(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0018025
(43) 공개일자 2011년02월23일

(51) Int. Cl.
H04W 12/06 (2009.01) *H04W 12/04* (2009.01)
H04W 12/02 (2009.01)
(21) 출원번호 10-2009-0075612
(22) 출원일자 2009년08월17일
심사청구일자 2009년08월17일

(71) 출원인
이화여자대학교 산학협력단
서울 서대문구 대현동 11-1 이화여자대학교내
(72) 발명자
조동섭
서울 송파구 문정동 패밀리아파트 223동 506호
서대희
서울 영등포구 도림동 대우 미래사랑 아파트 101-909
(뒷면에 계속)
(74) 대리인
특허법인우인

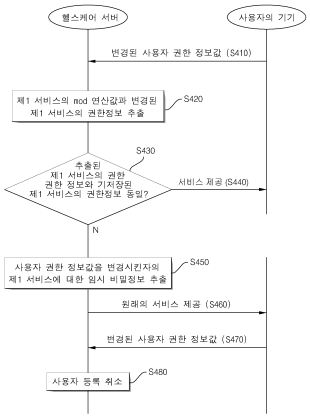
전체 청구항 수 : 총 8 항

(54) 사용자에 따라 서비스 제공을 제한하는 방법

(57) 요 약

서비스 제공방법 이 개시된다. 본 서비스 제공방법은, mod 연산을 이용하여 사용자 등록을 수행하는 단계; 1-out-2분실 통신로를 이용하여 사용자와 상호 통신을 위한 세션키를 생성하는 단계; 서비스에 따른 사용자 권한 정보를 설정하는 단계; 및 상기 설정된 사용자 권한 정보에 대응되는 서비스를 제공하는 단계;를 포함한다. 그리하여 추가적인 기기를 이용하지 않고 기본적인 기기 즉 서비스를 제공하는 기기와 서비스를 제공받는 기기를 기준으로 사용자의 프라이버시 보호 및 관리의 효율성을 갖으면서 서비스를 제공하는 보안사항을 관리할 수 있는 효과가 있다.

대 표 도 - 도4



(72) 발명자

백장미

서울 영등포구 도림동 대우 미래사랑아파트 101-909

유승희

경기도 남양주시 도농동 부영아파트5단지 502-2504

이 발명을 지원한 국가연구개발사업

과제고유번호 핵C6A1907

부처명 교육과학기술부

연구관리전문기관

연구사업명 2단계 두뇌한국(BK)21 사업

연구과제명 U-Commerce 소프트웨어 여성전문인력양성사업

기여율

주관기관 이화여자대학교 산학협력단

연구기간 2006년 3월 1일 ~ 2013년 2월 28일

특허청구의 범위

청구항 1

mod 연산을 이용하여 사용자 등록을 수행하는 단계;

1-out-2분실 통신로를 이용하여 사용자와 상호 통신을 위한 세션키를 생성하는 단계;

서비스에 따른 사용자 권한 정보를 설정하는 단계; 및

상기 설정된 사용자 권한 정보에 대응되는 서비스를 제공하는 단계;를 포함하는 것을 특징으로 하는 서비스 제공방법.

청구항 2

제 1항에 있어서,

상기 사용자 등록을 수행하는 단계는,

서비스 메시지, 랜덤 수 및 공개 계수를 기초로 mod 연산하여 암호화시킨 서비스를 사용자 기기에 브로드캐스팅하는 단계;

제공받고자 하는 서비스에 대한 서비스 요청값이 다른 서비스의 mod 연산값을 기반으로 암호화되어, 상기 사용자의 기기로부터, 수신받는 단계;

상기 서비스 요청값을 기초로 사용자 임시 비밀 정보 및 서비스 요청 응답값을 산출하여 상기 사용자의 기기로 전송하는 단계;

상기 서비스 요청 응답값을 포함하는 서비스 제공 요청값을 상기 사용자의 기기로부터 수신받는 단계; 및

상기 서비스 제공 요청값에 포함되어 있는 서비스 응답값이 기산출된 서비스 응답값과 동일하면, 상기 사용자의 기기에 제공하고자 하는 서비스에 대한 임시 비밀값을 산출하여 저장함으로써, 상기 사용자 등록을 수행하는 단계;를 포함하는 것을 특징으로 하는 서비스 제공방법.

청구항 3

제 1항에 있어서,

상기 세션키를 생성하는 단계;

상기 사용자의 기기와의 암호 통신을 위한 임시 세션키 쌍을 생성하여 상기 사용자의 기기에게 전송하는 단계;

상기 사용자의 기기로부터 상기 임시 세션키 쌍 및 서비스 권한 정보의 기초값에 기초한 세션키의 기본 정보를 수신받는 단계; 및

상기 세션키의 기본 정보를 이용하여 세션키를 생성하는 단계;를 포함하는 것을 특징으로 하는 서비스 제공방법.

청구항 4

제 3항에 있어서,

상기 임시 세션키 쌍을 수신받은 사용자는 1-out-2분실 통신로를 복수 번 수행하여 상기 임시 세션키 쌍의 구성요소가 0이면, 상기 세션키의 기본 정보를 산출하는 것을 특징으로 하는 서비스 제공방법.

청구항 5

제 1항에 있어서,

상기 사용자 권한 정보를 설정하는 단계는

상기 사용자의 기기에 제공하고자 하는 서비스에 대한 서비스 권한 정보값을 산출하여 상기 사용자의 기기에 전송하는 단계;

상기 서비스 권한 정보값을 이용하여 산출된 사용자 권한 정보값을 상기 사용자의 기기로부터 수신받는 단계; 및

상기 수신된 사용자 권한 정보 값을 복호화하여 상기 서비스 권한 정보 및 상기 서비스의 mod 연산값을 일대일 대응하여 저장하는 단계;를 포함하는 것을 특징으로 하는 서비스 제공방법.

청구항 6

제1 항에 있어서,

상기 서비스를 제공하는 단계는,

상기 설정된 사용자 권한 정보와 동일한 사용자 권한 정보를 갖는 사용자로부터 서비스 제공을 요청받는 경우, 상기 설정된 사용자 권한 정보에 대응되는 서비스를 제공하는 것을 특징으로 하는 서비스 제공방법.

청구항 7

제1 항에 있어서,

상기 서비스를 제공하는 단계는,

상기 설정된 사용자 권한 정보와 다른 사용자 권한 정보를 갖는 사용자로부터 서비스 제공을 요청받는 경우, 상기 사용자가 갖는 사용자 권한 정보에 대응되는 서비스를 제공하는 것을 특징으로 하는 서비스 제공방법.

청구항 8

제7 항에 있어서,

상기 설정된 사용자 권한 정보와 다른 사용자 권한 정보를 갖는 사용자로부터 재차 서비스 제공을 요청받은 경우, 상기 다른 사용자 권한 정보를 갖는 사용자의 사용자 등록을 취소하는 것을 특징으로 하는 서비스 제공방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명의 서비스 제공방법에 관한 것으로, 보다 구체적으로 사용자에 따라 서비스 제공을 제한하는 방법에 관한 것이다.

배 경 기 술

[0002] 기존의 서비스 제공방식 특히 헬스케어 방식은 크게 2가지로 요약할 수 있으며 첫 번째로 실제 네트워크 기반의 헬스케어 서비스를 제공하기 위한 방식이다. 본 방식의 경우 통신상의 안전성과 사용자 정보의 안전성 확보 및 접근 제어를 제공한다. 따라서 신뢰된 헬스케어 서비스를 규정하고 안전한 통신 방법을 제공할 수 있는 아키텍처를 제시함으로써 안전한 통신과 관리의 효율성을 제공하고자 하였다.

[0003] 그러나 본 방식의 경우 통신상의 안전성 측면에서 통신상의 안전성을 위하여 인증서 기반으로 XML 서명과 암호화 방식을 이용하였다. 그러나 구체적인 통신에 대한 방식을 제시하지 않았으며, 관리적인 측면에서 미들웨어에서 제공되는 통신상의 보안을 정책적으로 규정함으로써 사용자의 기기와 시스템간의 통신상에서의 안전성을 확보할 수 없다.

[0004] 또한 저장, 전송 데이터의 안전성은 별도의 미들웨어를 정의하고 해당 미들웨어에서 이를 관리하도록 하였다. 그러나 저장 데이터 측면에서 별도의 보안 서비스를 제공하지 않아 저장 데이터에 대한 안전성을 보장할 수 없다. 따라서 모든 데이터에 대한 별도의 접근 제어 서비스를 통해 사용자의 기기의 접근 제어를 제공해야 하지만 본 방식에서는 별도의 접근 제어 방식을 제공하지 않는다. 이와 더불어 각각의 보안 서비스를 위해 해당 보안 서비스별 미들웨어를 필요로 함으로써 부가적인 미들웨어 증가로 인해 내부 통신의 증가와 이를 통합적으로 관리해야 하는 취약성을 내포하고 있다.

[0005] 두번째로 Ross 방식은 안전한 통신을 통해 헬스케어 서비스를 디바이스를 통해 제공받는다. 사용자의 기기는 홈 네트워크 환경에서 사용자의 기기의 개인 디바이스의 근거리 무선 통신을 통해 헬스케어 정보를 제공받고 사용자의 기기의 헬스케어 정보는 외부 공개 네트워크를 통해 헬스케어 센터에 제공된다.

[0006] 따라서 각각의 근거리 무선통신 기술에 대한 안전성과 사용자 정보의 전송시 안전한 통신 과정을 제한함으로써 홈 네트워크 환경에서의 안전하고 효율적인 헬스케어 서비스를 제공하는 방식이다. 그러나 본 방식의 경우 통신상의 안전성 측면에서 근거리 무선통신을 기반으로 홈 네트워크 환경에서의 안전성을 제공하는 헬스케어 서비스를 제공하고자 하였다. 그러나 기존의 근거리 무선 통신 기술의 보완 사항 없이 그대로를 적용함으로써 기존 근거리 무선 통신의 취약성을 그대로 내포하고 있다. 따라서 전송 데이터의 경우 블루투스의 자체 보안 서비스나 WEP를 이용하였다.

[0007] 그러나 블루투스 자체 보안 서비스와 WEP의 경우 전송 데이터의 안전성 및 저장 데이터에 대한 보안 취약성을 내포하고 있어 본 방식에서는 데이터의 안전성을 보장하지 못한다. 또한 Ross방식에서는 멀티레이어 보안을 제시하였다. 이는 다수의 근거리 무선 통신 보안 기술을 구조적인 측면에서 제공함으로써 사용자의 프라이버시를 보호 하고자 하였다. 그러나 해당 사용자 프라이버시 정보가 전송될 때 공격자로부터 안전성을 보장하기 위한 별도의 방식이 없이 사용자 프라이버시 보호에 대한 문제점을 내포하고 있다. 따라서 Ross 방식은 내부 네트워크에 대한 안전성 확보를 통해 홈 네트워크 기반의 안전한 헬스케어 시스템을 구축하고자 하였다. 그러나 다양한 근거리 무선 통신 그룹을 멀티 레이어에 적용하기 위해서는 별도의 관리 체계가 요구됨으로서 관리의 효율성이 저하된다.

발명의 내용

해결 하고자하는 과제

[0008] 본 발명은 상기한 문제점을 해결하기 위해 인가되지 않은 제 3자에 의한 서비스의 불법적인 접근을 방지하기 위하여 사용자의 기기의 안전한 인증 및 관리 방식을 제공함에 목적이 있다.

[0009] 또한, 본 발명은 효율적인 형태의 보안 서비스 제공를 통해 전체 네트워크의 효과적인 보안 관리를 지원할 뿐 아니라, 사용자 프라이버시 보호 정보들에 대한 안전성을 확보하여 네트워크 공격자로부터 네트워크의 안전 및 사용자의 프라이버시를 보호할 수 있는 관리 방법을 제공함에 다른 목적이 있다.

과제 해결수단

[0010] 상기 목적을 달성하기 위한 본 발명에 따른, 서비스 제공방법은, mod 연산을 이용하여 사용자 등록을 수행하는 단계; 1-out-2분실 통신로를 이용하여 사용자와 상호 통신을 위한 세션키를 생성하는 단계; 서비스에 따른 사용자 권한 정보를 설정하는 단계; 및 상기 설정된 사용자 권한 정보에 대응되는 서비스를 제공하는 단계;를 포함한다.

[0011] 그리고, 상기 사용자 등록을 수행하는 단계는, 서비스 메시지, 랜덤 수 및 공개 계수를 기초로 mod 연산하여 암호화시킨 서비스를 사용자 기기에 브로드캐스팅하는 단계; 제공받고자 하는 서비스에 대한 서비스 요청값이 다른 서비스의 mod 연산값을 기반으로 암호화되어, 상기 사용자의 기기로부터, 수신받는 단계; 상기 서비스 요청값을 기초로 사용자 임시 비밀 정보 및 서비스 요청 응답값을 산출하여 상기 사용자의 기기로 전송하는 단계;상기 서비스 요청 응답값을 포함하는 서비스 제공 요청값을 상기 사용자의 기기로부터 수신받는 단계; 및 상기 서비스 제공 요청값에 포함되어 있는 서비스 응답값이 기산출된 서비스 응답값과 동일하면, 상기 사용자의 기기에 제공하고자 하는 서비스에 대한 임시 비밀값을 산출하여 저장함으로써, 상기 사용자 등록을 수행하는 단계;를 포함하는 것이 바람직하다.

[0012] 또한, 상기 세션키를 생성하는 단계; 상기 사용자의 기기와의 암호 통신을 위한 임시 세션키 쌍을 생성하여 상기 사용자의 기기에게 전송하는 단계; 상기 사용자의 기기로부터 상기 임시 세션키 쌍 및 서비스 권한 정보의 기초값에 기초한 세션키의 기본 정보를 수신받는 단계; 및 상기 세션키의 기본 정보를 이용하여 세션키를 생성하는 단계;를 포함하는 것이 바람직하다.

[0013] 그리고, 상기 임시 세션키 쌍을 수신받은 사용자는 1-out-2분실 통신로를 복수 번 수행하여 상기 임시 세션키 쌍의 구성요소가 0이면, 상기 세션키의 기본 정보를 산출하는 것이 바람직하다.

[0014] 또한, 상기 사용자 권한 정보를 설정하는 단계는 상기 사용자의 기기에 제공하고자 하는 서비스에 대한 서비스 권한 정보값을 산출하여 상기 사용자의 기기에 전송하는 단계; 상기 서비스 권한 정보값을 이용하여 산출된 사

용자 권한 정보값을 상기 사용자의 기기로부터 수신받는 단계; 및 상기 수신된 사용자 권한 정보 값을 복호화하여 상기 서비스 권한 정보 및 상기 서비스의 mod 연산값을 일대일 대응하여 저장하는 단계;를 포함하는 것이 바람직하다.

[0015] 그리고, 상기 서비스를 제공하는 단계는, 상기 설정된 사용자 권한 정보와 동일한 사용자 권한 정보를 갖는 사용자로부터 서비스 제공을 요청받는 경우, 상기 설정된 사용자 권한 정보에 대응되는 서비스를 제공하는 것이 바람직하다.

[0016] 또한, 상기 서비스를 제공하는 단계는, 상기 설정된 사용자 권한 정보와 다른 사용자 권한 정보를 갖는 사용자로부터 서비스 제공을 요청받는 경우, 상기 사용자가 갖는 사용자 권한 정보에 대응되는 서비스를 제공하는 것이 바람직하다.

[0017] 그리고, 상기 설정된 사용자 권한 정보와 다른 사용자 권한 정보를 갖는 사용자로부터 재차 서비스 제공을 요청받은 경우, 상기 다른 사용자 권한 정보를 갖는 사용자의 사용자 등록을 취소하는 것이 바람직하다.

효 과

[0018] 본 발명에 의하면, 추가적인 기기를 이용하지 않고 기본적인 기기 즉 서비스를 제공하는 기기와 서비스를 제공받는 기기를 기준으로 사용자의 프라이버시 보호 및 관리의 효율성을 갖으면서 서비스를 제공하는 보안사항을 관리할 수 있는 효과가 있다.

[0019] 또한, 본 발명은 사용자 측면에서는 임시 비밀값에 기반한 사용자 등록 과정을 거쳐 OP_1^2 통신으로 통신의 효율성을 제공하였으며, 사용자와 서비스에 대하여 접근제어 방식을 제공함으로써 불법적인 제 3자에 의한 불법적인 데이터 접근이 가능한 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0020] 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.

[0021] 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 아니되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다.

[0022] 따라서, 본 명세서에 기재된 실시예와 도면에 도시된 구성은 본 발명의 가장 바람직한 일실시예에 불과할 뿐이고 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형예들이 있을 수 있음을 이해하여야 한다.

[0023] 도 1은 본 발명의 일 실시예에 따른 특정 서비스를 제공받고자 하는 사용자 등록 과정을 설명하기 위한 흐름도이다.

[0024] 헬스케어 서버는 헬스케어 서버가 제공하는 서비스를 mod 연산값으로 암호화하여 사용자의 기기들에게 브로드캐스팅한다(S110). 구체적으로 헬스케어 서버는 헬스케어 서버가 제공하는 서비스 중 제i 서비스를 사용자의 기기에게 제공하기 위해 제i 서비스 메시지(m_i)를 밑수로 하고, 제1 랜덤 수(α_A)를 제곱수로 하며, 공개계수(n)을 나눌 수로 하는 mod 연산값인 제i 서비스 mod 연산값(c_i)을 하기와 같이 산출한다. 여기서 제1 랜덤 수(α_A)는 헬스케어 서버가 서비스 mod 연산값을 산출할 때 정수 중에서 임의로 선택한 값이다. 그리고, 제i 서비스 mod 연산값(c_i)을 사용자의 기기에게 브로드캐스팅한다.

[0025] $$c_i = m_i^{\alpha_A} \bmod n$$

[0026] 여기서 제i 서비스 mod 연산값(c_i)은 헬스케어 서버에 제공되는 제i 서비스를 특정하며 제i 서비스 메시지(m_i)와도 일대일 대응된다.

[0027] 사용자의 기기는 헬스케어 서버로부터 브로드 캐스팅된 서비스 중 제공받고자 하는 서비스에 대한 서비스 요청값을 다른 서비스의 mod 연산값을 기반으로 암호화하고 그것을 헬스케어 서버에 전송한다(S120).

[0028] 예를 들어 사용자는 헬스케어 서버가 제공하는 서비스 중 제1 서비스를 제공받고자 하는 경우, 사용자의 명령에 따라 사용자의 기기는 다른 서비스 예를 들어, 제2 서비스의 mod 연산값(c_2) 및 제3 서비스의 mod 연산값(c_3)을 기반으로 하기와 같은 제1 서비스 요청값(l_1)를 생성한다.

$$C_1 = c_1 \oplus m_1 \oplus ID_{s_1} ,$$

[0029]

$$b_1 = c_2 * c_3 * r_{s_1} , \quad l_1 = C_1^{b_1} \bmod n$$

[0030] 여기서, c_1 은 제1 서비스에 대한 정보로서, 제1 서비스 mod 연산값(c_1), 제1 서비스 메시지(m_1) 및 제1 서비스를 제공받고자 하는 사용자의 아이디(ID_{S_1})의 논리합이다. b_1 은 제1 서비스의 암호값으로서, 제2 서비스 mod 연산값(c_2), 제3 서비스 mod 연산값(c_3) 및 제2 랜덤수(r_{s_1})의 곱으로 표현할 수 있다. 여기서 제2 랜덤 수는 사용자의 기기가 제1 서비스 요청 값을 생성할 때 정수 중에서 임의로 선택한 값이다. 제1 서비스 요청값은 제1 서비스에 대한 정보(C_1), 제1 서비스의 암호값(b_1) 및 공개 계수(n)를 mod 연산을 이용하여 암호화된 값이다.

[0031] 헬스케어 서버는 사용자의 기기로부터 전송된 제1 서비스 요청값을 복호화하고 제1 서비스 요청값에 포함되어 있는 인자를 이용하여 사용자의 기기에 대한 복수 개의 임시 비밀 정보인 제1 사용자 임시 비밀 정보(u_1) 및 제2 사용자 임시 비밀 정보(l_{hs})를 산출한다. 그리고, 정수 중에서 제3 랜덤 수(r_{hs})를 선택한 후 제2 사용자 임시 비밀 정보 (l_{hs}) 및 서비스 요청 응답값인 제1 서비스 요청 응답값(l_{hs_1})을 하기와 같이 산출하여 사용자의 기기에 전송한다(S130).

[0032]

$$u_1 = c_1 * c_2 * c_3 ,$$

[0033]

$$l_{hs} = l_1^{u_1^{-1}} \bmod n , \quad l_{hs_1} = l_{hs}^{r_{hs}} \bmod n$$

[0034] 여기서, 제1 사용자 임시 비밀 정보(u_1)는 제1 내지 제3 서비스의 mod 연산값(c_1 , c_2 및 c_3)의 곱으로 나타내고, 제2 사용자의 임시 비밀 정보 (l_{hs}) 는 제1 서비스 요청값(l_1), 제1 사용자 임시 비밀 정보(u_1)의 역수 및 공개 계수(n)를 기초로 mod 연산한 값이고, 제1 서비스 요청 응답값(l_{hs_1})은 제2 사용자

임시 비밀 정보 (l_{hs}), 제3 랜덤 수(r_{hs}) 및 공개 계수(n)를 기초로 mod 연산한 값이다.

[0035] 사용자의 기기는 헬스케어 서버로부터 전송된 제2 사용자 임시 비밀 정보 (l_{hs})에 대한 검증을 수행한다(S140). 제2 사용자 임시 비밀 정보 (l_{hs})를 검증하기 위해 사용자의 기기는 제2 사용자 임시 비밀 정보 (l_{hs})를 복호화하고, 제2 사용자 임시 비밀 정보 (l_{hs})에 포함되어 있는 서비스 요청 값이 사용자의 기기가 생성한 제1 서비스 요청값(l_1)과 동일하면, 사용자의 기기는 제2 사용자의 기기 임시 비밀 정보 (l_{hs})가 올바르다고 판단한다.

[0036] 제2 사용자의 기기 임시 비밀 정보 (l_{hs})가 올바르면(S140-Y), 사용자의 기기는 서비스 제공 요청값인 제1 서비스 제공 요청값(l_1')를 하기와 같이 산출하여 헬스케어 서버에 전송한다(S150).

[0037]
$$l_1' = l_{hs_1}^{r_{s1}^{-1}} \bmod n$$

[0038] 도시된 바와 같이, 사용자의 기기는 제1 서비스 제공 요청값(l_1')을 제1 서비스 응답값(l_{hs_1}), 제1 서비스의 랜덤수(r_{s_1})의 역수 및 공개 계수(n)를 기초로 mod 연산하여 획득한다.

[0039] 헬스케어 서버는 사용자의 기기로부터 전송된 서비스 제공 요청값인 제1 서비스 제공 요청값(l_1')을 검증한다(S160). 구체적으로, 헬스케어 서버는 제1 서비스 제공 요청값(l_1')을 복호화하여 제1 서비스 응답값을 획득한다. 획득된 제1 서비스 응답값이 헬스케어 서버가 생성한 제1 서비스 요청 응답값(l_{hs_1})와 동일하면, 헬스케어 서버는 제1 서비스 제공 요청값(l_1')이 올바르다고 판단한다.

[0040] 헬스케어 서버는 사용자의 기기로부터 전송된 제1 서비스 제공 요청값(l_1')이 올바르다고 판단되면(S160-Y), 제공하고자 하는 서비스에 대한 임시 비밀값인 제1 서비스에 대한 임시 비밀값(y_{u_1})을 하기와 같이 산출하여 저장한다(S170).

[0041]
$$y_{u_1} = (l_1')^{\alpha_A} \bmod n$$

[0042] 상기와 같이, 제1 서비스에 대한 임시 비밀값 (y_{u_1})은 제1 서비스 제공 요청값(l_1'), 제1 랜덤수(α_A), 및 공개 계수(n)를 기초로 mod 연산한 값이다.

[0043] 상기와 같이, 사용자는 자신이 제공받고자 서비스에 대한 사용자 등록을 mod 연산을 이용하여 암호화한 뒤 헬스케어 서버와 통신을 하기 때문에 사용자의 기기 등록이 보다 안전하다.

[0044] 도 2는 본 발명의 일 실시예에 따른 사용자와 헬스케어 서버간의 상호 통신을 위한 세션키 생성 방법에 제공되

는 흐름도이다.

[0045] 헬스케어 서버와 사용자의 기기는 Chang' s OP_1^2 (1-out-2분실 통신로)를 이용하여 안전한 통신 과정을 수행하는 것이 바람직하다.

[0046] 헬스케어 서버는 정수 중에서 제4 랜덤수(r_y)를 선택하고, 사용자의 기기와의 암호 통신을 위한 임시 세션키 쌍인 $(r_y, v_{ij} + r_{ij})$ 를 생성하여 사용자의 기기에게 전송한다(S210). 임시 세션키 쌍 중 제1 랜덤수를 제1 임시 세션키이고, $v_{ij} + r_{ij}$ 를 제2 임시 세션키라고 한다. 그리고, 제2 임시 세션키인 $v_{ij} + r_{ij}$ 중 $v_{ij} = 2^{j-1} x^i$ 이고, r_{ij} 는 임시 세션키 쌍을 생성할 때 헬스케어 서버가 정수 중에서 선택한 제5 랜덤수이다. 그리고, 여기서 $i \in \{1,...,d\}$ 및 $i \in \{1,...,d\} = [d]$ $j \in \{1,...,m\} = [m]$ 이고, d 및 m은 정수이다.

[0047] 사용자의 기기는 제1 다항식($P(x)$)을 하기와 같이 정의하고, 헬스케어 서버에 전송한다.

[0048] $$P(x) = \sum_{i=0}^{d} a_i x_i \quad , \quad a_i = \sum_{j \in [m]} a_{ij} 2^{j-1}$$

[0049] 여기서, a_{ij} 는 분실 통신로의 검증값이다.

[0050] 사용자의 기기는 OP_1^2 (1-out-2분실 통신로)를 $i * j$ 번을 반복 수행한 뒤 a_{ij} 및 $v_{ij} + r_{ij}$ 중 적어도 하나가 0인지를 확인한다.

[0051] a_{ij} 및 $v_{ij} + r_{ij}$ 중 적어도 하나가 0인 것으로 확인되면, 사용자의 기기는 $a_0 + \sum_{d*m} (r_{ij} \mid v_{ij} + r_{ij})$ 를 산출하여 헬스케어 서버에 전송한다.

[0052] 헬스케어 서버와 사용자의 기기는 다음과 같이 mod 연산을 이용하여 세션키를 생성한다(S240).

[0053] $$Sk_{temp} = (y_{u_1} \oplus a_0 + \sum_{d*m} (r_{ij} \mid v_{ij} + r_{ij})) \bmod n$$

[0054] 도 3은 본 발명의 일 실시예에 따른 서비스에 따른 사용자의 권한 정보 설정 방법에 제공되는 흐름도이다.

[0055] 사용자의 기기는 특정 서비스에 대한 권한 설정을 헬스케어 서버에 요청한다. 설명의 편의를 도모하기 위해 상기한 특정 서비스를 제1 서비스라고 한다.

[0056] 헬스케어 서버는 제1 서비스에 대한 권한 정보를 설정하여 하기와 같은 서비스 권한 정보값(w)를 생성하여 전송한다(S310).

[0057] $$w = E_{Sk_{temp}} (a \| m_1) + h(m_1 \| t_{hs})$$

[0058] 여기서, a는 전체 분신 통신로 검증값이고, m_1 은 제1 서비스 메시지이며, t_{hs} 는 권한 정보값을 전송하는 시간이다. 권한 정보값은 a 및 m_1 을 세션키로 암호 알고리즘화한 값과 m_1 및 t_{hs} 을 해쉬 알고리즘화한

값의 합이다. 특히 $a=(a_1, a_2, \ldots, a_n)$ 이고, a_i 는 제i 서비스의 권한 정보이다.

[0059] 사용자의 기기는 서비스 권한 정보값(w) 중 암호 알고리즘화한 값($E_{Sk_{temp}}(a \| m_1)$)을 기설정된 세션키로 복호화 한 뒤 해쉬 알고리즘화한 값($h(m_1 \| t_{ks})$)를 검증하여 서비스 권한 정보값(w)에 대한 검증을 수행한다(S320).

[0060] 서비스 권한 정보값(w)에 대한 검증은 암호 알고리즘화한 값($E_{Sk_{temp}}(a \| m_1)$)에 포함되어 있는 제1 서비스 메시지와 해쉬 알고리즘화한 값($h(m_1 \| t_{ks})$)에 포함되어 있는 제1 서비스 메시지의 동일성 여부로 판단한다.

[0061] 검증이 올바른 경우(S320-Y) 사용자의 기기는 서비스 권한 정보값에서 전체 서비스에 대한 권한 정보(a)의 위수 (s)를 산출한 뒤 사용자 권한 정보값(w_s)을 하기와 같이 산출하여 헬스케어 서버에 전송한다(S330). 여기서, 전체 서비스에 대한 권한 정보의 위수(S)는 $s=|a|=lcm\{|a_1|,|a_2|,\ldots,|a_n|\}$ 이다.

[0062] $$w_s = E_{Sk_{temp}}(s \| c_1 \| a_1)$$

[0063] 상기한 바와 같이, 사용자 권한 정보값(w_s)은 전체 서비스에 대한 권한 정보의 위수(s), 제1 서비스의 mod 연산값(c_1) 및 제1 서비스의 권한 정보(a_1)를 세션키로 암호 알고리즘화한 값이다. 여기서

[0064] 헬스케어 서버는 세션키 (Sk_{temp})로 사용자 권한 정보값(W_S)를 복호화한 뒤 제1 서비스의 mod 연산값(c_1), 제1 서비스의 권한 정보(a_1)를 추출한 뒤 제1 서비스의 권한 정보(a_1)와 제1 서비스의 mod 연산값(c_1)을 일대일 대응하여 저장한다(S340).

[0065] 도 4는 본 발명의 일 실시예에 따른 정보를 요구하는 사용자의 권한이 기설정된 사용자의 권한 정보와 다른 경우, 사용자의 접근을 차단하는 과정을 설명하기 위한 흐름도이다.

[0066] 불법적인 접근을 요구하는 사용자의 기기(u_2)는 제1 서비스에 대한 비인가된 사용을 위하여 변경된 제1 서비스의 권한 정보(a_1')를 생성한 후 하기와 같은 변경된 사용자 권한 정보값(w_1')을 헬스케어 서버에 전송한다(S410).

[0067] $$w_s' = E_{Sk_{temp}}(s' \| c_1 \| a_1')$$

[0068] 헬스케어 서버는 변경된 사용자 권한 정보값(w_s')을 세션키 Sk_{temp} 로 복호화한 뒤 제1 서비스의 mod 연산값

(c_1), 변경된 제1 서비스의 권한 정보(a_1')를 추출한다(S420).

[0069] 그리고, 추출된 제1 서비스의 권한 정보(a_1') 및 제1 서비스의 mod 연산값(c_1) 각각을 기저장된 제1 서비스의 권한 정보(a_1)와 제1 서비스의 mod 연산값(c_1)과 비교하여 동일성 여부를 판단한다(S430).

[0070] 비교 결과 제1 서비스에 대한 권한 정보가 동일하면(S430-Y), 제1 서비스를 사용자의 기기에 제공한다(S440).

[0071] 그러나, 비교 결과 제1 서비스에 대한 권한정보가 동일하지 않으면 ($a_1 \neq a_1'$)(S430-N), 기저장된 세션키($Sk_{temp} = (y_{u_i} \oplus a_0 + \sum_{d*m} (r_{ij} | v_{ij} + r_{ij})) \bmod n$)에서 사용자 권한 정보값을 변경시킨 자의 제1 서비스에 대한 임시 비밀정보 (y_{u_i})를 독출한다(S450).

[0072] 그리고, 제1 서비스에 대한 임시 비밀정보 (y_{u_i})를 기반으로 사용자의 기기 권한 정보값을 변경시킨 자가 제공받을 수 있는 원래의 서비스를 확인한다. 그리고, 헬스케어 서버는 사용자의 기기 권한 정보값을 변경시킨 자에게 원래의 서비스를 제공한다(S460).

[0073] 그리고, 다시 동일한 사용자의 기기가 사용자 권한 정보값을 변경하여 서비스를 제공받고자 하는 경우(S470), 상기한 사용자의 기기의 제1 서비스에 대한 임시 비밀정보 (y_{u_i}) 및 상기한 사용자의 세션키를 제거하여 상기한 사용자 등록을 취소시킨다(S480).

[0074] 본 실시예에서는 헬스케어 서버가 사용자 등록, 서비스 제공에 관하여 설명하였으나, 이에 한정되지 않는다. 본 발명의 사용자에 따라 서비스를 제공하는 임의의 시스템에 적용가능함은 물론이다.

[0075] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

도면의 간단한 설명

[0076] 도 1은 본 발명의 일 실시예에 따른 특정 서비스를 제공받고자 하는 사용자 등록 과정을 설명하기 위한 흐름도,

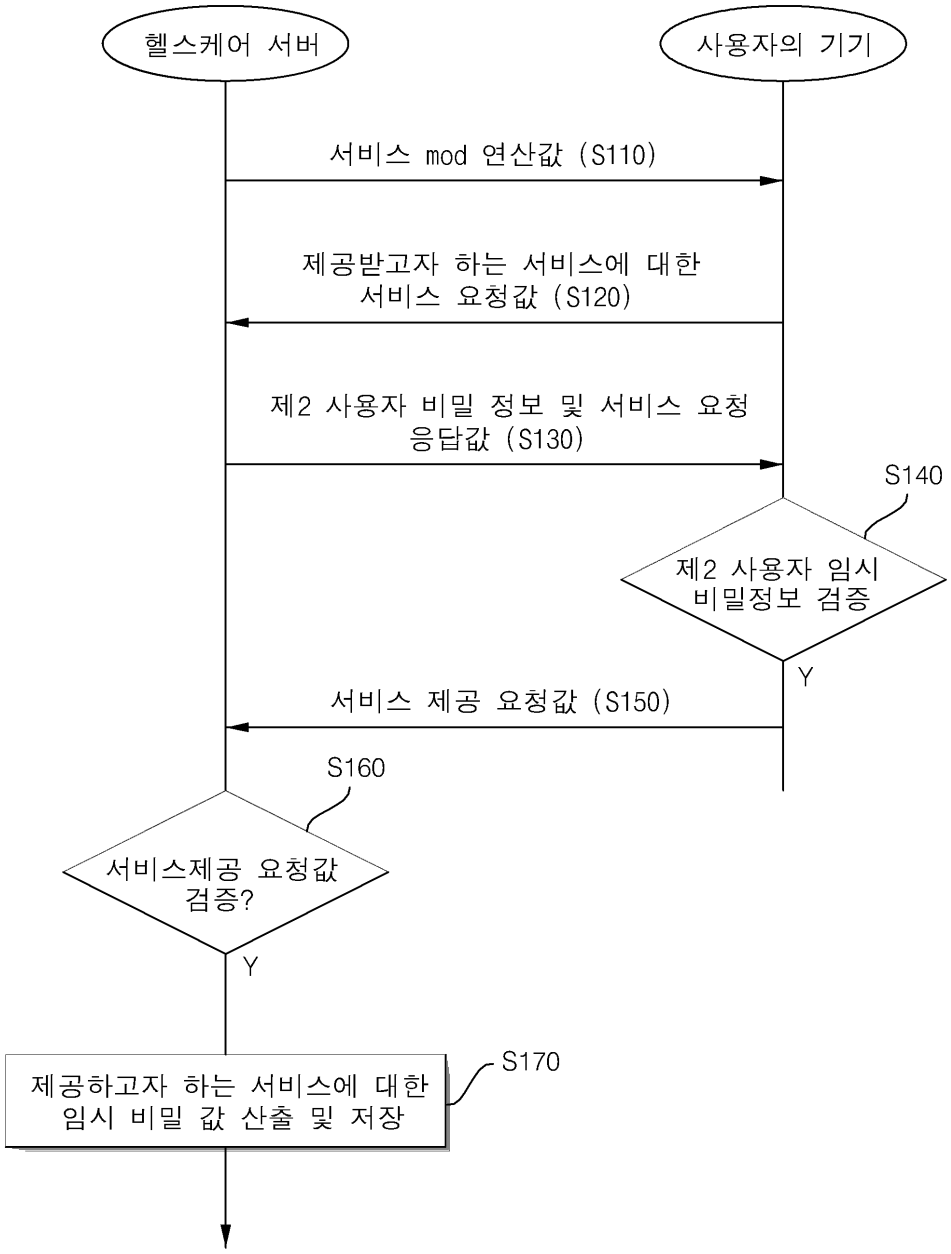
[0077] 도 2는 본 발명의 일 실시예에 따른 사용자와 헬스케어 서버간의 상호 통신을 위한 세션키 생성 방법에 제공되는 흐름도,

[0078] 도 3은 본 발명의 일 실시예에 따른 서비스에 따른 사용자의 권한 정보 설정 방법에 제공되는 흐름도, 그리고,

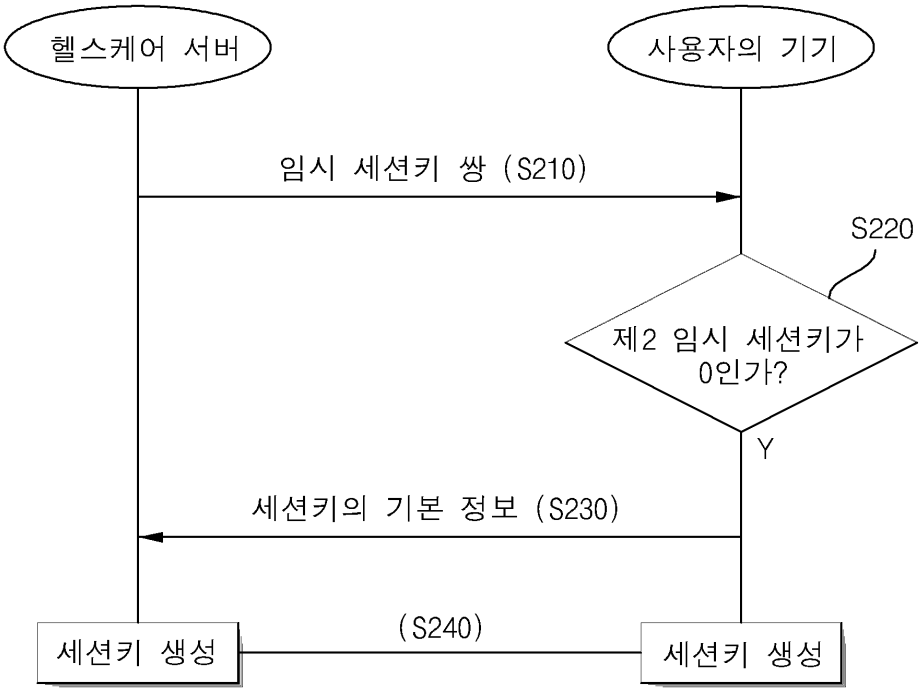
[0079] 도 4는 본 발명의 일 실시예에 따른 정보를 요구하는 사용자의 권한이 기설정된 사용자의 권한 정보와 다른 경우, 사용자의 접근을 차단하는 과정을 설명하기 위한 흐름도이다.

도면

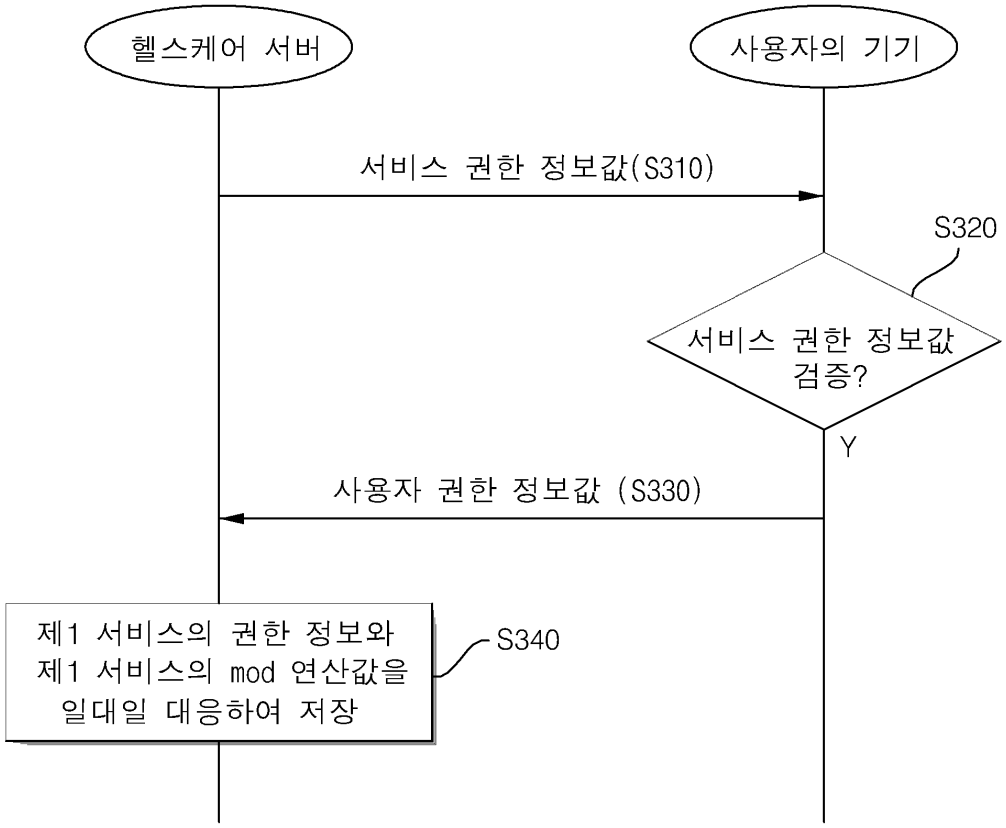
도면1


헬스케어 서버
사용자의 기기
서비스 mod 연산값 (S110)
제공받고자 하는 서비스에 대한
서비스 요청값 (S120)
제2 사용자 비밀 정보 및 서비스 요청
응답값 (S130)
S140
제2 사용자 임시
비밀정보 검증
Y
서비스 제공 요청값 (S150)
S160
서비스제공 요청값
검증?
Y
제공하고자 하는 서비스에 대한
임시 비밀 값 산출 및 저장
S170

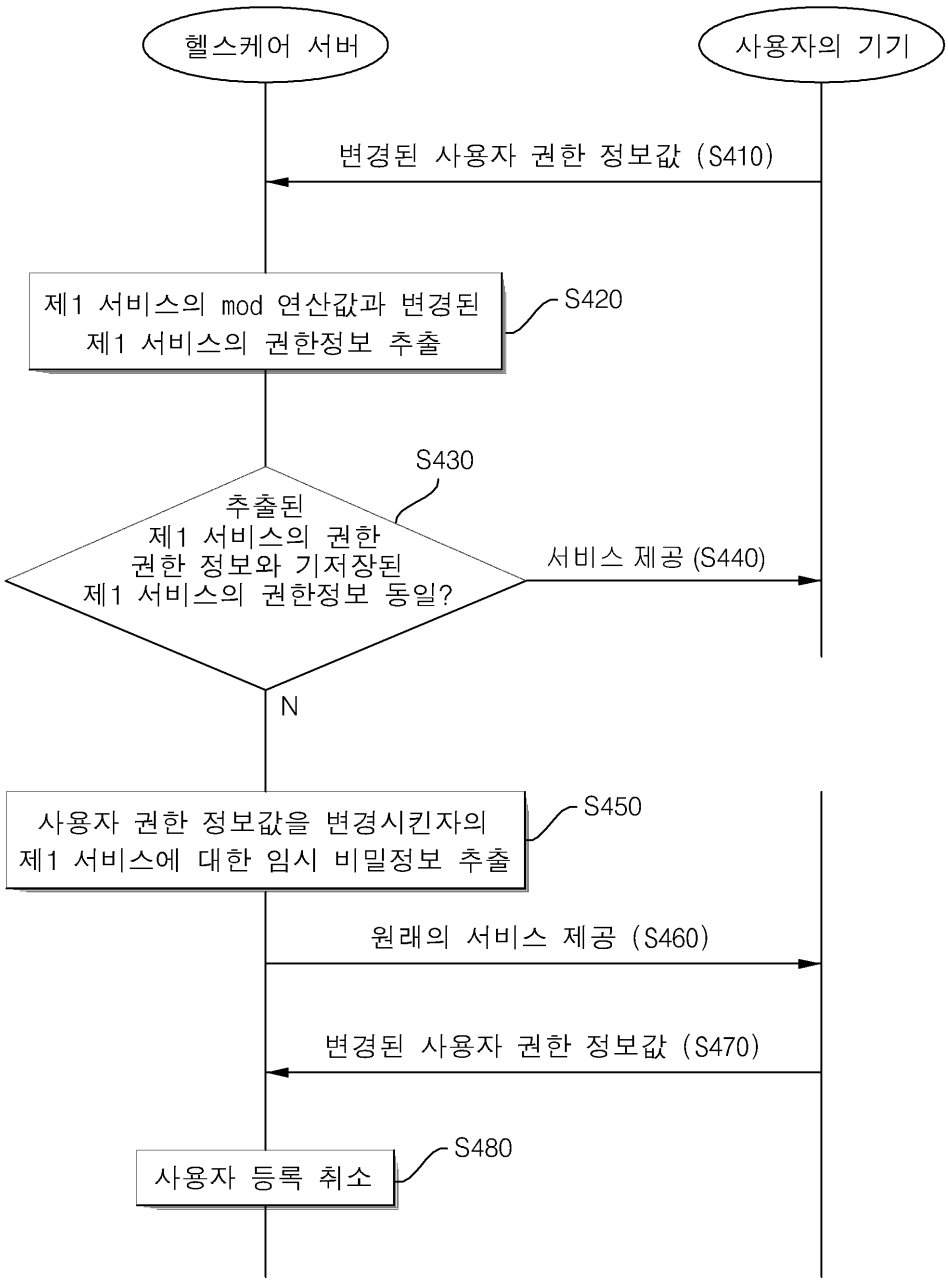
도면2


헬스케어 서버
사용자의 기기
임시 세션키 쌍 (S210)
S220
제2 임시 세션키가 0인가?
Y
세션키의 기본 정보 (S230)
(S240)
세션키 생성
세션키 생성

도면3


헬스케어 서버
사용자의 기기
서비스 권한 정보값(S310)
S320
서비스 권한 정보값 검증?
Y
사용자 권한 정보값 (S330)
제1 서비스의 권한 정보와 제1 서비스의 mod 연산값을 일대일 대응하여 저장
S340

도면4


헬스케어 서버
사용자의 기기
변경된 사용자 권한 정보값 (S410)
제1 서비스의 mod 연산값과 변경된
제1 서비스의 권한정보 추출
S420
S430
추출된
제1 서비스의 권한
권한 정보와 기저장된
제1 서비스의 권한정보 동일?
서비스 제공 (S440)
N
사용자 권한 정보값을 변경시킨자의
제1 서비스에 대한 임시 비밀정보 추출
S450
원래의 서비스 제공 (S460)
변경된 사용자 권한 정보값 (S470)
사용자 등록 취소
S480