(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년06월20일
(11) 등록번호 10-1745482
(24) 등록일자 2017년06월02일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04L 9/30* (2006.01)
H04L 9/32 (2006.01) *H04W 12/04* (2009.01)
H04W 12/10 (2009.01)
(52) CPC특허분류
H04W 12/08 (2013.01)
H04L 9/30 (2013.01)
(21) 출원번호 10-2015-0082721
(22) 출원일자 2015년06월11일
심사청구일자 2015년06월11일
(65) 공개번호 10-2016-0146090
(43) 공개일자 2016년12월21일
(56) 선행기술조사문헌
KR1020030061512 A*
KR100690417 B1*
KR100596400 B1
KR100521570 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
아주대학교산학협력단
경기도 수원시 영통구 월드컵로 206 (원천동)
(72) 발명자
곽진
충청남도 천안시 서북구 한들3로 100, 101동 1401호 (백석동, 백석마을아이파크아파트)
류호석
경기도 의왕시 모락로 89-16, 104동 203호 (오전동, 신원수선화아파트)
(74) 대리인
특허법인 제나

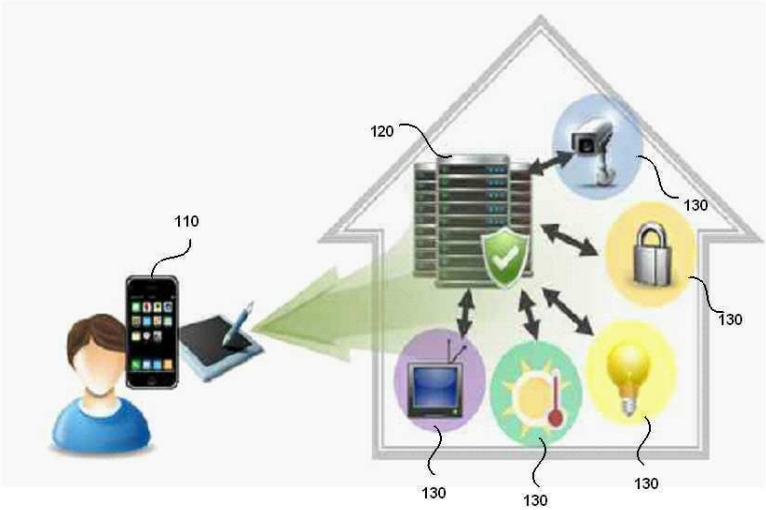
전체 청구항 수 : 총 8 항 심사관 : 안병일

(54) 발명의 명칭 **스마트홈 시스템에서의 통신 방법 및 그 장치**

(57) 요 약

스마트홈 시스템에서의 통신 방법 및 그 장치가 개시된다. 서버에서의 데이터 통신 방법은, 모바일 단말로부터 서버 공개키로 암호화된 데이터 요청을 수신하는 단계; 상기 서버의 서버 공개키에 대응하는 제1 서버 비밀키로 상기 암호화된 데이터 요청을 복호한 후 상기 데이터 요청을 제2 서버 비밀키로 암호화하여 스마트 디바이스로 전송하는 단계; 및 상기 스마트 디바이스로부터 상기 데이터 요청에 상응하여 상기 제2 서버 비밀키로 암호화된 데이터를 수신하고, 상기 제2 서버 비밀키로 상기 암호화된 데이터를 복호한 후 단말 공개키로 암호화하여 상기 모바일 단말로 전송하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3236 (2013.01)
H04W 12/04 (2013.01)
H04W 12/10 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2014R1A2A1A11050818
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 중간연구자지원사업(도약-전략)
연구과제명 IoT 환경에서의 통합 보안 프레임워크 기술 개발
기 여 율 1/1
주관기관 아주대학교
연구기간 2014.11.01 ~ 2017.10.31
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

서버에서의 데이터 통신 방법에 있어서,

(a) 모바일 단말로부터 단말 정보를 등록받고, 상기 서버 공개키를 상기 모바일 단말로 전송하며, 상기 모바일 단말로부터 단말 공개키를 수신하는 단계;

(b) 모바일 단말로부터 서버 공개키로 암호화된 데이터 요청을 수신하는 단계;

(c) 상기 서버의 서버 공개키에 대응하는 제1 서버 비밀키로 상기 암호화된 데이터 요청을 복호한 후 상기 데이터 요청을 제2 서버 비밀키로 암호화하여 스마트 디바이스로 전송하는 단계; 및

(d) 상기 스마트 디바이스로부터 상기 데이터 요청에 상응하여 상기 제2 서버 비밀키로 암호화된 데이터를 수신하고, 상기 제2 서버 비밀키로 상기 암호화된 데이터를 복호한 후 단말 공개키로 암호화하여 상기 모바일 단말로 전송하는 단계를 포함하는 데이터 통신 방법.

청구항 2

제1 항에 있어서,

상기 암호화된 데이터 요청은 데이터 요청 메시지, 상기 모바일 단말의 단말 정보, 임의의 난수값 및 모바일 단말 서명값 중 적어도 하나를 포함하는 것을 특징으로 하는 데이터 통신 방법.

청구항 3

제2 항에 있어서,

상기 (c) 단계는,

상기 복호된 데이터 요청에서 상기 단말 정보를 추출한 후 기등록된 단말 정보와의 일치 여부를 확인하여 상기 모바일 단말을 인증한 후 인증이 성공하면 수행되는 것을 특징으로 하는 데이터 통신 방법.

청구항 4

제2 항에 있어서,

상기 (d) 단계의 상기 단말 공개키로 암호화된 데이터는 상기 데이터 요청에 상응하는 데이터와 상기 난수값을 연접하여 해쉬한 결과값을 더 포함하되,

상기 (d) 단계 이후에,

상기 모바일 단말은 단말 공개키로 상기 암호화된 데이터를 복호한 후, 상기 복호된 데이터와 상기 난수값을 연접하여 해쉬한 결과값과 상기 암호화된 데이터에 포함된 결과값을 비교하여 상기 데이터의 무결성을 검증하는 것을 특징으로 하는 데이터 통신 방법.

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

스마트홈 환경에서 모바일 단말과 스마트 디바이스간의 통신을 위한 서버에 있어서,

모바일 단말로부터 서버 공개키로 암호화된 데이터 요청을 수신한 후 상기 서버의 서버 공개키에 대응하는 제1 서버 비밀키로 복호하고, 상기 데이터 요청에 포함된 단말 정보와 기등록된 단말 정보를 이용하여 상기 모바일 단말을 인증하는 인증부; 및

상기 인증부의 인증 결과 인증 성공이면, 상기 복호된 데이터 요청을 제2 서버 비밀키로 암호화하여 상기 스마트 디바이스로 전송하고, 상기 스마트 디바이스로부터 상기 데이터 요청에 상응하여 상기 제2 서버 비밀키로 암호화된 데이터를 수신한 후 상기 제2 서버 비밀키로 상기 암호화된 데이터를 복호한 후 단말 공개키로 상기 복호된 데이터를 암호화하여 상기 모바일 단말로 전송하는 데이터 전송부를 포함하는 서버.

청구항 11

제10 항에 있어서,

상기 암호화된 데이터 요청은 데이터 요청 메시지, 임의의 난수값 및 모바일 단말 서명값 중 적어도 하나를 더 포함하는 것을 특징으로 하는 서버.

청구항 12

제11 항에 있어서,

상기 단말 공개키로 암호화된 데이터는 상기 데이터 요청에 상응하는 데이터와 상기 난수값을 연접하여 해쉬한 결과값을 더 포함하되,

상기 모바일 단말은 단말 비밀키로 상기 암호화된 데이터를 복호한 후, 상기 복호된 데이터와 상기 난수값을 연접하여 해쉬한 결과값과 상기 암호화된 데이터에 포함된 결과값을 비교하여 상기 데이터의 무결성을 검증하는 것을 특징으로 하는 서버.

청구항 13

제10 항에 있어서,

상기 모바일 단말로부터 단말 정보를 등록받고, 상기 서버 공개키를 상기 모바일 단말로 전송하며, 상기 모바일 단말로부터 단말 공개키를 수신하는 단말 등록 과정을 선행하는 것을 특징으로 하는 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 스마트홈 환경에서 안전한 통신 방법 및 그 장치에 관한 것이다.

배 경 기 술

[0002] 정보통신기술의 발달로 주변 사물은 지능화, 네트워크화 되었고 인간 생활에서 유비쿼터스 사회는 현실로 다가왔다. 유비쿼터스 사회의 실현은 IoT(Internet of Things)를 통해 가속화되고 있다. 스마트홈은 가전기기가 네트워크로 연결되어 사람에게 편리하고 유용한 서비스를 제공하는 가정환경을 의미한다. IoT를 통해 스마트홈의 기술과 서비스는 빠르게 발전하고 다양해지고 있다.

[0003] 스마트홈는 스마트폰, 스마트 TV의 스마트 디바이스의 발달로 다양한 가전제품과 전기, 통신, 복지 등 영향을 미치게 되었다. 또한 스마트 디바이스의 발달과 증가로 헬스케어 서비스, 환경 서비스, 모니터링 서비스 등 스마트홈의 서비스는 다양해졌다. 스마트홈의 상호적 통신을 위해 스마트 디바이스 간의 네트워크 통신을 기반으로 연결망을 구축하고 있다. 사용자가 필요한 자원을 관리하고 외부에서도 사용자가 원하는 스마트홈 데이터를 네트워크 통신을 통해 제공받는다.

[0004] 하지만 다양한 스마트 디바이스 및 네트워크 통신으로 인해 새로운 보안 위협들이 발생하게 되었으며 이로 인한 보안사고가 많이 증가하고 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국공개특허 10-2008-0005344호(2008.01.11.)

발명의 내용

해결하려는 과제

[0006] 본 발명은 스마트홈 환경에서 안전한 통신 방법 및 그 장치를 제공하기 위한 것이다.

[0007] 또한, 본 발명은 스마트홈에서의 스마트 디바이스들을 인증하고 외부의 접근을 차단하여 안전하게 데이터를 전달할 수 있는 스마트홈 환경에서의 통신 방법 및 그 장치를 제공하기 위한 것이다.

[0008] 또한, 본 발명은 데이터 위변조를 사전에 차단할 수 있으며, 난수를 기반으로 한 해쉬한 결과값을 이용하여 전송받은 데이터의 무결성을 검증할 수 있는 스마트홈 환경에서의 통신 방법 및 그 장치를 제공하기 위한 것이다.

과제의 해결 수단

[0009] 본 발명의 일 측면에 따르면, 스마트홈 환경에서 안전한 통신 방법이 제공된다.

[0010] 본 발명의 일 실시예에 따르면, 서버에서의 데이터 통신 방법에 있어서, (a) 모바일 단말로부터 서버 공개키로 암호화된 데이터 요청을 수신하는 단계; (b) 상기 서버의 제1 서버 비밀키로 상기 암호화된 데이터 요청을 복호한 후 상기 데이터 요청을 제2 서버 비밀키로 암호화하여 스마트 디바이스로 전송하는 단계; 및 (c) 상기 스마트 디바이스로부터 상기 데이터 요청에 상응하여 상기 제2 서버 비밀키로 암호화된 데이터를 수신하고, 상기 제2 서버 비밀키로 상기 암호화된 데이터를 복호한 후 단말 공개키로 암호화하여 상기 모바일 단말로 전송하는 단계를 포함하는 데이터 통신 방법이 제공될 수 있다.

[0011] 상기 암호화된 데이터 요청은 데이터 요청 메시지, 상기 모바일 단말의 단말 정보, 임의의 난수값 및 모바일 단말 서명값 중 적어도 하나를 포함할 수 있다.

[0012] 상기 (b) 단계는, 상기 복호된 데이터 요청에서 상기 단말 정보를 추출한 후 기등록된 단말 정보와의 일치 여부를 확인하여 상기 모바일 단말을 인증한 후 인증이 성공하면 수행될 수 있다.

[0013] 상기 (c) 단계의 상기 단말 공개키로 암호화된 데이터는 상기 데이터 요청에 상응하는 데이터와 상기 난수값을 연접하여 해쉬한 결과값을 더 포함하되, 상기 (c) 단계 이후에, 상기 모바일 단말은 상기 단말 공개키에 대응하는 단말 비밀키를 이용하여 상기 암호화된 데이터를 복호한 후, 상기 복호된 데이터와 상기 난숙값을 연접하여 해쉬한 결과값과 상기 암호화된 데이터에 포함된 결과값을 비교하여 상기 데이터의 무결성을 검증할 수 있다.

[0014] 상기 (a) 단계 이전에, 상기 모바일 단말로부터 단말 정보를 등록받고, 상기 서버 공개키를 상기 모바일 단말로 전송하며, 상기 모바일 단말로부터 단말 공개키를 수신하는 단말 등록 과정을 선행할 수 있다.

[0015] 본 발명의 다른 실시예에 따르면, 모바일 단말의 데이터 통신 방법에 있어서, 데이터 요청 메시지, 상기 모바일 단말의 단말 정보, 임의의 난수값 및 모바일 단말 서명값 중 적어도 하나를 포함하는 데이터 요청을 서버 공개키로 암호화하여 서버로 전송하는 단계; 상기 서버로부터 상기 데이터 요청에 상응하는 데이터와 상기 난수값을 연접하여 해쉬한 결과값과 데이터를 단말 공개키로 암호화한 데이터를 수신하는 단계; 및 상기 단말 비밀키로 상기 암호화된 데이터를 복호하고, 상기 복호된 데이터와 상기 난수값을 연접하여 해쉬한 결과값과 상기 암호화된 데이터에 포함된 결과값의 일치여부를 비교하여 상기 데이터의 무결성을 검증하는 단계를 포함하는 데이터 통신 방법이 제공될 수 있다.

[0016] 상기 암호화된 데이터 요청을 전송하는 단계 이전에, 상기 서버로 상기 모바일 단말의 단말 정보를 등록한 후 상기 서버로부터 상기 서버 공개키를 수신하고, 상기 모바일 단말의 단말 공개키를 상기 서버로 전송하는 단말 등록하는 단계를 선행할 수 있다.

[0017] 본 발명의 또 다른 실시예에 따르면, 스마트 디바이스에서의 데이터 통신 방법에 있어서, 서버로부터 비밀키로 암호화된 모바일 단말의 데이터 요청을 수신하는 단계-상기 암호화된 데이터 요청은 난수값을 포함함; 및 기수신한 비밀키로 상기 암호화된 데이터 요청을 복호한 후 상기 데이터 요청에 따른 데이터와 상기 난수값을 연접하여 해쉬한 결과값과 상기 데이터를 상기 비밀키로 암호화하여 상기 서버를 통해 상기 모바일 단말로 전송 요청하는 단계를 포함하되, 상기 서버는 상기 비밀키로 상기 암호화된 데이터를 복호한 후 단말 공개키로 상기 데이터와 상기 해쉬한 결과값을 암호화하여 상기 단말로 전송하는 것을 특징으로 하는 데이터 통신 방법이 제공될 수 있다.

[0018] 상기 데이터 요청을 수신하는 단계 이전에, 상기 스마트 디바이스의 디바이스 정보를 등록한 후 상기 비밀키를 상기 서버로부터 수신하는 디바이스 등록 단계를 포함할 수 있다.

[0019] 본 발명의 다른 측면에 따르면, 스마트홈 환경에서 안전한 통신 방법을 제공하는 장치가 제공된다.

[0020] 본 발명의 일 실시예에 따르면, 스마트홈 환경에서 모바일 단말과 스마트 디바이스간의 통신을 위한 서버에 있어서, 모바일 단말로부터 서버 공개키로 암호화된 데이터 요청을 수신한 후 상기 서버의 제1 서버 비밀키로 복호하고, 상기 데이터 요청에 포함된 단말 정보와 기등록된 단말 정보를 이용하여 상기 모바일 단말을 인증하는 인증부; 및 상기 인증부의 인증 결과 인증 성공이면, 상기 복호된 데이터 요청을 제2 서버 비밀키로 암호화하여 상기 스마트 디바이스로 전송하고, 상기 스마트 디바이스로부터 상기 데이터 요청에 상응하여 상기 제2 서버 비밀키로 암호화된 데이터를 수신한 후 상기 제2 서버 비밀키로 상기 암호화된 데이터를 복호한 후 단말 공개키로 상기 복호된 데이터를 암호화하여 상기 모바일 단말로 전송하는 데이터 전송부를 포함하는 서버가 제공될 수 있다.

[0021] 상기 암호화된 데이터 요청은 데이터 요청 메시지, 임의의 난수값 및 모바일 단말 서명값 중 적어도 하나를 더 포함할 수 있다.

[0022] 상기 단말 공개키로 암호화된 데이터는 상기 데이터 요청에 상응하는 데이터를 상기 난수값으로 해쉬한 결과값을 더 포함하되, 상기 모바일 단말은 단말 공개키에 대응하는 단말 비밀키를 이용하여 상기 암호화된 데이터를 복호한 후, 상기 복호된 데이터와 상기 난수값을 연접하여 해쉬한 결과값과 상기 암호화된 데이터에 포함된 결과값을 비교하여 상기 데이터의 무결성을 검증할 수 있다.

[0023] 상기 모바일 단말로부터 단말 정보를 등록받고, 상기 서버 공개키를 상기 모바일 단말로 전송하며, 상기 모바일 단말로부터 단말 공개키를 수신하는 단말 등록 과정을 선행할 수 있다.

발명의 효과

[0024] 본 발명의 일 실시예에 따른 스마트홈 환경에서의 통신 방법 및 그 장치를 제공함으로써, 스마트홈에서의 스마트 디바이스들을 인증하고 외부의 접근을 차단하여 안전하게 데이터를 전달할 수 있는 이점이 있다.

[0025] 이를 통해, 본 발명은 데이터 위변조를 사전에 차단할 수 있으며, 난수를 기반으로 한 해쉬한 결과값을 이용하여 전송받은 데이터의 무결성을 검증할 수 있는 이점이 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명의 일 실시예에 따른 스마트홈 시스템의 구조를 개략적으로 도시한 도면.

도 2는 본 발명의 일 실시예에 따른 스마트홈 시스템내의 서버에 모바일 단말을 등록하는 과정을 나타낸 흐름도.

도 3은 본 발명의 일 실시예에 따른 스마트홈 시스템의 통신 방법을 나타낸 흐름도.

도 4는 본 발명의 일 실시예에 따른 서버의 내부 구성을 개략적으로 도시한 블록도.

도 5는 본 발명의 일 실시예에 따른 모바일 단말의 내부 구성을 개략적으로 도시한 블록도.

도 6은 본 발명의 일 실시예에 따른 스마트 디바이스의 내부 구성을 개략적으로 도시한 블록도.

발명을 실시하기 위한 구체적인 내용

[0027] 본 발명은 다양한 변환을 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 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0028] 본 발명을 설명함에 있어서, 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 본 명세서의 설명 과정에서 이용되는 숫자(예를 들어, 제1, 제2 등)는 하나의 구성요소를 다른 구성요소와 구분하기 위한 식별기호에 불과하다.

[0029] 또한, 본 명세서에서, 일 구성요소가 다른 구성요소와 "연결된다" 거나 "접속된다" 등으로 언급된 때에는, 상기 일 구성요소가 상기 다른 구성요소와 직접 연결되거나 또는 직접 접속될 수도 있지만, 특별히 반대되는 기재가 존재하지 않는 이상, 중간에 또 다른 구성요소를 매개하여 연결되거나 또는 접속될 수도 있다고 이해되어야 할 것이다.

[0030] 이하, 첨부된 도면들을 참조하여 본 발명의 실시예를 상세히 설명한다.

[0031] 도 1은 본 발명의 일 실시예에 따른 스마트홈 시스템의 구조를 개략적으로 도시한 도면이다.

[0032] 도 1을 참조하면, 본 발명의 일 실시예에 따른 스마트홈 시스템은 모바일 단말(110), 서버(120) 및 복수의 스마트 디바이스(130)를 포함하여 구성된다.

[0033] 모바일 단말(110)은 외부에서 스마트홈 시스템에 접속하여 데이터를 요청하기 위한 주체이다.

[0034] 모바일 단말(110)은 예를 들어, 이동통신 단말기, 노트북과 같은 휴대용 단말일 수 있다.

[0035] 모바일 단말(110)은 스마트홈 시스템에 접속하기 위해, 사전에 댁내 통신을 담당하는 서버(120)에 단말 정보를 등록한 후 서버(120)와 각자의 공개키를 교환하는 등록 과정을 선행할 수도 있다.

[0036] 또한, 모바일 단말(110)은 댁내 존재하는 스마트 디바이스(130)와의 통신을 위해 서버(120)와 통신을 요청할 수 있다. 이때, 모바일 단말(110)과 서버(120)는 각자 공유한 공개키를 이용하여 데이터 통신을 수행할 수 있다.

[0037] 서버(120)는 스마트홈내(댁내)에 존재하는 서버로, 모바일 단말(110)과는 비대칭키로 통신하고, 스마트홈내(댁내)에서는 대칭키로 스마트 디바이스(130)와 통신하여 스마트홈 환경에서 안전하게 모바일 단말(110)과 스마트 디바이스(130)간의 통신을 제공하는 주체이다. 이에 대해서는 하기에서 도 3에 의해 보다 명확하게 이해될 것이다.

[0038] 스마트 디바이스(130)는 스마트홈내(댁내)에 존재하는 다양한 기기로, 서버(120)와 대칭키로 통신하는 장치이다.

[0039] 스마트 디바이스(130)의 유형으로는 냉장고, TV, 댁내 전화기, 조명, 오디오 등과 같은 스마트홈내에 존재하는 다양한 기기일 수 있다.

[0040] 본 명세서에서는 별도로 상세히 설명되어 있지는 않으나, 스마트 디바이스(130)는 스마트홈 시스템에서의 통신을 위해, 최초 서버(120)에 스마트 디바이스를 등록하는 과정을 수행할 수 있다. 이때, 스마트 디바이스는 당해 스마트 디바이스의 기기 정보를 서버(120)에 등록하고, 서버(120)로부터 비밀키(대칭키)를 공유받을 수 있다.

[0041] 본 발명의 일 실시예에 따른 스마트 디바이스(130)는 스마트홈 시스템에서의 데이터 통신시 서버(120)로부터 제공받은 비밀키로 데이터를 암호화하여 전송하므로, 사전에 등록되지 않은 비인가된 디바이스의 접근을 차단할 수 있는 이점이 있다.

[0042] 도 2는 본 발명의 일 실시예에 따른 스마트홈 시스템내의 서버에 모바일 단말을 등록하는 과정을 나타낸 흐름도이다.

[0043] 단계 210에서 서버(120)는 사용자로부터 모바일 단말의 단말정보를 등록받는다. 여기서, 모바일 단말의 단말정보는 모바일 단말의 시리얼 번호 및 식별정보(예를 들어, 전화번호) 중 적어도 하나일 수 있다.

[0044] 즉, 서버(120)는 모바일 단말(110)이 아닌 다른 장치를 이용하여 모바일 단말의 단말 정보를 등록받을 수 있다.

[0045] 다른 예를 들어, 모바일 단말(110)은 사전 등록된 사용자 계정(예를 들어, 아이디 및 패스워드)을 이용하여 서버(120)에 접속한 후 서버(120)에 당해 모바일 단말(110)의 단말 정보를 등록할 수도 있다.

[0046] 단계 215에서 모바일 단말(110)은 서버(120)로 접속 요청을 전송한다. 이때, 접속 요청은 모바일 단말(110)의 단말 정보를 포함한다.

[0047] 단계 220에서 서버(120)는 모바일 단말(110)의 접속 요청에 포함된 단말 정보를 확인한 후 사전 등록된 단말인 경우, 당해 서버(120)의 공개키(PK_{SS})를 모바일 단말(110)로 전송한다. 이하에서는 서버의 공개키를 서버 공개키로 통칭하기로 한다.

[0048] 단계 220에서 모바일 단말(110)은 서버(120)로부터 공개키가 수신되면, 자신의 공개키(즉, 모바일 단말(110)의 공개키(PK_{MT})를 서버(120)로 전송한다.

[0049] 이와 같이, 모바일 단말(110)과 서버(120)는 상호간 비대칭키를 기반으로 통신을 수행하기 위해 모바일 단말의 등록 과정에서 각자의 공개키를 교환한 후 이를 기반으로 비대칭키를 이용하여 통신을 위한 메시지를 암호화하여 통신을 수행할 수 있다. 이에 대해서는 도 3의 설명에 의해 보다 명확하게 이해될 것이다.

[0050] 도 2에서는 모바일 단말(110)의 등록 과정에 대해서만 설명하고 있으나, 스마트 디바이스(130)의 등록 과정 또한 모바일 단말(110)의 등록 과정과 매우 유사할 수 있다. 다만, 본 발명의 일 실시예에 따른 스마트홈 시스템의 경우, 댁내 통신은 대칭키를 기반으로 수행되므로, 스마트 디바이스(130)는 서버(120)로부터 비밀키를 공유받는 과정만 있을 뿐, 스마트 디바이스(130)의 비밀키를 서버(120)로 전송하는 과정은 존재하지 않는 점에서 차이가 있을 수 있다. 이외의 나머지 스마트 디바이스(130)의 등록 과정은 모바일 단말(110)의 등록 과정과 사실상 동일하므로 중복되는 설명은 생략하기로 한다.

[0051] 도 3은 본 발명의 일 실시예에 따른 스마트홈 시스템의 통신 방법을 나타낸 흐름도이다.

[0052] 단계 310에서 모바일 단말(110)은 사전에 단말 등록 과정에서 서버(120)로부터 수신한 서버 공개키를 이용하여 데이터 요청을 암호화하여 서버(120)로 전송한다. 여기서, 데이터 요청은 스마트홈 환경에서 댁내에 위치하는

스마트 디바이스로의 데이터 요청으로, 모바일 단말(110)은 직접 스마트 디바이스와 통신하지 않고 서버(120)를 통해 스마트 디바이스와 통신할 수 있다.

[0053] 예를 들어, 모바일 단말(110)은 댁내에 위치하는 스마트 디바이스로의 데이터 요청을 위해, 데이터 요청 메시지, 단말 정보, 임의의 난수값 및 해당 데이터 요청 메시지가 모바일 단말에서 왔음을 인증해주는 모바일 단말 서명값(S_{MT})중 적어도 하나를 단말 등록 과정에서 서버(120)로부터 수신받은 서버 공개키(PK_{SS})를 이용하여 암호화한 후 암호화된 데이터 요청을 서버(120)로 전송할 수 있다.

[0054] 이에 따라, 단계 315에서 서버(120)는 모바일 단말(110)에서 수신된 암호화된 데이터 요청을 자신(즉, 서버(120))의 공개키에 대응하는 비밀키(이하, 제1 서버 비밀키라 칭하기로 함) 복호한 후 모바일 단말에 대한 인증을 수행한다.

[0055] 예를 들어, 서버(120)는 자신의 제1 서버 비밀키로 암호화된 데이터 요청을 복호한 후 복호된 데이터 요청에 포함된 단말 정보와 기등록된 단말 정보의 일치 여부를 확인하여 모바일 단말을 인증할 수 있다.

[0056] 단계 320에서 서버(120)는 인증 수행 결과 인증 성공인지 여부를 판단한다.

[0057] 만일 인증 수행 결과 인증이 실패한 경우, 단계 325에서 서버(120)는 모바일 단말과 통신을 해제할 수 있다. 이때, 서버(120)는 인증 실패에 따른 안내 메시지를 모바일 단말(110)로 전송할 수도 있다.

[0058] 만일 인증 수행 결과 인증이 성공하면, 단계 330에서 서버(120)는 스마트 디바이스와 공유하고 있는 비밀키(SK_{Home})로 복호된 데이터 요청을 암호화하여 스마트 디바이스(130)로 전송한다.

[0059] 이때, 비밀키로 암호화된 데이터 요청은 데이터 요청 메시지 및 난수값을 포함할 수 있다.

[0060] 본 명세서에서는 스마트 디바이스에 대한 별도의 등록 과정에 대해서는 상세히 설명되어 있지 않으나, 단말 등록 과정과 마찬가지로 스마트 디바이스로 서버(120)와 최초 등록 과정을 선행할 수 있다. 이때, 스마트 디바이스(130)는 서버(120)로 디바이스 정보를 전송한 후 서버(120)로부터 비밀키를 제공받을 수 있다.

[0061] 단계 335에서 스마트 디바이스(130)는 사전에 서버(120)로부터 제공받은 비밀키로 암호화된 데이터 요청을 복호한 후 모바일 단말(110)의 데이터 요청을 확인한다.

[0062] 이어, 단계 340에서 스마트 디바이스(130)는 모바일 단말(110)의 데이터 요청에 상응하는 데이터와 난수값을 연접하여 해쉬한 결과값과, 데이터를 비밀키로 암호화하여 서버(120)로 전송한다.

[0063] 단계 345에서 서버(120)는 스마트 디바이스로부터 수신된 암호화된 데이터를 복호한 후 데이터와 해쉬한 결과값을 단말 공개키로 암호화하여 모바일 단말(110)로 전송한다. 여기서, 암호화된 데이터는 이외에도, 해당 암호화된 데이터가 서버에서 전송된 것임을 인증하는 서버 서명 값(S_{SS})을 더 포함할 수 있다.

[0064] 단계 350에서 모바일 단말(110)은 자신의 공개키에 대응하는 비밀키(이하, 단말 비밀키라 칭하기로함)를 이용하여 암호화된 데이터를 복호한 후 자신이 서버(120)로 전송한 난수값과 전송 받은 데이터를 연접하여 해쉬한 결과값과 복호된 데이터에 포함된 결과값의 일치 여부를 비교하여 무결성을 검증한다.

[0065] 무결성 검증 결과 일치하지 않으면, 모바일 단말(110)은 해당 데이터를 신뢰할 수 없는 데이터로 판단하여 이를 폐기할 수 있다.

[0066] 도 4는 본 발명의 일 실시예에 따른 서버의 내부 구성을 개략적으로 도시한 블록도이다.

[0067] 도 4를 참조하면, 서버(120)는 통신부(410), 인증부(415), 데이터 전송부(420), 메모리(425) 및 프로세서(430)를 포함하여 구성된다.

[0068] 통신부(410)는 다른 장치(예를 들어, 모바일 단말(110), 스마트 디바이스(130))과 데이터를 송수신하기 위한 수단이다.

[0069] 인증부(415)는 모바일 단말로부터 서버 공개키로 암호화된 데이터 요청을 수신한 후 상기 서버의 제1 서버 비밀키로 복호하고, 복호된 데이터 요청에 포함된 단말 정보와 기등록된 단말 정보를 이용하여 모바일 단말을 인증

하기 위한 수단이다.

[0070] 데이터 전송부(420)는 모바일 단말(110)과는 상호 교환한 비대칭키를 이용하여 데이터를 전송하고, 댁내에 위치하는 스마트 디바이스(130)와는 대칭키(비밀키)를 이용하여 데이터를 전송하기 위한 수단이다.

[0071] 예를 들어, 데이터 전송부(420)는 인증부의 인증 결과 인증 성공이면, 복호된 데이터 요청을 비밀키로 암호화하여 스마트 디바이스로 전송하고, 스마트 디바이스로부터 데이터 요청에 상응하여 비밀키로 암호화된 데이터를 수신한 후 비밀키로 암호화된 데이터를 복호한 후 단말 공개키로 복호된 데이터를 암호화하여 모바일 단말로 전송하기 위한 수단이다.

[0072] 데이터 전송부(420)의 상세 동작은 도 3에서 설명된 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0073] 메모리(425)는 스마트홈 시스템내에서 모바일 단말(110)과 스마트 디바이스(130)간의 데이터 통신을 위해 필요한 다양한 알고리즘, 어플리케이션, 이 과정에서 파생된 다양한 데이터를 저장하는 수단이다.

[0074] 프로세서(430)는 본 발명의 일 실시예에 따른 서버(120)의 내부 구성 요소들(예를 들어, 통신부(410), 인증부(415), 데이터 전송부(420), 메모리(425) 등)을 제어하기 위한 수단이다.

[0075] 도 5는 본 발명의 일 실시예에 따른 모바일 단말의 내부 구성을 개략적으로 도시한 블록도이다.

[0076] 도 5를 참조하면, 본 발명의 일 실시예에 따른 모바일 단말(110)은 통신부(510), 암호화부(515), 복호부(520), 무결성 검증부(525), 메모리(530) 및 프로세서(535)를 포함하여 구성된다.

[0077] 통신부(510)는 통신망을 통해 다른 장치(예를 들어, 서버(120))와 데이터를 송수신하기 위한 수단이다.

[0078] 암호화부(515)는 스마트 디바이스로의 데이터 요청을 위해, 데이터 요청 메시지, 상기 모바일 단말의 단말 정보, 임의의 난수값 및 모바일 단말 서명값 중 적어도 하나를 포함하는 데이터 요청을 서버 공개키로 암호화하는 수단이다. 암호화된 데이터 요청은 프로세서(535)의 제어에 의해 통신부(510)를 통해 서버(120)로 전송될 수 있다.

[0079] 복호부(520)는 서버(120)로부터 수신된 단말 공개키로 암호화된 데이터를 복호하는 수단이다. 예를 들어, 복호부(520)는 단말 공개키에 대응하는 단말 비밀키로 암호화된 데이터를 복호할 수 있다.

[0080] 무결성 검증부(525)는 복호된 데이터와 자신이 서버(120)로 전송한 난수값을 연접하여 해쉬한 결과값과 복호된 데이터에 포함된 결과값의 일치 여부를 판단하여 데이터의 무결성을 검증하기 위한 수단이다.

[0081] 메모리(530)는 스마트홈 내의 서버(120)와 비대칭키를 기반으로 데이터 통신을 수행하기 위해 필요한 다양한 알고리즘, 어플리케이션, 이 과정에서 파생된 다양한 데이터를 저장하는 수단이다.

[0082] 프로세서(535)는 본 발명의 일 실시예에 따른 모바일 단말(110)의 내부 구성 요소들(예를 들어, 통신부(510), 암호화부(515), 복호부(520), 무결성 검증부(525), 메모리(530) 등)을 제어하기 위한 수단이다.

[0083] 도 6은 본 발명의 일 실시예에 따른 스마트 디바이스의 내부 구성을 개략적으로 도시한 블록도이다.

[0084] 도 6을 참조하면, 본 발명의 일 실시예에 따른 스마트 디바이스(130)는 통신부(610), 암호화부(615), 복호화부(620), 메모리(625) 및 컨트롤러(630)를 포함하여 구성된다.

[0085] 통신부(610)는 다른 장치들(예를 들어, 서버(120))와 데이터를 송수신하기 위한 수단이다.

[0086] 암호화부(615)는 서버(120)로부터 사전에 제공받은 비밀키를 이용하여 데이터를 암호호하기 위한 수단이다.

[0087] 이때, 암호화부(615)는 모바일 단말(110)을 통해 제공받은 난수값과 데이터를 연접하여 해쉬한 결과값을 데이터와 함께 암호화하여 데이터 무결성 검증에 이용하도록 할 수도 있다.

[0088] 복호화부(620)는 서버(120)로부터 사전에 제공받은 제2 서버 비밀키를 이용하여 서버(120)로부터 수신된 암호화된 데이터 요청을 복호하기 위한 수단이다.

[0089] 메모리(625)는 스마트홈 내의 서버(120)와 대칭키를 기반으로 데이터 통신을 수행하기 위해 필요한 다양한 알고리즘, 어플리케이션, 이 과정에서 파생된 다양한 데이터를 저장하는 수단이다.

[0090] 컨트롤러(630)는 본 발명의 일 실시예에 따른 스마트 디바이스의 내부 구성 요소들(예를 들어, 통신부(610), 암호화부(615), 복호화부(620), 메모리(625) 등)을 제어하기 위한 수단이다.

[0091] 상술한 본 발명에 따른 모바일 기기에서의 동적 전력 관리 방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체로는 컴퓨터 시스템에 의하여 해독될 수 있는 데이터가 저장된 모든 종류의 기록 매체를 포함한다. 예를 들어, ROM(Read Only Memory), RAM(Random Access Memory), 자기 테이프, 자기 디스크, 플래쉬 메모리, 광 데이터 저장장치 등이 있을 수 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 통신망으로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

[0092] 이상에서는 본 발명의 실시예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 쉽게 이해할 수 있을 것이다.

부호의 설명

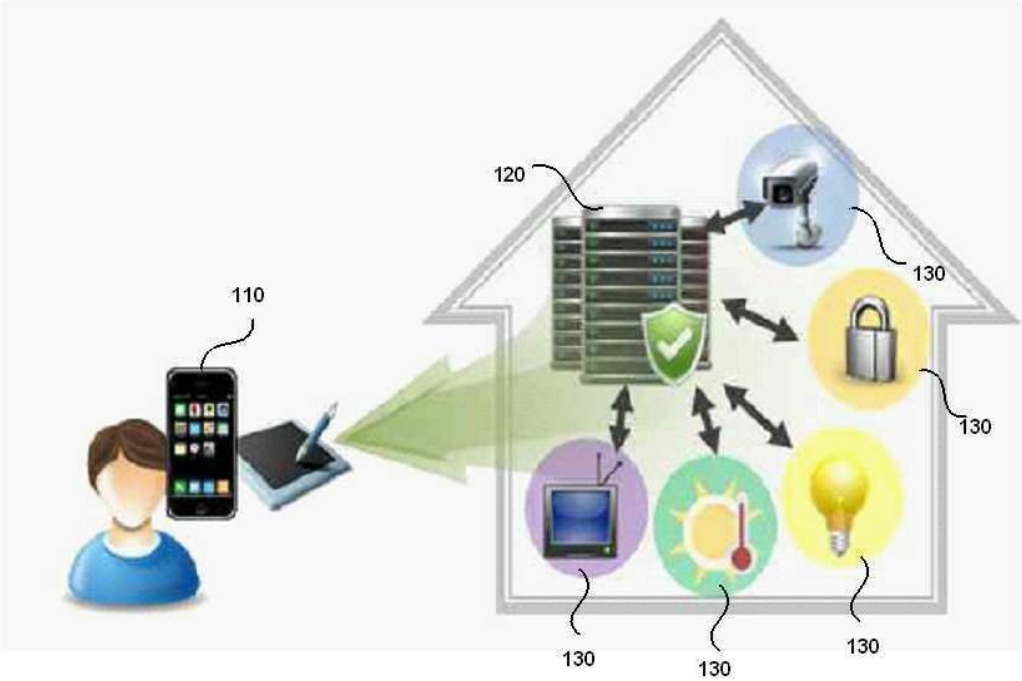
[0093] 110: 모바일 단말

120: 서버

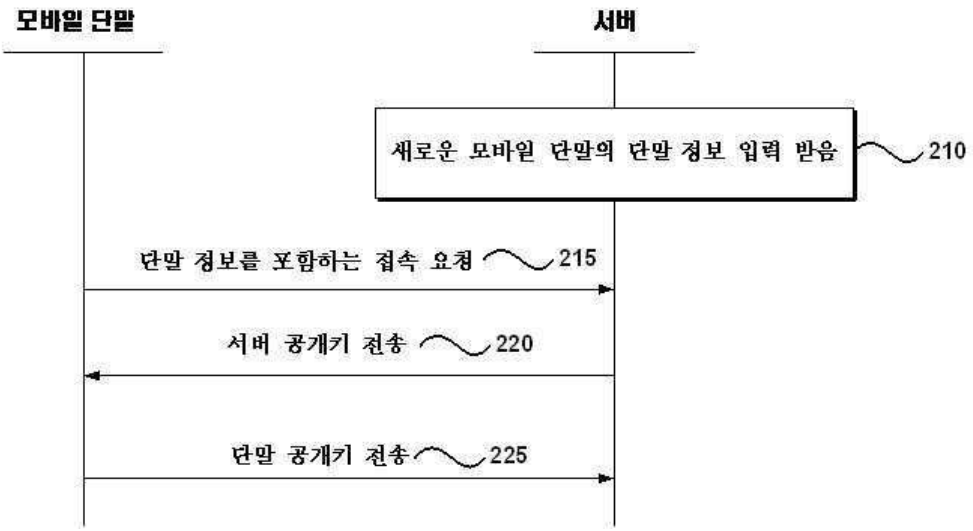
130: 스마트 디바이스

도면

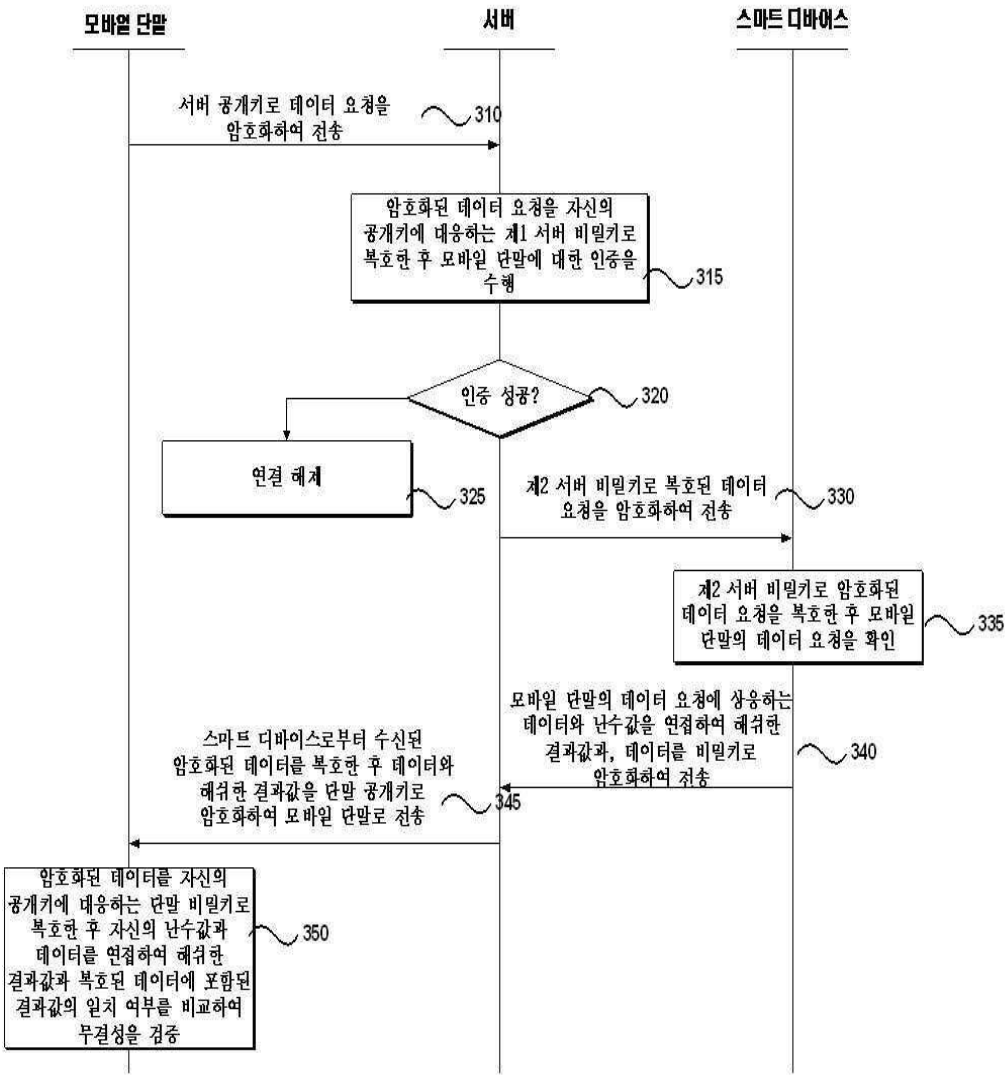
도면1



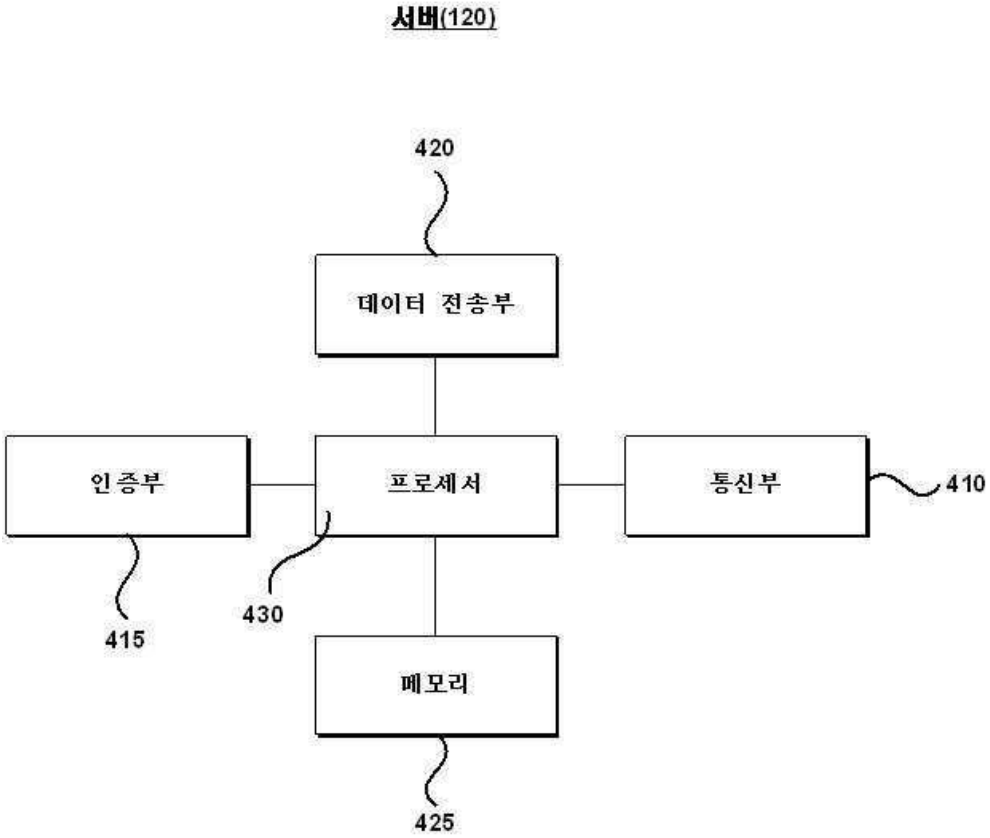
도면2


모바일 단말
서버
새로운 모바일 단말의 단말 정보 입력 받음
210
단말 정보를 포함하는 접속 요청
215
서버 공개키 전송
220
단말 공개키 전송
225

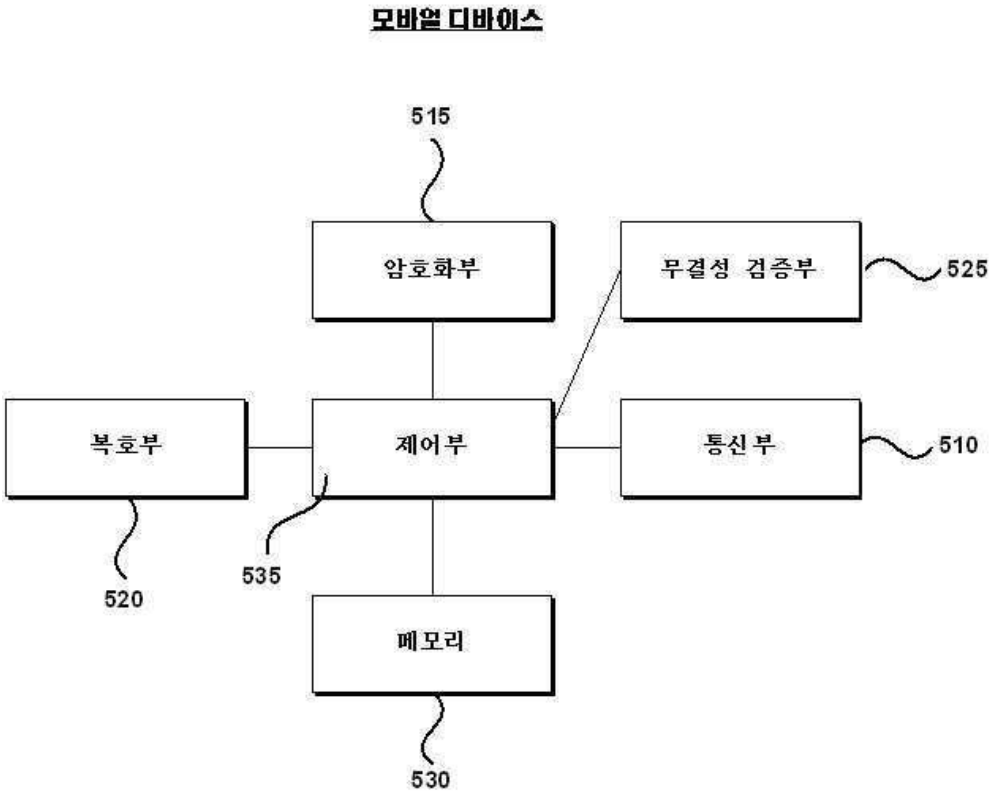
도면3


모바일 단말
서버
스마트 디바이스
서버 공개키로 데이터 요청을 암호화하여 전송
310
암호화된 데이터 요청을 자신의 공개키에 대응하는 제1 서버 비밀키로 복호한 후 모바일 단말에 대한 인증을 수행
315
인증 성공?
320
연결 해제
325
제2 서버 비밀키로 복호된 데이터 요청을 암호화하여 전송
330
제2 서버 비밀키로 암호화된 데이터 요청을 복호한 후 모바일 단말의 데이터 요청을 확인
335
모바일 단말의 데이터 요청에 상응하는 데이터와 난수값을 연접하여 해쉬한 결과값과, 데이터를 비밀키로 암호화하여 전송
340
스마트 디바이스로부터 수신된 암호화된 데이터를 복호한 후 데이터와 해쉬한 결과값을 단말 공개키로 암호화하여 모바일 단말로 전송
345
암호화된 데이터를 자신의 공개키에 대응하는 단말 비밀키로 복호한 후 자신의 난수값과 데이터를 연접하여 해쉬한 결과값과 복호된 데이터에 포함된 결과값의 일치 여부를 비교하여 무결성을 검증
350

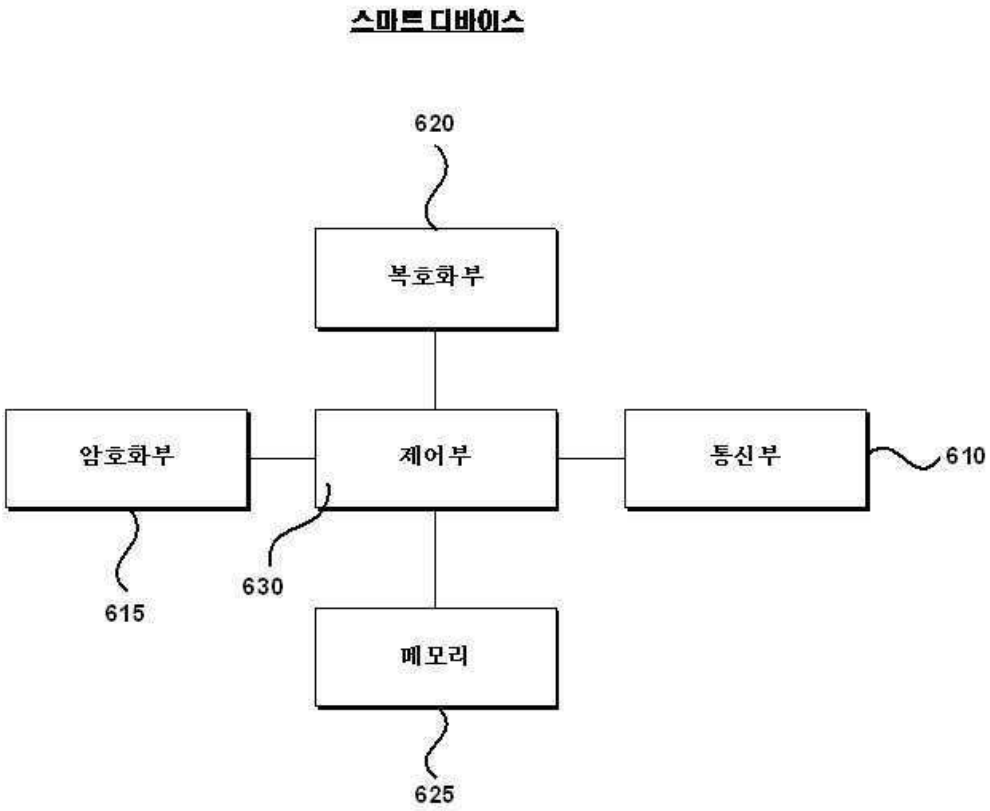
도면4


서버(120)
420
데이터 전송부
인증부
프로세서
통신부
410
415
430
메모리
425

도면5


모바일 디바이스
515
암호화부
무결성 검증부
525
복호부
제어부
통신부
510
520
535
메모리
530

도면6



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 1

【변경전】

(a) 상기 모바일 단말로부터

【변경후】

(a) 모바일 단말로부터