나 암호화된 상기 키를 복호화하는 기능을 수행하기 위한 AES(Advanced Encryption Standard) 엔진 코어; 및

RTOS(Real Time Operating System) 및 상기 메시지 암호화 동작을 수행하기 위한 펌웨어에 기반하여, 상기 AES 엔진 코어 및 상기 인증부를 제어하기 위한 제어부를 포함하는 시스템 온 칩.

청구항 2

제1항에 있어서,

상기 인증부는, ECDSA(Elliptic Curve Digital Signature Algorithm) 및 RSA(Rivest Shamir Adleman) 알고리즘을 수행하기 위한 회로를 포함하는 시스템 온 칩.

청구항 3

제1항에 있어서,

상기 메시지 암호화 동작을 위해 사용되는 난수를 발생시키기 위한 난수 발생기;

상기 메시지 또는 상기 키를 해시하기 위한 해시부; 및

개인키를 저장하기 위한 개인키 저장부를 더 포함하는 시스템 온 칩.

청구항 4

제3항에 있어서,

상기 AES 엔진 코어, 상기 난수 발생기, 및 상기 해시부를 포함하는 MCU(Micro Controller Unit); 및

상기 인증부 및 상기 개인키 저장부를 포함하는 TPM(Trusted Platform Module)을 포함하는 시스템 온 칩.

청구항 5

제1항에 있어서,

메모리를 더 포함하고,

상기 메모리에는, 상기 RTOS, 상기 펌웨어, 및 X.509 인증서를 발급받기 위한 소프트웨어 어플리케이션이 저장되는 시스템 온 칩.

청구항 6

제1항에 있어서,

상기 펌웨어는, 상기 메시지 암호화 동작을 수행하기 위해 상용 또는 범용 운영체제에서 수행되는 시그널 전달을 상기 RTOS 에서의 메시지 전달로서 대체하기 위한 코드 또는 함수를 포함하는 시스템 온 칩.

청구항 7

제1항에 있어서,

상기 펌웨어에는, 파일 입출력이 가능한 메모리 영역을 지시하는 물리적 또는 논리적 주소에 대한 정보가 기록

되는 시스템 온 칩.

청구항 8

제1항의 시스템 온 칩을 포함하는 전자 디바이스.

청구항 9

가상사설망(Virtual Private Network)을 통해 메시지를 전송하기 위한 시스템에 있어서,

상기 메시지를 생성하기 위한 클라이언트 디바이스;

통신 채널을 통해 상기 클라이언트 디바이스로부터 수신된 메시지에 TLS 기반 암호화 동작을 수행함으로써 캡슐화된 메시지를 출력하기 위한 VPN 클라이언트;

상기 VPN 클라이언트로부터 VPN터널을 통해 상기 캡슐화된 메시지를 수신하고 상기 캡슐화된 메시지를 복호화하기 위한 VPN 서버; 및

상기 VPN 서버로부터 상기 복호화된 메시지를 수신하기 위한 서버를 포함하고,

상기 VPN 클라이언트는, RTOS(Real Time Operating System) 및 펌웨어에 기반하여 상기 TLS 기반 암호화 동작을 수행하기 위한 시스템 온 칩을 포함하는 시스템.

청구항 10

제9항에 있어서,

상기 시스템 온 칩은, MCU(Micro Controller Unit)를 포함하고,

상기 MCU는,

키를 이용하여 메시지를 암호화하거나 암호화된 상기 메시지를 복호화하는 기능, 상기 키를 암호화하거나 암호화된 상기 키를 복호화하는 기능을 수행하기 위한 AES(Advanced Encryption Standard) 엔진 코어;

상기 TLS 기반 암호화 동작을 위해 사용되는 난수를 발생시키기 위한 난수 발생기; 및

상기 메시지 또는 상기 키를 해시하기 위한 해시부를 포함하는 시스템.

청구항 11

제10항에 있어서,

상기 시스템 온 칩은, TPM(Trusted Platform Module)을 더 포함하고,

상기 TPM은,

ECDSA(Elliptic Curve Digital Signature Algorithm) 및 RSA(Rivest Shamir Adleman) 알고리즘을 수행하기 위한 회로; 및

개인키를 저장하기 위한 개인키 저장부를 포함하는 시스템.

청구항 12

제9항에 있어서,

상기 통신 채널은, 이더넷(Ethernet), LTE(Long Term Evolution), USB(Universal Serial Bus) 및 WIFI(Wireless Fidelity) 중 적어도 하나를 포함하는 시스템.

청구항 13

제9항에 있어서,

상기 VPN 클라이언트는, 상기 클라이언트 디바이스에 내장되는 시스템.

청구항 14

제9항에 있어서,

상기 클라이언트 디바이스는, 사물인터넷 디바이스인 시스템.

청구항 15

제9항에 있어서,

상기 펌웨어는, 상기 TLS 기반 암호화 동작을 위해 상용 또는 범용 운영체제에서 수행되는 시그널 전달을 상기 RTOS 에서의 메시지 전달로서 대체하기 위한 코드 또는 함수를 포함하는 시스템.

청구항 16

제9항에 있어서,

상기 펌웨어에는, 파일 입출력이 가능한 메모리 영역을 지시하는 물리적 또는 논리적 주소에 대한 정보가 기록되는 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 전자 디바이스에 관한 것으로, 보다 구체적으로는 가상사설망 기능을 수행하기 위한 시스템 온 칩 및 이를 포함하는 시스템에 관한 것이다.

배 경 기 술

[0002] 사물인터넷(Internet of Things, 이하 IoT) 디바이스에서의 보안 위협이 나날이 증가하고 있다. 예를 들어, 인공지능 로봇 청소기는 인터넷 기반 해킹 위협이나 내장된 카메라를 통해 사용자의 집을 모니터링하는 위험에 노출될 수 있다. 카메라는 사진 또는 동영상을 공격자의 서버로 전송하거나 네트워크를 통해 카메라를 원격 제어하여 임의 촬영할 수 있는 위험에 노출될 수 있다. 또한, 디지털 도어락은 제어기능 탈취로 인한 임의 개폐 위험에 노출될 수도 있다. 따라서, IoT 디바이스에서의 보안 강화 이슈가 대두되고 있다.

[0003] 가상사설망(Virtual Private Network, 이하 VPN)은 공중 네트워크를 통해 회사나 단체가 내용을 외부에 드러내지 않고 통신할 목적으로 사용되는 사설 통신망으로 개발되었다. VPN 은 터널링 프로토콜이라는 특별한 TCP/IP 기반 프로토콜을 사용하여 디바이스들 사이에 보안 채널을 형성할 수 있다. VPN 에서 메시지는 인터넷과 같은 공공망 위에서 표준 프로토콜을 써서 전달되거나, VPN 서비스 제공자와 고객이 서비스 수준 계약을 맺은 후 서비스 제공자의 사설망을 통해 전달될 수 있다.

[0004] VPN 은 윈도우나 리눅스와 같은 상용/범용 운영체제에서 동작하는 소프트웨어 어플리케이션 또는 하드웨어로서 구현될 수 있다. VPN은 높은 수준의 복잡도를 갖는 다양한 암호알고리즘, 키 교환 프로토콜, 및 해쉬 알고리즘 등을 사용하기 때문에 많은 오버헤드를 초래하여 고사양의 프로세서와 메모리를 갖춘 컴퓨팅 환경에서만 동작이 가능하여 제한적으로 사용되었다.

발명의 내용

해결하려는 과제

[0005] VPN 기능을 수행하는 소형화된 시스템 온 칩(System-On-Chip, 이하 SoC)이 제공될 수 있다. 마이크로 컨트롤러 유닛(Micro Controller Unit, 이하 MCU) 기반의 SoC가 전자 디바이스에 탑재되어 VPN 터널을 구현함으로써, 전자 디바이스에서의 보안이 크게 향상될 수 있다.

[0006] 본 실시 예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 이하의 실시 예들로부터 또 다른 기술적 과제들이 유추될 수 있다.

과제의 해결 수단

[0007] TLS(Transport Layer Security) 방식에 기반하여 메시지 암호화 동작을 수행하기 위한 시스템 온 칩에 있어서, 상기 메시지 암호화 동작을 위해 사용되는 키를 교환하고 통신을 수행할 주체에 대한 인증을 수행하기 위한 인

증부, 키를 이용하여 메시지를 암호화하거나 암호화된 상기 메시지를 복호화하는 기능, 상기 키를 암호화하거나 암호화된 상기 키를 복호화하는 기능을 수행하기 위한 AES(Advanced Encryption Standard) 엔진 코어, 및 RTOS(Real Time Operating System) 및 상기 메시지 암호화 동작을 수행하기 위한 펌웨어에 기반하여, 상기 AES 엔진 코어 및 상기 인증부를 제어하기 위한 제어부를 포함할 수 있다.

[0008] 상기 인증부는, ECDSA(Elliptic Curve Digital Signature Algorithm) 및 RSA(Rivest Shamir Adleman) 알고리즘을 수행하기 위한 회로를 포함할 수 있다.

[0009] 상기 시스템 온 칩은 상기 메시지 암호화 동작을 위해 사용되는 난수를 발생시키기 위한 난수 발생기, 상기 메시지 또는 상기 키를 해시하기 위한 해시부, 및 개인키를 저장하기 위한 개인키 저장부를 더 포함할 수 있다.

[0010] 상기 시스템 온 칩은 상기 AES 엔진 코어, 상기 난수 발생기, 및 상기 해시부를 포함하는 MCU(Micro Controller Unit), 및 상기 인증부 및 상기 개인키 저장부를 포함하는 TPM(Trusted Platform Module)을 포함할 수 있다.

[0011] 상기 시스템 온 칩은 메모리를 더 포함하고, 상기 메모리는, 상기 RTOS, 상기 펌웨어, 및 X.509 인증서를 발급받기 위한 소프트웨어 어플리케이션이 저장될 수 있다.

[0012] 상기 펌웨어는, 상용 또는 범용 운영체제에서 수행되는 시그널 전달을 상기 RTOS 에서의 메시지 전달로서 대체하기 위한 코드 또는 함수를 포함할 수 있다.

[0013] 상기 펌웨어는, 파일 입출력이 가능한 메모리 영역을 지시하는 물리적 또는 논리적 주소에 대한 정보를 포함할 수 있다.

[0014] 상기 시스템 온 칩을 포함하는 전자 디바이스가 제공될 수 있다.

[0015] 가상사설망(Virtual Private Network)을 통해 메시지를 전송하기 위한 시스템에 있어서, 상기 메시지를 생성하기 위한 클라이언트 디바이스, 통신 채널을 통해 상기 클라이언트 디바이스로부터 수신된 메시지를 TLS 기반 암호화 동작을 수행함으로써 캡슐화된 메시지를 출력하기 위한 VPN 클라이언트, 상기 VPN 클라이언트로부터 캡슐화된 메시지를 VPN터널을 통해 수신하고 상기 캡슐화된 메시지를 복호화하기 위한 VPN 서버, 및 상기 VPN 서버로부터 상기 복호화된 메시지를 수신하기 위한 서버를 포함하고, 상기 VPN 클라이언트는, RTOS(Real Time Operating System) 및 펌웨어에 기반하여 상기 TLS 기반 암호화 동작을 수행하기 위한 시스템 온 칩을 포함할 수 있다.

[0016] 상기 시스템 온 칩은, MCU(Micro Controller Unit)를 포함하고, 상기 MCU는, 키를 이용하여 메시지를 암호화하거나 암호화된 상기 메시지를 복호화하는 기능, 상기 키를 암호화하거나 암호화된 상기 키를 복호화하는 기능을 수행하기 위한 AES(Advanced Encryption Standard) 엔진 코어, 상기 TLS 기반 암호화 동작을 위해 사용되는 난수를 발생시키기 위한 난수 발생기, 및 상기 메시지 또는 상기 키를 해시하기 위한 해시부를 포함할 수 있다.

[0017] 상기 시스템 온 칩은, TPM(Trusted Platform Module)을 더 포함하고, 상기 TPM은, ECDSA(Elliptic Curve Digital Signature Algorithm) 및 RSA(Rivest Shamir Adleman) 알고리즘을 수행하기 위한 회로, 및 개인키를 저장하기 위한 개인키 저장부를 포함할 수 있다.

[0018] 상기 통신 채널은, 이더넷(Ethernet), LTE(Long Term Evolution), 및 WIFI(Wireless Fidelity) 중 적어도 하나를 포함할 수 있다.

[0019] 상기 VPN 클라이언트는, 상기 클라이언트 디바이스에 내장될 수 있다.

[0020] 상기 클라이언트 디바이스는, 사물인터넷 디바이스일 수 있다.

[0021] 상기 펌웨어는, 상용 또는 범용 운영체제에서 수행되는 시그널 전달을 상기 RTOS 에서의 메시지 전달로서 대체하기 위한 코드 또는 함수를 포함할 수 있다.

[0022] 상기 펌웨어는, 파일 입출력이 가능한 메모리 영역을 지시하는 물리적 또는 논리적 주소에 대한 정보를 포함할 수 있다.

발명의 효과

[0023] VPN 기능을 수행하는 소형화된 SoC가 제공됨으로 인해, IoT 디바이스와 같은 소형화·경량화된 전자 디바이스들 사이 또는 전자 디바이스와 서버 사이에 VPN을 통한 보안 채널을 형성하는 것이 가능하다. VPN 기능을 SoC에 구현하는 솔루션은 국내/국제 CC(Common Criteria) EAL4 등급(국제표준 ISO/IEC 15408) 인증을 통해 보안성을 보

장받을 수 있다.

도면의 간단한 설명

[0024] 도1은 일 실시 예에 따른 TCP/IP 네트워크에서 전송 계층 보안(Transport Layer Security) 에 기반하여 구현된 VPN을 나타낸 것이다.

도2는 일 실시 예에 따라, VPN기능이 임베디드된 SoC를 이용하여 형성된 보안 채널을 나타낸다.

도3은 일 실시 예에 따라, VPN기능을 구현하기 위한 SoC의 블록도를 나타낸다.

도4는 일 실시 예에 따라, VPN기능을 구현하기 위한 SoC의 블록도를 나타낸다.

도5는 일 실시 예에 따라, VPN기능을 구현하기 위한 SoC의 상세한 블록도를 나타낸다.

도6은 일 실시 예에 따라, 도2 내지 5의 SoC 가 내장된 전자 디바이스를 포함하는 시스템을 나타낸다.

도7은 일 실시 예에 따라, 도2 내지 5의 SoC 가 내장된 VPN 장비를 포함하는 시스템을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0025] 아래에서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자들(이하, 통상의 기술자들)이 본 발명을 용이하게 실시할 수 있도록, 첨부되는 도면들을 참조하여 몇몇 실시 예가 명확하고 상세하게 설명될 것이다.

[0026] 명세서에서 사용되는 "부"이라는 용어는 FPGA(field-programmable gate array) 또는 ASIC(application specific integrated circuit)과 같은 하드웨어 구성 요소, 하드웨어 구성 요소들의 집합, 및/또는 회로를 의미할 수 있다.

[0027] TCP/IP(Transmission Control Protocol/Internet Protocol) 통신 프로토콜은 컴퓨터 간의 주고 받는 메시지를 전송할 때 에러가 발생하지 않도록 알맞은 크기로 나누어져 전송하고 이를 받아서 다시 원래의 정보로 변환하는 것을 약속해 놓은 규약이다.

[0028] 전송 계층 보안(Transport Layer Security, 이하 TLS)은 인터넷에서 인증서로 상대방을 인증하고 기밀성과 무결성을 제공하기 위한 보안 소켓 계층(Secure Sockets Layer, SSL)이 표준화된 기술이다. TLS는 TCP/IP 통신 네트워크에 보안 기능을 제공할 수 있다. TLS 는 지원 가능한 알고리즘을 서로 교환하는 제1단계, 암호화 키 교환 및 인증을 수행하는 제2단계, 및 대칭키 암호로 메시지를 암호화하고 메시지를 인증하여 캡슐화된 메시지를 출력하는 제3단계를 포함할 수 있다.

[0029] 도1은 일 실시 예에 따른 TCP/IP 네트워크에서의 TLS에 기반 VPN을 나타낸 것이다.

[0030] 도1을 참조하면, 시스템(1000)은 클라이언트(1200), VPN 클라이언트(1400), VPN 서버(1600), 및 서버(1800)를 포함할 수 있다.

[0031] 클라이언트(1200)는 서버(1800)와 TCP/IP 프로토콜에 기반하여 메시지를 주고 받는 통신을 수행하기 위한 디바이스를 의미할 수 있다. 일 실시 예에 따라, 클라이언트(1200)는 컴퓨터, 스마트폰, 웨어러블 디바이스, 카메라, 캠코더, TV, 각종 검침기(전력 검침기, 가스, 수도 등), ATM 디바이스, POS 단말기, 차량용 블랙박스, IoT 디바이스 등과 같은 전자 디바이스를 포함할 수 있으나 이에 제한되지 않는다.

[0032] 일 실시 예에 따라, 클라이언트(1200)와 서버(1800)는 각각 가정에 위치한 전력 검침기와 전력 공급자의 서버일 수 있다. 전력 공급자의 서버는, 각 가정에 위치한 검침기로부터 수신된 데이터에 기초하여 공급된 전력에 대한 요금을 산정하고 산정된 요금을 부과할 수 있다.

[0033] 일 실시 예에 따라, 클라이언트(1200)는 IoT 디바이스고 서버(1800)는 IoT 디바이스로부터 데이터를 수집하는 다른 IoT디바이스 또는 서버일 수 있다. 클라이언트(1200)와 서버(1800) 각각은 접근 가능한 유선 또는 무선 인터페이스를 가지며, 유선 또는 무선 인터페이스를 통해 적어도 하나 이상의 다른 디바이스와 통신하여 데이터를 송신 또는 수신할 수 있다.

[0034] 일 실시 예에 따라, 클라이언트(1200)는 IP(Internet Protocol) 카메라이고 서버(1800)는 IP 카메라로부터 영상 데이터를 수집하는 정부 또는 공공기관에서 관리되는 서버일 수 있다.

[0035] TCP/IP 통신에서 보안을 강화하기 위해 VPN이 시스템(1000)에 적용될 수 있다. 도1을 참조하면, 클라이언트(1200)와 서버(1800) 사이에 VPN 터널을 형성하기 위한 VPN 클라이언트(1400)와 VPN 서버(1600)가 위치할 수

있다. VPN 클라이언트(1400)와 VPN 서버(1600)는 TLS 방식에 기초하여 메시지를 암호화하고, 암호화된 메시지를 VPN 터널을 통해 전송할 수 있다. 일 실시 예에 따라, VPN 클라이언트(1400)는 클라이언트(1200)의 내부에 위치하는 하드웨어 모듈을 의미할 수 있다. 또는, VPN 클라이언트(1400)는 클라이언트(1200)의 외부에 위치하는 전자 디바이스(전자 장비) 또는 전자 디바이스 내에 포함된 하드웨어 모듈을 의미할 수 있다.

[0036] 먼저 지원 가능한 알고리즘을 서로 교환하는 단계에서, VPN 클라이언트(1400)와 VPN 서버(1600)는 암호 스위트를 교환할 수 있다. 이 단계에서, 키 교환과 인증에 사용될 암호화 방법, 메시지 인증 코드(MAC)가 결정될 수 있다. 메시지 인증 코드들은 HMAC 해시 함수로 만들 수 있다.

[0037] 키 교환 및 인증 단계에서, 키 교환과 인증 알고리즘은 공개키 방법을 사용하거나 미리 공유된 키(TLS-PSK)를 사용할 수 있다. 일 실시 예에 따라, 키교환 알고리즘은 RSA(Rivest Shamir Adleman), Diffie-Hellman, ECDH(Elliptic-curve Diffie-Hellman), SRP(Secure Remote Password), PSK(Pre Shared Key) 알고리즘을 포함할 수 있다. 일 실시 예에 따른 인증 알고리즘은, RSA, DSA(Digital Signature Algorithm), ECDSA(Elliptic Curve Digital Signature Algorithm)을 포함할 수 있다.

[0038] 메시지 암호화 및 인증 단계에서, 대칭키 암호 알고리즘으로서, RC4, 트리플 DES(Data Encryption Standard), AES(Advanced Encryption Standard), IDEA(International Data Encryption Algorithm), DES, Camellia 알고리즘이 사용될 수 있다. 일 실시 예에 따른 해시 함수는 HMAC-MD5 또는 HMAC-SHA 알고리즘이 사용될 수 있다. 메시지 인증 코드들이 해시 함수에 의해 생성될 수 있다.

[0039] VPN 클라이언트(1400)와 VPN 서버(1600) 각각은 TLS 방식에 기반하여 암호화된 메시지를 전송하고 수신하기 위한 새로운 TCP 와 새로운 IP를 포함할 수 있다. 새로운 TCP 와 IP는 TLS 방식에 기반하여 형성된 VPN 터널에서 사용되는 프로토콜 스택(protocol stack)을 의미할 수 있다.

[0040] 일 실시 예에 따라, VPN 기능을 구현하기 위해 윈도우나 리눅스와 같은 상용/범용 운영 체제가 VPN 클라이언트(1400)와 VPN 서버(1600)에 각각 탑재될 수 있다. 상술한 바와 같이, VPN 기능을 구현하기 위한 동작들은 복잡도가 높고 요구되는 메모리 사용량이 높으므로 고사양의 프로세서와 메모리를 갖춘 컴퓨팅 환경에서 운영 체제의 관리 하에 사용될 수 있다. 이러한 경우, VPN 클라이언트(1400)와 VPN 서버(1600)는 상용/범용 운영 체제에서 동작하는 소프트웨어 어플리케이션이나 상용/범용 운영 체제에 의해 운용되는 하드웨어 모듈의 형태로 제작될 수 있다. 이러한 실시 예에서, VPN 서버(1600)는 클라우드 및 오픈소스 VPN 서버를 포함할 수 있다. 또한, VPN 서버(1600)는 상용 VPN 게이트웨이를 포함할 수 있다.

[0041] 이하, IoT 디바이스 및 웨어러블 디바이스 등과 같이 상용/범용 운영체제가 설치되지 않은 소형화 및 경량화된 전자 디바이스에서 발생될 수 있는 보안 위협을 해소하기 위한 SoC 가 개시된다.

[0042] 도2는 일 실시 예에 따라, VPN 기능이 임베디드된 SoC를 이용하여 형성된 VPN 터널을 나타낸다.

[0043] 도2의 클라이언트(2200), VPN 클라이언트(2400), VPN 서버(2600), 및 서버(2800)는 도1의 클라이언트(1200), VPN 클라이언트(1400), VPN 서버(1600), 및 서버(1800)와 각각 대응될 수 있다. 따라서, 이하 생략되는 내용이라 하더라도 도1의 클라이언트(1200), VPN 클라이언트(1400), VPN 서버(1600), 및 서버(1800)에 관하여 상술된 내용은 도2의 클라이언트(2200), VPN 클라이언트(2400), VPN 서버(2600), 및 서버(2800)에도 적용될 수 있다.

[0044] 일 실시 예에 따라, VPN 클라이언트(2400)는 클라이언트(2200)의 내부 또는 외부에 위치할 수 있다. VPN 클라이언트(2400)는 클라이언트(2200)로부터 통신 경로를 통해 메시지를 수신할 수 있다. 통신 채널은, 이더넷(Ethernet), LTE(Long Term Evolution), USB(Universe Serial Bus), 또는 WIFI(Wireless Fidelity)와 같은 유/무선 인터페이스를 포할 수 있다.

[0045] VPN 클라이언트(2400)는 VPN 클라이언트(2400)에 전원을 공급하기 위한 전원 공급 장치를 포함할 수 있다. 예를 들어, VPN 클라이언트(2400)가 클라이언트(2200)의 외부에 위치하는 경우, VPN 클라이언트(2400)는 VPN 클라이언트(2400)에 전원을 공급하기 위한 전원 공급 장치를 포함할 수 있다. 일 실시 예에 따라, VPN 클라이언트(2400)를 POE(Power Over Ethernet)으로부터 전원을 공급받던 클라이언트(2200)와 연결시키는 구성에 있어서, VPN 클라이언트(2400)가 POE로부터 전원을 대신 공급받고 공급받은 전원을 클라이언트(2200)에게 전달해주기 위해, VPN 클라이언트(2400)에 POE 바이패스(Power Over Ethernet Bypass)가 내장될 수 있다. VPN 클라이언트(2400)가 클라이언트(2200)의 내부에 위치하는 경우, VPN 클라이언트(2400)는 별도의 전원 공급 장치 없이 클라이언트(2200)에 내장된 전원 공급 장치로부터 필요한 전원을 공급받을 수 있다.

[0046] VPN 클라이언트(2400)는 클라이언트(2200)로부터 수신된 메시지를 암호화하고, 암호화된 메시지를 캡슐화함으로

써 VPN 터널을 통해 캡슐화된 메시지를 VPN 서버(2600)로 전송할 수 있다. VPN 서버(2600)는 VPN 터널을 통해 수신된 캡슐화된 메시지를 복호화하여 서버(2800)로 전송할 수 있다.

[0047] 다른 실시 예에 따라, VPN 서버(2600)는 서버(2800)로부터 수신된 메시지를 암호화하고, 암호화된 메시지를 캡슐화함으로써 VPN 터널을 통해 캡슐화된 메시지를 VPN 클라이언트(2400)로 전송할 수 있다. VPN 클라이언트(2400)는 VPN 터널을 통해 수신된 캡슐화된 메시지를 복호화하여 클라이언트(2200)로 전송할 수 있다.

[0048] VPN 클라이언트(2400)와 VPN 서버(2600) 중 적어도 하나는 난수, 암호, 인증, 해쉬 등의 보안기술을 보안 엔진이 탑재된 마이크로 컨트롤러 유닛(Micro Controller Unit, 이하 MCU)에 기반하여 초저가·초경량으로 구현될 수 있는 VPN 기능이 내장된 SoC를 포함할 수 있다.

[0049] 먼저, VPN 클라이언트(2400)는 VPN 기능을 구현하기 위한(또는, VPN 터널을 형성하기 위한) 제1SoC(SoC#1)를 포함할 수 있다. 제1SoC(SoC#1)은 TLS 방식에 기반하여 메시지를 암호화하거나 캡슐화된 메시지를 복호화하는 동작을 수행할 수 있다.

[0050] 제1SoC(SoC#1)은 보안 모듈을 포함하는 적어도 하나의 MCU를 포함할 수 있다. 제1 SoC(SoC#1)은 보안 모듈을 포함하는 적어도 하나의 MCU를 활용하여 리눅스나 윈도우와 같은 운영 체제가 없는 환경(예를 들어, IoT 디바이스)에서 VPN 터널을 형성하도록 할 수 있다. 제1SoC(SoC#1)에는 ARM 사에서 개발한 Coretex-M 에 기반하는 MCU 가 사용될 수 있다. 예를 들어, 제1SoC(SoC#1)은 ST마이크로일렉트로닉스(STMicroelectronics) 사에서 개발한 STM32 MCU를 탑재할 수 있으나 이에 제한되지 않는다.

[0051] VPN 클라이언트(2400)에 의해 출력되는 캡슐화된 메시지는 VPN 서버(2600)로 전송될 수 있다. VPN 서버(2600)는 VPN 클라이언트로부터 캡슐화된 메시지를 수신하고 캡슐화된 메시지를 복호화할 수 있다. VPN 서버(2600) 역시 VPN 기능을 구현하기 위한 제2SoC(SoC#2)를 포함할 수 있다. VPN 서버(2600)에 탑재되는 제2SoC(SoC#2)은 VPN 클라이언트(2400)에 탑재된 제1SoC(SoC#1)와 동일하므로 상세한 설명은 생략한다.

[0052] 도2에는 VPN 서버(2600)가 VPN 클라이언트(2400)와 마찬가지로 VPN 기능 구현을 위한 제2SoC(SoC#2)를 포함하는 것으로 도시하였으나, VPN 서버(2600)는 VPN 기능을 구현하기 위해 제2SoC(SoC#2)을 포함하지 않고 리눅스나 윈도우와 같은 상용/범용 운영 체제에 의해 관리되는 소프트웨어 어플리케이션 또는 하드웨어 모듈을 포함할 수 있다. 즉, VPN 클라이언트(2400)는 제1SoC(SoC#1)로VPN 기능을 구현하되, VPN 서버(2600)는 리눅스나 윈도우와 같은 상용/범용 운영 체제에 의해 관리되는 방식의 VPN 소프트웨어 또는 하드웨어를 포함함으로써 VPN 기능을 구현할 수도 있다. 이와 반대로, VPN 서버(2600)는 제2SoC(SoC#2)로 VPN 기능을 구현하되, VPN 클라이언트(2400)는 리눅스나 윈도우와 같은 상용/범용 운영 체제에 의해 관리되는 방식의 VPN 소프트웨어 또는 하드웨어를 포함함으로써 VPN 기능을 구현할 수도 있다.

[0053] 도3은 일 실시 예에 따라, VPN 기능을 구현하기 위한 SoC의 블록도를 나타낸다.

[0054] 도3의 SoC(3000)는 도2의 제1SoC(SoC#1) 및 제2SoC(SoC#2) 중 어느 하나의 블록도를 나타낼 수 있다. 도3을 참조하면, SoC(3000)는 제어부(3200), 인증부(3400), 및 AES(Advanced Encryption Standard) 엔진 코어(3600)를 포함할 수 있다.

[0055] 제어부(3200)는 SoC(3000)의 전반적인 동작들을 제어함으로써 TLS 기반 메시지 암호화 동작을 수행할 수 있다. 일 실시 예에 따라, 제어부(3200)는 MCU 내의 CPU(Central Processing Unit)과 같은 프로세서 코어를 포함할 수 있다. 제어부(3200)는 RTOS(Real Time Operating System) 및 SoC(3000)에 탑재된 펌웨어에 기반하여 SoC(3000)의 다른 구성 요소들을 제어함으로써 TLS 기반의 암호화 동작을 수행할 수 있다.

[0056] 인증부(3400)는 암호화를 위해 사용되는 키를 교환하고 통신을 수행할 주체에 대한 인증을 수행할 수 있다. 인증부(3400)는 ECDSA(Elliptic Curve Digital Signature Algorithm) 알고리즘 또는 RSA(Rivest Shamir Adleman) 알고리즘과 같은 서명 알고리즘에 기초하여 인증을 수행할 수 있다. 서명 알고리즘은 공개키 알고리즘이라고도 하며, 개인키와 공개키 쌍을 사용하여 인증서를 발급받고 통신 상대방과 신원을 인증하는 동작을 위해 사용될 수 있다.

[0057] 일 실시 예에 따라, 인증부(3400)는 암호칩의 한 종류인 신뢰 플랫폼 모듈(Trusted Platform Module, 이하 TPM)을 SoC(3000)에 포함시킴으로써 구현될 수 있다. TPM은 게이트웨이의 시스템 하드웨어에 통합되어 암호 생성과 저장 등과 같은 암호 관련 작업을 실행하는 마이크로프로세서로, 비밀번호나 소프트웨어 부팅을 위한 데이터 등과 같은 소규모의 민감한 정보를 보호하는 등 하드웨어 기반의 보안을 수행할 수 있다. SoC(3000)에 포함되는 TPM 은, ECDSA 알고리즘 및 RSA 알고리즘을 수행하기 위한 회로를 포함할 수 있다. SoC(3000)에 포함되는

TPM 은 TLS 기반 메시지 암호화 동작에 필요한 복잡도 높은 연산 또는 메모리를 많이 필요로 하는 연산을 수행할 수 있다.

[0058] AES 엔진 코어(3600)는 키를 이용하여 메시지를 암호화하거나 암호화된 메시지를 복호화하는 기능, 키를 암호화하거나 암호화된 키를 복호화하는 기능을 수행할 수 있다. 동일한 암호키를 공유하는 제1파티와 제2파티에 있어서, 제1파티가 암호화한 메시지를 제2파티가 해독할 수 있다. 암호화키를 갖지 않은 제3파티는 메시지를 해독할 수 없다. 일 실시 예에 따라, AES 엔진 코어(3600)는 AES 알고리즘을 수행하기 위한 회로가 탑재된 MCU 를 SoC(3000)에 포함시킴으로써 구현될 수 있다.

[0059] 일 실시 예에 따라, MCU와 TPM 은 인쇄회로기판을 통해 연결될 수 있다. 이러한 경우, SoC(3000)는 인쇄회로기판 형태일 수 있다.

[0060] 도4는 일 실시 예에 따라, VPN 기능을 구현하기 위한 SoC의 블록도를 나타낸다.

[0061] 도4의 SoC(4000)는 도3의 SoC(3000)의 추가적인 실시 예를 나타낸다. SoC(4000)의 제어부(4200), 인증부(4400), 및 AES 엔진 코어(4600)는 도3의 SoC(3000)의 제어부(3200), 인증부(3400), 및 AES 엔진 코어(3600)와 각각 대응될 수 있다.

[0062] 도4를 참조하면, SoC(4000)는 난수발생기(4300), 해시부(4500), 및 개인키 저장부(4700)를 더 포함할 수 있다.

[0063] 난수발생기(4300)는 암호화 동작을 위해 필요한 난수를 발생시킬 수 있다. 발생된 난수는, 확정적 난수와 불확정적 난수를 포함할 수 있다. 불확정적 난수는 진성 난수로 취급될 수 있다. 일 실시 예에 따라, 난수발생기(4300)는 씨드를 사용하여 난수를 발생시키기 위한 알고리즘이 구현된 하드웨어 회로를 포함할 수 있다. 일 실시 예에 따라, 난수발생기(4300)는 난수발생모듈이 탑재된 MCU 를 SoC(4000)에 포함시킴으로써 구현될 수 있다.

[0064] 해시부(4500)는 해시알고리즘을 수행할 수 있다. 해시부(4500)는 SHA-1, SHA-2와 같은 SHA(Secure Hash Algorithm)을 사용하여 메시지, 공개키, 또는 개인키를 해시할 수 있다. 예를 들어, 해시부(4500)는 원본 메시지를 해시하여 32바이트 길이의 요약 값을 생성할 수 있다. 일 실시 예에 따라, 서로 다른 메시지는 서로 다른 요약값으로 해시될 수 있다. 이러한 경우, 원본 메시지 중 일부(예를 들어, 1비트)가 상이하더라도 요약값은 매우 큰 차이를 보일 수 있다. 일 실시 예에 따라, 해시부(4500)는 해시 모듈이 탑재된 MCU 를 SoC(4000)에 포함시킴으로써 구현될 수 있다.

[0065] 개인키 저장부(4700)는 개인키를 저장하기 위한 메모리 공간이다. 암호 알고리즘을 수행하기 위해서는 개인키가 필요한데, 개인키를 외부에 노출시키지 않고 메시지를 암호화하기 위해서는 개인키를 노출시키지 않고 보관하는 것이 중요하다. 일 실시 예에 따라, 개인키 저장부(4700)는 개인키를 저장하기 위한 공간이 탑재된 TPM을 SoC(4000)에 포함시킴으로써 구현될 수 있다.

[0066] 도5는 일 실시 예에 따라, VPN 기능을 구현하기 위한 SoC의 상세한 블록도를 나타낸다.

[0067] 도5의 SoC(5000)은 도4의 SoC(4000)의 추가적인 실시 예를 나타낸다. SoC(5000)의 제어부(5100), AES 엔진 코어(5300), 난수발생기(5400), 해시부(5500), 인증부(5700), 및 개인키 저장부(5800)는 도4의 SoC(4000)의 제어부(4200), AES 엔진 코어(4600), 난수발생기(4300), 해시부(4500), 인증부(4400), 및 개인키 저장부(4700)와 각각 대응될 수 있다.

[0068] 도5를 참조하면 메모리(5200)는 RTOS, 펌웨어, 및 X.509 동작을 수행하기 위한 명령어 집합이 저장될 수 있다. X.509 동작은 공인인증기관(Certification Authority : CA)으로부터 인증서를 발급받는 동작을 의미하는 것으로서, 공개키와 개인키를 분배하는 역할을 수행할 수 있다. 일 실시 예에 따라, 메모리(5200)는 동적 랜덤 액세스 메모리(DRAM), 정적 랜덤 액세스 메모리(SRAM)와 같은 휘발성 메모리, 플래시 메모리, ROM(Read Only Memory), PRAM(Phase-change Random Access Memory), MRAM(Magnetic Random Access Memory), ReRAM(Resistive Random Access Memory), 및 FRAM(Ferroelectrics Random Access Memory)과 같은 비휘발성 메모리를 포함할 수 있다.

[0069] 상술한 바와 같이, 도5의 SoC(5000)는 리눅스, 윈도우, IOS, 안드로이드와 같은 상용 /범용 운영체제가 설치되어 있지 않은 환경에서 동작하므로, RTOS 와 설치된 펌웨어에 기반하여 TLS 기반의 암호화 동작을 수행할 수 있다. 따라서, 일 실시 예에 따라, VPN 기능을 구현하기 위해 필요한 상용/범용 운영체제에서의 시그널(signal) 전달은 SoC(5000)의 RTOS 에서의 메시지 전달로 대체될 수 있다. 예를 들어, 펌웨어는 상용/범용 운영체제에서의 시그널 전달을 RTOS에서의 메시지 전달로 대체하기 위한 코드 또는 함수를 포함할 수 있다. 또한, VPN 기능을 구현하기 위해 필요한 상용/범용 운영체제에서의 파일 입출력(또는, 파일 시스템)을 대체하기 위해, SoC(5000) 내의 지정된 특정 메모리 위치에서만 파일 입출력이 가능하도록 SoC(5000)를 구성할 수 있다. 예를

들어, 펌웨어에는 파일 입출력이 가능한 메모리 영역을 지시하는 물리적 또는 논리적 주소에 대한 정보가 기록될 수 있다.

[0070] 제어부(5100)는 RTOS 및 펌웨어에 기반하여 SoC(5000) 내의 구성 요소들(5200, 5300, 5400, 5500, 5600, 5700, 및 5800)을 제어함으로써 TLS 기반의 암호화 동작을 수행할 수 있다.

[0071] 통신 채널(5600)은 외부(예를 들어, 도2의 클라이언트(2200))로부터 원본 메시지를 수신하기 위한 동작, 원본 메시지를 암호화하여 캡슐화된 메시지(즉, 암호화된 메시지)를 외부(예를 들어, 도2의 VPN 서버(2600))로 출력하는 동작, 외부(예를 들어, 도2의 VPN 서버(2600))로부터 캡슐화된 메시지(즉, 암호화된 메시지)를 수신하는 동작, 캡슐화된 메시지를 복호화하여 외부(예를 들어, 도2의 클라이언트(2200))로 전송하는 동작을 수행하기 위한 유/무선 인터페이스를 의미할 수 있다.

[0072] 예를 들어, 통신 채널(5600)은, 이더넷(Ethernet), USB(Universal Serial Bus), 유선 근거리통신망(Local Area Network; LAN), WIFI(Wireless Fidelity)와 같은 무선 근거리 통신망(Wireless Local Area Network; WLAN), 블루투스(Bluetooth)와 같은 무선 개인 통신망(Wireless Personal Area Network; WPAN), Zigbee, NFC(Near Field Communication), RFID(Radio-frequency identification), PLC(Power Line communication), 또는 3G(3rd Generation), 4G(4th Generation), LTE(Long Term Evolution) 등 이동 통신망(mobile cellular network)에 접속 가능한 모뎀 통신 인터페이스 등을 포함할 수 있다.

[0073] 도6은 일 실시 예에 따라, 도2 내지 5의 SoC 가 내장된 전자 디바이스를 포함하는 시스템을 나타낸다.

[0074] 시스템(6000)은 제1전력검침기(6220)가 위치하는 제1가정집(6200), 제2전력검침기(6420)가 위치하는 제2가정집(6400), 제3전력검침기(6620)가 위치하는 제3가정집(6600), VPN 서버(6800), 및 전력공급자의 서버(6900)를 포함할 수 있다.

[0075] 제1전력검침기(6220), 제2전력검침기(6420), 및 제3전력검침기(6620)는 제1가정집(6200)의 제1전력 사용량 데이터, 제2가정집(6400)의 제2전력 사용량 데이터, 및 제3가정집(6600)의 제3전력 사용량 데이터를 유선 또는 무선 통신 인터페이스에 기반하여 전력공급자의 서버(6900)로 각각 전송할 수 있다.

[0076] 제1전력검침기(6220), 제2전력검침기(6420), 및 제3전력검침기(6620) 각각은 전력 사용량 데이터에 대한 해킹 위험, 전력 사용량 데이터의 변경 및 조작 위험과 같은 보안 위협에 노출될 수 있다. 따라서, 제1전력검침기(6220), 제2전력검침기(6420), 및 제3전력검침기(6620) 각각은 전력 사용량 데이터를 VPN 터널을 통해 안전하게 전력공급자의 서버(6900)로 전송할 수 있다.

[0077] 제1전력검침기(6220), 제2전력검침기(6420), 및 제3전력검침기(6620) 각각에는 도2 내지 5를 참조하여 상술한 SoC가 내장될 수 있다. 전력검침기는, 리눅스와 윈도우와 같은 상용/범용 운영 체제가 탑재되기 어려운 소형화 디바이스로서, 도2 내지 5를 참조하여 상술한 소형화된 SoC를 내장함으로써 VPN 기능을 구현할 수 있다.

[0078] 예를 들어, 도3의 SoC(3000)가 제1전력검침기(6220)에 내장되어, 제1전력 사용량 데이터를 TLS 기반 암호화 알고리즘에 기초하여 암호화하고, 캡슐화된 제1전력 사용량 데이터를 VPN 터널을 통해 VPN 서버(6800)로 출력할 수 있다. VPN 서버(6800)는 캡슐화된 제1전력 사용량 데이터를 복호화하여 전력공급자의 서버(6900)로 전송할 수 있다.

[0079] 제2전력 사용량 데이터와 제3전력 사용량 데이터 역시 제1전력 사용량 데이터와 동일한 방식으로 해킹이나 위조, 변조의 위험 없이 안전하게 서버(6900)로 전송될 수 있다.

[0080] 도7은 일 실시 예에 따라, 도2 내지 5의 SoC 가 내장된 VPN 장비를 포함하는 시스템을 나타낸다.

[0081] 시스템(7000)은 IP 카메라(7200) 및 IP 카메라(7200)와 연결된 제1VPN장비(7300), IoT 디바이스들(7400) 및 IoT 디바이스들(7400)과 연결된 제2VPN장비(7500), 제조 장비(7600) 및 제조 장비(7600)와 연결된 제3VPN장비(7700), 제1VPN장비(7300), 제2VPN장비(7500), 및 제3VPN장비(7700)와 연결된 PoE(Power Over Ethernet) 스위치(7800), 및 PoE 스위치(7800)와 연결된 VPN 서버(7900)를 포함할 수 있다.

[0082] 제1VPN장비(7300), 제2VPN장비(7500), 및 제3VPN장비(7700) 각각은 도2 내지 도5의 SoC가 내장된 장비로서, 수신된 데이터를 암호화하여 캡슐화된 데이터를 VPN 터널을 통해 PoE 스위치(7800)로 전송할 수 있다.

[0083] 예를 들어, 제1VPN장비(7300)는 IP 카메라(7200)로부터 수신되는 영상 데이터를 암호화하여 이를 PoE 스위치(7800)로 전송할 수 있다. 일 실시 예에 따라, 제1VPN장비(7300)는 IP 카메라(7200)의 외부에 위치하며 통신 채널을 통해 영상 데이터를 수신할 수 있다. 예를 들어, 제1VPN장비(7300)에는 이더넷 포트가 구비될 수 있으며,

제1VPN장비(7300)는 이더넷 포트를 통해 IP 카메라(7200)로부터 영상 데이터를 수신할 수 있다. 일 실시 예에 따라, 제1VPN장비(7300)는 영상 데이터를 처리할 수 있도록 이더넷과 USB 2.0 에 기반한 고속 인터페이스(예를 들어, 10Mbps 이상)를 적어도 하나 포함할 수 있다.

[0084] 제2VPN장비(7500)는 IoT 디바이스들(7400)로부터 수신되는 IoT 데이터를 암호화하여 이를 PoE 스위치(7800)로 전송할 수 있다. 일 실시 예에 따라, 제2VPN장비(7500)는 IoT 디바이스들(7400)의 외부에 위치하며 통신 채널을 통해 IoT 데이터를 수신할 수 있다. 예를 들어, 제2VPN장비(7500)에는 블루투스 인터페이스가 구비될 수 있으며, 제2VPN장비(7500)는 블루투스 인터페이스를 통해 IoT 디바이스들(7400)로부터 IoT 데이터를 수신할 수 있다.

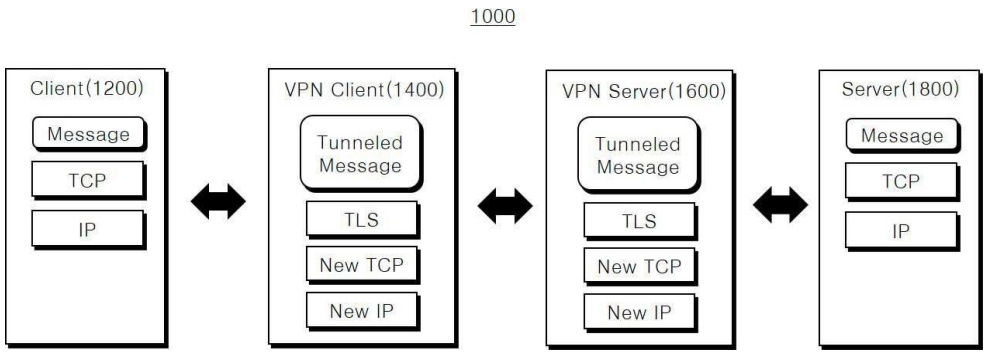
[0085] 제3VPN장비(7700)는 제조 장비(7600)로부터 수신되는 다양한 데이터를 암호화하여 이를 PoE 스위치(7800)로 전송할 수 있다. 일 실시 예에 따라, 제3VPN장비(7700)는 제조 장비(7600)의 외부에 위치하며 통신 채널을 통해 다양한 데이터를 수신할 수 있다. 예를 들어, 제3VPN장비(7700)에는 이더넷 포트가 구비될 수 있으며, 제3VPN장비(7700)는 이더넷 포트를 통해 제조 장비(7600)로부터 다양한 데이터를 수신할 수 있다.

[0086] PoE 스위치(7800)는 제1VPN장비(7300), 제2VPN장비(7500), 및 제3VPN장비(7700)로부터 수신된 데이터를 VPN 터널을 통해 VPN 서버(7900)로 전송할 수 있다.

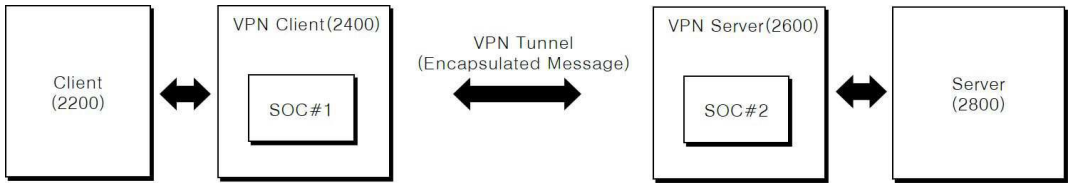
[0087] 위 설명들은 본 발명을 구현하기 위한 예시적인 구성들 및 동작들을 제공하도록 의도된다. 본 발명의 기술 사상은 위에서 설명된 실시 예들뿐만 아니라, 위 실시 예들을 단순하게 변경하거나 수정하여 얻어질 수 있는 구현들도 포함할 것이다. 또한, 본 발명의 기술 사상은 위에서 설명된 실시 예들을 앞으로 용이하게 변경하거나 수정하여 달성될 수 있는 구현들도 포함할 것이다.

도면

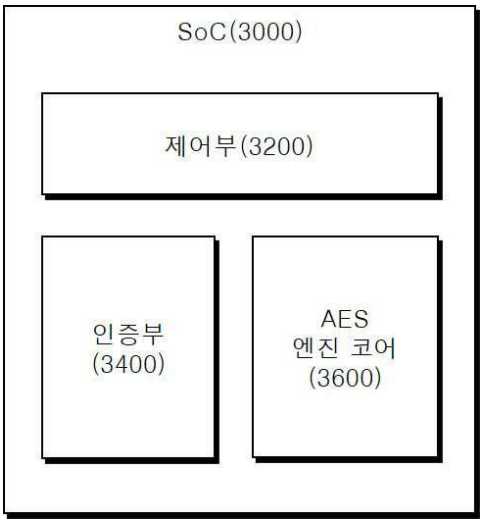
도면1



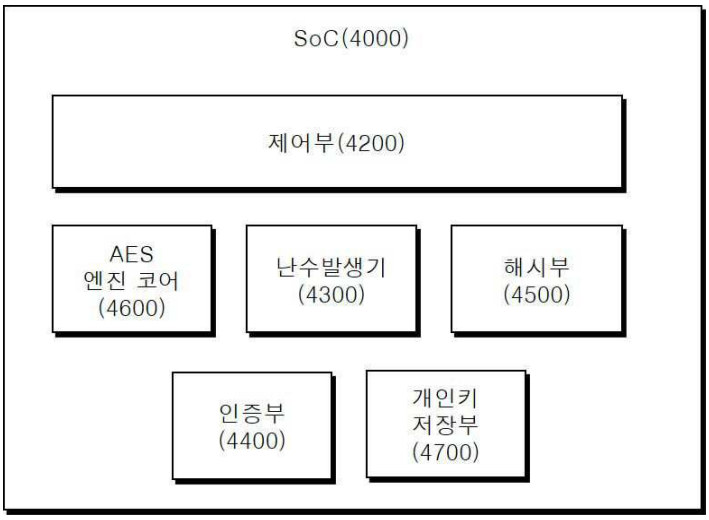
도면2



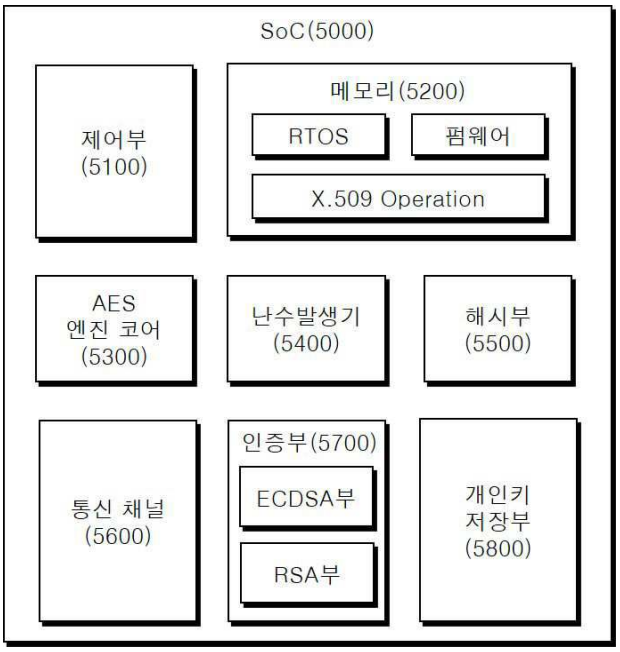
도면3


SoC(3000)
제어부(3200)
인증부
(3400)
AES
엔진 코어
(3600)

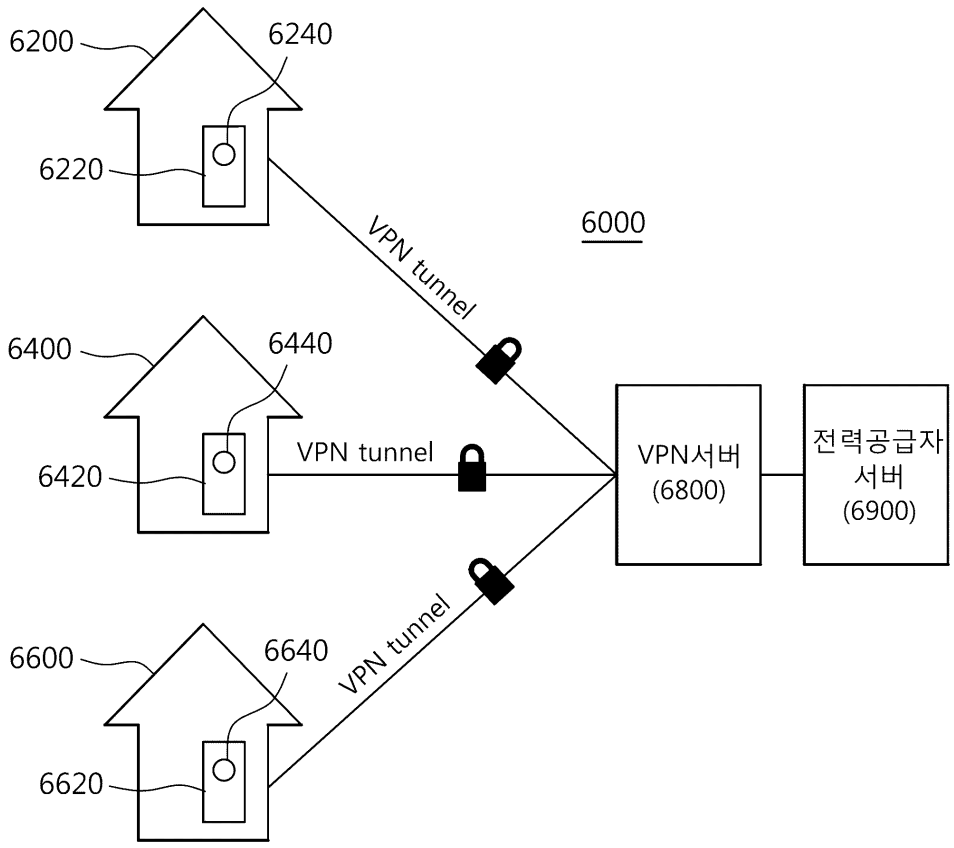
도면4


SoC(4000)
제어부(4200)
AES
엔진 코어
(4600)
난수발생기
(4300)
해시부
(4500)
인증부
(4400)
개인키
저장부
(4700)

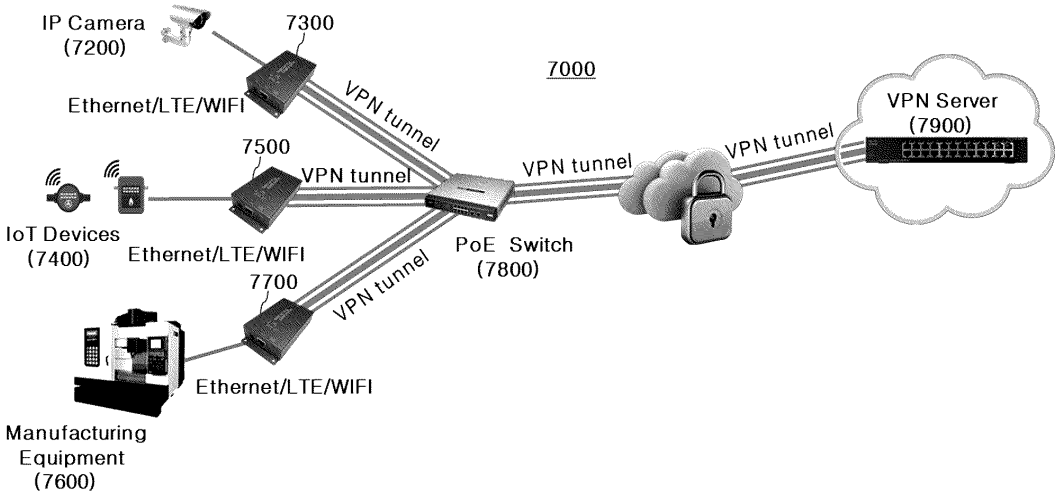
도면5


SoC(5000)
제어부
(5100)
메모리(5200)
RTOS
펌웨어
X.509 Operation
AES
엔진 코어
(5300)
난수발생기
(5400)
해시부
(5500)
통신 채널
(5600)
인증부(5700)
ECDSA부
RSA부
개인키
저장부
(5800)

도면6


6200
6240
6220
6000
VPN tunnel
6400
6440
VPN tunnel
6420
VPN서버
(6800)
전력공급자
서버
(6900)
6600
6640
VPN tunnel
6620

도면7


IP Camera
(7200)
7300
Ethernet/LTE/WIFI
VPN tunnel
7000
VPN Server
(7900)
7500
VPN tunnel
VPN tunnel
VPN tunnel
IoT Devices
(7400)
Ethernet/LTE/WIFI
PoE Switch
(7800)
7700
VPN tunnel
Ethernet/LTE/WIFI
Manufacturing
Equipment
(7600)