(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년04월26일
(11) 등록번호 10-0954428
(24) 등록일자 2010년04월15일

(51) Int. Cl.
G06F 15/00 (2006.01)
(21) 출원번호 10-2007-0115251
(22) 출원일자 2007년11월13일
심사청구일자 2007년11월13일
(65) 공개번호 10-2009-0049625
(43) 공개일자 2009년05월19일
(56) 선행기술조사문헌
한국해양정보통신학회*
KR1020060058789 A
JP2005115869 A
한국정보보호학회
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
인천 남구 용현3동 인하대학교 하이테크센터 317호
맹영재
인천 남구 용현3동 인하대학교 하이테크센터 307호
(뒷면에 계속)
(74) 대리인
특허법인이지

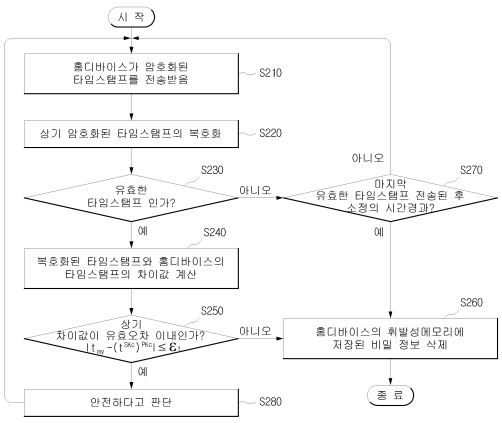
전체 청구항 수 : 총 17 항 심사관 : 천대식

(54) 홈 디바이스의 비밀 정보 보호 방법

(57) 요 약

홈 디바이스의 비밀 정보 보호 방법이 개시된다. 홈 네트워크 내에 포함되어 제어장치의 관리를 받는 홈 디바이스에서의 비밀 정보를 보호하는 방법에 있어서, 상기 홈 디바이스가 상기 제어장치로부터 안전 보증 메시지를 전송 받는 단계-상기 안전 보증 메시지는 상기 홈 네트워크 안전 정보를 포함함-; 상기 안전 보증 메시지의 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보를 비교하는 단계; 상기 비교 결과에 따라 상기 홈 네트워크의 안전 여부를 판단하는 단계; 및 상기 판단 결과에 상응하여 보안 동작의 수행 여부를 결정하는 단계를 포함하되, 상기 보안 동작은 상기 홈 디바이스의 휘발성 메모리에 저장된 비밀 정보를 삭제하는 동작인 것을 특징으로 한다. 이러한 홈 디바이스 에서의 비밀 정보를 보호하는 방법에 의하면, 간단하고 저렴한 비용으로 비밀 정보 저장의 안정성을 높이면서 홈 디바이스에 저장된 비밀 정보를 보호할 수 있다.

대 표 도 - 도2



(72) 발명자
강전일
충남 공주시 옥룡동 284-1

아브델아지즈 모하이센
인천 남구 용현3동 인하대학교 하이테크센터 307호

특허청구의 범위

청구항 1

홈 네트워크 내에 포함되어 제어장치의 관리를 받는 홈 디바이스에서의 비밀 정보를 보호하는 방법에 있어서,

상기 홈 디바이스가 상기 제어장치로부터 안전 보증 메시지를 전송 받는 단계-상기 안전 보증 메시지는 상기 홈 네트워크 안전 정보를 포함함-;

상기 안전 보증 메시지의 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보를 비교하는 단계;

상기 비교 결과에 따라 상기 홈 네트워크의 안전 여부를 판단하는 단계; 및

상기 판단 결과에 상응하여 보안 동작의 수행 여부를 결정하는 단계를 포함하되,

상기 보안 동작은 상기 홈 디바이스의 휘발성 메모리에 저장된 비밀 정보를 삭제하는 동작이며,

상기 안전 보증 메시지는 타임스탬프로 이루어지고 상기 홈 디바이스의 디바이스 안전 정보는 상기 홈 디바이스의 현재 타임스탬프로 이루어진 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 2

제1항에 있어서,

상기 홈 디바이스는 일정 시간을 주기로 안전 보증 메시지를 전송 받으며,

상기 일정 시간은 외부 디바이스가 상기 홈 디바이스의 상기 비밀 정보를 획득하기 위해 소요되는 예상 공격 시간보다 짧은 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 3

제1항에 있어서,

상기 안전 보증 메시지는 암호화된 상태로 상기 홈 디바이스로 전송되는 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 4

제3항에 있어서,

상기 안전 보증 메시지는 공개키 암호화 방식으로 암호화된 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 5

제3항에 있어서,

상기 안전 보증 메시지는 공유키 암호화 방식으로 암호화된 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 6

제3항에 있어서,

일정 시간 내에 유효한 상기 안전 보증 메시지가 상기 홈 디바이스로 전송되지 않는 경우 상기 보안 동작을 행하되,

상기 유효한 상기 안전 보증 메시지는 상기 홈 디바이스의 디바이스 안전 정보와 동일한 형식인 것을 특징으로 하는 디바이스의 비밀 정보 보호 방법.

청구항 7

제3항에 있어서,

상기 홈 네트워크의 안전 여부를 판단하는 단계는

상기 제어장치로부터 전송 받은 암호화된 안전 보증 메시지를 상기 홈 네트워크 안전 정보로 복호화 하는 단계; 및

상기 홈 네트워크 안전 정보를 상기 디바이스 안전 정보와 비교하는 단계를 포함하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 8

삭제

청구항 9

제1항에 있어서,

상기 제어장치 및 상기 홈 디바이스는 시간적으로 동기화되어 있는 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 10

제9항에 있어서,

상기 홈 네트워크 안전 정보와 상기 디바이스 안전 정보의 비교 결과,

비교 값이 상기 홈 디바이스에 미리 설정되어 있는 유효 오차 이하일 경우 상기 홈 네트워크가 안전하다고 판단하는 단계를 더 포함하고,

비교 값이 상기 홈 디바이스에 미리 설정되어 있는 유효 오차를 초과하는 경우 상기 보안 동작을 수행하는 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 11

제1항에 있어서,

상기 안전 보증 메시지는 랜덤수 및 오더(order)의 조합으로 이루어지고 상기 홈 디바이스의 디바이스 안전 정보는 상기 홈 디바이스의 랜덤수 및 오더의 조합으로 이루어진 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 12

제11항에 있어서,

상기 제어장치와 상기 홈 디바이스는 씨드(seed)를 공유하고 있는 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 13

제12항에 있어서,

상기 홈 네트워크 안전 정보와 상기 디바이스 안전 정보의 비교 결과,

상기 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보가 동일한 경우 상기 홈 네트워크가 안전하다고 판단하는 단계를 더 포함하고,

상기 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보가 동일하지 않은 경우 상기 보안 동작을 수행하는 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 14

홈 네트워크 내에 포함되어 제어장치의 관리를 받는 홈 디바이스에서의 비밀 정보를 보호하는 방법에 있어서,

상기 홈 네트워크에 참여를 원하는 상기 홈 디바이스가 상기 제어장치에 코드 인증을 요구하는 단계;

상기 코드 인증을 통해 인증된 상기 홈 디바이스가 비밀 정보를 복구하여 상기 홈 디바이스의 휘발성 메모리에 저장하는 단계;

상기 홈 디바이스는 상기 제어장치로부터 안전 보장 메시지를 전송 받는 단계-상기 안전 보장 메시지는 상기 홈 네트워크 안전 정보가 포함되어 있음-;

상기 안전 보장 메시지의 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보를 비교하는 단계;

상기 비교 결과에 따라 상기 홈 네트워크의 안전 여부를 판단하는 단계;

상기 판단 결과에 상응하여 보안 동작의 수행 여부를 결정하는 단계를 포함하되,

상기 보안 동작은 상기 홈 디바이스의 휘발성 메모리에 저장된 비밀 정보를 삭제하는 동작인 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 15

제14항에 있어서,

상기 홈 디바이스는 일정 시간을 주기로 안전 보증 메시지를 전송 받으며,

상기 일정 시간은 외부 디바이스가 상기 디바이스의 상기 비밀 정보를 획득하기 위해 소요되는 예상 공격 시간보다 짧은 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 16

제14항에 있어서,

상기 홈 디바이스의 비밀 정보는

상기 홈 네트워크 상의 다른 홈 디바이스의 비 휘발성 메모리에 부분 비밀 정보의 형태로 분산 저장되어 있는 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 17

제16항에 있어서,

상기 홈 디바이스가 비밀 정보를 복구하여 상기 홈 디바이스의 휘발성 메모리에 저장하는 단계는

상기 홈 디바이스가 공유된 상기 부분 비밀 정보를 요청하는 단계;

상기 부분 비밀 정보를 이용하여 상기 비밀 정보를 복원하는 단계; 및

상기 복원된 비밀 정보를 상기 홈 디바이스의 휘발성 메모리에 저장하는 단계를 포함하는 것을 특징으로 하는 홈 디바이스의 비밀 정보 보호 방법.

청구항 18

제1항 내지 제17항의 어느 한 항에 기재된 상기 홈 디바이스의 비밀 정보 보호 방법을 수행하는 프로그램이 기록된 컴퓨터에서 판독 가능한 기록 매체.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 홈 네트워크에 관련한 것으로 보다 상세하게는 홈 네트워크에 포함된 홈 디바이스의 비밀 정보 보호 방법에 관한 것이다.

배 경 기 술

[0002] 홈 네트워크는 일반 가정에서 네트워크 능력을 가진 여러 디바이스들로 구성되어 내부의 다른 디바이스들과 통신하고, 게이트웨이를 통해 외부와 통신하는 네트워크를 의미한다. 이러한 홈 네트워크에서는 사용자들의 편리한 생활환경을 위해 사용자의 입력이 다른 디바이스들의 동작에도 영향을 주게 된다.

[0003] 또한, 홈 네트워크의 디바이스들은 사용자의 생활과 직접적으로 연결되어 있으므로 디바이스가 저장하고 있는 비밀 정보 보호에 대해 신중해야 할 필요가 있다. 따라서 홈 네트워크에서 가장 중요한 한 가지 과제가 바로 디바이스가 가진 비밀 정보를 공격자로부터 안전하게 보호하는 일이다.

[0004] 비밀 정보를 보호하기 위한 특별한 보호 장치가 없다면 공격자는 디바이스에 내장되어 있는 비밀 정보에 쉽게 접근할 수 있다. 비밀 정보가 디바이스의 내부에서 암호화 되어 있다고 하더라도 비밀 정보를 암호화한 비밀 키를 다시 꺼낼 수 있고, 이러한 비밀 키가 외부에 있다고 하더라도 자신이 필요한 비밀 정보를 사용하기 위해서는 디바이스 역시 외부에서 인증 과정을 거친 후 비밀 키를 가져와야 하는데, 이 인증 과정에서 사용하는 정보가 다시 비밀 정보가 되기 때문이다.

[0005] 이렇게 홈 네트워크에 참여한 디바이스의 비밀 정보를 보호하기 위해서 종래의 홈 네트워크 보안 기술의 경우 물리적인 방법을 사용하였다. 이러한 물리적인 보안 방법 중 하나는 TPM(trusted platform module)과 같은 하드웨어 지원 칩을 이용하는 것이다. 이러한 하드웨어 지원 칩을 이용하면 디바이스의 비밀 정보를 노리는 공격자는 물리적으로 디바이스에서 어떠한 정보 즉 비밀 정보를 꺼내기 힘들어진다. 하지만 TPM 칩을 이용하고자 할 경우, 디바이스의 하드웨어뿐만 아니라, 운영 체제(operating system)와 응용 프로그램(application)의 지원 또한 필요하기 때문에 전체적인 구조가 복잡해질 뿐만 아니라, 디바이스를 위한 비용이 증가하게 된다. 또한 현재 많은 홈 디바이스들이 이러한 안전상의 고려 없이 사용되고 있어 디바이스의 비밀 정보 보호를 위한 하드웨어의 추가는 기대하기 어렵다.

발명의 내용

해결 하고자하는 과제

[0006] 따라서, 본 발명은 홈 네트워크에 있어서 홈 네트워크를 구성하는 홈 디바이스에 저장된 비밀 정보를 외부 디바이스로부터 보호하는 방법을 제공한다.

[0007] 또한, 본 발명은 하나의 홈 디바이스의 비밀 정보를 여러 개의 부분 비밀 정보로 나누어 다른 디바이스에 저장함으로써 비밀 정보 저장의 안정성을 높일 수 있는 방법을 제공한다.

[0008] 또한, 본 발명은 소프트웨어적인 방법을 홈 네트워크에 적용하여 간단하고 저렴한 비용으로 홈 디바이스의 비밀

정보를 보호할 수 있는 방법을 제공한다.

과제 해결수단

[0009] 본 발명의 일 측면에 따르면, 홈 네트워크 내에 포함되어 제어장치의 관리를 받는 홈 디바이스에서의 비밀 정보를 보호하는 방법은 상기 홈 디바이스가 상기 제어장치로부터 안전 보증 메시지를 전송 받는 단계-상기 안전 보증 메시지는 상기 홈 네트워크 안전 정보를 포함함-; 상기 안전 보증 메시지의 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보를 비교하는 단계; 상기 비교 결과에 따라 상기 홈 네트워크의 안전 여부를 판단하는 단계; 및 상기 판단 결과에 상응하여 보안 동작의 수행 여부를 결정하는 단계를 포함하되, 상기 보안 동작은 상기 홈 디바이스의 휘발성 메모리에 저장된 비밀 정보를 삭제하는 동작인 것을 특징으로 하며, 상기 홈 디바이스는 일정 시간을 주기로 안전 보증 메시지를 전송 받으며, 상기 일정 시간은 외부 디바이스가 상기 홈 디바이스의 상기 비밀 정보를 획득하기 위해 소요되는 예상 공격 시간보다 짧을 수 있다.

[0010] 또한, 상기 안전 보증 메시지는 공개키 및 공유키 방식으로 암호화된 상태로 상기 홈 디바이스로 전송되며, 일정 시간 내에 유효한 상기 안전 보증 메시지가 상기 홈 디바이스로 전송되지 않는 경우 상기 보안 동작을 행하되, 상기 유효한 상기 안전 보증 메시지는 상기 홈 디바이스의 디바이스 안전 정보와 동일한 형식일 수 있다.

[0011] 또한, 상기 홈 네트워크의 안전 여부를 판단하는 단계는 상기 제어장치로부터 전송 받은 암호화된 안전 보증 메시지를 상기 홈 네트워크 안전 정보로 복호화 하는 단계; 및 상기 홈 네트워크 안전 정보를 상기 디바이스 안전 정보와 비교하는 단계를 포함할 수 있다.

[0012] 상기 안전 보증 메시지는 암호화된 타임스탬프로 이루어지고 상기 홈 디바이스의 디바이스 안전 정보는 상기 홈 디바이스의 현재 타임스탬프로 이루어지며 상기 제어장치 및 상기 홈 디바이스는 시간적으로 동기화되어 있다. 상기 홈 네트워크 안전 정보와 상기 디바이스 안전 정보의 비교 결과, 비교 값이 상기 홈 디바이스에 미리 설정되어 있는 유효 오차 이하일 경우 상기 홈 네트워크가 안전하다고 판단하는 단계를 더 포함하고, 비교 값이 상기 홈 디바이스에 미리 설정되어 있는 유효 오차를 초과하는 경우 상기 보안 동작을 수행할 수 있다.

[0013] 또한, 상기 안전 보증 메시지는 암호화된 랜덤수 및 오더(order)의 조합으로 이루어지고 상기 홈 디바이스의 디바이스 안전 정보는 상기 홈 디바이스의 랜덤수 및 오더의 조합으로 이루어질 수 있으며 상기 제어장치와 상기 홈 디바이스는 씨드(seed)를 공유하고 있을 수 있다.

[0014] 상기 홈 네트워크 안전 정보와 상기 디바이스 안전 정보의 비교 결과,상기 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보가 동일한 경우 상기 홈 네트워크가 안전하다고 판단하는 단계를 더 포함하고, 상기 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보가 동일하지 않은 경우 상기 보안 동작을 수행할 수 있다.

[0015] 본 발명의 또 다른 측면에 따르면, 홈 네트워크 내에 포함되어 제어장치의 관리를 받는 홈 디바이스에서의 비밀 정보를 보호하는 방법에 있어서, 상기 홈 네트워크에 참여를 원하는 상기 홈 디바이스가 상기 제어장치에 코드 인증을 요구하는 단계; 상기 코드 인증을 통해 인증된 상기 홈 디바이스가 비밀 정보를 복구하여 상기 홈 디바이스의 휘발성 메모리에 저장하는 단계; 상기 홈 디바이스는 상기 제어장치로부터 안전 보장 메시지를 전송 받는 단계-상기 안전 보장 메시지는 상기 홈 네트워크 안전 정보가 포함되어 있음-; 상기 안전 보장 메시지의 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보를 비교하는 단계; 상기 비교 결과에 따라 상기 홈 네트워크의 안전 여부를 판단하는 단계; 상기 판단 결과에 상응하여 보안 동작의 수행 여부를 결정하는 단계를 포함하되, 상기 보안 동작은 상기 홈 디바이스의 휘발성 메모리에 저장된 비밀 정보를 삭제하는 동작일 수 있다.

[0016] 이 때, 상기 홈 디바이스는 일정 시간을 주기로 안전 보증 메시지를 전송 받으며, 상기 일정 시간은 외부 디바이스가 상기 디바이스의 상기 비밀 정보를 획득하기 위해 소요되는 예상 공격 시간보다 짧으며 상기 홈 네트워크 상의 다른 홈 디바이스의 비 휘발성 메모리에 부분 비밀 정보의 형태로 분산 저장되어 있을 수 있다.

[0017] 또한, 상기 홈 디바이스가 비밀 정보를 복구하여 상기 홈 디바이스의 휘발성 메모리에 저장하는 단계는 상기 홈 디바이스가 공유된 상기 부분 비밀 정보를 요청하는 단계; 상기 부분 비밀 정보를 이용하여 상기 비밀 정보를 복원하는 단계; 및 상기 복원된 비밀 정보를 상기 홈 디바이스의 휘발성 메모리에 저장하는 단계를 포함하며 상기 안전 보증 메시지는 공개키 또는 공유키 암호화 방식으로 암호화된 상태로 상기 홈 디바이스로 전송될 수 있다.

[0018] 또한, 일정 시간 내에 유효한 상기 안전 보증 메시지가 상기 홈 디바이스로 전송되지 않는 경우 상기 보안 동작을 행하되, 상기 유효한 상기 안전 보증 메시지는 상기 홈 디바이스의 디바이스 안전 정보와 동일한 형식이며, 상기 제어장치로부터 전송 받은 암호화된 안전 보증 메시지를 상기 홈 네트워크 안전 정보로 복호화 하는 단계; 및 상기 홈 네트워크 안전 정보를 상기 디바이스 안전 정보와 비교하는 단계를 포함할 수 있다.

[0019] 상기 안전 보증 메시지는 암호화된 타임스탬프로 이루어지고 상기 홈 디바이스의 디바이스 안전 정보는 상기 홈 디바이스의 현재 타임스탬프로 이루어지며, 상기 제어장치 및 상기 홈 디바이스는 시간적으로 동기화되어 있을 수 있다. 이 경우, 상기 홈 네트워크 안전 정보와 상기 디바이스 안전 정보의 비교 결과, 비교 값이 상기 홈 디바이스에 미리 설정되어 있는 유효 오차 이하일 경우 상기 홈 네트워크가 안전하다고 판단하는 단계를 더 포함하고, 비교 값이 상기 홈 디바이스에 미리 설정되어 있는 유효 오차를 초과하는 경우 상기 보안 동작을 수행할 수 있다.

[0020] 또한, 상기 안전 보증 메시지는 암호화된 랜덤수 및 오더(order)의 조합으로 이루어지고 상기 홈 디바이스의 디바이스 안전 정보는 상기 홈 디바이스의 랜덤수 및 오더의 조합으로 이루어질 수 있으며, 상기 제어장치와 상기 홈 디바이스는 씨드(seed)를 공유할 수 있다. 이 경우, 상기 홈 네트워크 안전 정보와 상기 디바이스 안전 정보의 비교 결과, 상기 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보가 동일한 경우 상기 홈 네트워크가 안전하다고 판단하는 단계를 더 포함하고, 상기 홈 네트워크 안전 정보와 상기 홈 디바이스의 디바이스 안전 정보가 동일하지 않은 경우 상기 보안 동작을 수행할 수 있다.

[0021] 본 발명의 또 다른 측면에 따르면, 전술 한바 있는 상기 홈 디바이스의 비밀 정보 보호 방법을 수행하는 프로그램이 기록된 컴퓨터에서 판독 가능한 기록 매체가 제공될 수 있다.

효 과

[0022] 본 발명에 따른 홈 네트워크 상의 비밀 정보 보호 방법에 따르면 홈 네트워크를 구성하는 홈 디바이스의 비밀 정보를 외부 디바이스로부터 보호 할 수 있다.

[0023] 또한, 본 발명은 비밀 정보를 분산 저장함으로써 비밀 정보 저장의 안정성을 높일 수 있다.

[0024] 또한, 소프트웨어적인 방법을 홈 네트워크에 적용하여 간단하고 저렴한 비용으로 홈 디바이스의 비밀 정보를 보호할 수 있다.

발명의 실시를 위한 구체적인 내용

[0025] 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.

[0026] 제1, 제2 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.

[0027] 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.

[0028] 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. 일

반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0029] 이하, 본 발명의 실시예를 첨부한 도면들을 참조하여 상세히 설명하기로 한다.

[0030] 도 1을 참조하여 본 발명의 일 실시예에 따른 홈 네트워크 상의 비밀 정보 보호 방법의 개념에 대하여 개략적으로 살펴보도록 한다. 도 1은 본 발명의 일 실시예에 따른 홈 네트워크 상의 비밀 정보 보호 방법의 개념도이다.

[0031] 본 발명의 일 실시예에 따른 홈 네트워크(100)는 제어장치(110)와 복수개의 홈 디바이스(121,122,123,…,12n-이하,12n으로 칭함)를 포함한다. 제어장치(110)는 전체 홈 네트워크(100)를 책임지고 외부와의 통신을 수행하는 게이트웨이(gateway) 서버와 같은 역할을 수행한다. 도 1에 도시되어 있듯, 제어장치(110)는 복수의 홈 디바이스(12n) 각각에 안전 보증 메시지(Safe Guarantee Message)를 전송한다.

[0032] 안전 보증 메시지는 제어장치(110)에서 홈 디바이스(12n)들이 안전한 상태에 있다는 것을 알려주는 메시지이다. 홈 디바이스(12n)들은 홈 네트워크(100) 상에서 자신이 처한 상황을 판단하기 위해 홈 디바이스(12n)로 전송되는 메시지를 이용한다. 즉, 제어장치(110)는 홈 네트워크(100)가 안전한 상태(예를 들어, 외부 공격자가 홈 네트워크(100) 상에 존재하지 않는 상태 등)에 있음을 알리기 위한 메시지를 각각의 홈 디바이스(12n)로 전송하게 된다. 이때, 제어장치(110)에서 홈 디바이스(12n)로 홈 네트워크(100)가 안전한 상태임을 알리는 메시지 즉, 홈 네트워크의 안전 정보를 포함하는 메시지를 안전 보증 메시지라고 한다. 본 발명의 일 실시예에 따르면 안전 보증 메시지는 타임스탬프(timestamp) 형식 또는 랜덤수(random number) 및 랜덤수의 오더(order)의 조합으로 이루어진 형식일 수 있다. 즉, 안전 보증 메시지는 홈 네트워크의 안전 정보를 포함하는데 홈 네트워크의 안전 정보는 타임스탬프 또는 랜덤수 및 오더의 조합일 수 있다. 이하 본 발명의 이해와 설명의 편의를 위하여 안전 보증 메시지 및 홈 네트워크의 안전 정보는 상기와 같은 의미로 사용되는 것으로 가정한다.

[0033] 또한, 홈 네트워크의 안전 정보와 홈 디바이스의 디바이스 안전 정보는 동일한 형식으로 이루어져 있어야 한다. 따라서 홈 디바이스의 디바이스 안전 정보 역시, 타임스탬프 또는 랜덤수 및 오더의 조합이어야 한다.

[0034] 안전 보증 메시지는 일정 시간을 주기로 홈 디바이스(12n)로 전송되는데, 일정 시간은 외부 디바이스가 상기 디바이스의 상기 비밀 정보를 획득하기 위해 소요되는 예상 공격 시간보다 짧다. 외부 디바이스에 의한 공격 시간보다 안전 보증 메시지 전송 주기가 길다면, 안전 보증 메시지가 도착하기 전에 외부 디바이스에 의해 홈 디바이스의 비밀 정보가 공격 당할 수 있기 때문이다.

[0035] 복수의 홈 디바이스(12n) 각각은 통신 기능이 있어 홈 네트워크(100)에 포함된 다른 홈 디바이스(12n)들과 통신을 수행할 수 있다. 홈 디바이스(12n)는 각각 별도의 휘발성 메모리(volatile memory)를 구비하고 있어, 각각의 비밀 정보를 저장한다. 메모리는 메모리로 공급되는 전원을 끊었을 때 메모리에 저장되어 있는 데이터가 보존되었는지 여부에 따라 휘발성 메모리와 비 휘발성 메모리로 구분된다. 이때, 휘발성 메모리는 메모리로 공급되는 전원이 차단되는 경우 저장하고 있는 데이터가 모두 삭제되는 메모리를 말하며, 비 휘발성 메모리는 반대로 전원 공급이 차단되어도 저장된 데이터가 계속 유지되는 기억 장치를 말한다. 본 발명의 일 실시예에 따른 홈 디바이스(12n)는 휘발성 메모리에 비밀 정보를 저장한다. 따라서, 홈 디바이스(12n)로 공급되는 전원이 중단되는 경우 메모리에 저장되어 있던 비밀 정보가 삭제되므로 이를 통해 비밀 정보가 외부 공격자에게 유출되는 것을 방지 할 수 있다. 이러한 과정에 대하여는 후에 상술하도록 한다.

[0036] 본 발명에서 비밀 정보는 자신 이외의 다른 개체가 그 정보를 알았을 때 직접적으로 다른 개체가 이득을 얻거나 자신이 피해를 보는 정보를 의미한다. 이 때, 이득이나 피해는 잠재적으로 발생할지 모르는 이득이나 피해의 경우가 아니라 직접적인 이득이나 피해의 경우만을 한정하는 의미임을 명확히 한다. 따라서 본 발명의 일 실시예에 따른 비밀 정보는 노출되었을 경우 직접적인 영향이 발생하는 정보들을 말한다. 예를 들어 공개키 암호화 방식의 개인키(private key)나 비밀키 암호화 방식의 비밀키(secret key), 인증을 위한 생체정보(bio-information)나 인증키(authentication key)와 같은 것을 의미한다. 이하, 본 발명의 설명과 이해의 편의를 위하며 비밀 정보는 상기와 같은 의미로 사용됨을 명확히 한다.

[0037] 이하, 도 2를 참조하여 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 보호 방법에 대하여 살펴 보도록

한다. 도 2는 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 보호 방법의 제어 흐름도 이다.

[0038] 제어장치로부터 홈 디바이스가 안전 보증 메시지를 전송 받는다(S210). 도 2의 제어흐름도에서는 안전 보증 메시지가 제어장치의 비밀키로 암호화된 타임 스탬프의 형식인 경우를 가정한다. 그러나, 이는 본 발명의 일 실시예일뿐, 안전 보증 메시지가 언제나 타임 스탬프 형식이어야 하는 것은 아니다. 본 발명의 또 다른 실시예에 따르면 안전 보증 메시지는 랜덤 수 및 오더의 조합으로 구성될 수 있다. 이에 대하여는 도 3를 참조하여 후술하도록 한다. 이와 같이 안전 보증 메시지가 암호화된 타임 스탬프인 경우, 홈 네트워크에 포함된 제어장치 및 홈 디바이스는 시간적으로 동기화되어 있다.

[0039] 전술한 바와 같이 제어장치의 비밀키(SK_c)로 암호화된 타임스탬프(t^{SK_c})를 홈 네트워크에 포함된 모든 홈 디바이스가 전송 받는다. 이때, 제어장치의 비밀키(SK_c)로 암호화된 타임스탬프(t^{SK_c})가 전송되는 주기는 전술한 바와 같이 외부 디바이스에 의한 공격 시간보다 짧아야 한다.

[0040] 각각의 홈 디바이스는 홈 디바이스로 전송된 제어장치의 비밀키로 암호화된 타임스탬프(t^{SK_c})를 제어장치의 공개키(PK_c)를 이용하여 본래의 타임스탬프$(t^{SK_c})^{PK_c}$로 복호화 한다(S220).

[0041] 이와 같이 비밀키와 공개키를 이용한 암호화 시스템을 공개키 암호 시스템이라고 하는데, 공개키 암호 시스템은 비밀 영역과 공개 영역으로 구분하여 두 개의 키를 생성하는 것을 특징으로 한다. 공개키 암호 시스템을 이용하여 특정인에게 비밀 메시지를 전송하고자 한다면 특정인의 공개키를 이용하여 메시지를 암호화해서 보낸다. 그러면 그 특정인은 자신만이 아는 비밀키로 메시지를 복호화할 수 있는데 이러한 시스템은 공개키 암호 시스템이라고 한다.

[0042] 공개키 암호화 시스템에 대응하는 개념으로 공유키 암호화 시스템이 있다. 공유키암호화 시스템은 공개키 암호 시스템과 달리, 암호화하는 키와 복호화하는 키가 동일한 암호 시스템을 말한다. 예를 들어, 특정 메시지를 암호화 하여 전송할 때 사용하는 키가 k라고 한다면, 암호화된 특정 메시지를 복호화하는 키도 역시나 k로 동일한 시스템을 말한다.도 2에서는 공개키 암호 시스템을 사용하는 방법에 대하여 설명하나, 공유키 암호 시스템에도 본 발명이 적용될 수 있음은 자명하다.

[0043] 홈 디바이스는 이렇게 상기와 같은 과정을 통해 복호화된 타임 스탬프$(t^{SK_c})^{PK_c}$가 유효한 안전 보증 메시지 형식인지 판단한다(S230). 이 때, 복호화된 타임 스탬프의 형식이 유효하다 함은 후술할 홈 디바이스의 디바이스 안전 정보의 형식과 일치함을 말하는 것으로, 그렇지 않은 경우 복호화된 타임 스탬프와 홈 디바이스의 디바이스 안전 정보와 정확하게 비교할 수 없기에 유효하지 않은 것으로 판단하게 된다.

[0044] 복호화된 타임 스탬프가 유효한 형식의 타임 스탬프가 아닌 경우 마지막으로 유효한 타임 스탬프가 전송된 후 소정의 시간이 경과되었는지 여부를 판단한다(S270). 여기서, 소정의 시간은 홈 디바이스에 마지막 유효 타임 스탬프가 전송 된 후 다음 타임 스탬프가 도착할 때까지 안전하다고 판단 내릴 수 있는 최대의 시간의 말한다. 따라서, 소정의 시간 경과 후에도 타임 스탬프가 전송 되지 않는 경우 즉, 마지막 유효 타임 스탬프가 전송된 후 소정이 시간이 지난 경우에는 홈 디바이스는 홈 디바이스의 비밀 정보가 외부 디바이스에 의해 유출될 수 있는 상황이라고 간주하여 휘발성 메모리에 저장된 비밀 정보를 삭제한다(S260). 그리고, 소정의 시간이 경과하지 않은 경우 즉 소정의 시간이 경과 전에 타임 스탬프를 전송 받은 경우에는 다시 처음으로 돌아가 보호 방법을 수행하게 된다.

[0045] 복호화된 타임 스탬프가 유효한 형식일 경우, 복호화된 타임스탬프$(t^{SK_c})^{PK_c}$와 홈 디바이스의 디바이스 안전 정보 즉, 홈 디바이스의 타임 스탬프t_{my}와의 차이 값($|t_{my} - (t^{SK_c})^{PK_c}|$)을 계산한다(S240). 이때 상기 차이 값($|t_{my} - (t^{SK_c})^{PK_c}|$)이 유효오차$\epsilon_t$이하의 값인지 판단한다(S250).

[0046] 만약 상기 차이 값이 유효 오차ϵ_t이하의 값이라면 홈 디바이스는 홈 네트워크가 안전하다고 판단한다(S280).

그러나, 상기 차이 값이 유효 오차 ϵ_t 의 값을 초과하는 경우 외부 디바이스가 홈 네트워크에 침입했다고 판단하여 홈 디바이스의 휘발성 메모리에 저장된 비밀 정보를 삭제한다(S260). 이때, 휘발성 메모리에 저장된 비밀 정보는 휘발성 메모리로 공급되는 전원을 차단하게 되면 휘발성 메모리의 특성 때문에 저장된 비밀 정보가 모두 삭제된다.

[0047] 상기에서는 안전 보증 메시지가 타임 스탬프로 이루어진 경우를 설명하였으나, 본 발명의 또 다른 실시예에 의하면 안전 보증 메시지는 랜덤수 및 오더(Oder)의 조합일 수 있다.

[0048] 이하, 도 3을 참조하여 안전 보증 메시지가 랜덤수 및 오더의 조합으로 이루어진 경우, 홈 디바이스의 비밀 정보 보호 방법에 대하여 살펴보도록 한다. 도 3은 본 발명의 또 다른 실시예에 따른 홈 디바이스의 비밀 정보의 보호 방법에 대한 제어 흐름도 이다.

[0049] 안전 보증 메시지가 랜덤수 및 오더의 조합으로 이루어진 경우의 홈 디바이스 비밀 정보 보호방법은 전술한 바 있는 도 2의 비밀 정보 보호 방법과 유사하므로, 중복되는 경우의 설명은 본 발명의 이해와 설명의 편의를 위해 생략하도록 한다.

[0050] 또한, 안전 보증 메시지가 랜덤수 및 오더의 조합으로 이루어진 경우, 홈 네트워크에 포함된 제어장치와 홈 디바이스는 씨드(Seed)를 공유하고 있다.

[0051] 먼저, 홈 디바이스가 제어장치로부터 암호화된 랜덤수 및 오더의 조합으로 이루어진 안전 보증 메시지를 전송받는다(S310). 이때, 제어장치가 홈 디바이스로 안전 보증 메시지를 전송하는 주기는 전술한 바와 같이 외부 디바이스가 홈 디바이스의 비밀 정보를 획득하기 위해 소요되는 예상 공격 시간보다 짧다.

[0052] 암호화된 안전 보증 메시지를 전송 받은 홈 디바이스는 안전 보증 메시지를 복호화 한다(S320). 이때, 복호화하는 방식은 안전 보증 메시지가 암호화된 방식에 의해 결정되는데, 안전 보증 메시지는 공유키 암호화 시스템 또는 공유키 암호화 시스템에 의해 암호화 될 수 있다. 이에 대하여, 도 2에서 상세하게 전술한 바 있으므로 이에 대한 설명은 생략하도록 한다. 복호화된 안전 보증 메시지는 랜덤수 및 오더의 조합으로 이루어져 있다.

[0053] 다음으로, 홈 디바이스는 복호화된 안전 보증 메시지가 유효한 메시지인지 여부를 판단한다(S330). 이때, 복호화된 안전 보증 메시지가 유효하다 함은 후술할 홈 디바이스의 디바이스 안전 정보의 형식과 일치함을 말한다. 랜덤수 및 오더의 조합으로 이루어진 안전 보증 메시지와 역시 동일하게 랜덤수 및 오더의 조합으로 이루어진 홈 디바이스의 디바이스 안전 정보의 형식이 일치하여야 한다. 이는 후에 복호화된 랜덤수 및 오더와 홈 디바이스의 디바이스 안전 정보가 동일한지 여부를 정확하게 판단하여야 하기 때문이다.

[0054] 복호화된 랜덤수 및 오더의 조합이 유효한 형식이 아닌 경우 마지막으로 유효한 랜덤수 및 오더의 조합이 전송된 후 소정의 시간이 경과되었는지 여부를 판단한다(S360). 여기서, 소정의 시간은 홈 디바이스에 마지막 랜덤수 및 오더의 조합이 전송 된 후 다음 타임 스탬프가 도착할 때까지 안전하다고 판단 내릴 수 있는 최대의 시간의 말한다. 따라서, 소정의 시간 경과 후에도 랜덤수 및 오더의 조합이 전송 되지 않는 경우 즉, 마지막 유효 랜덤수 및 오더의 조합이 전송된 후 소정이 시간이 지난 경우에는 홈 디바이스는 홈 디바이스의 비밀 정보가 외부 디바이스에 의해 유출될 수 있는 상황이라고 간주하여 휘발성 메모리에 저장된 비밀 정보를 삭제한다(S350). 그리고, 소정의 시간이 경과하지 않은 경우 즉 소정의 시간이 경과 전에 랜덤수 및 오더의 조합을 전송 받은 경우에는 다시 처음으로 돌아가 보호 방법을 수행하게 된다.

[0055] 복호화된 랜덤수 및 오더의 조합이 유효한 형식인 경우, 복호화된 랜덤수 및 오더의 조합과 홈 디바이스의 디바이스 안전 정보가 일치하는지 여부를 판단한다(S340). 이 경우, 홈 디바이스의 디바이스 안전 정보는 랜덤수 및 오더의 조합으로 이루어져 있음은 자명하다.

[0056] 복호화된 랜덤수 및 오더의 조합과 홈 디바이스의 디바이스 정보인 랜덤수 및 오더의 조합이 일치하는 경우 안전하다고 판단 된다(S370). 그리고, 홈 디바이스는 계속적으로 보호 방법을 수행하게 된다.

[0057] 그러나, 홈 디바이스의 디바이스 안전 정보인 랜덤수 및 오더의 조합과 제어장치에서 홈 디바이스로 전송된 안전 보증 메시지의 홈 네트워크 안전 정보인 랜덤수 및 오더의 조합이 일치하지 않은 경우, 외부 디바이스가 홈 네트워크에 침입했다고 판단하여 홈 디바이스는 휘발성 메모리에 저장된 비밀 정보를 삭제한다(S350).

[0058] 도 2와 도 3을 참조하여 설명한 홈 디바이스의 비밀 정보 보호 방법을 안전 우산 방법이라고 칭하며, 이하 안전 우산 방법은 상기와 같은 의미로 사용됨을 명확히 한다.

[0059] 본 발명의 홈 디바이스의 비밀 정보 보호 방법에 따라 상기와 같은 과정에 의해 홈 디바이스의 휘발성 메모리에 저장되어 있는 비밀 정보가 삭제된 홈 디바이스가 홈 네트워크에 재 참여를 원하는 경우, 코드 인증을 통하여 네트워크에 참여한 후 다시 비밀 정보를 복원하게 되는데 이에 대하여 후술하도록 한다.

[0060] 이하, 도 4을 참조하여 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 보호 방법에 의해 비밀 정보가 삭제된 홈 디바이스가 홈 네트워크에 재 참여를 원하는 경우 비밀 정보를 복원하는 과정에 대하여 살펴 본다. 도 4은 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 복원 과정에 대한 순서도 이다.

[0061] 복수의 홈 디바이스 중 전술한 바와 같은 비밀 정보 보호 방법에 의해 비밀 정보가 삭제된 홈 디바이스(121)는 제어장치(110)에 코드 인증을 요청한다(410). 이는 외부 공격자가 아닌 홈 네트워크에 포함된 홈 디바이스(121)임을 확인 받는 과정이다.

[0062] 비밀 정보 보호를 위해 휘발성 메모리에 저장되어 있는 비밀 정보를 모두 삭제한 홈 디바이스(121)가 네트워크에 재 참여하고자 한다면 본래 홈 네트워크에 포함된 홈 디바이스였음을 확인 받아야 한다. 이러한 과정을 코드 인증 과정이라고 칭하는데, 이러한 코드 인증 과정은 제어장치(110)가 홈 디바이스(121)에서 현재 실행되고 있는 코드를 포함하여 메모리상의 모든 코드와 데이터를 확인하는 과정이다.

[0063] 이러한 코드 인증 과정을 위해서는 코드 인증을 요청하는 디바이스 및 코드 인증을 요청 받은 디바이스 모두 동일한 코드를 가지고 있어야 한다. 따라서 제어장치(110)가 홈 디바이스(121)를 코드 인증하기 위해서는 제어장치(110)가 모르는 데이터는 제외되어야 한다.

[0064] 코드 인증은 보통 원격으로 실행 코드를 디바이스에게 전송해주고 이를 실행하게 하거나, 아니면 자체적으로 코드 인증을 위한 코드를 담고 있어 스스로의 메모리를 증명해 보일 수도 있다. 이 때, 중요한 것은 메모리에 코드 인증을 회피하고자 하는 다른 공격코드를 넣을 가능성을 완전히 배제하거나 다른 공격코드가 넣어져 있다면 이를 찾아내는 방법이다. 이러한 코드 인증 방법으로는 SWATT, PIONEER 또는 원격 코드 인증 방법 등이 있다.

[0065] 홈 디바이스(121)가 코드인증을 요청한 후 코드 인증이 되면, 제어장치(110)는 다른 복수의 홈 디바이스(121,122,123,…,12n-이하 12n이라 칭함)로 코드 인증 결과를 알린다(420).

[0066] 다음으로 홈 디바이스(121)는 비밀 정보 복원을 위해서 다른 홈 디바이스(12n)에 다른 홈 디바이스(12n)의 비 휘발성 메모리에 저장하고 있는 홈 디바이스(121)의 부분 비밀 정보들을 요청한다(430). 하나의 홈 디바이스의 비밀 정보는 다른 홈 디바이스에 분산 저장되어 있다. 이는 본 발명에 따른 홈 네트워크 상의 비밀 정보 방법에 의해 홈 디바이스의 휘발성 메모리에 저장되어 있던 비밀 정보가 삭제되는 경우 복원하기 어려워지기 때문이다.

[0067] 이렇게 하나의 홈 디바이스의 비밀 정보를 다른 홈 디바이스가 부분 비밀 정보의 형태로 비 휘발성 메모리에 저장하는 것을 비밀 공유(secret sharing)라고 칭한다. 이때, 부분 비밀 정보는 각 홈 디바이스의 비 휘발성 메모리에 저장되므로 비밀 정보 보호를 위해 전원이 차단되는 경우가 발생한다고 하더라도 부분 비밀 정보는 삭제되지 않고 계속 비 휘발성 메모리에 저장된 상태를 유지 할 수 있다.

[0068] 본 발명의 일 실시예에 따르면 하나의 홈 디바이스 비밀 정보는 임의의 상수를 가진 t-1차 다항식 $f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$ 을 만들고 각각의 다른 홈 디바이스에 $f(i)$의 값을 나누어 줌으로써 분산 저장 될 수 있다. 그리고 이 중에 t 개 이상의 부분 비밀 정보를 모았을 때 다항식의 상수를 복원하여 비밀 값 s를 찾을 수 있다. 이는 라그랑주(Lagrange) 보간법을 사용하면 된다. 여기서의 차수 t와 k(n개의 디바이스 중 비밀을 복구하기 위한 k개의 디바이스)는 홈 네트워크의 환경과 요구되는 보안 수준에 따라 정해진다.

[0069] 홈 디바이스(121)가 다른 복수의 홈 디바이스(12n)에 부분 비밀 요청하면, 다른 복수의 홈 디바이스(12n)는 비 휘발성 메모리에 저장하고 있던 홈 디바이스(121)의 부분 비밀 정보를 홈 디바이스(121)로 전송한다(440). 이때, 전송하는 부분 비밀 정보는 전술한 바 있는 $f(i)$ 값일 수 있으며, 이 경우 홈 디바이스(121)는 다른 복수

의 홈 디바이스(12n)로부터 전송 받은 $f(i)$ 값을 모아 라그랑주 보간법을 사용하여 비밀 값 s를 복원하게 된다.

[0070] 이하, 도 5를 참조하여 본 발명의 또 다른 실시예에 따른 홈 디바이스의 비밀 정보를 이용한 서비스 결과의 획득 방법에 대하여 살펴 본다. 도 5는 본 발명의 또 다른 실시예에 따른 홈 디바이스의 비밀 정보를 이용한 서비스 결과의 획득 방법에 대한 순서도 이다.

[0071] 서비스를 요청하고자 하는 홈 디바이스(121)는 제어 장치(110)에 코드 인증을 요청한다(510). 코드 인증은 전술한 바와 같이 서비스를 요청하고자 하는 홈 디바이스(121)가 홈 네트워크에 포함된 디바이스라는 것을 인증 받는 과정으로 외부 공격자와 홈 디바이스(121)를 구별하기 위한 과정이다.

[0072] 제어 장치(110)코드 인증을 요청한 홈 디바이스(121)는 다시, 제어 장치로 서비스를 요청한다(520). 이렇게 서비스 요청을 받은 제어 장치(110)는 복수의 다른 홈 디바이스(122,123,…,12n-이하, 12n으로 칭함)로 홈 디바이스(121)의 코드인증 결과를 알리는 메시지를 전송한다(520). 이러한 과정을 통해 서비스를 요청한 홈 디바이스(121)가 홈 네트워크에 포함되어 있던 홈 디바이스(121)임을 알 수 있다. 그리고 복수의 홈 디바이스(12n) 각각에는 홈 디바이스(121)의 비밀 정보가 부분 비밀 정보의 형태로 분산되어 저장되어 있다.

[0073] 코드 인증 결과가 복수의 다른 홈 디바이스(12n)로 알려지게 되면, 제어 장치(110)가 복수의 홈 디바이스(12n) 각각에 부분 서비스 요청을 하게 된다(540). 서비스 요청을 받은 복수의 홈 디바이스(12n)는 부분 서비스 요청에 대한 응답을 제어부(110)로 전송한다(550). 그리고, 제어부(110)는 부분 서비스 응답을 모아 홈 디바이스(121)로 서비스 응답을 전송하게 된다(560).

[0074] 이와 같이 상기와 같은 과정을 통해 부분 비밀 정보를 이용하여 어떠한 일을 수행한 후 수행된 결과들을 모아 원래 비밀 정보를 이용한 것과 동일한 결과를 얻을 수 있으므로 홈 디바이스(121)는 제어장치(110)에게 코드 인증 후에 서비스 요청(service request)을 이용하여 제어장치(110)에게 자신이 서비스 받고 싶다는 의사를 밝히고 이에 대한 서비스를 받을 수 있게 된다. 이와 같은 과정은 임계 암호화 기법을 이용하여 수행될 수 있다.

[0075] 이하, 도 6을 참조하여 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 보호 및 이후 홈 네트워크에 재참여한 홈 디바이스의 비밀 정보 복원 방법에 대하여 살펴보도록 한다. 도 6은 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 보호 및 복원 방법에 대한 제어 흐름도 이다.

[0076] 이는 전술한 바 있는 홈 디바이스의 비밀 정보 보호 방법 및 휘발성 메모리에 저장된 후 삭제된 비밀 정보를 복원하기 위한 방법을 결합한 방법이라고 볼 수 있다. 이에 본 발명의 이해 및 설명의 편의를 위하여 중복되는 부분의 설명은 생략하고 간략하게 개괄적 과정만을 살펴보도록 한다.

[0077] 외부 디바이스의 공격으로부터 홈 네트워크에 포함된 홈 디바이스의 비밀 정보를 보호하기 위해 외부 디바이스가 홈 네트워크에 침입하였다고 판단되는 경우, 홈 디바이스로 공급되는 전원을 차단하여 휘발성 메모리에 저장된 비밀 정보를 삭제한다. 따라서 비밀 정보가 삭제된 홈 디바이스는 홈 네트워크로의 재 참가 또는 삭제한 비밀 정보의 복원이 불가능해진다. 따라서 비밀 공유 방법을 통하여 삭제된 비밀 정보를 복원하는 방법이 홈 디바이스의 비밀 정보 보호 방법에 추가 될 필요가 있다.

[0078] 먼저 홈 네트워크에 참여 또는 재 참여를 원하는 홈 디바이스는 제어 장치에게 코드 인증을 요청한다(S610). 코드 인증이 이루어 졌는지 여부를 판단(S620)한 후, 코드가 인증되었으면 인증된 홈 디바이스의 비밀 정보를 복원한다(S630). 이때, 홈 디바이스의 코드 인증 과정 및 비밀 정보 복원 과정은 앞서 도 4 내지 도 5를 참조하여 설명한 바 있다. 이렇게 복원된 비밀 정보는 다시 홈 디바이스의 휘발성 메모리에 저장된다(S640). 비밀 정보가 복원된 홈 디바이스는 도2 내지 도3을 참조하여 전술한 바 있는 안전 우산 방법을 통하여 비밀 정보를 보호하게 된다(S650). 비밀 정보를 보호하기 위해 휘발성 메모리에 저장되어 있는 비밀 정보를 삭제한 홈 디바이스가 다시 홈 네트워크에 재 참여를 원하는 경우, 다시 제어 장치로부터 코드 인증을 요청(S610)한 후, 비밀 정보를 복원하게 된다.

[0079] 이하, 도 7을 참조하여 본 발명의 일 실시예에 따른 홈 디바이스의 내부 구조에 대하여 살펴보도록 한다. 도 7은 본 발명의 일 실시예에 따른 홈 디바이스의 내부 구조에 대한 구조도 이다.

[0080] 본 발명의 일 실시예에 따른 홈 디바이스(121)는 비밀 정보를 보호하기 위하여 휘발성 메모리(710)에 비밀 정보(SK, 711)를 저장하고 있다. 휘발성 메모리(710)에 저장된 비밀 정보(SK, 711)는 외부 디바이스가 홈 네트워크에 침입한 경우, 휘발성 메모리(710)로 공급되는 전원이 차단되어 삭제됨으로써 보호된다. 반면, 비 휘발성 메모리(720)에는 복수의 다른 홈 디바이스(12n) 각각의 부분 비밀 정보(S1,S2,S3,….,Sn, 721,722,723,….,72n - 이하, Sn,72n으로 칭함)가 저장되어 있다. 이렇게 홈 디바이스(121)가 복수의 다른 홈 디바이스(12n)의 부분 비밀 정보(Sn,72n)를 저장하여, 후에 복수의 다른 홈 디바이스가(12n) 부분 비밀 정보(Sn,72n)를 이용하여, 자신의 비밀 정보를 복원할 수 있게 한다.

[0081] 홈 디바이스(121)는 기본적으로 비밀 정보 보호를 위한 안전 우산(730), 전술한 바 있는 비밀 공유(740), 코드 인증(750) 및 임계 암호화(760) 부분으로 나뉜다.

[0082] 안전 우산(730)에서는 외부 디바이스에 의해 침입되었다고 판단되는 경우, 휘발성 메모리(710)에 저장된 비밀 정보(SK, 711)를 삭제하는 동작을 수행한다. 비밀 공유(740)에서는 홈 디바이스(121)의 비밀 정보(SK, 711)가 다른 복수의 홈 디바이스(12n)에 부분 비밀 정보의 형태로 분산 저장되고, 이를 다시 비밀 정보(SK, 711)로 복원한다. 코드 인증(750) 및 임계 암호화(760) 부분은 도 4 내지 도 5를 참조하여 전술한 바와 같다.

[0083] 그리고, 안전 우산(730) 방법 사용시, 안전 보증 메시지의 암호화 및 복호화를 위한 암호화(770)부분도 존재한다.

[0084] 한편, 상술한 홈 디바이스에서의 비밀 정보 보호 방법은 컴퓨터 프로그램으로 작성 가능하다. 상기 프로그램을 구성하는 코드들 및 코드 세그먼트들은 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 또한, 상기 프로그램은 컴퓨터가 읽을 수 있는 정보저장매체(computer readable media)에 저장되고, 컴퓨터에 의하여 읽혀지고 실행됨으로써 문서 탐색 서비스 제공 방법을 구현한다. 상기 정보저장매체는 자기 기록매체, 광기록매체, 및 캐리어 웨이브 매체를 포함한다.

[0085] 상기에서는 본 발명의 바람직한 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 이해할 수 있을 것이다.

도면의 간단한 설명

[0086] 도 1은 본 발명의 일 실시예에 따른 홈 네트워크 상의 비밀 정보 보호 방법의 개념도.

[0087] 도 2는 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 보호 방법의 제어 흐름도.

[0088] 도 3은 본 발명의 또 다른 실시예에 따른 홈 디바이스의 비밀 정보의 보호 방법에 대한 제어 흐름도.

[0089] 도 4은 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 복원 과정에 대한 순서도.

[0090] 도 5는 본 발명의 또 다른 실시예에 따른 홈 디바이스의 비밀 정보를 이용한 서비스 결과의 획득 방법에 대한 순서도.

[0091] 도 6은 본 발명의 일 실시예에 따른 홈 디바이스의 비밀 정보 보호 및 복원 방법에 대한 제어 흐름도.

[0092] 도 7은 본 발명의 일 실시예에 따른 홈 디바이스의 내부 구조에 대한 구조도.

[0093] <도면의 주요부분에 대한 부호의 설명>

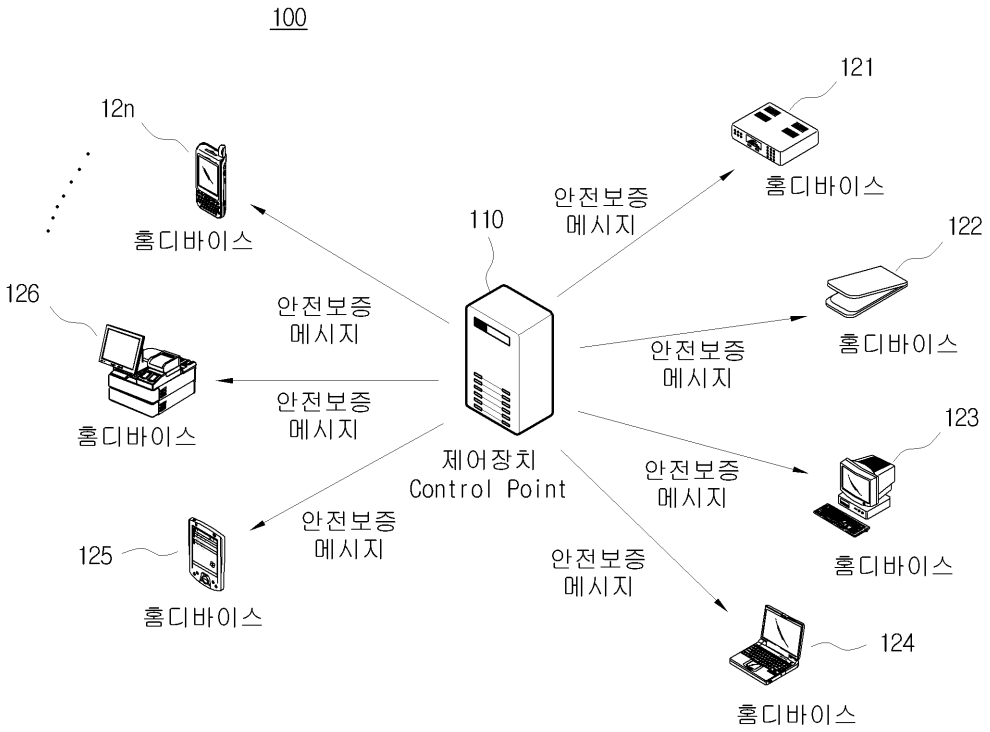
[0094] 100: 홈 네트워크

[0095] 110: 제어 장치

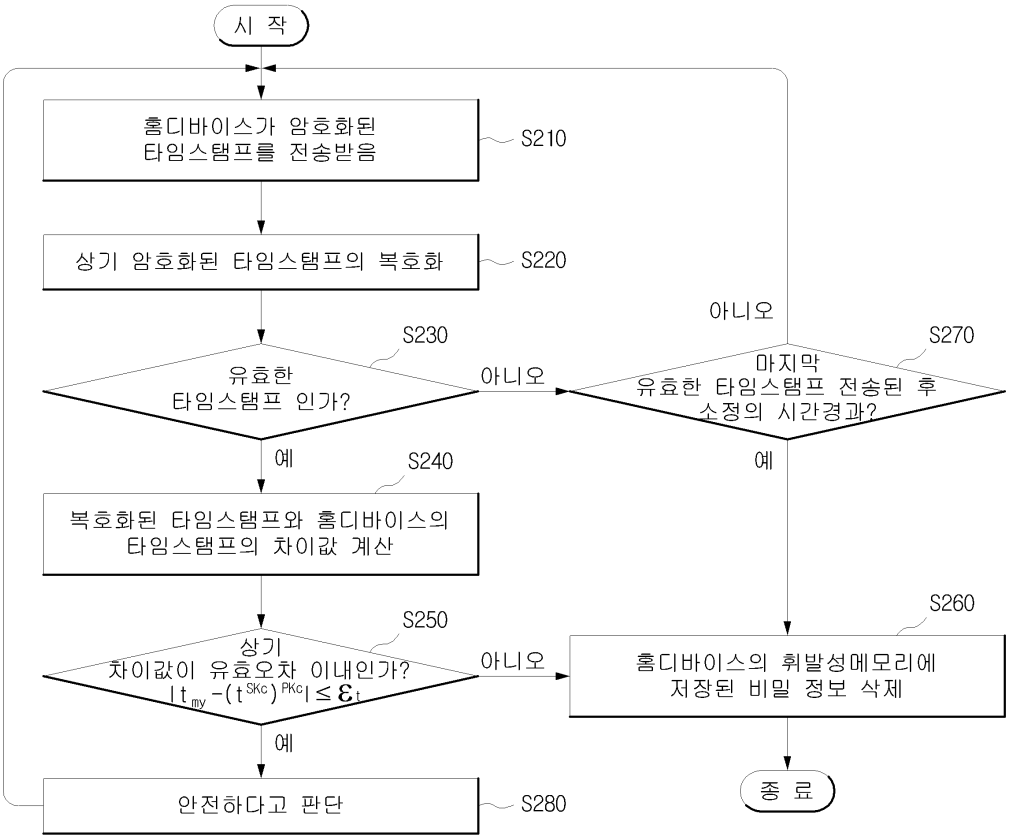
[0096] 12n: 홈 디바이스

도면

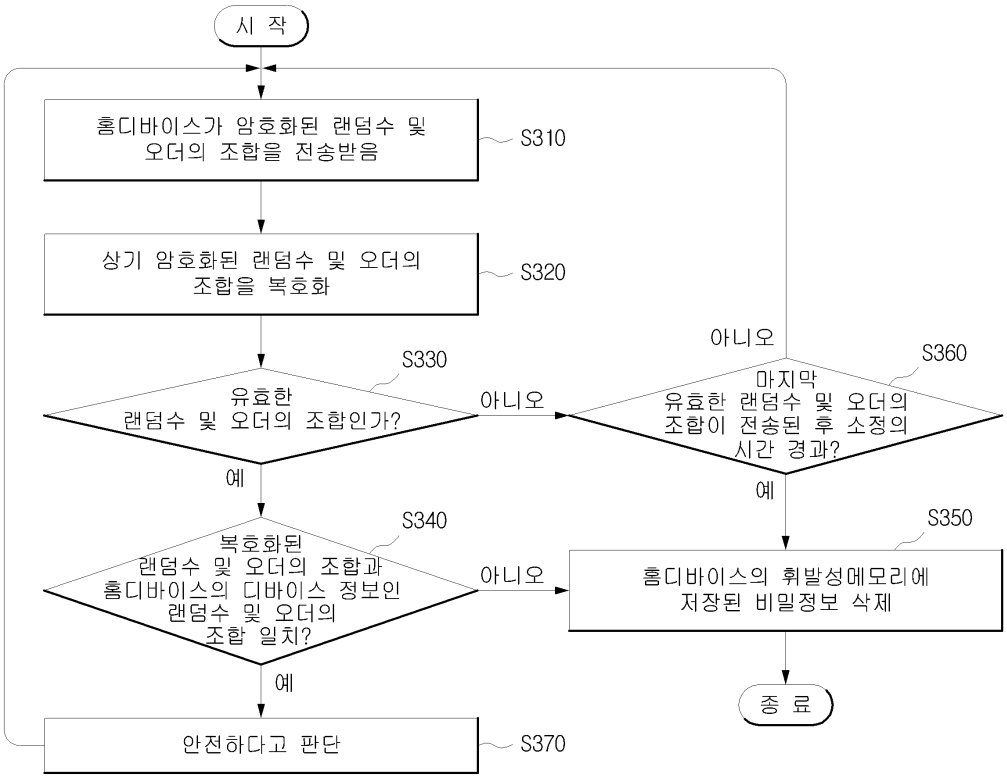
도면1


100
121
12n
홈디바이스
안전보증
메시지
110
122
126
안전보증
메시지
홈디바이스
안전보증
메시지
안전보증
메시지
123
제어장치
Control Point
안전보증
메시지
125
안전보증
메시지
안전보증
메시지
홈디바이스
124
홈디바이스

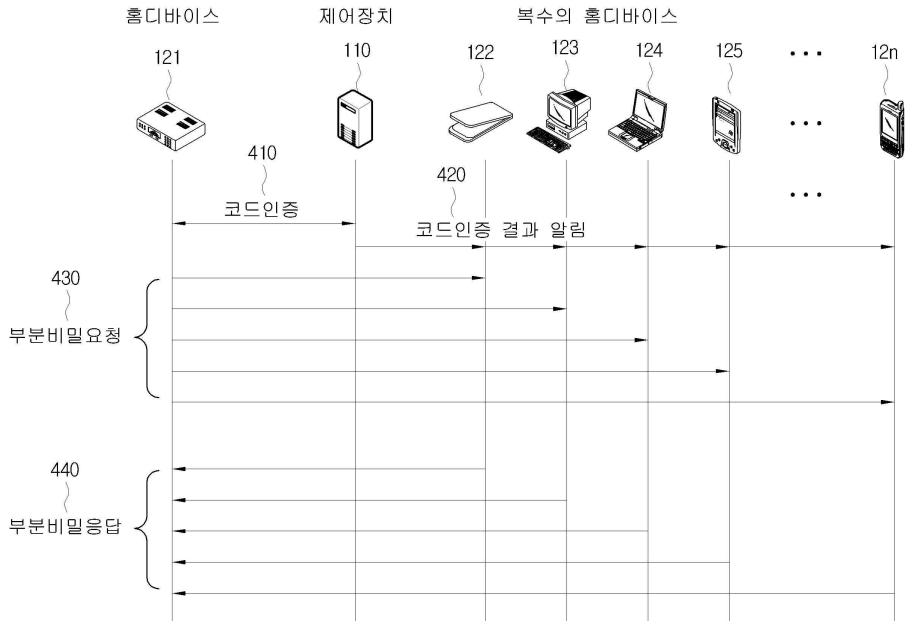
도면2


시 작
홈디바이스가 암호화된 타임스탬프를 전송받음
S210
상기 암호화된 타임스탬프의 복호화
S220
S230
유효한 타임스탬프 인가?
아니오
예
S240
복호화된 타임스탬프와 홈디바이스의 타임스탬프의 차이값 계산
S250
상기 차이값이 유효오차 이내인가?
$|t_{my}-(t^{Skc})^{Pkc}| \leq \varepsilon_t$
아니오
예
안전하다고 판단
S280
아니오
S270
마지막 유효한 타임스탬프 전송된 후 소정의 시간경과?
예
S260
홈디바이스의 휘발성메모리에 저장된 비밀 정보 삭제
종 료

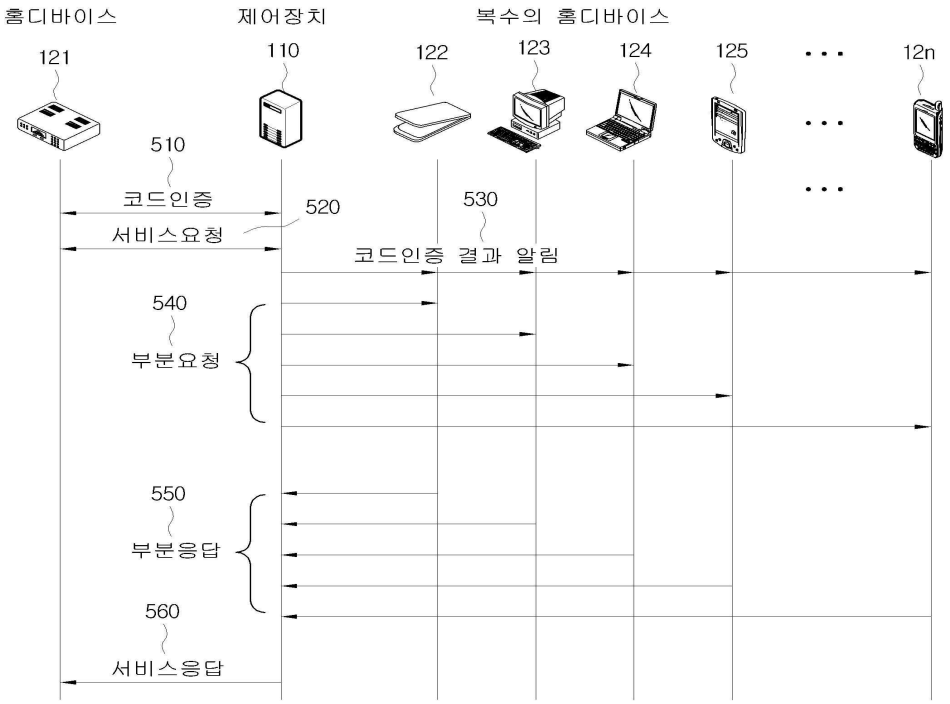
도면3


시 작
홈디바이스가 암호화된 랜덤수 및 오더의 조합을 전송받음
S310
상기 암호화된 랜덤수 및 오더의 조합을 복호화
S320
S330
유효한 랜덤수 및 오더의 조합인가?
아니오
예
S340
복호화된 랜덤수 및 오더의 조합과 홈디바이스의 디바이스 정보인 랜덤수 및 오더의 조합 일치?
아니오
예
안전하다고 판단
S370
아니오
S360
마지막 유효한 랜덤수 및 오더의 조합이 전송된 후 소정의 시간 경과?
예
S350
홈디바이스의 휘발성메모리에 저장된 비밀정보 삭제
종 료

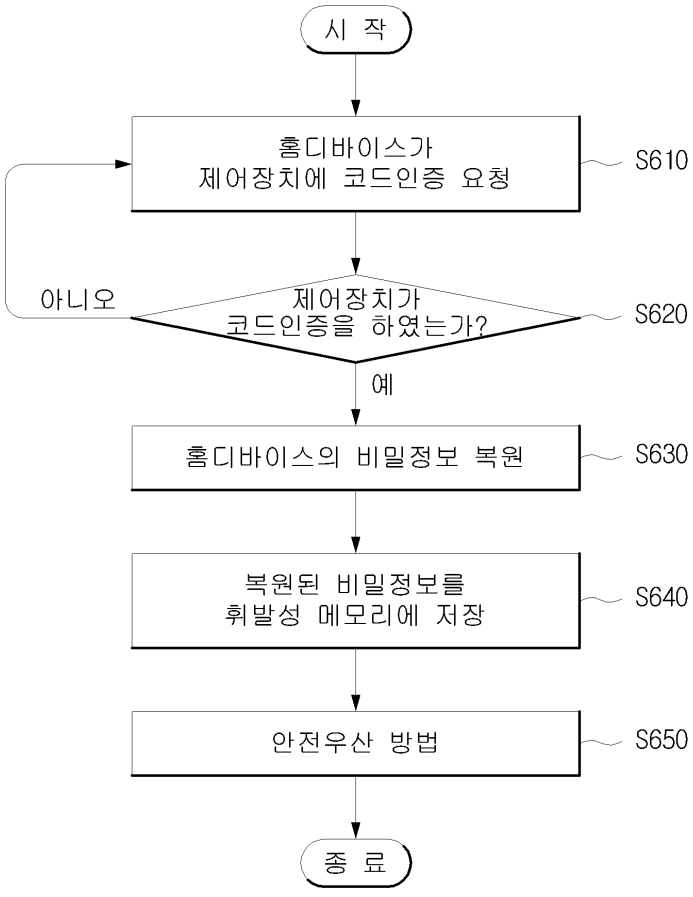
도면4


홈디바이스
121
제어장치
110
복수의 홈디바이스
122
123
124
125
12n
410
코드인증
420
코드인증 결과 알림
430
부분비밀요청
440
부분비밀응답

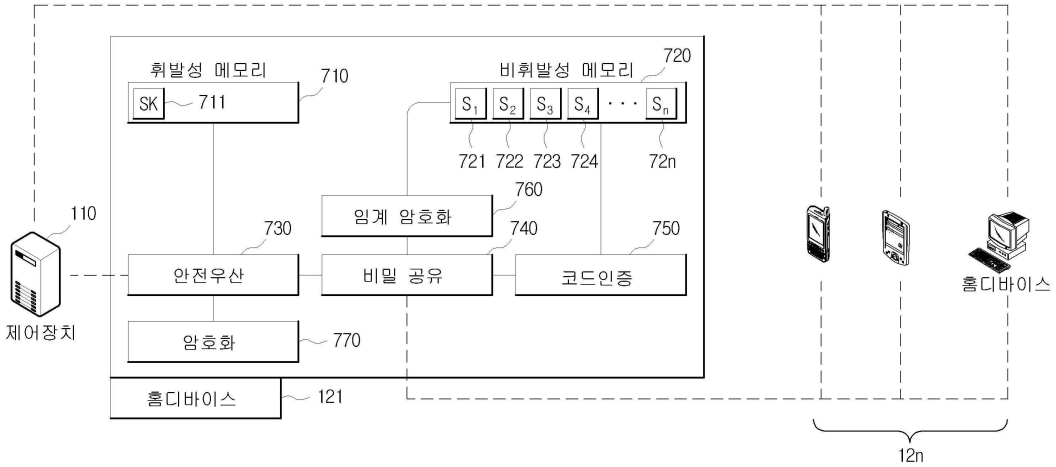
도면5


홈디바이스
제어장치
복수의 홈디바이스
121
110
122
123
124
125
12n
510
코드인증
520
서비스요청
530
코드인증 결과 알림
540
부분요청
550
부분응답
560
서비스응답

도면6


시 작
홈디바이스가
제어장치에 코드인증 요청
S610
아니오
제어장치가
코드인증을 하였는가?
S620
예
홈디바이스의 비밀정보 복원
S630
복원된 비밀정보를
휘발성 메모리에 저장
S640
안전우산 방법
S650
종 료

도면7


휘발성 메모리
710
SK
711
비휘발성 메모리
720
S1
S2
S3
S4
Sn
721
722
723
724
72n
760
임계 암호화
730
740
750
안전우산
비밀 공유
코드인증
110
제어장치
암호화
770
홈디바이스
121
홈디바이스
12n