



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0075895
(43) 공개일자 2012년07월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) G06F 21/20 (2006.01)
(21) 출원번호 10-2010-0137792
(22) 출원일자 2010년12월29일
심사청구일자 2010년12월29일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
최진영
서울특별시 노원구 동일로248길 16, 506동 1003호 (상계동, 수락파크빌)
김영진
서울특별시 금천구 두산로11길 22, 1502호 (독산동, 청광플러스원아파트 101동)
김현석
경기도 성남시 분당구 장미로 139, 매화마을 211동 801호 (야탑동)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 9 항

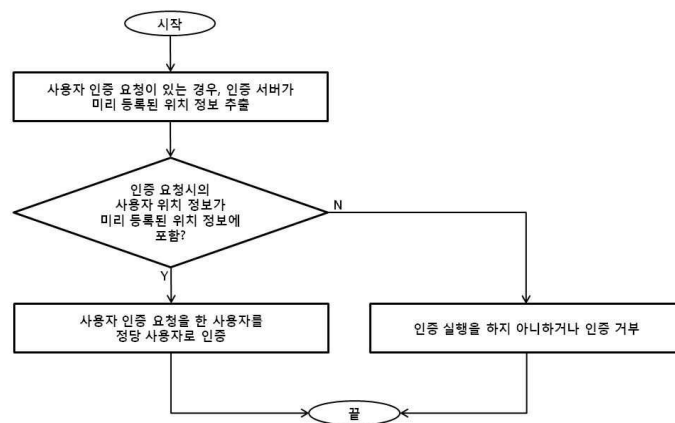
(54) 발명의 명칭 사용자 인증 방법

(57) 요약

본 발명은 사용자 인증 방법에 관한 것으로, 사용자가 서비스 제공자의 서버에 접속하여 원하는 서비스를 이용하고자 사용자 인증이 요구되는 경우, 사용자가 미리 지정한 위치(장소) 이외의 위치에서 서비스 제공자의 서버(인증 서버)에 인증을 시도하면 사용자 인증 자체를 할 수 없도록 하여 사용자의 개인 정보 보호의 만전을 기할 수 있는 사용자 인증 방법에 관한 것이다.

본 명세서에서 개시하는 사용자 인증 방법은 (a)사용자의 정당 사용자임을 인증하는 인증 서버가 상기 사용자로부터 인증 요청을 받는 경우, 상기 사용자에게 의해 지정되어 상기 인증 서버에 미리 등록된 위치 정보(GPS_{USER})를 추출하는 단계; 및 (b)상기 인증 서버가 상기 인증 요청시의 상기 사용자의 위치 정보(GPS_U)가 상기 추출된 GPS_{USER}에 포함됨을 판단하여, 포함되는 경우에만 상기 사용자를 정당 사용자로 인증하는 단계를 포함하여 본 발명의 과제를 해결한다.

대표도 - 도1



특허청구의 범위

청구항 1

(a)사용자의 정당 사용자임을 인증하는 인증 서버가 상기 사용자로부터 인증 요청을 받는 경우, 상기 사용자에게 의해 지정되어 상기 인증 서버에 미리 등록된 위치 정보(GPS_{USER})를 추출하는 단계; 및

(b)상기 인증 서버가 상기 인증 요청시의 상기 사용자의 위치 정보(GPS_U)가 상기 추출된 GPS_{USER} 에 포함됨을 판단하여, 포함되는 경우에만 상기 사용자를 정당 사용자로 인증하는 단계를 포함하는 사용자 인증 방법.

청구항 2

제 1 항에 있어서,

상기 GPS_{USER} 는 상기 등록을 요청한 시점의 상기 단말의 타임스탬프(Time Stamp: TS) 정보에 연결(concatenation)되고, 상기 연결된 정보의 해시(hash) 값의 형태로 상기 인증 서버에 등록되는 것을 특징으로 하는 사용자 인증 방법.

청구항 3

제 2 항에 있어서, 상기 (a)단계는

(a1)상기 인증 서버가 상기 해시 값의 독출을 시도하는 단계; 및

(a2)상기 인증 서버가 상기 해시 값이 독출된 경우에만 상기 사용자의 정당 사용자임을 인증하기 위한 인증용 패스워드의 발급 허가를 상기 단말에 통지하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 4

제 3 항에 있어서,

상기 인증용 패스워드는 One Time Password(OTP)를 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 5

제 4 항에 있어서, 상기 단말에 의한 상기 인증용 패스워드의 발급은

상기 단말이 상기 인증 요청 시점의 자신의 TS 정보와 상기 인증 요청 시점의 자신의 위치 정보(GPS_U)를 상호 연결(concatenation)한 정보의 해시(hash) 값(GC_U)을 산출하는 단계;

상기 GC_U 산출시의 상기 단말의 카운터(counter) 값의 HMAC(keyed-Hash Message Authentication Code)(HC_U)를 추출하는 단계; 및

상기 HC_U 를 Dynamic Truncation(DT)한 값을 상기 인증용 패스워드로 지정하는 단계를 포함하여 이루어지는 것을 특징으로 하는 사용자 인증 방법.

청구항 6

제 5 항에 있어서, 상기 (a)단계는

(a3)상기 발급 허가 통지를 한 경우, 상기 인증 서버가 상기 인증 요청 시점의 자신의 TS 정보와 상기 GPS_{USER} 를 상호 연결(concatenation)한 정보의 해시(hash) 값(GC_S)을 산출하는 단계;

(a4)상기 인증 서버가 상기 GC_S 산출시의 상기 서버의 카운터(counter) 값의 HMAC(keyed-Hash Message Authentication Code)(HC_S)를 추출하는 단계; 및

(a5)상기 인증 서버가 상기 HC_S 를 Dynamic Truncation(DT)한 값을 추출하는 단계를 더 포함하는 것을 특징으로

로 하는 사용자 인증 방법.

청구항 7

제 6 항에 있어서,

상기 (b)단계는 상기 인증용 패스워드와 상기 HCs를 상기 DT한 값의 일치 여부를 판단하는 것으로 이루어지는 것을 특징으로 하는 사용자 인증 방법.

청구항 8

제 1 항 내지 제 7 항 중 어느 한 항에 있어서,

상기 모든 위치 정보는 GPS(Global Positioning System)를 이용하여 획득되는 것을 특징으로 하는 사용자 인증 방법.

청구항 9

제 8 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체.

명세서

기술 분야

[0001] 본 발명은 사용자 인증 방법에 관한 것으로, 보다 상세하게는 사용자가 자신의 단말을 이용하여 서비스 제공자(service provider)가 제공하는 서비스를 이용함에 있어 사용자 인증(user authentication)이 요구되는 경우에 사용자가 지정한 위치(장소)에서 인증을 요구하는 경우에만 사용자 인증이 가능하도록 하는 사용자 인증 방법에 관한 것이다.

배경 기술

[0002] 사용자 인증은 개인 정보 보호의 필요성 증대에 수반하여 그 중요성이 날로 증가하고 있다. 특히 유비쿼터스(ubiquitous)화 되어가고 있는 각급의 컴퓨팅 환경을 고려하면 개인 정보 유출의 위험성은 한층 배가되므로 개인 정보에 대한 보안성 제고는 정보 처리 분야의 화두가 되고 있다.

[0003] 기존의 사용자 인증 방안으로는 One Time Password(OTP), 공인 인증서(NPKI), 보안 카드(Secure Card), SMS(Short Message Service) 등을 이용한 인증 방안 등이 있다. 하지만 이러한 방안들은 개인 단말(예를 들어 스마트폰 등)을 분실하거나 도난당했을 때 또는 개인 단말에 내장된 개인 정보가 복제되어 유출되었을 때 개인 정보에 대한 보안에 심각한 문제를 일으킬 수 있다. 개인 단말이 악의적인 사용자에게 의해 분실 내지는 도난을 당하여 사용자의 금융결제 관련 비밀번호, 공인 인증서의 비밀번호 등의 개인 정보가 해킹 등을 통하여 유출되면 정당 사용자(authenticated user)는 개인 정보의 유출로 인한 심각한 손해를 볼 수 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명은 상기한 문제점을 해결하기 위해 창안된 것으로, 본 발명이 해결하려는 과제는 사용자 인증이 요구되는 경우 소정의 조건을 만족하는 경우에만 사용자 인증을 하도록 하여, 상기 소정의 조건을 만족하지 아니한 경우에는 정당 사용자라도 사용자 인증 자체를 불허하여 사용자의 개인 정보를 보호함에 만전을 기할 수 있는 사용자 인증 방안을 제시하는 것이다.

과제의 해결 수단

[0005] 상기한 과제를 해결하기 위해 본 명세서에서 개시하는 사용자 인증 방법은

[0006] (a)사용자의 정당 사용자임을 인증하는 인증 서버가 상기 사용자로부터 인증 요청을 받는 경우, 상기 사용자에게 의해 지정되어 상기 인증 서버에 미리 등록된 위치 정보(GPS_{USER})를 추출하는 단계; 및 (b)상기 인증 서버가 상기 인증 요청 시점의 상기 사용자의 위치 정보(GPS_U)가 상기 추출된 GPS_{USER}에 포함됨을 판단하여, 포함되는 경우에만 상기 사용자를 정당 사용자로 인증하는 단계를 포함하여 본 발명의 과제를 해결한다.

발명의 효과

[0007] 본 발명에 의할 경우, 사용자의 패스워드 등 사용자의 개인 정보가 임의적으로 유출되더라도, 사용자 인증을 요청한 장소(위치)가 사용자가 미리 지정하여 등록한 위치가 아닌 경우에는 인증 자체가 이루어지지 아니하고 아울러 인증 요청이 발생할 때마다 인증용 패스워드를 달리 발생시키므로 개인 정보 보호의 보안성을 획기적으로 제고할 수 있다.

도면의 간단한 설명

[0008] 도 1은 본 발명의 전체적인 흐름을 제시한 도면이다.
도 2a 내지 도 2c는 본 발명의 상세한 흐름을 제시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0009] 본 발명을 실시하기 위한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하려는 과제의 해결 방안의 개요를 우선 제시한다.

[0010] 본 발명은 사용자 인증을 함에 있어 어느 경우에도 인증 실행(허용)을 실시함이 아닌 것을 그 출발 개념으로 한다. 즉, 상기한 바와 같이 소정의 조건을 만족하는 경우에만 사용자 인증을 실행하는(허용하는) 것인데, 여기서 소정의 조건이란 바로 사용자가 서비스 제공자의 서버에 접속하여 원하는 서비스를 이용하고자 사용자 인증이 요구되는 경우, 사용자가 미리 지정한 위치(장소) 이외의 위치에서 서비스 제공자의 서버에 인증을 시도하면 사용자 인증 자체를 할 수 없도록 하는 것이다. 이하에서는 서비스 제공자의 서버는 서비스 제공자가 제공하는 서비스의 이용을 위해 사용자 인증을 필히 요구하는 서버이며, 따라서 간략히 인증 서버라고 칭하기로 한다.

[0011] 즉, 사용자가 인증 서버에 접속하여 사용자 인증이 가능하게 하기 위해서는 사용자의 ID와 패스워드 등이 올바른 것뿐만이 아니라, 여기에 더해 사용자가 미리 지정한 위치에서 인증을 시도하는 경우에만 사용자 인증이 가능하도록 하는 것이다. 다시 말하면 사용자의 ID와 패스워드 등이 제3자에게 임의적으로 유출되더라도 접속 위치가 미리 지정한 위치가 아닌 경우에는 사용자의 ID와 패스워드만으로는 정당 사용자에게조차도 사용자 인증 자체를 불허하여 사용자의 개인 정보 보호의 만전을 기하는 것이 본 발명이 해결하고자 하는 과제의 해결 방안의 개요이다.

[0012] 이하, 본 발명을 실시하기 위한 구체적인 내용을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0013] 도 1은 본 발명의 전체적인 흐름을, 도 2a 내지 도 2c는 본 발명의 상세한 흐름을 제시한 도면이다.

[0014] 사용자는 자신의 단말을 이용하여 인증 서버에 접속하여 인증을 요청한다(S21). 접속은 자신의 ID(ID₀), 접속용 패스워드(Password)를 이용하여 이루어지며, 이들 두 정보는 사용자가 자신의 단말을 이용하여 인증 서버에 미리 등록한다.

[0015] 한편 상기한 등록이 이루어질 때에는 사용자가 지정한 위치(장소) 정보도 아울러 등록된다. 사용자가 지정한 위치 정보의 등록은 본 발명의 목적을 달성하기 위해서 즉, 사용자가 지정한 위치에서 인증을 시도하는 경우에만 사용자 인증이 가능하도록 하기 위함이다. 사용자가 지정한 위치 정보의 등록은 예를 들어 다음과 같이 이루어질 수 있다.

[0016] 사용자가 지정한 위치 정보를 등록을 요청한 시점의 단말의 타임스탬프(Time Stamp: TS) 정보에 연결(concatenation)시키고, 연결된 정보의 해시(hash) 값(GC)의 형태로 인증 서버에 등록한다.

[0017] $GC = H(TS || GPS_{USER})$.

[0018] 여기서 H()는 해시 함수를, ||는 concatenation을, GPS_{USER}은 사용자가 지정한 위치 정보를 의미한다. 이 경우 사용자가 지정한 위치 정보(GPS_{USER})는 예를 들어 GPS(Global Positioning System)가 제공하는 위치 좌표를 이

용할 수 있는데, 이는 이하에 언급될 모든 위치 정보에도 마찬가지이다.

[0019] 인증 서버는 사용자로부터 인증 요청을 받으면, GPS_{USER} 를 추출한다(S22). 이를 위해 인증 서버는 자신에 기록된 상기한 해시 값(GC)의 독출을 시도하여(S221), 만일 해시 값(GC)의 독출이 실패한 경우에는 사용자에게 인증을 진행할 수 없음(사용자 인증 실패(거부), GPS_{USER} 가 추출되지 아니함)을 통지하고(S222) 다시 인증을 시도할지를 문의하며, 독출된 경우에는 상기한 GPS_{USER} 가 추출된 것으로 간주하고 사용자 인증 절차가 진행될 수 있다는 차원에서 사용자의 정당 사용자임을 인증하기 위한 인증용 패스워드의 발급 허가를 단말에 통지한다(S223).

[0020] 여기서 인증용 패스워드는 상기한 접속용 패스워드>Password)와는 다른 패스워드로, 사용자가 인증 서버와의 접속에 성공하더라도 정당 사용자임을 인증하는 절차가 따로 요구되는데 이 인증 절차에 요구되는 패스워드이다.

[0021] 상기한 발급 허가를 통지받은 단말은 인증용 패스워드를 발급하게 되는데(S23), 인증용 패스워드의 발급은 다음과 같이 이루어질 수 있다.

[0022] 우선 단말은 인증 요청 시점의 자신의 TS 정보(TS_U)와 인증 요청 시점의 자신의 위치 정보(GPS_U)를 상호 연결(concatenation)한 정보의 해시(hash) 값(GC_U)을 산출한다(S231).

[0023] $GC_U = H(TS_U || GPS_U)$.

[0024] GC_U 를 산출한 후 단말은 GC_U 산출시의 자신의 카운터(counter) 값(C_U)의 HMAC(keyed-Hash Message Authentication Code)(HC_U)를 추출한다(S232).

[0025] $HC_U = HMAC_{GC_U}(C_U)$.

[0026] 여기서 $HMAC_a()$ 는 어떤 해시 메시지 a의 인증 코드(authentication code)를 산출하는 함수를 의미한다. 한편 단말의 카운터(counter) 값(C_U)은 후술할 인증 서버의 카운터 값(C_S)과 동기화(synchronization)되어 있다.

[0027] HC_U 를 추출한 후 단말은 HC_U 를 Dynamic Truncation(DT)한 값을 인증용 패스워드(AP_U)로 지정하고, AP_U 를 인증 서버에 전송한다(S233).

[0028] $DT(HC_U) = AP_U$.

[0029] 여기서 $DT(a)$ 는 a의 값을 일련의 문자나 숫자로 표현되는 a의 시작 또는 끝을 소정의 기준에 따라(Dynamic) 절단(Truncation)하는 함수를 의미하는 것이다. $DT()$ 는 암호화가 요구되는 제반 환경에서 암호 생성에 통상적으로 쓰이는 함수이며, 생성된 암호의 데이터량이 너무 많게 되는 것을 방지하기 위해 쓰이는 함수이다.

[0030] 한편 단말로부터의 인증 요청이 발생하면 인증 서버도 사용자 인증을 수행하기 위한 값을 산출한다(S24).

[0031] 먼저 인증 서버는 인증 요청 발생 시점의 자신의 TS 정보(TS_S)와 위치 정보(GPS_{USER})를 상호 연결(concatenation)한 정보의 해시(hash) 값(GC_S)을 산출한다(S241).

[0032] $GC_S = H(TS_S || GPS_{USER})$.

[0033] 여기서 TS_S 는 상기한 TS_U 와 동기화된 인증 서버의 타임스탬프 정보이다.

[0034] GC_S 를 산출한 후 인증 서버는 GC_S 산출시의 상기 단말의 카운터(counter) 값(C_S)의 HMAC(keyed-Hash Message Authentication Code)(HC_S)를 추출한다(S242).

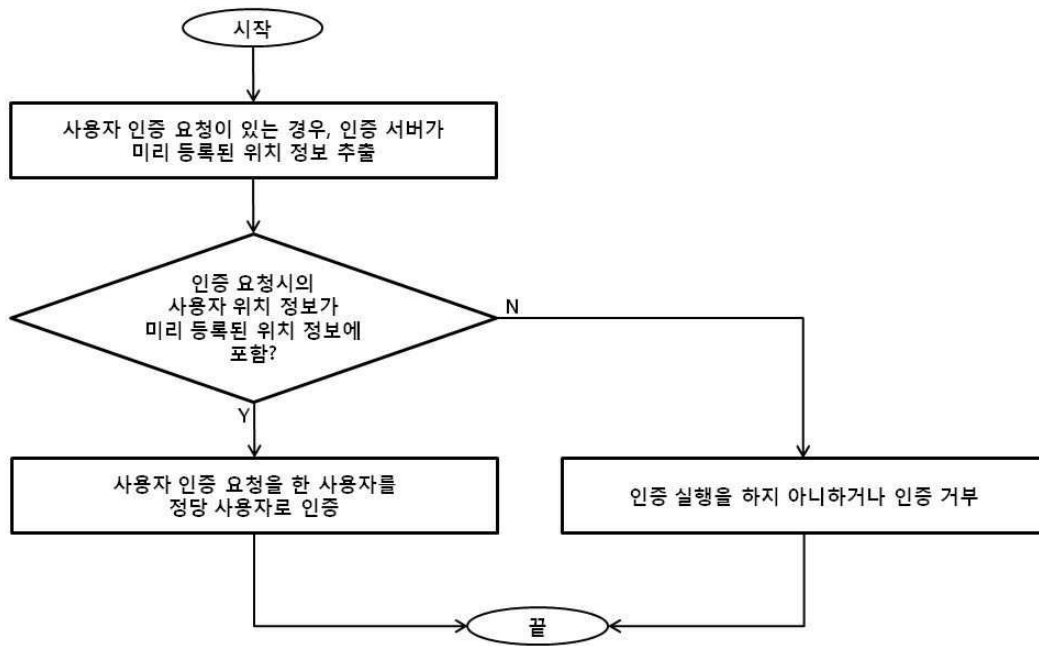
[0035] $HC_S = HMAC_{GC_S}(C_S)$.

[0036] HC_S 를 추출한 후 인증 서버는 HC_S 를 Dynamic Truncation(DT)한 값(AP_S)을 추출(S243)한다.

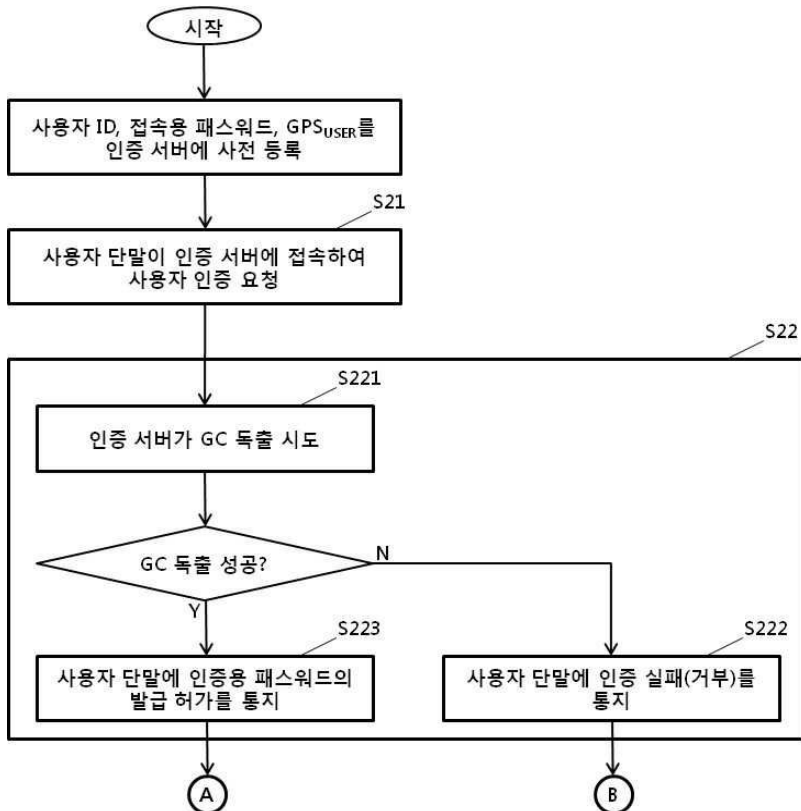
- [0037] $DT(HC_S) = AP_S$.
- [0038] AP_S 가 추출되면 인증 서버는 GPS_U 가 GPS_{USER} 에 포함됨을 판단하는데(S25), 이는 단말로부터 전송받은 AP_U 와 AP_S 가 동일한지를 판단하는 것이다. 동일한 경우에는 인증 요청 사용자를 정당 사용자로 인증하고, 동일하지 아니한 경우에는 인증이 실패했음을 단말에 통보하고 다시 인증을 시도할지를 문의한다.
- [0039] 한편 상기한 인증용 패스워드(AP_U)는 One Time Password(OTP)인 것이 바람직하며 AP_S 도 일회성임이 바람직하다. 이의 일환으로, 상기의 설명에 제시된 바와 같이, 인증용 패스워드(AP_U)의 발급시와 AP_S 의 추출시에 각각 인증 요청 시점의 타임스탬프 정보(TS_U , TS_S)를 활용한다. 즉, 인증 요청이 발생할 때마다 새로운 타임스탬프 정보를 활용하여 인증용 패스워드(AP_U) 및 AP_S 를 달리 하므로 사용자의 개인 정보 보호에 대한 보안성을 획기적으로 제고시킬 수 있다.
- [0040] 사용자 인증이 성공하면 사용자는 자신의 단말을 통해 인증 서버가 제공하는 서비스(예를 들어 전자 금융 거래 등)를 안전하게 이용할 수 있게 된다.
- [0041] <본 발명의 이점>
- [0042] 1. OTP 생성 불가능
- [0043] 본 발명의 가장 큰 특징은 위에서 언급한 바와 같이 사용자가 미리 지정하여 등록한 곳에서 인증을 요청하는 경우에만 사용자 인증이 가능하도록 하는 것이다. 이는 다른 지역에서 도청, 해킹, 피싱, 파밍 등의 공격을 통해 해커가 사용자의 개인 정보(결제 정보 등)를 알아냈다고 하더라도 해커는 물리적인 장소에 직접적으로 위치해야 하기 때문에 공격을 어렵게 한다. 또한 직접 위치했다 하더라도 사용자 개인 단말에 대한 해킹이 한 번 더 이루어 져야 하기 때문에 악의적인 사용자의 공격으로부터 안전하다.
- [0044] 2. 세션 하이재킹 공격에 안전
- [0045] 만약 공격자가 사용자의 이전 세션을 가로채고, 획득한 세션을 이용하여 사용자로 가장하고 서버와 OTP값을 인증 받으려고 하는 경우에도 공격자는 서버와 OTP 값을 인증받을 수 없다. 세션정보를 획득한다 해도 공격자는 GC 값을 알 수 없기 때문에 다음 OTP 값을 생성해 내지 못한다. 따라서 제안된 인증방식은 세션 하이재킹 공격으로부터 안전하다.
- [0046] 3. 사전 공격에 안전
- [0047] 사전 공격의 경우 패스워드를 추측하여 공격하는 방법으로서, 본 발명은 사용자의 OTP 값과 서버의 OTP 값을 서로 비교하여 인증을 하고 서비스를 제공하기 때문에 패스워드를 추측하여 공격하는 사전 공격에 안전하며 본 발명에 의한 해시 함수의 일방향성의 특징 때문에 사전공격으로부터 안전하다.
- [0048] 4. 위장공격에 안전
- [0049] 악의적인 공격자가 정당 사용자로 위장하기 위해서는 위장하고자 하는 사용자의 ID 와 OTP 값을 알아야 한다. 사용자의 ID는 공개된 정보이기 때문에 쉽게 알 수 있지만, 사용자의 OTP 값은 $HC(=HMAC_{cc}(C))$ 값을 알아내고 $AP(=DT(HC))$ 를 추출하여야 하기 때문에 추측하기 어렵다. 따라서 위장공격은 불가능하다.
- [0050] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.
- [0051] 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- [0052] 이제까지 본 발명에 대하여 그 바람직한 실시예를 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 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

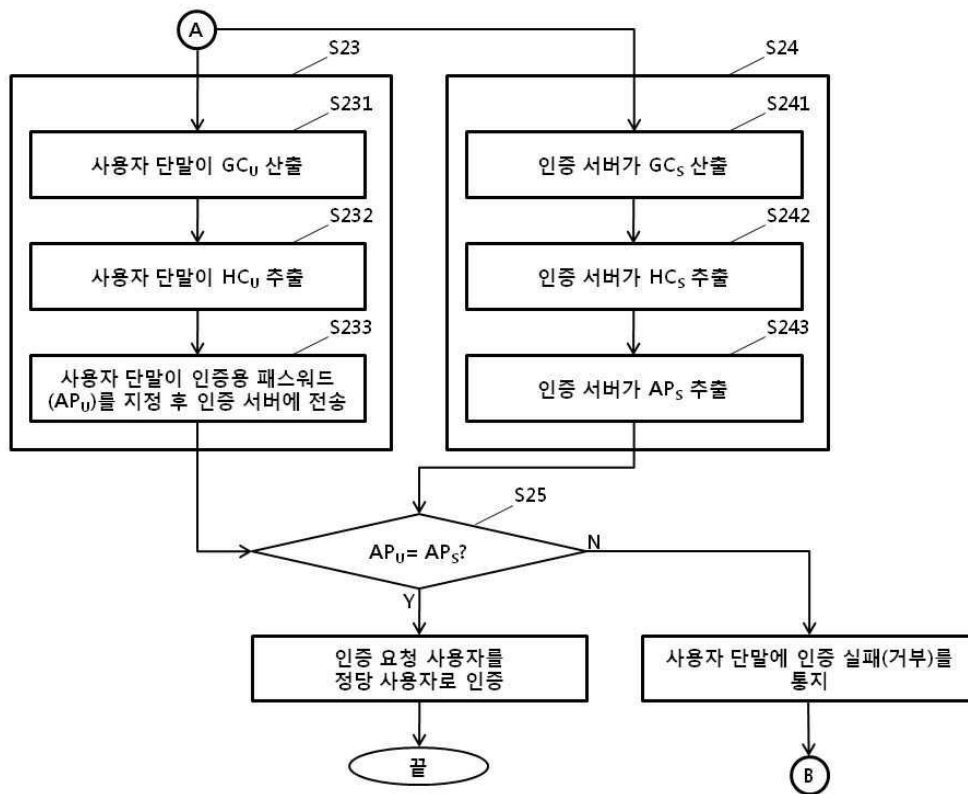
도면1



도면2a



도면2b



도면2c

