



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0097430
(43) 공개일자 2010년09월03일

(51) Int. Cl.

G06F 21/00 (2006.01) H04L 9/32 (2006.01)

G06F 17/00 (2006.01) G06F 9/00 (2006.01)

(21) 출원번호 10-2009-0016363

(22) 출원일자 2009년02월26일

심사청구일자 2009년02월26일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

인호

서울 용산구 이촌동 402 강촌아파트 109-1604

김승빈

경기 안양시 동안구 부림동 한가람삼성아파트 20
4동 1003호

(뒷면에 계속)

(74) 대리인

특허법인충현

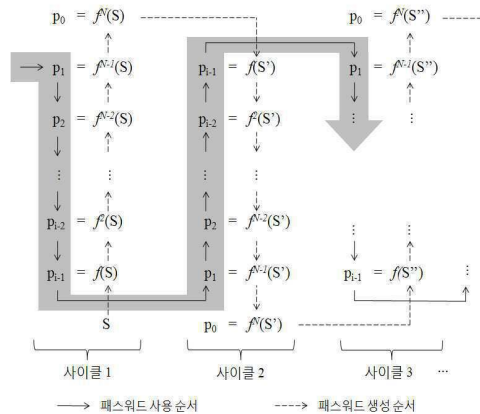
전체 청구항 수 : 총 15 항

(54) 해시 체인을 이용한 무한 인증 방법 및 이를 적용한 장치

(57) 요약

해시 체인을 이용한 무한 인증 방법 및 이를 적용한 장치가 개시된다. 본 발명의 일 실시 예에 따른 해시 체인을 이용한 무한 인증 방법은 사용자 컴퓨터에서 시작값을 이용하여 미리 지정된 길이의 해시 체인을 구성하는 복수의 패스워드를 생성하고, 상기 패스워드 중 어느 하나를 인증 컴퓨터에 전송하여 인증을 시도하고, 상기 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하며, 상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우, 상기 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 과정을 포함한다. 본 발명의 실시 예들에 의하면, 해시 체인으로 구성된 패스워드를 이용한 인증에서 해시 체인 특성으로 인해 인증 회수가 제한되는 문제점을 해결할 수 있고, 별도의 함수가 필요하지 않으며, 매번 다른 패스워드값을 사용하면서도 해시 체인 길이를 유지하기 때문에 효율적인 저장 공간 할당이 가능하다. 본 발명의 실시 예들은 패스워드 기반의 시스템 인증 및 OTP 인증에 적용할 수 있다.

대표도 - 도3



(72) 발명자

이택

충청남도 아산시 권곡동 579번지

이명락

경기 의정부시 장암동 장암동아아파트 107동 1502호

박성준

서울특별시 성북구 안암동 고려대학교 자연계캠퍼스
과학도서관 608B

특허청구의 범위

청구항 1

사용자 컴퓨터에서 시작값을 이용하여 미리 지정된 길이의 해시 체인을 구성하는 복수의 패스워드를 생성하는 단계;

상기 패스워드 중 어느 하나를 인증 컴퓨터에 전송하여 인증을 시도하고, 상기 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계; 및

상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우, 상기 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 단계

를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 2

제 1 항에 있어서,

상기 다음 사이클의 해시 체인은,

상기 시작값과는 다른 값을 해시 함수에 사용하여 생성되는 것을 특징으로 하는, 해시 체인을 이용한 무한 인증 방법.

청구항 3

제 1 항에 있어서,

상기 다음 사이클의 해시 체인을 구성하는 패스워드는,

바로 이전에 인증이 성공한 패스워드 값을 해시 함수로 한번 해시한 값인 것을 특징으로 하는, 해시 체인을 이용한 무한 인증 방법.

청구항 4

제 1 항에 있어서,

상기 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계는,

상기 인증이 성공한 패스워드를 상기 생성된 다음 사이클의 패스워드로 업데이트하는 단계를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 5

제 1 항에 있어서,

상기 다음 사이클의 해시 체인의 패스워드를 전송하여 인증하는 단계는,

마지막 패스워드를 이용한 인증에 성공한 후 생성된 다음 사이클의 패스워드를 상기 다음 사이클의 참조값으로서 전송하는 단계를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 6

제 1 항에 있어서,

상기 다음 사이클의 해시 체인의 패스워드를 전송하여 인증하는 단계는,

상기 인증이 성공할 때마다 해당 사이클의 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 7

하나 이상의 사용자 컴퓨터와 인증 컴퓨터로 구성되는 인증 시스템에서 해시 체인을 이용하여 인증하는 방법이 있어서,

사용자 컴퓨터가 시작값을 이용하여 미리 지정된 길이의 해시 체인을 구성하는 복수의 패스워드를 생성하는 단계;

인증 컴퓨터가 상기 사용자 컴퓨터로부터 상기 패스워드 중 어느 하나를 수신하면, 상기 인증 컴퓨터에 미리 저장된 값을 한 번 해시한 값과 상기 수신된 패스워드를 비교하여 인증 성공 여부를 판단하는 단계;

상기 사용자 컴퓨터가 상기 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 상기 인증에 성공한 패스워드 대신 저장하는 단계; 및

상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우, 상기 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 단계

를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 8

제 7 항에 있어서,

상기 다음 사이클의 해시 체인은,

상기 시작값과는 다른 값을 해시 함수에 사용하여 생성되는 것을 특징으로 하는, 해시 체인을 이용한 무한 인증 방법.

청구항 9

제 7 항에 있어서,

상기 다음 사이클의 해시 체인을 구성하는 패스워드는,

바로 이전에 인증이 성공한 패스워드 값을 해시 함수로 한번 해시한 값인 것을 특징으로 하는, 해시 체인을 이용한 무한 인증 방법.

청구항 10

제 7 항에 있어서,

상기 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계는,

상기 인증이 성공한 패스워드를 상기 생성된 다음 사이클의 패스워드로 업데이트하는 단계를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 11

제 7 항에 있어서,

상기 다음 사이클의 해시 체인의 패스워드를 전송하여 인증하는 단계는,

상기 인증이 성공할 때마다 해당 사이클의 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 12

제 7 항에 있어서,

상기 다음 사이클의 해시 체인의 패스워드를 전송하여 인증하는 단계는,

마지막 바로 이전 패스워드를 한번 해시하여 생성된 다음 사이클의 참조값을 상기 인증 시스템에 전송하는 단계; 및

상기 인증 시스템이 상기 전송된 다음 사이클의 참조값을 저장하는 단계를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 13

시작값을 이용하여 생성된, 해시 체인을 구성하는 복수의 패스워드 중 어느 하나를 사용자 컴퓨터가 인증 컴퓨

터에 전송하여 인증을 시도하는 단계;

상기 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계; 및

상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우, 상기 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 단계

를 포함하는, 해시 체인을 이용한 무한 인증 방법.

청구항 14

제 1 항 내지 제 13 항 중 어느 한 항에 따른 해시 체인을 이용한 무한 인증 방법을 컴퓨터 시스템에서 실행하기 위한 프로그램이 기록된 컴퓨터 시스템이 판독할 수 있는 기록매체.

청구항 15

시작값을 이용하여 생성된, 해시 체인을 구성하는 복수의 패스워드 중 어느 하나를 이용한 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하는 패스워드 갱신부;

상기 복수의 패스워드 및 상기 다음 사이클의 패스워드를 저장하는 메모리부; 및

상기 패스워드 중 어느 하나를 인증 컴퓨터에 전송하여 인증을 시도하고, 상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우 상기 메모리부에 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 인증부

를 포함하는, 해시 체인을 이용하여 무한 인증을 수행하는 장치.

명세서

발명의 상세한 설명

기술분야

[0001] 본 발명은 전자 인증 방법에 관한 것으로, 컴퓨터 기반의 통신 과정에서 상호간의 안전한 통신을 위한 인증 방법에 관한 것이다.

배경기술

[0002] 두 시스템 간의 통신은 그 과정에서 다양한 위험에 노출될 수 있다. 특정 객체에 대하여 올바르지 않은 객체가 정상적인 객체로 위장하여 통신을 시도할 경우 상호간의 통신은 모두 노출되므로 안전한 통신이 보장되지 않는다. 따라서 이를 막기 위해서는 상대방이 올바른 객체인지 확인하는 인증 절차가 필요하다.

[0003] 패스워드를 사용하여 패스워드가 일치할 때 접근이 허용되는 패스워드 인증 방식은 구현 방법이 간단하기 때문에 다양한 분야에 적용되고 있다. 대표적으로 컴퓨터 기반의 시스템에서 패스워드를 사용하여 사용자 접근을 제한하는 방법이 사용되고 있다. 이 방법은 패스워드가 인증 시마다 변경되는 OTP(One-Time Password)로 발전하여 금융 시스템에서 안전한 거래를 위한 방법으로 사용되기도 한다.

[0004] OTP로 많이 사용되는 해시 체인은 Lamport가 제안한 방법이다. 이는 해시 함수를 사용하여 강력한 보안수준을 보이면서도 적은 계산량을 보이는 방법이다. 해시 체인은 일 방향 해시 함수 특성상 해시한 결과 값으로 해시 전 값을 유추하기 어려운 특성으로 인해서 현재 사용한 패스워드로 다음에 사용할 패스워드를 유추할 수 없는 장점이 있다. 그리고 인증 시마다 매번 다른 패스워드를 사용하기 때문에 고정된 값을 사용하는 방식에 비해서 암호를 알아내기가 힘들며 비허가 접근을 더욱 어렵게 한다. 이 방법은 소프트웨어로 쉽게 구현 가능하며 하나의 해시 함수만을 사용하기 때문에 효율성이 우수하다. 또한, 이 방법은 패스워드 도청과 리플레이(Replay) 공격에 안전하며, 공개키 수준의 강력한 보안 성능을 보이면서도 적은 계산량으로 인증할 수 있는 장점이 있다. 그러나 해시 체인 특성상 인증 횟수가 제한되기 때문에 지정된 횟수 이상 인증을 하고자 할 때는 더 이상 인증할 수 없는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

- [0005] 해시 체인은 해시 함수로 생성한 값을 역순으로 사용하기 때문에 N번의 유한한 길이를 가지며, 이로 인해 인증 회수가 제한되는 문제점이 있다. 이를 해결하기 위해 해시 체인의 길이를 늘이는 경우, 해시 체인의 길이는 사용자 컴퓨터의 메모리 사용량과 비례하므로 메모리 사용량이 증가하는 문제점이 있다.
- [0006] 따라서 본 발명이 이루고자 하는 기술적 과제는 패스워드를 일정 개수로 유지하면서 무한하게 인증하기 위해 해시 체인을 무한 길이로 구성할 수 있는 방법 및 장치를 제공하는 데 있다.

과제 해결수단

- [0007] 상기의 기술적 과제를 이루기 위하여, 본 발명의 일 실시 예에 따른 해시 체인을 이용한 무한 인증 방법은 사용자 컴퓨터에서 시작값을 이용하여 미리 지정된 길이의 해시 체인을 구성하는 복수의 패스워드를 생성하고, 상기 패스워드 중 어느 하나를 인증 컴퓨터에 전송하여 인증을 시도하고, 상기 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하며, 상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우, 상기 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 과정을 포함한다.
- [0008] 바람직하게는, 상기 다음 사이클의 해시 체인은, 상기 시작값과는 다른 값을 해시 함수에 사용하여 생성될 수 있다.
- [0009] 바람직하게는, 상기 다음 사이클의 해시 체인을 구성하는 패스워드는, 바로 이전에 인증이 성공한 패스워드 값을 해시 함수로 한번 해시한 값일 수 있다.
- [0010] 바람직하게는, 상기 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계는, 상기 인증이 성공한 패스워드를 상기 생성된 다음 사이클의 패스워드로 업데이트하는 단계를 포함할 수 있다.
- [0011] 바람직하게는, 상기 다음 사이클의 해시 체인의 패스워드를 전송하여 인증하는 단계는, 마지막 패스워드를 이용한 인증에 성공한 후 생성된 다음 사이클의 패스워드를 상기 다음 사이클의 참조값으로서 전송하는 단계를 포함할 수 있다.
- [0012] 바람직하게는, 상기 다음 사이클의 해시 체인의 패스워드를 전송하여 인증하는 단계는, 상기 인증이 성공할 때마다 해당 사이클의 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계를 포함할 수 있다.
- [0013] 상기의 기술적 과제를 이루기 위하여 본 발명의 다른 실시 예에 따른 해시 체인을 이용한 무한 인증 방법은 시작값을 이용하여 생성된, 해시 체인을 구성하는 복수의 패스워드 중 어느 하나를 사용자 컴퓨터가 인증 컴퓨터에 전송하여 인증을 시도하고, 상기 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하며, 상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우, 상기 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 과정을 포함한다.
- [0014] 상기의 기술적 과제를 이루기 위하여 본 발명의 또 다른 실시 예에 따른 해시 체인을 이용한 무한 인증 방법은 하나 이상의 사용자 컴퓨터와 인증 컴퓨터로 구성되는 인증 시스템에서, 사용자 컴퓨터가 시작값을 이용하여 미리 지정된 길이의 해시 체인을 구성하는 복수의 패스워드를 생성하는 단계; 인증 컴퓨터가 상기 사용자 컴퓨터로부터 상기 패스워드 중 어느 하나를 수신하면, 상기 인증 컴퓨터에 미리 저장된 값을 한 번 해시한 값과 상기 수신된 패스워드를 비교하여 인증 성공 여부를 판단하는 단계; 상기 사용자 컴퓨터가 상기 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 상기 인증에 성공한 패스워드 대신 저장하는 단계; 및 상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우, 상기 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 단계를 포함한다.
- [0015] 바람직하게는, 상기 다음 사이클의 해시 체인은, 상기 시작값과는 다른 값을 해시 함수에 사용하여 생성될 수 있다.
- [0016] 바람직하게는, 상기 다음 사이클의 해시 체인을 구성하는 패스워드는, 바로 이전에 인증이 성공한 패스워드 값을 해시 함수로 한번 해시한 값일 수 있다.
- [0017] 바람직하게는, 상기 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계는, 상기 인증이 성공한 패스워드를 상기 생성된 다음 사이클의 패스워드로 업데이트하는 단계를 포함할 수 있다.

- [0018] 바람직하게는, 상기 다음 사이클의 해시 체인의 패스워드를 전송하여 인증하는 단계는, 상기 인증이 성공할 때마다 해당 사이클의 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하여 저장하는 단계를 포함할 수 있다.
- [0019] 바람직하게는, 상기 다음 사이클의 해시 체인의 패스워드를 전송하여 인증하는 단계는, 마지막 바로 이전 패스워드를 한번 해시하여 생성된 다음 사이클의 참조값을 상기 인증 시스템에 전송하는 단계; 및 상기 인증 시스템이 상기 전송된 다음 사이클의 참조값을 저장하는 단계를 포함할 수 있다.
- [0020] 상기의 기술적 과제를 이루기 위하여 본 발명의 일 실시 예에 따른 해시 체인을 이용하여 무한 인증을 수행하는 장치는 시작값을 이용하여 생성된, 해시 체인을 구성하는 복수의 패스워드 중 어느 하나를 이용한 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성하는 패스워드 갱신부; 상기 복수의 패스워드 및 상기 다음 사이클의 패스워드를 저장하는 메모리부; 및 상기 패스워드 중 어느 하나를 인증 컴퓨터에 전송하여 인증을 시도하고, 상기 복수의 패스워드를 이용한 인증이 모두 완료된 경우 상기 메모리부에 저장된 다음 사이클의 해시 체인의 패스워드를 상기 인증 컴퓨터에 전송하여 인증하는 인증부를 포함한다.

효 과

- [0021] 본 발명의 실시 예들에 의하면, 해시 체인으로 구성된 패스워드를 이용한 인증에서 해시 체인 특성으로 인해 인증 회수가 제한되는 문제점을 해결할 수 있고, 별도의 함수가 필요하지 않으며, 매번 다른 패스워드값을 사용하면서도 해시 체인 길이를 유지하기 때문에 효율적인 저장 공간 할당이 가능하다. 본 발명의 실시 예들은 패스워드 기반의 시스템 인증 및 OTP 인증에 적용할 수 있다.

발명의 실시를 위한 구체적인 내용

- [0022] 이하에서는 도면을 참조하여 본 발명의 바람직한 실시 예를 설명하기로 한다. 그러나, 다음에 예시하는 본 발명의 실시 예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시 예에 한정되는 것은 아니다.
- [0023] 해시 함수는 값 s 로부터 $f(s)$ 를 생성할 수 있지만 생성된 $f(s)$ 로부터 s 를 구할 수 없다는 특성이 있다. 따라서 상대방으로부터 받은 s 를 해시 함수 $f()$ 를 이용하여 해시한 값과 자신의 $f(s)$ 와 같은 경우 상대방을 올바른 대상으로 간주할 수 있다.
- [0024] 도 1은 사용자 컴퓨터와 인증 컴퓨터 사이에서 패스워드 인증 과정을 도시한 것이다.
- [0025] 일 방향(One-way) 함수 $f()$ 를 이용하여 초기 값 S 를 해시 하여 값을 생성한다. 그리고 이 값을 다시 해시하여 새로운 값을 만든다. 이 과정을 미리 지정된 길이인 N 번만큼 재귀 호출하여 패스워드를 N 개 생성한다. 이 경우, 패스워드의 생성 순서는 $f(S)$, $f(f(S))$, $f(f(f(S)))$, $\dots$, $f^{N-1}(S)$, $f^N(S)$ 이다. 사용자 컴퓨터는 생성된 N 개의 패스워드를 저장하고, 인증 컴퓨터는 마지막으로 생성한 N 번 해시한 값을 저장한다.
- [0026] 사용자 컴퓨터는 생성된 패스워드를 $f^{N-1}(S)$ 부터 $f(S)$ 까지 역순으로 순차적으로 사용하며, 인증 컴퓨터는 사용자 컴퓨터로부터 수신한 값을 한 번 해시하여 저장된 값과 일치하는지 비교한다. 이 경우, 패스워드의 사용 순서는 $f^{N-1}(S)$, $f^{N-2}(S)$, $\dots$, $f(f(S))$, $f(S)$ 이다. 일치할 경우 인증이 성공하고, 인증 컴퓨터는 사용자 컴퓨터로부터 받은 값을 새로운 비교 값으로 저장하여 다음 번 인증 시 비교 값으로 사용한다.
- [0027] 이하에서는 인증을 시도하는 객체를 사용자 컴퓨터로 가정하고 인증을 허용하는 객체를 인증 컴퓨터로 가정한다. 그러나, 사용자 컴퓨터는 단순히 개인용 PC에 국한되지 않는다. 해시 체인을 생성하는 객체는 소형화된 OTP 디바이스, 휴대폰 등으로 대체될 수 있다.
- [0028] 사용자 컴퓨터와 인증 컴퓨터는 패스워드를 사용하여 인증을 수행하여 서로 동일한 패스워드 일때 올바른 대상으로 간주한다. 인증을 위해서는 최초 초기화 과정을 통해서 상호간에 약속된 정보를 저장할 필요가 있다.
- [0029] 초기화 과정은 인증 값을 최초 생성하는 과정으로써 사용자 컴퓨터와 인증 컴퓨터가 구성될 때 최초 한 번만 수행되는 것이 바람직하다. 이때, 미리 지정된 길이만큼 해시 체인으로 패스워드를 구성해야 한다. 이때 구성된 패스워드는 한 사이클의 인증 값이다. 이하에서 N 은 패스워드 길이, $f()$ 는 해시 함수, S 는 시작 값을 의미한다.
- [0030] 유일한 수인 시작 값 S 를 해시 함수 $f()$ 를 이용하여 한 번 해시한다. 이렇게 생성된 값을 해시 함수 $f()$ 로 다시 해시하여 값을 만들고, 이 과정을 미리 정해진 길이 N 만큼 반복하여 총 N 개의 값을 생성한다. 사용자 컴퓨터는

생성된 N개의 패스워드를 모두 저장해둔다. 따라서 사용자 컴퓨터는 N 길이만큼의 메모리 공간이 필요하다. 그리고 사용자 컴퓨터는 해시 체인으로 구성된 패스워드 갱신을 위해서 해시 함수 $f()$ 를 가진다. 인증 컴퓨터는 생성된 패스워드 중에서 N번 해시한 값을 보관한다. 따라서 인증 컴퓨터는 1개의 사용자 컴퓨터에 대해서 하나의 패스워드 저장 공간이 필요하다. 초기화 과정이 모두 완료되면 사용자 컴퓨터와 인증 컴퓨터가 패스워드를 사용하여 상호간의 인증을 하는 과정이 수행된다.

- [0031] 도 2는 해시 체인을 이용한 인증 방법의 흐름도이다.
- [0032] 먼저, 사용자 컴퓨터가 전송할 패스워드의 순서에 대한 변수 i 를 초기화한다(S210). 다음, 사용자 컴퓨터는 i 번째 패스워드를 인증 컴퓨터에 전송한다(S220).
- [0033] 인증 컴퓨터는 사용자 컴퓨터로부터 전송된 패스워드를 해시한 값과 자신이 가지고 있는 값이 동일한지 판단한다(S230). 동일한 경우 인증이 성공한 것으로 판단(S231)하고, 동일하지 않은 경우 인증이 실패한 것으로 판단(S235)한다.
- [0034] 이때, 인증이 성공할 때마다 인증 컴퓨터는 i 번째 패스워드를 새로운 참조값으로 저장한다(S240). 다음, 변수 i 를 1만큼 증가시킨다(S250).
- [0035] 마지막으로, 복수의 패스워드를 이용한 인증이 모두 완료된 경우(S260), 인증 절차를 종료하고, 복수의 패스워드를 모두 사용하지 않은 경우에는 패스워드를 전송하는 과정(S220)부터 상술한 절차를 반복한다.
- [0036] 본 발명의 일 실시 예에 따라 해시 체인으로 구성한 패스워드의 유한한 길이를 무한한 인증을 위해서는 패스워드 값을 재 초기화하여 해시 체인을 새롭게 연속적으로 구성하여야 한다. 무한한 인증을 위해 해시 체인을 생성할 때 패스워드 값들이 반복되지 않도록 구성한다. 안전한 인증을 위해 이미 사용한 패스워드를 저장한 후 이 값을 다시 사용해서 인증하는 것을 방지하여야 하기 때문이다.
- [0037] 일정 길이의 해시 체인을 연속적으로 구성하여 지속적으로 인증하는 방법은 미리 지정된 길이로 해시 체인을 생성하여 복수의 패스워드를 구성하고, 각각의 패스워드를 사용하여 인증하며, 인증이 성공적으로 이루어질 때마다 다음 사이클의 해시 체인 패스워드를 생성하여 저장해두며, 모든 패스워드를 사용하여 미리 지정된 길이만큼 인증한 후에는, 다음 사이클의 해시 체인의 패스워드 값을 사용하여 인증하는 과정을 포함한다.
- [0038] 이 방법은 유한한 길이의 해시 체인이 생성된 후 인증을 수행할 때마다 다음 사이클의 인증 값을 생성한다. 따라서 한 사이클의 해시 체인의 사용이 완료되면 동일한 길이의 다음 사이클의 해시 체인 생성이 완료되므로 연속적인 인증이 가능하다.
- [0039] 도 3은 패스워드 사용 순서 및 패스워드 생성 순서의 예를 도시한 것이다.
- [0040] 도 3은 무한한 인증을 위한 새로운 사이클 생성에 대한 세부 과정을 나타낸다. 여기서, $p_1, p_2, \dots, p_{i-2}, p_{i-1}$ 은 해시 체인을 구성하는 복수의 패스워드이다. S, S', S'' 등은 각 사이클의 패스워드를 생성하기 위한 시작값이다.
- [0041] 다음 사이클의 시작값 S' 은 예를 들어, $f^N(S)$ 를 사용자 컴퓨터 고유의 비밀키 또는 비밀번호와 XOR 연산하여 생성할 수 있다. 이 방식은 $f^N(S')$ 를 3번째 사이클의 시작값 S'' 으로 변환하는 과정에도 적용될 수 있다. 그러나, 여기에 설명된 방법은 예시적인 것에 불과하며, 실제 구현 과정에서 시스템의 운영자가 정하는 임의의 방식으로 다음 사이클의 시작값이 정해질 수도 있다.
- [0042] 도 4 내지 9는 본 발명의 일 실시 예에 따른 해시 체인을 이용한 무한 인증 방법의 예를 도시한 것이다.
- [0043] 여기서, 사용자 컴퓨터는 적어도 길이 N만큼의 저장 공간을 갖는 것을 가정한다.
- [0044] 먼저, 사용자 컴퓨터는 i 번째 패스워드를 인증 컴퓨터에게 전송한다. 인증 컴퓨터는 사용자 컴퓨터로부터 받은 i 번째 패스워드를 한번 해시하여 미리 저장된 값과 같은지 비교한다. 이 과정은 도 4에 도시되어 있다. 이 과정에서 양자의 값이 일치할 경우 인증이 성공한 것으로 판단한다.
- [0045] 인증이 성공하면 사용자 컴퓨터는 다음 사이클의 패스워드 생성을 수행한다. 이 과정은 도 5에 도시되어 있다. 현재 인증 컴퓨터에 전송된 패스워드가 1번째 일 경우, 이 값은 시작값 S 을 N-1번 해시한 값(즉, $H^{N-1}(S)$)이다. 사용자 컴퓨터는 현재 패스워드의 이전 값인 S 를 N번 해시한 값(즉, $H^N(S)$)을 새로운 값으로 만들어 해시하는

방식으로 업데이트한다. 따라서 1번째 이전 값은 새로운 값(즉, $H(S')$)으로 변경되며 이 값은 새로운 사이클의 패스워드가 된다. 새로운 값은 다양한 방법, 예를 들어 난수 생성기로 생성된 임의의 값이거나 기존의 패스워드에 XOR, 시프트(Shift) 연산 등을 사용한 완전히 다른 값일 수 있다.

[0046] 현재 패스워드가 $i(2 \leq i \leq N-2)$ 번째 패스워드인 경우, 다시 말해서 첫 번째 패스워드가 아니고 마지막 패스워드가 아닐 경우에 인증이 성공하면, 사용자 컴퓨터는 $i-2$ 번째 값을 한번 해시하여 $i-1$ 번째 패스워드가 저장된 공간에 저장한다. 따라서 이전의 인증 값은 새로운 값을 갖게 된다. 예를 들어, 2번째 인증일 경우 사용자 컴퓨터는 시작 값 S' 을 한번 해시한 값을 다시 한번 해시하여 1번째 인증 값이 저장된 공간에 저장한다. 3번째 인증일 경우 사용자 컴퓨터는 1번째 인증 값을 한 번 해시하여 2번째 인증 값이 저장된 공간에 저장한다. 이 과정은 도 6에 도시되어 있다.

[0047] 현재 패스워드가 $N-1$ 번째일 경우, 다시 말해서 마지막 패스워드일 경우 사용자 컴퓨터는 $i-2$ 번째 값을 한 번 해시하여 $i-1$ 번째 저장된 값에 저장한다. 그리고 $i-1$ 번째 값을 한 번 해시하여 i 번째 값에 저장한다. 마지막 패스워드까지 모든 패스워드가 사용되면 저장된 패스워드는 새로운 값으로 전부 교체된다. 이 값들은 다음 사이클의 해시 체인으로 사용된다. 이 과정은 도 7에 도시되어 있다.

[0048] 마지막으로 해시하여 i 번째 값에 저장된 값은 인증 컴퓨터에 전송하여 다음 사이클의 참조 값으로 저장하게 한다. 이 과정은 도 8에 도시되어 있다.

[0049] 다음 번 사이클에서 사용자 컴퓨터는 현재 사이클에서 사용했던 순서의 역순으로, 다시 말해서 $N-1$ 번째 갱신된 값에서부터 시작하여 $N-2$ 번째 갱신된 값 등의 순서로 사용한다. 따라서 지속적으로 무한한 인증이 가능하다. 새로운 사이클에서의 1번째 인증 과정은 도 9에 도시되어 있다.

[0050] 도 10은 본 발명의 일 실시 예에 따른 무한 인증을 수행하는 사용자 컴퓨터의 블록도이다.

[0051] 초기화부(1010)는 사용자 컴퓨터(1000) 및 인증 컴퓨터(1090) 외부에 배치된다. 초기화부(1010)는 시작값을 이용하여 일정한 길이의 해시 체인을 구성하는 복수의 패스워드를 생성한다. 이렇게 생성된 패스워드들은 사용자 컴퓨터(1000) 및 인증 컴퓨터(1090)의 메모리부(1020, 1091)에 저장된다.

[0052] 메모리부(1020)는 초기화부(1010)에 의해 생성된 복수의 패스워드, 패스워드 갱신부(1040)에 의해 생성되는 패스워드들을 저장한다.

[0053] 패스워드 갱신부(1040)는 초기화부(1010)에 의해 생성된 복수의 패스워드 중 어느 하나를 이용한 인증이 성공할 때마다 다음 사이클의 해시 체인을 구성하는 패스워드를 생성한다.

[0054] 인증부(1030)는 메모리부(1020)에 저장된 패스워드 중 어느 하나를 인증 컴퓨터에 전송하여 인증을 시도한다. 한편, 인증 컴퓨터(1090)의 인증부(1092)는 메모리부(1091)에 저장된 참조값과 사용자 컴퓨터(1000)로부터 전송되는 패스워드를 해시한 값을 비교하여 인증의 성공 여부를 판단한다. 인증이 성공하면, 인증 컴퓨터(1090)의 인증부(1092)는 사용자 컴퓨터(1000)의 인증부(1030)에 인증 성공을 알리는 메시지를 전송할 수 있다.

[0055] 인증부(1030)는 복수의 패스워드를 이용한 인증이 모두 완료된 경우 메모리부(1020)에 저장된 다음 사이클의 해시 체인의 패스워드를 인증 컴퓨터(1090)에 전송하여 인증한다.

[0056] 본 발명은 소프트웨어를 통해 실행될 수 있다. 바람직하게는, 본 발명의 일 실시 예에 따른 해시 체인을 이용한 무한 인증 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

[0057] 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 인증 컴퓨터에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0058] 본 발명은 도면에 도시된 일 실시 예를 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시 예의 변형이 가능하다는 점을 이해할 것이다. 그리고, 이와 같은 변형은 본 발명의 기술적 보호범위 내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기

술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

산업이용 가능성

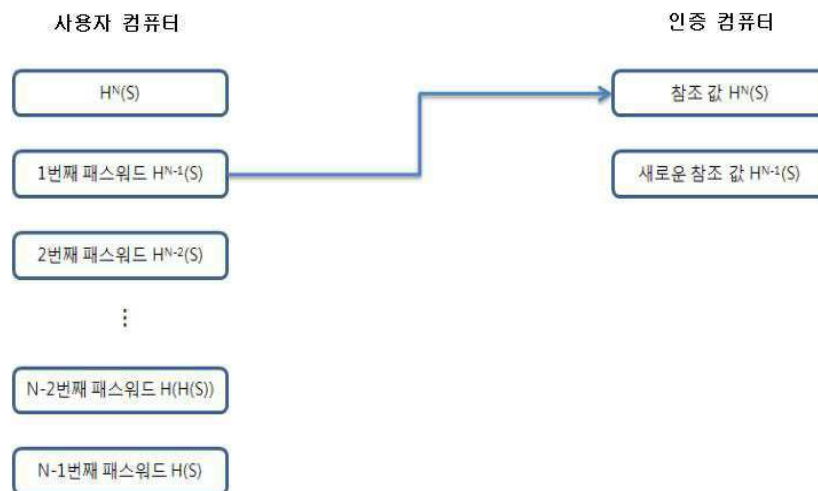
[0059] 본 발명은 해시 체인으로 구성된 패스워드를 이용한 인증에서 해시 체인 특성으로 인해 인증 회수가 제한되는 문제점을 해결할 수 있는 메모리 효율적인 인증 방법 및 장치에 관한 것으로, 모바일 뱅킹이나 인터넷 뱅킹 등의 금융 분야, 네트워크 시스템의 패스워드 인증 분야 등에서 패스워드 기반의 인증 시스템 및 OTP 인증 시스템에 적용될 수 있다.

도면의 간단한 설명

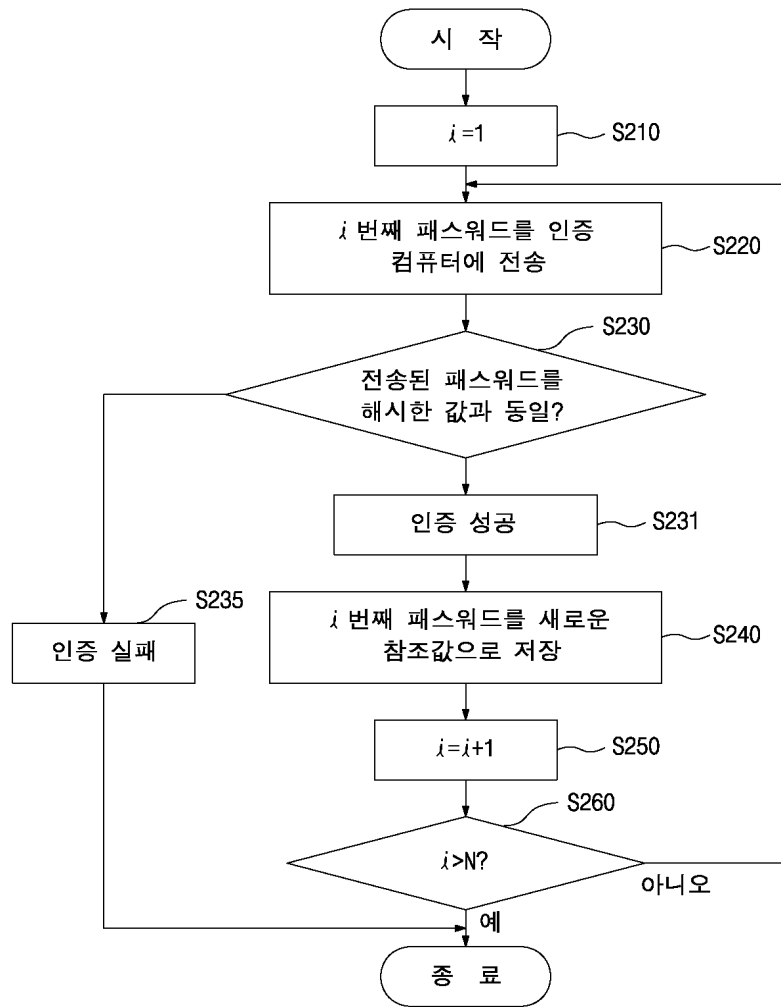
- [0060] 도 1은 사용자 컴퓨터와 인증 컴퓨터 사이에서 패스워드 인증 과정을 도시한 것이다.
- [0061] 도 2는 해시 체인을 이용한 인증 방법의 흐름도이다.
- [0062] 도 3은 패스워드 사용 순서 및 패스워드 생성 순서의 예를 도시한 것이다.
- [0063] 도 4 내지 9는 본 발명의 일 실시 예에 따른 해시 체인을 이용한 무한 인증 방법의 예를 도시한 것이다.
- [0064] 도 10은 본 발명의 일 실시 예에 따른 무한 인증을 수행하는 사용자 컴퓨터의 블록도이다.

도면

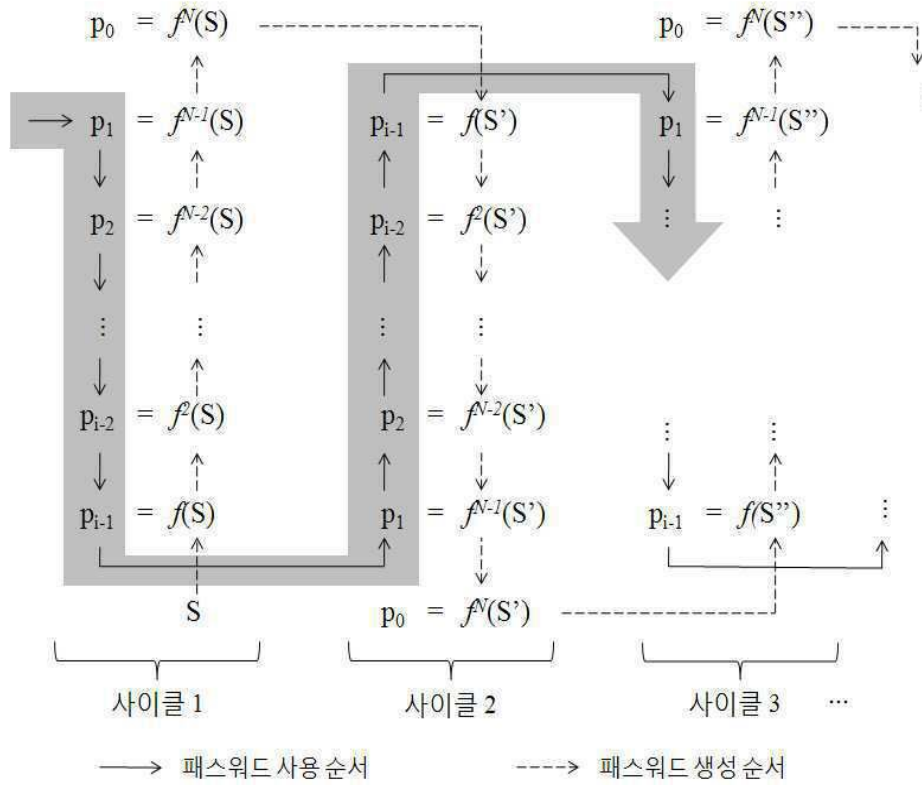
도면1



도면2



도면3



도면4

단계 1



도면5

단계 2-1



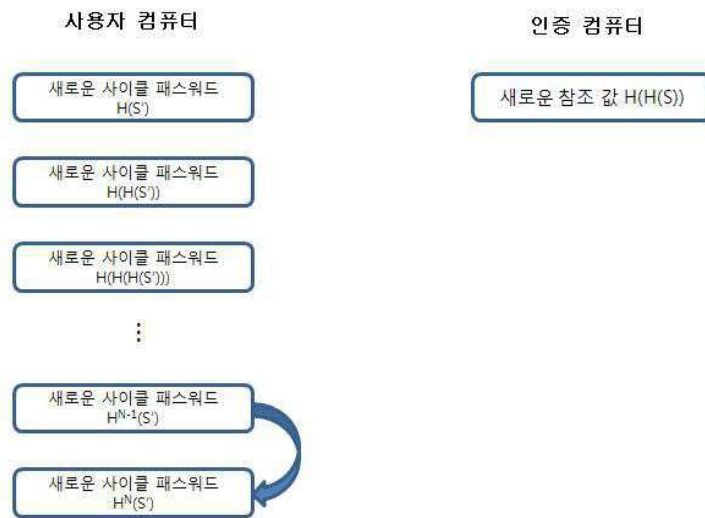
도면6

단계 2-2



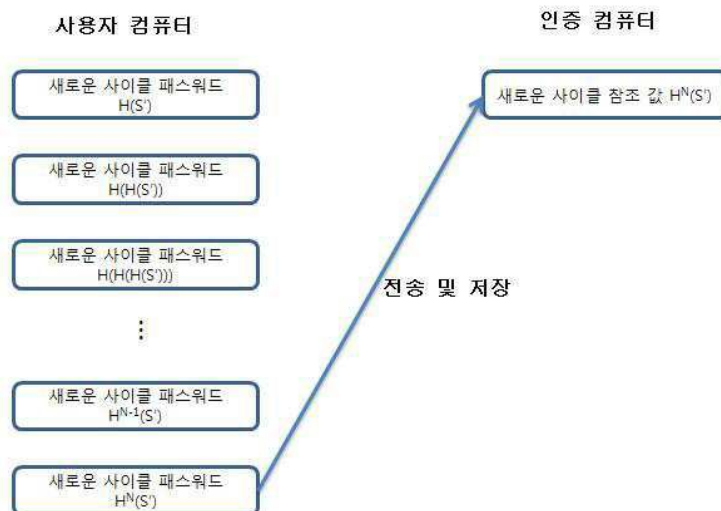
도면7

단계 2-3 : 모든 패스워드 갱신 완료



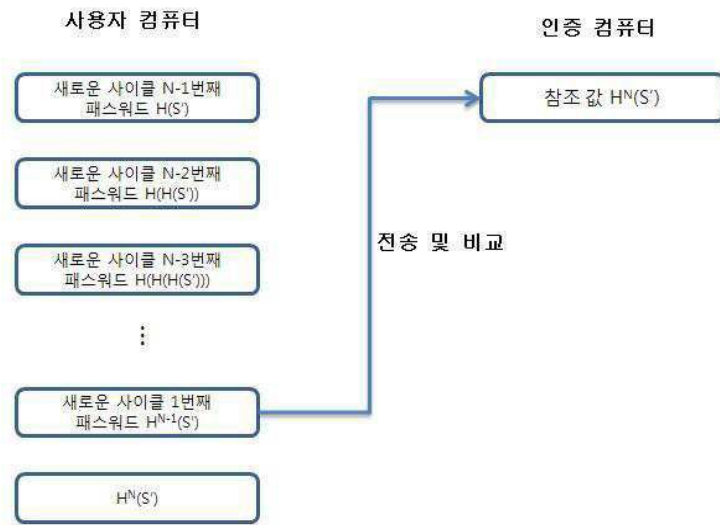
도면8

단계 2-3 : 새로운 사이클 참조 패스워드 전송



도면9

단계 4 : 새로운 사이클에서의 1번째 인증



도면10

