(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년02월01일
(11) 등록번호 10-1229128
(24) 등록일자 2013년01월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(21) 출원번호 10-2009-0127278
(22) 출원일자 2009년12월18일
심사청구일자 2010년12월13일
(65) 공개번호 10-2011-0070450
(43) 공개일자 2011년06월24일
(56) 선행기술조사문헌
KR1020030005468 A*
KR1020060038083 A
KR1019980050938 A
EP0689316 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 케이티
경기도 성남시 분당구 불정로 90 (정자동 206 번지)
(72) 발명자
박도진
서울특별시 서초구 태봉로 151 (우면동)
이민구
서울특별시 서초구 태봉로 151 (우면동)
(뒷면에 계속)
(74) 대리인
특허법인 신성

전체 청구항 수 : 총 5 항 심사관 : 양종필

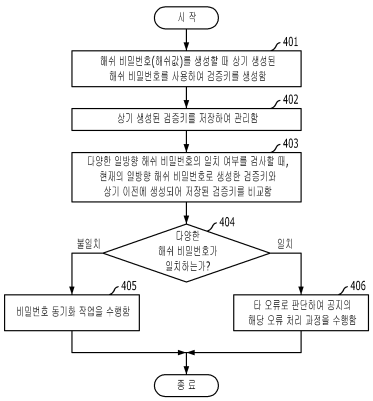
(54) 발명의 명칭 **검증키를 이용한 다양한 해쉬 비밀번호 관리 방법**

(57) 요 약

본 발명은 검증키를 이용한 다양한 해쉬 비밀번호 관리 방법에 관한 것으로, 서비스별로 해쉬 방식이 서로 다른 비밀번호를 관리해야 하는 시스템에서 검증키를 이용하여 다양한 해쉬 비밀번호를 관리하는 해쉬 비밀번호 관리 방법을 제공하고자 한다.

이를 위하여, 본 발명은, 해쉬 비밀번호 관리 방법에 있어서, 복수의 해쉬 비밀번호를 생성하고 상기 생성된 복수의 해쉬 비밀번호를 사용하여 검증키를 생성하는 검증키 생성 단계; 상기 생성된 검증키를 저장하여 관리하는 검증키 관리 단계; 현재의 해쉬 비밀번호로 생성한 검증키와 상기 저장된 검증키를 비교하는 검증키 비교 단계; 및 상기 비교 결과, 검증키가 불일치함에 따라 비밀번호 동기화를 수행하는 비밀번호 동기화 단계를 포함하되, 상기 검증키 생성 단계는, 비밀번호를 최초로 생성 또는 변경 시에 비밀번호를 다양한 일방향 해쉬 처리하여 복수의 해쉬 비밀번호를 생성하고, 상기 생성된 복수의 해쉬 비밀번호를 연산하여 검증키를 생성한다.

대 표 도 - 도4



(72) 발명자

이명원

서울특별시 서초구 태봉로 151 (우면동)

방정희

서울특별시 서초구 태봉로 151 (우면동)

특허청구의 범위

청구항 1

삭제

청구항 2

해쉬 비밀번호 관리 방법에 있어서,

복수의 해쉬 비밀번호를 생성하고 상기 생성된 복수의 해쉬 비밀번호를 사용하여 검증키를 생성하는 검증키 생성 단계;

상기 생성된 검증키를 저장하여 관리하는 검증키 관리 단계;

현재의 해쉬 비밀번호로 생성한 검증키와 상기 저장된 검증키를 비교하는 검증키 비교 단계; 및

상기 비교 결과, 검증키가 불일치함에 따라 비밀번호 동기화를 수행하는 비밀번호 동기화 단계를 포함하되,

상기 검증키 생성 단계는,

비밀번호를 최초로 생성 또는 변경 시에 비밀번호를 다양한 일방향 해쉬 처리하여 복수의 해쉬 비밀번호를 생성하고, 상기 생성된 복수의 해쉬 비밀번호를 연산하여 검증키를 생성하는, 해쉬 비밀번호 관리 방법.

청구항 3

제 2 항에 있어서,

상기 검증키 비교 단계는,

다양한 일방향 해쉬 비밀번호의 일치 여부를 검사할 때, 현재의 시스템들에 설정된 각 해쉬 비밀번호를 사용하여 새로 검증키를 생성한 후에, 상기 새로 생성한 검증키와 상기 기 저장하여 관리하고 있는 검증키를 비교하는, 해쉬 비밀번호 관리 방법.

청구항 4

제 2 항 또는 제 3 항에 있어서,

상기 비밀번호 동기화 단계는,

상기 비교 결과, 검증키가 불일치함에 따라 사용자 단말로 비밀번호 리셋(reset)을 요청하여, 비밀번호 리셋을 통해 비밀번호를 일치시키는, 해쉬 비밀번호 관리 방법.

청구항 5

제 4 항에 있어서,

상기 비교 결과, 검증키가 불일치함에 따라 상기 사용자 단말에 비밀번호 유효성 검사 오류를 표시하도록 하는 단계

를 더 포함하는 해쉬 비밀번호 관리 방법.

청구항 6

제 4 항에 있어서,

상기 검증키 관리 단계는,

상기 생성된 복수의 해쉬 비밀번호를 프로비저닝할 때 상기 생성된 검증키를 저장하는, 해쉬 비밀번호 관리 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 청약 처리 시스템 등에서 고객 청약을 기반으로 하는 프로비저닝 기술 분야에 관한 것으로, 더욱 상세하게는 서비스 시스템별로 해쉬 방식이 서로 다른 비밀번호를 다양한 시스템에 프로비저닝하는 프로비저닝 시스템 등에서 해쉬 비밀번호를 암호화하여 관리하는 해쉬 비밀번호 관리 방법에 관한 것이다.

[0002] 본 발명의 일실시예에서는 프로비저닝 시스템(System of Provisioning)에 본 발명이 적용되는 경우를 예로 들어 설명하나, 본 발명은 서비스별로 해쉬 방식이 서로 다른 비밀번호를 관리해야 하는 시스템에 적용될 수 있으므로, 본 발명이 프로비저닝 시스템에 한정되는 것이 아님을 미리 밝혀둔다.

배 경 기 술

[0003] '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 및 '정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령'의 비밀번호 암호화 요구에 따라 프로비저닝 시스템에서 비밀번호를 암호화하여 프로비저닝 시, 기존 레거시(legacy) 시스템과 신규 시스템, 그리고 업무 성격이 다른 시스템 등에 비밀번호를 해쉬하여 연동하는 경우, 암호화 기술 및 서비스 제공 방법 등에 따라 서비스 시스템별로 해쉬 방식을 통일할 수 없을 수도 있다.

[0004] 여기서, 프로비저닝은 고객 청약을 기반으로 고객이 청약한 서비스를 사용하는데 필요한 정보를 구성하여 서비스를 제공하는 것을 말하며, 사용자 인증을 수행하는 서비스의 경우에는 아이디와 비밀번호와 같은 인증 정보를 구성하는 것도 프로비저닝의 한 부분이다.

[0005] 개정된 정보통신망법에 따르면, 비밀번호는 반드시 일방향 암호화하여 저장을 하여야 하나, 암호화 방법에 대해서는 규정하지 않고 있으며, 접속 인증 시스템이나 서비스 인증 시스템, 웹 인증 시스템, 및 신규 암호화 방식 적용이 어려운 레거시(legacy) 시스템 등 다양한 시스템에 인증 정보를 프로비저닝 시에는 시스템 상황별로 다양한 암호화 방식을 사용해야 할 필요가 있다.

[0006] 예를 들면, 특정 시스템은 다양한 레거시(legacy) 시스템에서 이미 암호화를 사용하고 있지만, 레거시(legacy) 시스템에서 암호화 방식의 변경이 어려운 경우에는 해당 레거시(legacy) 시스템의 암호화 방식을 준용해야 한다. 이로 인하여 암호화 방식을 통일한다는 게 사실상 어렵다.

[0007] 종래에는 상기와 같이 암호화 방식의 통일이 어려운 상황에서 개인정보보호를 위해서 시스템별로 각기 다른 암호화를 수행하는 경우 암호화 데이터 간의 비교가 불가능하므로, 특정 시스템의 암호화 값이 알 수 없는 이유로 변경이 되더라도 변경 여부 자체를 알 수가 없는 문제점이 있었다. 도 1을 참조하여 종래의 비밀번호 암호화 관리 방식에 대하여 보다 상세히 살펴보면 다음과 같다.

[0008] 도 1은 종래의 검증키를 관리하지 않는 프로비저닝 시스템에서 다양한 방식의 해쉬 비밀번호를 관리하는 중 장애가 발생한 경우의 처리 과정을 나타내는 일실시예 흐름도로서, 사용자 단말(11), 프로비저닝 시스템(12), 접속 인증 시스템(13), 및 서비스 인증 시스템(14, 15)을 통하여 서비스를 제공한다.

[0009] 먼저, 청약 및 서비스 제공 절차를 간략하게 살펴보면, 사용자 단말(11)이 웹 또는 청약 시스템을 통해 서비스 청약을 요청한다. 그러면, 프로비저닝 시스템(12)은 접속 인증 시스템(13) 및 서비스 인증 시스템들(14, 15)에게 사용자 단말(11)이 웹 또는 청약 시스템을 통해 요청한 서비스 정보를 프로비저닝한다. 그러면, 접속 인증 시스템(13) 및 서비스 인증 시스템들(14, 15)은 프로비저닝 시스템(12)으로부터 전달받은 서비스 정보를 기반으로 사용자 단말(11)로 접속 서비스 또는 특정 서비스를 제공한다.

[0010] 한편, 도 1을 참조하여 프로비저닝 과정을 살펴보면, 사용자 단말(11)이 비밀번호를 리셋(reset)하여 프로비저닝 시스템(12)에 웹 등을 통해 비밀번호 구성을 요청하면(101), 프로비저닝 시스템(12)은 사용자 단말(11)로부터 전달받은 비밀번호를 시스템별로 다른 해쉬를 사용하여 해쉬값을 생성(비밀번호 해쉬)한 후(102) 각각의 시스템에 해쉬값을 전달한다(103 내지 105). 예를 들어, 도 1에 도시된 바와 같이 접속 인증 시스템(13)으로는 SHA-1 해쉬값을 전달하고(103), 서비스 인증 시스템 A(14)로는 MD5 해쉬값을 전달하고(104), 서비스 인증 시스템 B(15)로는 HAS160 해쉬값을 전달한다(105).

[0011] 상기와 같이 프로비저닝이 완료되면, 사용자 단말(11)은 상기 과정에서 신규 구성된 비밀번호로 접속 서비스, 서비스 A, 및 서비스 B를 사용하게 되는데(106 내지 108), 서비스 인증 시스템 A(14)의 비밀번호에 오류가 발생하게 되었을 때(109) 동일한 비밀번호를 입력하는데 서비스 A만 사용할 수 없다는 민원을 제기하게 된다(110 내지 113).

[0012] 이때, 상기와 같은 서비스 이용 오류 민원이 서비스 A를 제공하는 시스템의 문제인지, 아니면 서비스 A를 제공하는 네트워크의 문제인지, 아니면 고객의 설정 문제인지, 아니면 비밀번호가 틀려서 발생하는 민원인지를 파악하기 어려운 문제점이 있었다.

발명의 내용

해결 하고자하는 과제

[0013] 즉, 상기와 같은 종래 기술은 비밀번호 암호화로 인하여 민원에 대한 오류발생원인 파악이 어려운 문제점이 있으며, 이러한 문제점을 해결하고자 하는 것이 본 발명의 과제이다.

[0014] 따라서 본 발명은 서비스별로 해쉬 방식이 서로 다른 비밀번호를 관리해야 하는 시스템에서 검증키를 이용하여 다양한 해쉬 비밀번호를 관리하는 해쉬 비밀번호 관리 방법을 제공하는데 그 목적이 있다.

[0015] 즉, 본 발명은, 서비스별로 해쉬 방식이 서로 다른 비밀번호를 관리해야 하는 시스템에서 서비스 시스템별로 다양한 일방향 해쉬를 허용하는 경우, 해쉬 비밀번호 간의 비밀번호 일치/불일치를 판단할 수 있는 검증키를 추가로 생성하여 관리하도록 함으로써, 시스템의 오작업 등으로 발생할 수 있는 비밀번호 임의 변경에 따른 불일치를 판단하고, 비밀번호 불일치가 발생한 경우 비밀번호 동기화 작업을 수행하는 근거를 제공하고, 고객 민원을 신속하게 처리할 수 있도록 하기 위한, 해쉬 비밀번호 관리 방법을 제공하는데 그 목적이 있다.

[0016] 본 발명의 목적들은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

과제 해결수단

[0017] 상기 목적을 달성하기 위한 본 발명의 방법은, 해쉬 비밀번호 관리 방법에 있어서, 복수의 해쉬 비밀번호를 생성하고 상기 생성된 복수의 해쉬 비밀번호를 사용하여 검증키를 생성하는 검증키 생성 단계; 상기 생성된 검증키를 저장하여 관리하는 검증키 관리 단계; 현재의 해쉬 비밀번호로 생성한 검증키와 상기 저장된 검증키를 비교하는 검증키 비교 단계; 및 상기 비교 결과, 검증키가 불일치함에 따라 비밀번호 동기화를 수행하는 비밀번호 동기화 단계를 포함하되, 상기 검증키 생성 단계는, 비밀번호를 최초로 생성 또는 변경 시에 비밀번호를 다양한 일방향 해쉬 처리하여 복수의 해쉬 비밀번호를 생성하고, 상기 생성된 복수의 해쉬 비밀번호를 연산하여 검증키를 생성한다.

효 과

[0018] 상기와 같은 본 발명은, 인터넷 서비스 등에서 프로비저닝 시스템 등에 이용되어, 다양한 해쉬 비밀번호를 운용중에 일부 시스템에서 비밀번호 오류가 발생한 경우에도, 검증키를 사용하여 해쉬 방식이 다른 비밀번호의 불일치 여부를 확인할 수 있도록 함으로써, 다양한 해쉬 비밀번호를 관리하고, 관련 고객 민원을 정확히 처리할 수 있도록 하는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0019] 상술한 목적, 특징 및 장점은 첨부된 도면을 참조하여 상세하게 후술되어 있는 상세한 설명을 통하여 보다 명확해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용

이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명하기로 한다.

[0020] 그리고 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때 이는 "직접적으로 연결"되어 있는 경우뿐만 아니라 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한, 어떤 부분이 어떤 구성요소를 "포함" 또는 "구비"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함하거나 구비할 수 있는 것을 의미한다.

[0021] 먼저, 본 발명의 기술 요지를 정리하여 살펴보면 다음과 같다.

[0022] 본 발명은, 최초에 텍스트 비밀번호로부터 다양한 해쉬 비밀번호를 생성 시에 일치성 확인을 위한 값(검증키)을 별도로 생성해서 관리하여, 프로비저닝 시스템 등에 텍스트 비밀번호가 없더라도 서로 다르게 해쉬 처리된 비밀번호의 일치성을 확인할 수 있도록 한다.

[0023] 다시 말하면, 본 발명은, 개인정보보호를 위해서 비밀번호를 일방향 해쉬하여 관리 및 프로비저닝하는 프로비저닝 시스템 등에서, 프로비저닝을 하는 서비스 시스템별로 다양한 일방향 해쉬를 허용하는 경우, 다양한 방식으로 해쉬 비밀번호를 생성하여 프로비저닝 시에 해쉬 비밀번호 간의 비밀번호 일치/불일치를 판단할 수 있는 검증키를 추가로 생성하여 관리하도록 함으로써, 추후 해쉬 비밀번호 불일치 발생으로 고객 민원이 제기되었을 때 검증키를 사용하여 서로 다른 해쉬 방식으로 생성된 비밀번호의 불일치 여부를 판단하여, 비밀번호 불일치가 발생한 경우 비밀번호 리셋을 통해서 서비스 시스템 간의 비밀번호 동기화 작업을 수행하는 근거를 제공하고, 고객 민원을 신속하게 처리할 수 있도록 한다.

[0024] 도 2는 본 발명에 따른 검증키를 관리하는 프로비저닝 시스템에서 다양한 방식의 해쉬 비밀번호를 관리하는 중 장애가 발생한 경우의 해쉬 비밀번호 관리 방법에 대한 일실시예 흐름도로서, 프로비저닝 시스템과 데이터베이스(DB)에서 비밀번호 검증키를 관리하는 중 서비스 인증 시스템 A(14)에서 비밀번호 오류가 발생한 경우에 검증키를 사용하여 서로 다른 해쉬 방식으로 생성된 비밀번호의 불일치 여부를 판단하여, 비밀번호 불일치가 발생한 경우 비밀번호 리셋을 통해서 서비스 시스템 간의 비밀번호 동기화 작업을 수행하도록 하는 과정을 나타내고 있다.

[0025] 먼저, 도 2를 참조하여 프로비저닝 과정을 살펴보면, 사용자 단말(11)이 비밀번호를 리셋(reset)하여 프로비저닝 시스템(12)에 웹 등을 통해 비밀번호 구성을 요청하면(201), 프로비저닝 시스템(12)은 사용자 단말(11)로부터 전달받은 비밀번호를 시스템별로 다른 해쉬를 사용하여 각각의 해쉬값(비밀번호를 해쉬한 값으로서, 이하 "복수의 해쉬 비빌번호"라고도 함)을 생성하고(202), 또한 상기 생성된 해쉬값들(복수의 해쉬 비밀번호)을 사용(해쉬 연산 또는 OR 연산 등)하여 하나의 검증키(A)를 동시에 생성한 후(203), 각각의 시스템에는 해당하는 해쉬값만을 전달하고(204 내지 206), 프로비저닝 시스템에서 상기 생성된 검증키(A)를 관리한다. 예를 들어, 도 2에 도시된 바와 같이 접속 인증 시스템(13)으로는 SHA-1 해쉬값을 전달하고(204), 서비스 인증 시스템 A(14)로는 MD5 해쉬값을 전달하고(205), 서비스 인증 시스템 B(15)로는 HAS160 해쉬값을 전달한다(206).

[0026] 상기와 같이 프로비저닝이 완료되면, 사용자 단말(11)은 상기 과정에서 신규 구성된 비밀번호로 접속 서비스, 서비스 A, 및 서비스 B를 사용하게 되는데(207 내지 209), 서비스 인증 시스템 A(14)의 비밀번호에 오류가 발생하게 되었을 때(210) 동일한 비밀번호를 입력하는데 서비스 A만 사용할 수 없다는 민원을 제기하게 된다(211).

[0027] 이때, 프로비저닝 시스템(12)에서는 검증키(A)를 이용하여 오류발생원인을 분석한다(212). 즉, 프로비저닝 시스템(12)에서는 접속 인증 시스템(13)으로부터 SHA-1 해쉬값(해쉬 비밀번호)을 획득하고 서비스 인증 시스템 A(14)로부터 MD5 해쉬값을 획득하며 서비스 인증 시스템 B(15)로부터 HAS160 해쉬값을 획득하여 검증키(B)를 신규로 생성한 후에, 상기 생성된 검증키(B)와 현재 관리하고 있는 해당 검증키(A)를 비교한다(212). 상기 비교 결과, 사용자 단말(11)이 제기한 서비스 이용 오류 민원이 비밀번호가 틀려서 발생하는 민원인 경우(213)에는 사용자 단말(11)에게 비밀번호를 리셋(reset)하도록 요청하여(214), 비밀번호 리셋(reset)을 통해서(215) 비밀번호를 일치시켜 서비스를 정상 사용하도록 한다.

[0028] 즉, 본 발명에서는 프로비저닝 시스템에서 다양한 해쉬 비밀번호 프로비저닝 시에 검증키를 추가로 생성하여 관리하도록 함으로써, 해쉬 비밀번호 간의 불일치가 발생한 경우에 이를 판단하고 적절한 조치를 취할 수 있도록

한다.

[0029] 도 3은 본 발명에 따른 프로비저닝 데이터베이스(DB)의 구성 요소 및 검증키 성성 과정을 설명하기 위한 도면이다.

[0030] 도 3에 도시된 바와 같이, 프로비저닝한 모든 해쉬값(복수의 해쉬 비밀번호)을 연산(해쉬 연산 또는 OR 연산 등)하여 하나의 검증키를 생성한다. 이때, 비밀번호를 해쉬하여 해쉬값을 생성하는 과정에서 사용한 해쉬 함수와 유사한 해쉬 함수를 통해서 검증키를 생성한다.

[0031] 도 4는 본 발명에 따른 검증키를 이용한 다양한 해쉬 비밀번호 관리 방법에 대한 일실시예 흐름도이다.

[0032] 먼저, 프로비저닝 시스템에서는 복수의 해쉬 비밀번호(해쉬값들)를 생성할 때 상기 생성된 복수의 해쉬 비밀번호를 사용하여 하나의 검증키를 생성한다(401). 즉, 프로비저닝 시스템에서는 비밀번호를 최초로 생성 또는 변경 시마다 비밀번호를 다양한 일방향 해쉬 처리하여 복수의 해쉬 비밀번호(해쉬값들)를 생성하고, 상기 생성된 복수의 해쉬 비밀번호(해쉬값들)를 연산(해쉬 연산 또는 OR 연산 등)하여 하나의 검증키를 동시에 생성한다.

[0033] 이후, 상기 생성된 검증키를 저장하여 관리한다(402). 즉, 프로비저닝 시스템에서는 상기 생성된 복수의 해쉬 비밀번호(해쉬값들)를 프로비저닝할 때, 상기 생성된 검증키를 저장하여 관리한다.

[0034] 이후, 다양한 일방향 해쉬 비밀번호의 일치 여부를 검사할 때, 현재의 일방향 해쉬 비밀번호로 생성한 검증키와 상기 이전에 생성되어 저장된 검증키를 비교한다(403). 즉, 프로비저닝 시스템에서는 고객 민원 등 필요 시에 현재의 접속 인증 시스템 및 서비스 인증 시스템들에 구성된 해쉬 비밀번호를 사용하여 새로 검증키를 생성한 후에, 상기 새로 생성한 검증키와 프로비저닝 시스템에서 기 저장하여 관리하고 있는 검증키를 비교하여 다양한 해쉬 비밀번호의 일치 여부를 검사한다.

[0035] 이후, 상기 비교 결과에 따라 다양한 해쉬 비밀번호의 일치 여부를 확인하여(404) 검증키가 서로 달라 다양한 해쉬 비밀번호가 일치하지 않는 것으로 확인된 경우 비밀번호 동기화 작업을 수행한다(405). 즉, 검증키 비교 결과, 불일치하면 프로비저닝 시스템에서는 사용자 단말에게 비밀번호를 리셋(reset)하도록 요청하여, 비밀번호 리셋(reset)을 통해서 비밀번호를 일치시켜 서비스를 정상 사용하도록 한다. 이때, 프로비저닝 시스템에서는 사용자 단말에 비밀번호 유효성 검사 오류를 표시하도록 하는 과정을 더 수행할 수도 있다.

[0036] 한편, 상기 확인 결과(404), 검증키가 서로 일치하여 다양한 해쉬 비밀번호가 일치하는 것으로 확인된 경우 타 오류로 판단하여 공지의 해당 오류 처리 과정을 수행한다(406).

[0037]

[0038] 전술한 바와 같이, 본 발명은 서비스별로 해쉬 방식이 서로 다른 비밀번호를 관리해야 하는 시스템, 예를 들어 프로비저닝 시스템 등에 이용되어, 다양한 일방향 해쉬 비밀번호를 운용 중에 해쉬 비밀번호 간의 불일치가 발생한 경우 불일치 여부를 판단할 수 있는 근거를 제공하여, 다양한 해쉬 비밀번호 동기화를 관리할 수 있도록 한다.

[0039] 예를 들면, 프로비저닝 시스템에서 비밀번호를 접속 인증 시스템으로는 SHA-1 해쉬한 비밀번호를 프로비저닝하고, 서비스 인증 시스템으로는 MD5 해쉬한 비밀번호를 프로비저닝한 후에, 운용 중 알 수 없는 이유로 MD5 해쉬한 비밀번호만 변경되는 경우에, 고객은 동일 아이디/비밀번호(ID/PWD)로 접속 인증은 되는데, 서비스 인증은 되지 않는다는 민원을 요청하게 된다. 이때, 비밀번호가 암호화되어 있으면 암호화된 비밀번호만으로는, 접속 인증 비밀번호와 서비스 인증 비밀번호의 동일성 여부를 알 수 없으며, 이로 인해 정확한 원인을 모른 상태에서 민원 응대를 하게 되고, 적절한 조치도 취하지 못할 수 있다. 하지만, 검증키를 관리하는 경우에는 상기와 같은 민원이 비밀번호 불일치에 의해서 발생하였음을 알 수 있고, 그에 따라 바로 비밀번호를 리셋하도록 할 수 있게 된다.

[0040] 한편, 전술한 바와 같은 본 발명의 방법은 컴퓨터 프로그램으로 작성이 가능하다. 그리고 상기 프로그램을 구성하는 코드 및 코드 세그먼트는 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 또한, 상기 작성된 프로그램은 컴퓨터가 읽을 수 있는 기록매체(정보저장매체)에 저장되고, 컴퓨터에 의하여 판독되고 실행

됨으로써 본 발명의 방법을 구현한다. 그리고 상기 기록매체는 컴퓨터가 판독할 수 있는 모든 형태의 기록매체를 포함한다.

[0041] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

산업이용 가능성

[0042] 본 발명은 서비스별로 해쉬 방식이 서로 다른 비밀번호를 관리해야 하는 시스템(예 : 프로비저닝 시스템) 등에 이용될 수 있다.

도면의 간단한 설명

[0043] 도 1은 종래의 검증키를 관리하지 않는 프로비저닝 시스템에서 다양한 방식의 해쉬 비밀번호를 관리하는 중 장애가 발생한 경우의 처리 과정을 나타내는 일실시예 흐름도,

[0044] 도 2는 본 발명에 따른 검증키를 관리하는 프로비저닝 시스템에서 다양한 방식의 해쉬 비밀번호를 관리하는 중 장애가 발생한 경우의 해쉬 비밀번호 관리 방법에 대한 일실시예 흐름도,

[0045] 도 3은 본 발명에 따른 프로비저닝 데이터베이스(DB)의 구성 요소 및 검증키 성성 과정을 설명하기 위한 도면,

[0046] 도 4는 본 발명에 따른 검증키를 이용한 다양한 해쉬 비밀번호 관리 방법에 대한 일실시예 흐름도이다.

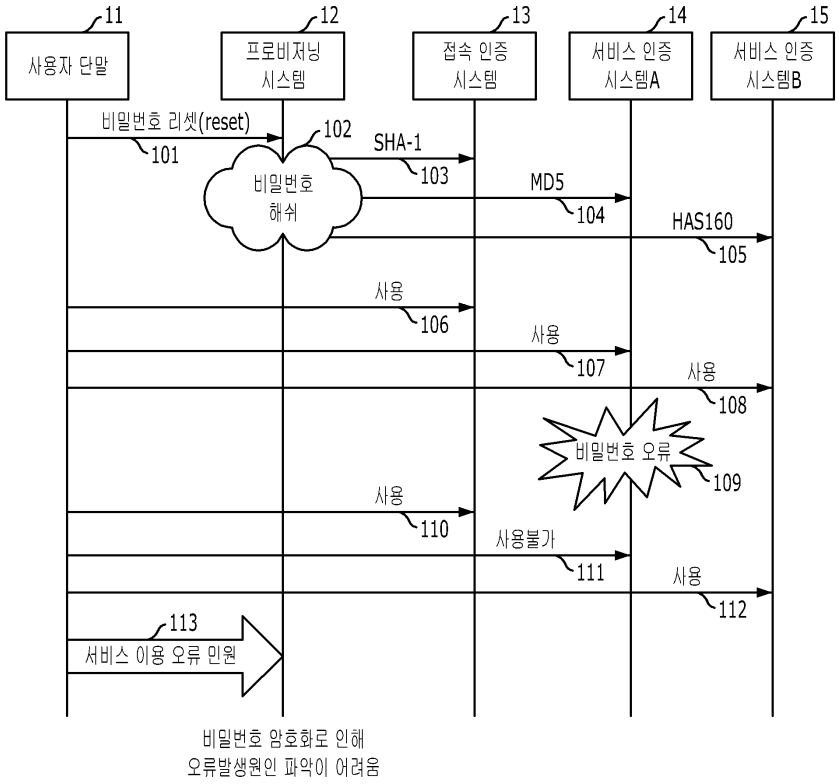
[0047] * 도면의 주요 부분에 대한 부호의 설명

[0048] 11 : 사용자 단말 12 : 프로비저닝 시스템

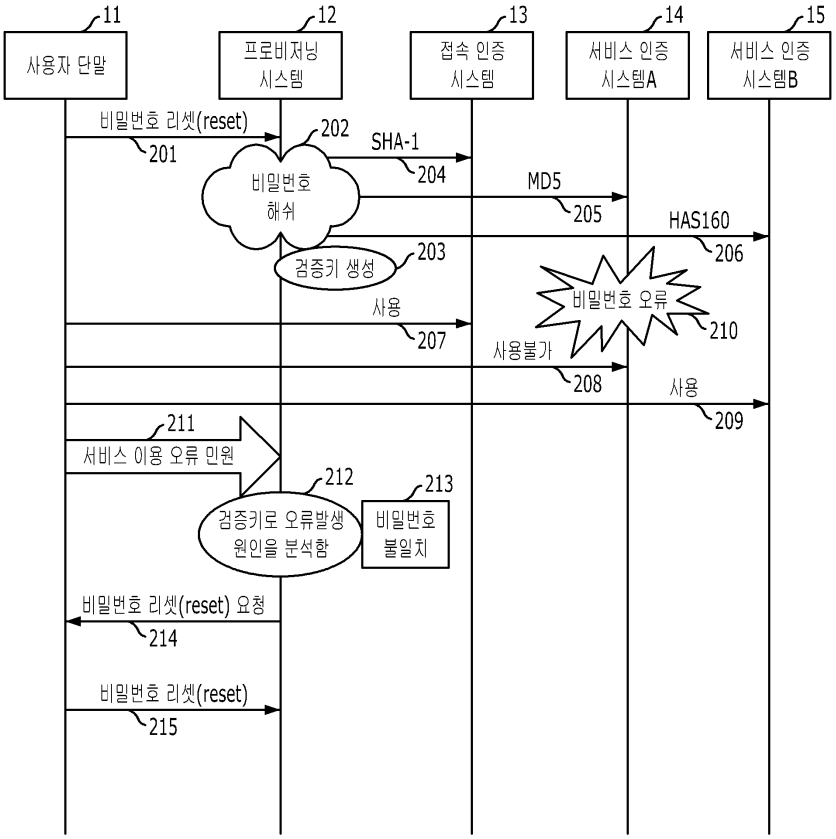
[0049] 13 : 접속 인증 시스템 14, 15 : 서비스 인증 시스템

도면

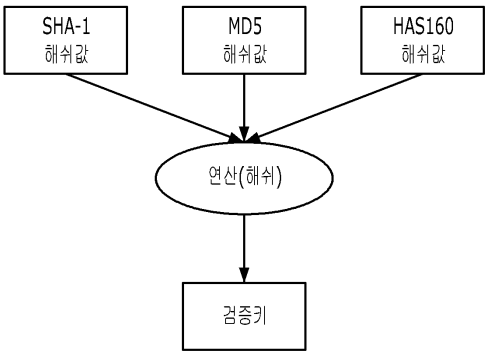
도면1


11
사용자 단말
12
프로비저닝 시스템
13
접속 인증 시스템
14
서비스 인증 시스템A
15
서비스 인증 시스템B
비밀번호 리셋(reset)
101
102
비밀번호 해쉬
SHA-1
103
MD5
104
HAS160
105
사용
106
사용
107
사용
108
비밀번호 오류
109
사용
110
사용불가
111
사용
112
113
서비스 이용 오류 민원
비밀번호 암호화로 인해
오류발생원인 파악이 어려움

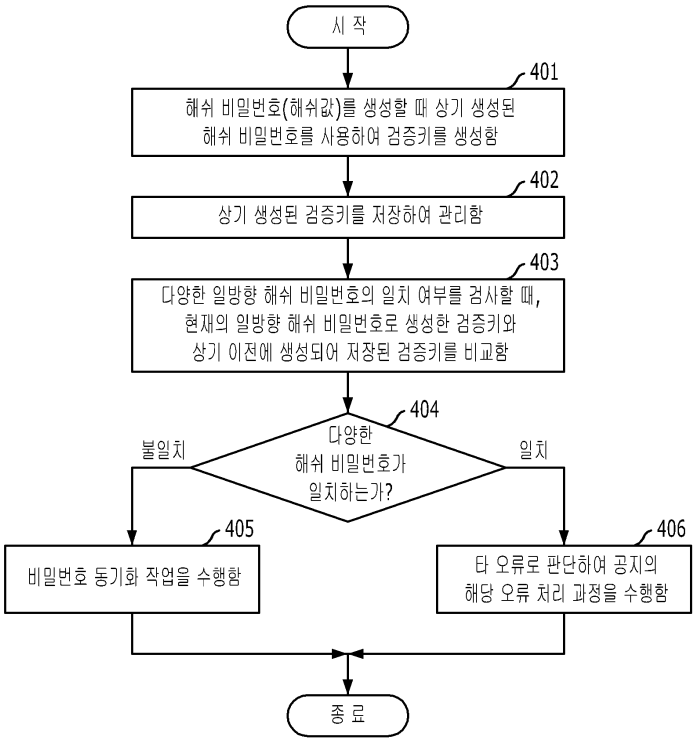
도면2


11
사용자 단말
12
프로비저닝 시스템
13
접속 인증 시스템
14
서비스 인증 시스템A
15
서비스 인증 시스템B
비밀번호 리셋(reset)
201
202
비밀번호 해쉬
SHA-1
204
MD5
205
HAS160
206
203
검증키 생성
비밀번호 오류
210
사용
207
사용불가
208
사용
209
211
서비스 이용 오류 민원
212
검증키로 오류발생 원인을 분석함
213
비밀번호 불일치
비밀번호 리셋(reset) 요청
214
비밀번호 리셋(reset)
215

도면3


SHA-1 해쉬값
MD5 해쉬값
HAS160 해쉬값
연산(해쉬)
검증키

도면4


시 작
401
해쉬 비밀번호(해쉬값)를 생성할 때 상기 생성된
해쉬 비밀번호를 사용하여 검증키를 생성함
402
상기 생성된 검증키를 저장하여 관리함
403
다양한 일방향 해쉬 비밀번호의 일치 여부를 검사할 때,
현재의 일방향 해쉬 비밀번호로 생성한 검증키와
상기 이전에 생성되어 저장된 검증키를 비교함
404
다양한
해쉬 비밀번호가
일치하는가?
불일치
일치
405
비밀번호 동기화 작업을 수행함
406
타 오류로 판단하여 공지의
해당 오류 처리 과정을 수행함
종 료