(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년07월22일
(11) 등록번호 10-2424873
(24) 등록일자 2022년07월20일

(51) 국제특허분류(Int. Cl.)
G06F 21/46 (2013.01) *G06F 21/31* (2013.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/46 (2013.01)
G06F 21/316 (2013.01)
(21) 출원번호 10-2020-0102207
(22) 출원일자 2020년08월14일
심사청구일자 2020년08월14일
(65) 공개번호 10-2022-0021543
(43) 공개일자 2022년02월22일
(56) 선행기술조사문헌
JP2020052605 A*
KR1020160029640 A*
KR1020200089971 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호(신천동, 파크리오)
이신철
서울특별시 광진구 뚝섬로49길 68, 203호(자양동, 연준빌)
(74) 대리인
두호특허법인

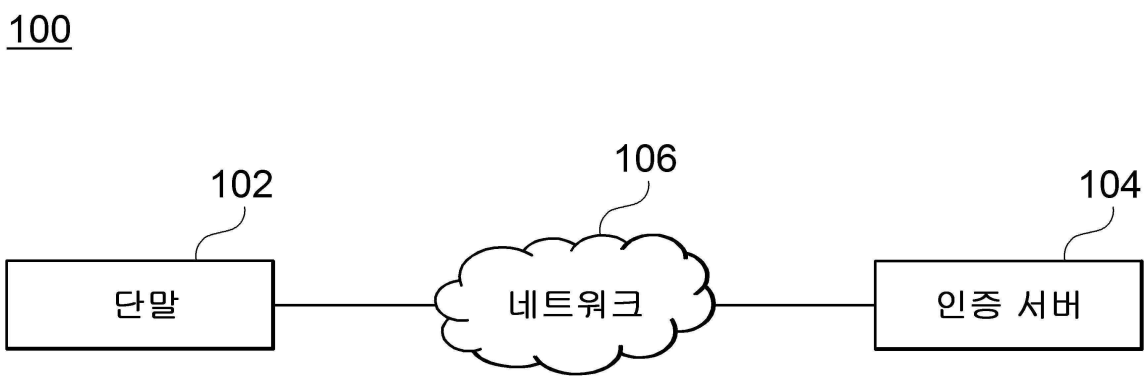
전체 청구항 수 : 총 11 항 심사관 : 정성훈

(54) 발명의 명칭 **비밀번호 및 행동 패턴을 이용한 멀티 팩터 인증 시스템 및 방법**

(57) 요 약

비밀번호 및 행동 패턴을 이용한 멀티 팩터 인증 시스템 및 방법이 개시된다. 일 실시예에 따른 멀티 팩터 인증 시스템은 단말 및 인증 서버를 포함하며, 상기 단말은, 상기 인증 서버와 사전 공유된 패스워드 기반 인증 정보를 이용하여 단말 사용자의 1차 인증을 수행하고, 상기 1차 인증 과정에서 생성된 단말측 세션키를 이용하여 상기 단말 사용자로부터 획득된 인증 대상 행동 패턴을 암호화하여 상기 인증 서버로 송신하며, 상기 인증 서버는, 상기 1차 인증 과정에서 생성된 서버측 세션키를 이용하여 상기 암호화된 인증 대상 행동 패턴을 복호화하고, 복호화된 인증 대상 행동 패턴을 상기 사용자의 행동 패턴 모델과 비교하여 상기 단말 사용자의 2차 인증을 수행한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3228 (2013.01)
G06F 2221/2113 (2013.01)
H04L 2463/062 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711117818
과제번호 2020R1F1A1072275
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)(R&D)
연구과제명 무인항공기를 위한 블록체인 기반 보안 강화 기술 개발
기 여 율 1/2
과제수행기관명 세종대학교
연구기간 2020.06.01 ~ 2021.02.28
이 발명을 지원한 국가연구개발사업
과제고유번호 1345321135
과제번호 2020R1A6A1A03038540
부처명 교육부
과제관리(전문)기관명 한국연구재단
연구사업명 이공학학술연구기반구축(R&D)
연구과제명 자율지능무인비행체연구소
기 여 율 1/2
과제수행기관명 세종대학교
연구기간 2020.06.01 ~ 2021.02.28

명 세 서

청구범위

청구항 1

단말 및 인증 서버를 포함하는 멀티 팩터 인증 시스템으로서,

상기 단말은, 상기 인증 서버와 사전 공유된 패스워드 기반 인증 정보를 이용하여 단말 사용자의 1차 인증을 수행하고, 상기 1차 인증 과정에서 생성된 단말측 세션키를 이용하여 상기 1차 인증 과정에서 상기 단말 사용자로부터 획득된 인증 대상 행동 패턴을 암호화하여 상기 인증 서버로 송신하며,

상기 인증 서버는, 상기 1차 인증 과정에서 생성된 서버측 세션키를 이용하여 상기 암호화된 인증 대상 행동 패턴을 복호화하고, 복호화된 인증 대상 행동 패턴을 상기 사용자의 행동 패턴 모델과 비교하여 상기 단말 사용자의 2차 인증을 수행하고,

상기 단말은, 랜덤하게 설정된 변환 함수(transformation function)를 이용하여 상기 사용자로부터 수집된 행동 패턴을 변환하고, 변환된 행동 패턴을 이용하여 상기 행동 패턴 모델을 생성하며, 생성된 상기 행동 패턴 모델을 상기 인증 서버에 등록하되, 상기 인증 서버에 등록된 상기 행동 패턴 모델이 외부로 노출된 것으로 판단되는 경우, 새로운 변환 함수를 이용하여 상기 수집된 행동 패턴을 재변환하여 상기 행동 패턴 모델을 재구성하고, 재구성된 상기 행동 패턴 모델을 상기 인증 서버에 재등록하는, 멀티 팩터 인증 시스템.

청구항 2

청구항 1에 있어서,

상기 패스워드 기반 인증 정보는, 상기 단말 사용자의 패스워드 또는 상기 패스워드의 해시값인, 멀티 팩터 인증 시스템.

청구항 3

삭제

청구항 4

삭제

청구항 5

청구항 1에 있어서,

상기 단말은, 상기 변환 함수를 이용하여 인증 대상 행동 패턴을 변환한 뒤 상기 인증 서버로 송신하는, 멀티 팩터 인증 시스템.

청구항 6

삭제

청구항 7

청구항 1에 있어서,

상기 인증 서버는, 상기 2차 인증에 성공한 경우 상기 인증 대상 행동 패턴을 이용하여 상기 행동 패턴 모델을 갱신하는, 멀티 팩터 인증 시스템.

청구항 8

청구항 1에 있어서,

상기 인증 서버는, 상기 2차 인증에 성공한 경우 상기 인증 대상 행동 패턴을 저장하고,

상기 행동 패턴 모델이 손상된 경우, 기 저장된 상기 인증 대상 행동 패턴을 이용하여 상기 행동 패턴 모델을 재생성하는, 멀티 팩터 인증 시스템.

청구항 9

사용자로부터 수집된 행동 패턴으로부터 행동 패턴 모델을 생성하고, 생성된 상기 행동 패턴 모델을 인증 서버에 등록하는 행동 패턴 수집 모듈;

상기 인증 서버와 사전 공유된 패스워드 기반 인증 정보를 이용하여 상기 인증 서버와 1차 인증을 수행하고, 상기 인증 서버와 공유되는 세션키를 생성하는 제1 인증 모듈; 및

상기 1차 인증 과정에서 상기 사용자로부터 획득된 인증 대상 행동 패턴을 상기 세션키로 암호화하여 상기 인증 서버로 송신함으로써 상기 인증 서버와 2차 인증을 수행하는 제2 인증 모듈을 포함하고,

상기 행동 패턴 수집 모듈은, 랜덤하게 설정된 변환 함수(transformation function)를 이용하여 상기 수집된 행동 패턴을 변환하고, 변환된 행동 패턴을 이용하여 상기 행동 패턴 모델을 생성하며, 상기 인증 서버에 등록된 상기 행동 패턴 모델이 외부로 노출된 것으로 판단되는 경우, 새로운 변환 함수를 이용하여 상기 수집된 행동 패턴을 재변환하여 상기 행동 패턴 모델을 재구성하고, 재구성된 상기 행동 패턴 모델을 상기 인증 서버에 재등록하는, 단말 장치.

청구항 10

청구항 9에 있어서,

상기 패스워드 기반 인증 정보는, 상기 사용자의 패스워드 또는 상기 패스워드의 해시값인, 단말 장치.

청구항 11

삭제

청구항 12

청구항 9에 있어서,

상기 제2 인증 모듈은, 상기 변환 함수를 이용하여 인증 대상 행동 패턴을 변환한 뒤 상기 인증 서버로 송신하는, 단말 장치.

청구항 13

삭제

청구항 14

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 단말 장치에서 수행되는 방법으로서,

사용자로부터 수집된 행동 패턴으로부터 행동 패턴 모델을 생성하고, 생성된 상기 행동 패턴 모델을 인증 서버에 등록하는 단계;

상기 인증 서버와 사전 공유된 패스워드 기반 인증 정보를 이용하여 상기 인증 서버와 1차 인증을 수행하고, 상기 인증 서버와 공유되는 세션키를 생성하는 제1 인증 단계; 및

상기 1차 인증 과정에서 상기 사용자로부터 획득된 인증 대상 행동 패턴을 상기 세션키로 암호화하여 상기 인증 서버로 송신함으로써 상기 인증 서버와 2차 인증을 수행하는 제2 인증 단계를 포함하고,

상기 행동 패턴 모델을 인증 서버에 등록하는 단계는,

랜덤하게 설정된 변환 함수(transformation function)를 이용하여 상기 수집된 행동 패턴을 변환하고, 변환된 행동 패턴을 이용하여 상기 행동 패턴 모델을 생성하며, 생성된 상기 행동 패턴 모델을 상기 인증 서버에 등록하는 단계; 및

상기 인증 서버에 등록된 상기 행동 패턴 모델이 외부로 노출된 것으로 판단되는 경우, 새로운 변환 함수를 이용하여 상기 수집된 행동 패턴을 재변환하여 상기 행동 패턴 모델을 재구성하고, 재구성된 상기 행동 패턴 모델을 상기 인증 서버에 재등록하는 단계를 포함하는, 방법.

청구항 15

청구항 14에 있어서,

상기 패스워드 기반 인증 정보는, 상기 사용자의 패스워드 또는 상기 패스워드의 해시값인, 방법.

청구항 16

삭제

청구항 17

청구항 14에 있어서,

상기 제2 인증 단계는, 상기 변환 함수를 이용하여 인증 대상 행동 패턴을 변환한 뒤 상기 인증 서버로 송신하는, 방법.

청구항 18

삭제

발명의 설명

기 술 분 야

[0001] 개시되는 실시예들은 비밀번호 및 행동 패턴을 이용한 인증 기술과 관련된다.

배 경 기 술

[0003] 인터넷 및 모바일 네트워크 등이 보편화되면서 온라인을 통해 대부분의 정보가 유통됨에 따라, 온라인상에서 사용자를 인증하기 위한 기술의 중요성 또한 점점 높아지고 있다. 인증 기술은 크게 암호 기반 인증, 생체 인증, OTP 등으로 대표되는 소지 기반 인증 등으로 나눌 수 있으며, 최근에는 사용자의 행동 패턴(behavior pattern)을 이용한 인증 기술이 개발되고 있다.

[0004] 사용자의 행동 패턴 기반 인증을 위해서는 사전에 사용자로부터 행동 패턴을 수집하고 이로부터 사용자별 행동 패턴 모델(behavior pattern model)을 구성하여야 한다. 행동 패턴 모델은 사용자가 임의로 설정한 것이 아닌 사용자의 자연스러운 행동 패턴을 반영하여 구성된다. 따라서 행동 패턴 모델은 그 자체로 개인정보의 성격을

갖고 있을 뿐 아니라, 임의로 변경 가능한 패스워드 등과 달리 제3자에게 노출되더라도 이를 변경하는 것이 불가능하거나 매우 어렵다. 이에 따라 기존의 행동 패턴 기반 인증은 주로 행동 패턴 모델을 전송할 필요가 없는 로컬 인증 등에만 제한적으로 사용되어 오고 있는 실정이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 등록특허공보 제10-1990454호 (2019. 10. 01)

발명의 내용

해결하려는 과제

[0007] 개시되는 실시예들은 비밀번호 및 행동 패턴을 이용한 멀티 팩터 인증을 통해 사용자 인증의 보안성을 강화하며, 특히 로컬이 아닌 원격(remote) 환경에서도 행동 기반 인증의 보안성을 보장하기 위한 기술적인 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0009] 예시적인 실시예에 따르면, 단말 및 인증 서버를 포함하는 멀티 팩터 인증 시스템으로서, 상기 단말은, 상기 인증 서버와 사전 공유된 패스워드 기반 인증 정보를 이용하여 단말 사용자의 1차 인증을 수행하고, 상기 1차 인증 과정에서 생성된 단말측 세션키를 이용하여 상기 단말 사용자로부터 획득된 인증 대상 행동 패턴을 암호화하여 상기 인증 서버로 송신하며, 상기 인증 서버는, 상기 1차 인증 과정에서 생성된 서버측 세션키를 이용하여 상기 암호화된 인증 대상 행동 패턴을 복호화하고, 복호화된 인증 대상 행동 패턴을 상기 사용자의 행동 패턴 모델과 비교하여 상기 단말 사용자의 2차 인증을 수행하는, 멀티 팩터 인증 시스템이 제공된다.

[0010] 상기 패스워드 기반 인증 정보는, 상기 단말 사용자의 패스워드 또는 상기 패스워드의 해시값일 수 있다.

[0011] 상기 단말은, 상기 사용자로부터 수집된 행동 패턴으로부터 상기 행동 패턴 모델을 생성하고, 생성된 상기 행동 패턴 모델을 상기 인증 서버에 등록할 수 있다.

[0012] 상기 단말은, 랜덤하게 설정된 변환 함수(transformation function)를 이용하여 상기 수집된 행동 패턴을 변환하고, 변환된 행동 패턴을 이용하여 상기 행동 패턴 모델을 생성할 수 있다.

[0013] 상기 단말은, 상기 변환 함수를 이용하여 인증 대상 행동 패턴을 변환한 뒤 상기 인증 서버로 송신할 수 있다.

[0014] 상기 단말은, 상기 인증 서버에 등록된 상기 행동 패턴 모델이 외부로 노출된 것으로 판단되는 경우, 새로운 변환 함수를 이용하여 상기 수집된 행동 패턴을 재변환하여 상기 행동 패턴 모델을 재구성하고, 재구성된 상기 행동 패턴 모델을 상기 인증 서버에 재등록할 수 있다.

[0015] 상기 인증 서버는, 상기 2차 인증에 성공한 경우 상기 인증 대상 행동 패턴을 이용하여 상기 행동 패턴 모델을 갱신할 수 있다.

[0016] 상기 인증 서버는, 상기 2차 인증에 성공한 경우 상기 인증 대상 행동 패턴을 저장하고, 상기 행동 패턴 모델이 손상된 경우, 기 저장된 상기 인증 대상 행동 패턴을 이용하여 상기 행동 패턴 모델을 재생성할 수 있다.

[0017] 다른 예시적인 실시예에 따르면, 사용자로부터 수집된 행동 패턴으로부터 행동 패턴 모델을 생성하고, 생성된 상기 행동 패턴 모델을 인증 서버에 등록하는 행동 패턴 수집 모듈; 상기 인증 서버와 사전 공유된 패스워드 기반 인증 정보를 이용하여 상기 인증 서버와 1차 인증을 수행하고, 상기 인증 서버와 공유되는 세션키를 생성하는 제1 인증 모듈; 및 상기 사용자로부터 획득된 인증 대상 행동 패턴을 상기 세션키로 암호화하여 상기 인증 서버로 송신함으로써 상기 인증 서버와 2차 인증을 수행하는 제2 인증 모듈을 포함하는, 단말 장치가 제공된다.

[0018] 상기 패스워드 기반 인증 정보는, 상기 사용자의 패스워드 또는 상기 패스워드의 해시값일 수 있다.

[0019] 상기 행동 패턴 수집 모듈은, 랜덤하게 설정된 변환 함수(transformation function)를 이용하여 상기 수집된 행동 패턴을 변환하고, 변환된 행동 패턴을 이용하여 상기 행동 패턴 모델을 생성할 수 있다.

[0020] 상기 제2 인증 모듈은, 상기 변환 함수를 이용하여 인증 대상 행동 패턴을 변환한 뒤 상기 인증 서버로 송신할

수 있다.

[0021] 상기 행동 패턴 수집 모듈은, 상기 인증 서버에 등록된 상기 행동 패턴 모델이 외부로 노출된 것으로 판단되는 경우, 새로운 변환 함수를 이용하여 상기 수집된 행동 패턴을 재변환하여 상기 행동 패턴 모델을 재구성하고, 재구성된 상기 행동 패턴 모델을 상기 인증 서버에 재등록할 수 있다.

[0022] 다른 예시적인 실시예에 따르면, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 단말 장치에서 수행되는 방법으로서, 사용자로부터 수집된 행동 패턴으로부터 행동 패턴 모델을 생성하고, 생성된 상기 행동 패턴 모델을 인증 서버에 등록하는 단계; 상기 인증 서버와 사전 공유된 패스워드 기반 인증 정보를 이용하여 상기 인증 서버와 1차 인증을 수행하고, 상기 인증 서버와 공유되는 세션키를 생성하는 제1 인증 단계; 및 상기 사용자로부터 획득된 인증 대상 행동 패턴을 상기 세션키로 암호화하여 상기 인증 서버로 송신함으로써 상기 인증 서버와 2차 인증을 수행하는 제2 인증 단계를 포함하는, 방법이 제공된다.

[0023] 상기 패스워드 기반 인증 정보는, 상기 사용자의 패스워드 또는 상기 패스워드의 해시값일 수 있다.

[0024] 상기 행동 패턴 모델을 인증 서버에 등록하는 단계는, 랜덤하게 설정된 변환 함수(transformation function)를 이용하여 상기 수집된 행동 패턴을 변환하고, 변환된 행동 패턴을 이용하여 상기 행동 패턴 모델을 생성하도록 구성될 수 있다.

[0025] 상기 제2 인증 단계는, 상기 변환 함수를 이용하여 인증 대상 행동 패턴을 변환한 뒤 상기 인증 서버로 송신하도록 구성될 수 있다.

[0026] 상기 행동 패턴 모델을 인증 서버에 등록하는 단계는, 상기 인증 서버에 등록된 상기 행동 패턴 모델이 외부로 노출된 것으로 판단되는 경우, 새로운 변환 함수를 이용하여 상기 수집된 행동 패턴을 재변환하여 상기 행동 패턴 모델을 재구성하고, 재구성된 상기 행동 패턴 모델을 상기 인증 서버에 재등록할 수 있다.

발명의 효과

[0028] 개시되는 실시예들에 따르면, 비밀번호 인증 및 행동 패턴 기반의 인증을 포함하는 멀티 팩터 인증을 통하여 사용자 인증의 보안성을 강화할 수 있다. 특히 상대적으로 노출되기 쉬운 비밀번호가 공격자(attacker)에게 노출되었을 경우에도, 행동 기반 인증으로 이를 보완할 수 있다.

[0029] 또한 개시되는 실시예들에 따르면 비밀번호 기반의 인증을 통해 생성된 세션키를 이용하여 행동 패턴 관련 정보를 안정하게 전송함으로써 로컬이 아닌 리모트 환경에서도 행동 기반 인증을 안전하게 사용할 수 있다.

도면의 간단한 설명

[0031] 도 1은 일 실시예에 따른 멀티 팩터 인증 시스템(100)을 설명하기 위한 블록도

도 2는 일 실시예에 따른 멀티 팩터 인증 시스템(100)에서의 인증 과정(200)을 좀 더 상세히 설명하기 위한 흐름도

도 3은 일 실시예에 따른 단말(102)을 설명하기 위한 블록도

도 4는 일 실시예에 따른 인증 서버(104)를 설명하기 위한 블록도

도 5는 일 실시예에 따른 단말(102)의 멀티 팩터 인증 과정(500)을 설명하기 위한 흐름도

도 6은 일 실시예에 따른 인증 서버(104)의 멀티 팩터 인증 과정(600)을 설명하기 위한 흐름도

도 7은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0032] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0033] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를

불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0035] 도 1은 일 실시예에 따른 멀티 팩터 인증 시스템(100)을 설명하기 위한 블록도이다. 도시된 바와 같이, 일 실시예에 따른 멀티 팩터 인증 시스템(100)은 단말(102) 및 인증 서버(104)를 포함한다.

[0036] 단말(102)은 인증 서버(104)와 네트워크(106)를 통해 연결되며, 인증 서버(104)와 멀티 팩터 인증을 수행한다. 개시되는 실시예들에서 멀티 팩터 인증(multi-factor authentication)이란, 패스워드 기반의 인증 및 단말(102) 사용자의 행동 패턴 기반 인증 등 둘 이상의 서로 다른 인증 수단을 이용한 다중 인증을 의미할 수 있다. 여기서 행동 패턴 기반 인증은 키스트로크 다이내믹스(keystroke dynamics) 등 사용자로부터 획득 가능한 행동 패턴 외에 지문 등의 바이오메트릭 데이터(biometric data) 등 퍼지 기반으로 머신러닝에서 활용 가능한 모든 종류의 데이터를 포함할 수 있다.

[0037] 개시되는 실시예들에서 행동 패턴 기반 인증의 경우 패스워드 기반 인증 과정에서 생성된 세션키를 이용하여 수행되는 바, 원격 행동 패턴 기반 인증에서 발생할 수 있는 행동 패턴 정보 전송의 보안성을 강화할 수 있다. 일 실시예에서, 단말(102)은 스마트폰, 태블릿, 데스크탑 컴퓨터, 랩탑 컴퓨터, IoT 디바이스, 웨어러블 디바이스 등의 네트워크 통신이 가능한 다양한 종류의 사용자 기기를 포함할 수 있다.

[0038] 인증 서버(104)는 단말(102)로부터 패스워드 기반 인증 정보 및 사용자의 행동 패턴 모델을 수신하여 저장한다. 이때 상기 패스워드 기반 인증 정보는 단말(102)의 사용자로부터 설정된 패스워드 또는 상기 패스워드의 해시값일 수 있다.

[0039] 일 실시예에서, 단말(102)은 인증 서버(104)와 사전 공유된 패스워드 기반 인증 정보를 이용하여 단말 사용자의 1차 인증을 요청한다. 그러면 인증 서버(104)는 기 등록된 상기 패스워드 기반 인증 정보를 이용하여 상기 단말(102)과 1차 인증을 수행한다.

[0040] 이후 단말(102)은 상기 1차 인증 과정에서 생성된 단말측 세션키를 이용하여 상기 단말 사용자로부터 획득된 인증 대상 행동 패턴을 암호화하여 인증 서버(104)로 송신하여 2차 인증을 요청한다. 인증 서버(104)는 단말(102)로부터 암호화된 인증 대상 행동 패턴을 수신하고, 상기 1차 인증 과정에서 생성된 서버측 세션키를 이용하여 암호화된 인증 대상 행동 패턴을 복호화한다. 이후 인증 서버(104)는 복호화된 인증 대상 행동 패턴을 상기 사용자의 행동 패턴 모델과 비교하여 단말(102) 사용자의 2차 인증을 수행하고 인증 결과를 단말(102)로 송신한다.

[0041] 앞서 기술한 바와 같이, 단말(102)은 인증 서버(104)와 네트워크(106)를 통해 연결될 수 있다. 몇몇 실시예들에서, 네트워크는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wire area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0043] 도 2는 일 실시예에 따른 멀티 팩터 인증 시스템(100)에서의 인증 과정(200)을 좀 더 상세히 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0044] 단계 202에서, 단말(102)은 인증 서버(104)로 자신의 계정 및 패스워드 기반 인증 정보를 등록한다. 일 실시예에서, 상기 패스워드 기반의 인증 정보는 단말(102) 사용자의 패스워드 또는 상기 패스워드의 해시값일 수 있다.

[0045] 또한 본 단계에서 단말(102)은 사용자의 행동 패턴 모델(M)을 인증 서버(104)에 등록할 수 있다. 일 실시예에서, 단말(102)은 행동 패턴 모델 생성 알고리즘을 결정하고, 결정된 알고리즘에 따라 사용자로부터 수집된 행동 패턴 정보를 학습하여 행동 패턴 모델을 생성할 수 있다. 이때 상기 행동 패턴 생성 모델은 머신 러

닝 또는 딥 러닝 기반의 알고리즘일 수 있다.

[0046] 단계 204에서, 단말(102)은 인증 서버(104)와 패스워드 기반의 1차 인증을 수행할 수 있다. 예를 들어, 단말(102)과 인증 서버(104) 간에 동일한 패스워드를 공유할 경우, 단말(102)과 인증 서버(104)는 PAKE(Password-based Authenticated Key Exchange)를 이용하여 인증을 수행할 수 있다. 만약 인증 서버(104)가 패스워드 자체가 아닌 패스워드의 해시값만을 알고 있을 경우, 단말(102)과 인증 서버(104)는 Asymmetric PAKE(Password-based Authenticated Key Exchange)를 이용하여 인증을 수행할 수 있다. 그러나 이는 예시적인 것으로서, 개시적인 실시예들에서 단말(102)과 인증 서버(104) 사이의 1차 인증은 다양한 패스워드 기반 인증 알고리즘에 의해 수행될 수 있다.

[0047] 단계 206에서, 단말(102)은 상기 204 단계의 패스워드 인증 결과로 획득한 정보를 이용하여 단말측 세션키(SK_A)를 생성한다. 전술한 PAKE 또는 Assymetric PAKE는 단말(102)과 인증 서버(104) 사이에 공유된 패스워드를 기반으로 랜덤한 세션키를 상호 공유할 수 있도록 구성된다. 따라서 이를 이용할 경우 단말(102)은 안전하게 단말측 세션키(SK_A)를 생성할 수 있다.

[0048] 단계 208에서, 인증 서버(104)는 단말(102)과 마찬가지로 상기 204 단계의 패스워드 인증 결과로 획득한 정보를 이용하여 서버측 세션키(SK_B)를 생성한다. 본 단계에서 생성되는 서버측 세션키(SK_B)는 단말측 세션키(SK_A)와 동일하다.

[0049] 단계 210에서, 단말(102)은 사용자의 행동 패턴을 획득하고 이로부터 행동 패턴 벡터(V)를 생성한다. 일 실시예에서, 단말(102)은 1차 인증 과정에서 사용자로부터 수집된 키스트로크 다이내믹스 등의 행동 패턴을 이용하여 행동 패턴 벡터(V)를 생성할 수 있다.

[0050] 단계 212에서, 단말(102)은 생성된 행동 패턴 벡터(V)를 단말측 세션키(SK_A)로 암호화하고, 암호화된 행동 패턴 벡터(C)를 인증 서버(104)로 송신한다. 이를 수식으로 나타내면 다음과 같다.

[0051] [수학식 1]

$$C = Enc_{SK_A}(V)$$

[0052]

[0053] 단계 214에서, 인증 서버(104)는 단말(102)로부터 암호화된 행동 패턴 벡터(C)를 수신하고, 이를 복호화하여 행동 패턴 벡터(V)를 획득한다. 이를 수식으로 나타내면 다음과 같다.

[0054] [수학식 2]

$$V = Dec_{SK_B}(C)$$

[0055]

[0056] 단계 216에서, 인증 서버(104)는 상기 행동 패턴 벡터(V)를 기 저장된 행동 패턴 모델(M)과 비교하여 단말(102)에 대한 행동 패턴 기반의 2차 인증을 수행하고, 인증 결과를 단말(102)에 제공한다. 만약 상기 행동 패턴 벡터(V)가 기 저장된 행동 패턴 모델(M)과 매칭되는 경우, 인증 서버(104)는 2차 인증에 성공한 것으로 판단할 수 있다. 그러나 이와 달리 만약 상기 행동 패턴 벡터(V)가 기 저장된 행동 패턴 모델(M)과 매칭되지 않는 경우, 인증 서버(104)는 2차 인증에 실패한 것으로 판단할 수 있다.

[0057] 한편, 일 실시예에서 단말(102)은 랜덤하게 설정된 변환 함수(transformation function)를 이용하여 사용자로부터 수집된 행동 패턴을 변환하고, 변환된 행동 패턴을 이용하여 행동 패턴 모델(M)을 생성할 수 있다. 예를 들어, 단말(102)은 길이 보전 암호화(length preserving encryption) 방식 또는 길이 보전 선형 변환(length preserving linear transformation) 방식 등을 이용하여 상기 행동 패턴을 변환할 수 있다. 이때 상기 방식에 따른 변환 함수는 랜덤하게 설정될 수 있다.

[0058] 일 실시예에서, 단말(102)은 사용자의 행동 패턴에 랜덤한 값을 더하거나 빼는 방식으로 상기 행동 패턴을 변환할 수 있다. 예를 들어 사용자로부터 수집된 행동 패턴이 (x, y, z)이고, 변환 함수가 (a, b, c)일 경우, 변환된 행동 패턴은 (x+a, y+b, z+c)일 수 있다. 이때 상기 a, b, c는 랜덤하게 정해질 수 있다. 다른 실시예에서, 상기 변환 함수는 랜덤하게 선택된 행렬일 수 있다. 예를 들어, 사용자로부터 수집된 행동 패턴이 n차원 벡터일 경우, 단말(102)은 랜덤하게 선택된 m x n 행렬(A)을 이용하여 T(x) = Ax 와 같이 행동 패턴을 m차원 벡터로 변환할 수 있다.

[0059] 이와 같이 행동 패턴 모델(M)이 변환된 행동 패턴에 기반하여 생성될 경우, 상기 210 단계에서 단말(102)은 행동 패턴 벡터(V)에 행동 패턴 모델을 생성한 것과 동일한 변환 함수를 적용하여 행동 패턴 벡터(V)를 변환하고, 변환된 행동 패턴 벡터(V')를 암호화하여 인증 서버(104)로 송신할 수 있다.

[0060] 만약 인증 서버(104)에 등록된 행동 패턴 모델(M)이 외부로 노출된 것으로 판단되는 경우, 단말(102)은 이전과는 다른 새로운 변환 함수를 이용하여 상기 수집된 행동 패턴을 재변환함으로써 행동 패턴 모델을 재구성하고, 재구성된 행동 패턴 모델(M')을 인증 서버(104)에 재등록할 수 있다. 이와 같이 랜덤한 변환 함수를 이용할 경우 행동 패턴 모델(M)이 악의적인 공격자에게 노출된 경우에도 변환 함수를 교체하는 것 만으로 행동 패턴 모델을 재생성할 수 있게 되므로 행동 패턴 모델의 보안성을 높일 수 있다.

[0061] 한편, 일 실시예에서 인증 서버(104)는, 216 단계에서 2차 인증에 성공한 경우, 214 단계에서 획득된 인증 대상 행동 패턴을 이용하여 행동 패턴 모델(M)을 갱신할 수 있다. 이와 같이 인증 성공시의 행동 패턴으로 행동 패턴 모델(M)을 지속적으로 갱신할 경우, 행동 패턴 모델(M)의 성능을 높일 수 있다.

[0062] 또한, 일 실시예에서 인증 서버(104)는 216 단계에서 2차 인증에 성공한 경우, 214 단계에서 획득된 인증 대상 행동 패턴을 저장해 둘 수 있다. 이후 만약 어떤 이유로든 인증 서버(104)에 저장된 행동 패턴 모델(M)이 손상된 경우, 인증 서버(104)는 기 저장된 상기 인증 대상 행동 패턴을 이용하여 재학습을 수행함으로써 상기 행동 패턴 모델을 재생성할 수 있다. 이 경우, 개인정보보호 및 보안성 강화를 위하여 인증 서버(104) 저장되는 행동 패턴은 단말(102)에 의해 변환(transformation)된 행동 패턴인 것이 바람직하다.

[0064] 도 3은 일 실시예에 따른 단말(102)을 설명하기 위한 블록도이다. 도시된 바와 같이, 일 실시예에 따른 단말(102)은 행동 패턴 수집 모듈(302), 단말측 제1 인증 모듈(304) 및 단말측 제2 인증 모듈(306)을 포함한다.

[0065] 행동 패턴 수집 모듈(302)은 사용자로부터 수집된 행동 패턴으로부터 행동 패턴 모델을 생성하고, 생성된 상기 행동 패턴 모델을 인증 서버(104)에 등록한다.

[0066] 단말측 제1 인증 모듈(304)은 인증 서버(104)와 사전 공유된 패스워드 기반 인증 정보를 이용하여 인증 서버(104)와 1차 인증을 수행하고, 인증 서버(104)와 공유되는 단말측 세션키(SK_A)를 생성한다. 앞서 설명한 바와 같이, 인증 서버(104)와 사전 공유된 패스워드 기반 인증 정보는, 상기 사용자의 패스워드 또는 상기 패스워드의 해시값일 수 있다.

[0067] 단말측 제2 인증 모듈(306)은 상기 사용자로부터 획득된 인증 대상 행동 패턴을 상기 단말측 세션키(SK_A)로 암호화하여 인증 서버(104)로 송신함으로써 인증 서버(104)와 2차 인증을 수행한다.

[0068] 일 실시예에서, 행동 패턴 수집 모듈(302)은 랜덤하게 설정된 변환 함수(transformation function)를 이용하여 상기 수집된 행동 패턴을 변환하고, 변환된 행동 패턴을 이용하여 상기 행동 패턴 모델을 생성할 수 있다. 이 경우 단말측 제2 인증 모듈(306)은, 행동 패턴 수집 모듈(302)과 동일한 변환 함수를 이용하여 인증 대상 행동 패턴을 변환한 뒤 인증 서버(104)로 송신할 수 있다.

[0069] 또한 행동 패턴 수집 모듈(302)은, 인증 서버(104)에 등록된 상기 행동 패턴 모델이 외부로 노출된 것으로 판단되는 경우, 새로운 변환 함수를 이용하여 상기 수집된 행동 패턴을 재변환하여 행동 패턴 모델을 재구성하고, 재구성된 행동 패턴 모델을 인증 서버(104)에 재등록할 수 있다.

[0071] 도 4는 일 실시예에 따른 인증 서버(104)를 설명하기 위한 블록도이다. 도시된 바와 같이, 일 실시예에 따른 인증 서버(104)는 저장 모듈(402), 서버측 제1 인증 모듈(404) 및 서버측 제2 인증 모듈(406)을 포함한다.

[0072] 저장 모듈(402)은 단말(102)로부터 등록된 패스워드 기반 인증 정보 및 사용자의 행동 패턴 모델(M)을 저장한다.

[0073] 서버측 제1 인증 모듈(404)은 단말(102)의 요청에 따라 패스워드 기반의 1차 인증을 수행하고, 이로부터 서버측 세션키(SK_B)를 생성한다. 본 단계에서 생성되는 서버측 세션키(SK_B)는 단말측 세션키(SK_A)와 동일하다.

[0074] 서버측 제2 인증 모듈(406)은 단말(102)로부터 암호화된 행동 패턴 벡터(C)를 수신하고, 이를 복호화하여 인증 대상 행동 패턴 벡터(V)를 획득한다. 이후 제2 인증 모듈(406)은 상기 행동 패턴 벡터(V)를 기 저장된 행동 패턴 모델(M)과 비교하여 단말(102)에 대한 행동 패턴 기반의 2차 인증을 수행하고, 인증 결과를 단말(102)에 제공한다.

[0075] 일 실시예에서 서버측 제2 인증 모듈(406)은 2차 인증에 성공한 인증 대상 행동 패턴을 이용하여 행동 패턴 모

델(M)을 갱신할 수 있다. 이와 같이 인증 성공시의 행동 패턴으로 행동 패턴 모델(M)을 지속적으로 갱신할 경우, 행동 패턴 모델(M)의 성능을 높일 수 있다. 또한, 일 실시예에서 서버측 제2 인증 모듈(406)은 2차 인증에 성공한 인증 대상 행동 패턴을 저장해 두었다가, 이후 만약 어떤 이유로든 인증 서버(104)에 저장된 행동 패턴 모델(M)이 손상된 경우 기 저장된 상기 인증 대상 행동 패턴을 이용하여 재학습을 수행함으로써 상기 행동 패턴 모델을 재생성할 수 있다.

[0077] 도 5는 일 실시예에 따른 단말(102)의 멀티 팩터 인증 과정(500)을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0078] 단계 502에서, 단말(102)은 사용자로부터 수집된 행동 패턴으로부터 행동 패턴 모델을 생성하고, 생성된 상기 행동 패턴 모델을 인증 서버(104)에 등록한다.

[0079] 단계 504에서, 단말(102)은 인증 서버(104)와 사전 공유된 패스워드 기반 인증 정보를 이용하여 인증 서버(104)와 1차 인증을 수행하고, 인증 서버(104)와 공유되는 단말측 세션키(SK_A)를 생성한다.

[0080] 단계 506에서, 단말(102)은 상기 사용자로부터 획득된 인증 대상 행동 패턴(V)을 단말측 세션키(SK_A)로 암호화하여 인증 서버(104)로 송신함으로써 인증 서버(104)와 2차 인증을 수행한다.

[0082] 도 6은 일 실시예에 따른 인증 서버(104)의 멀티 팩터 인증 과정(600)을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법 또는 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0083] 단계 602에서, 인증 서버(104)는 단말(102)로부터 등록된 패스워드 기반 인증 정보 및 사용자의 행동 패턴 모델(M)을 저장한다.

[0084] 단계 604에서, 인증 서버(104)는 단말(102)의 요청에 따라 패스워드 기반의 1차 인증을 수행하고, 이로부터 서버측 세션키(SK_B)를 생성한다. 본 단계에서 생성되는 서버측 세션키(SK_B)는 단말측 세션키(SK_A)와 동일하다.

[0085] 단계 606에서, 인증 서버(104)는 단말(102)로부터 암호화된 행동 패턴 벡터(C)를 수신하고, 이를 복호화하여 인증 대상 행동 패턴 벡터(V)를 획득한다.

[0086] 단계 608에서, 인증 서버(104)는 상기 행동 패턴 벡터(V)를 기 저장된 행동 패턴 모델(M)과 비교하여 단말(102)에 대한 행동 패턴 기반의 2차 인증을 수행하고, 인증 결과를 단말(102)에 제공한다.

[0088] 도 7은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0089] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 본 발명의 실시예들에 따른 인증 기관(102), 인증 요청자(104) 및 검증자(106)일 수 있다. 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0090] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0091] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴

포넌트들을 상호 연결한다.

[0092] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(102)와 연결될 수도 있다.

[0094] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0095] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0097] 100: 멀티 팩터 인증 시스템

102: 단말

104: 인증 서버

302: 행동 패턴 수집 모듈

304: 제1 인증 모듈

306: 제2 인증 모듈

402: 저장 모듈

404: 제1 인증 모듈

406: 제2 인증 모듈

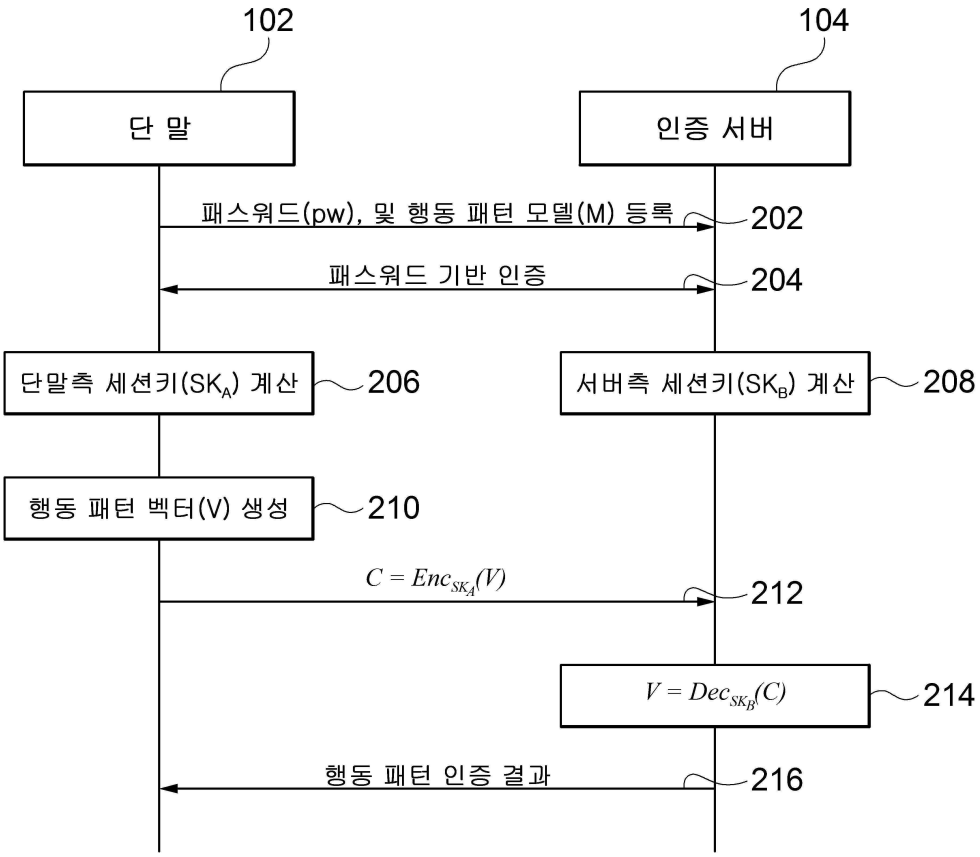
도면

도면1

100

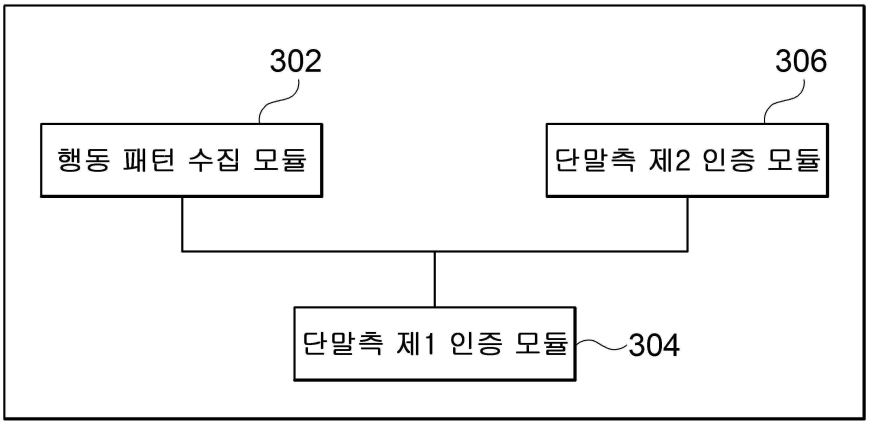
도면2

200



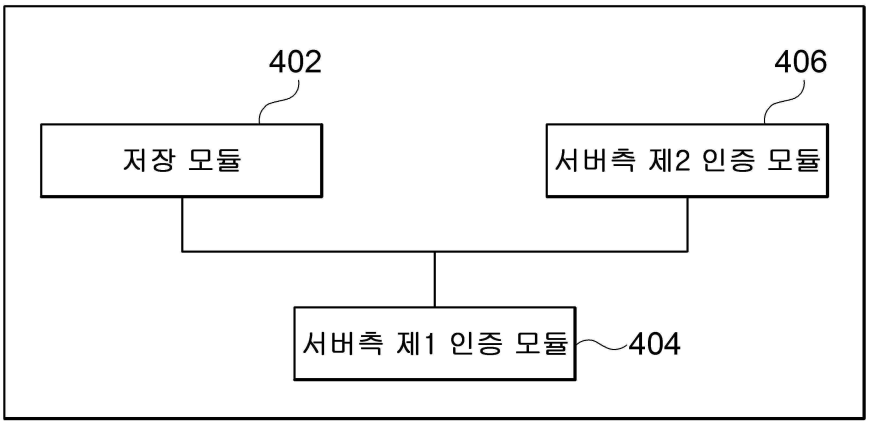
도면3

102



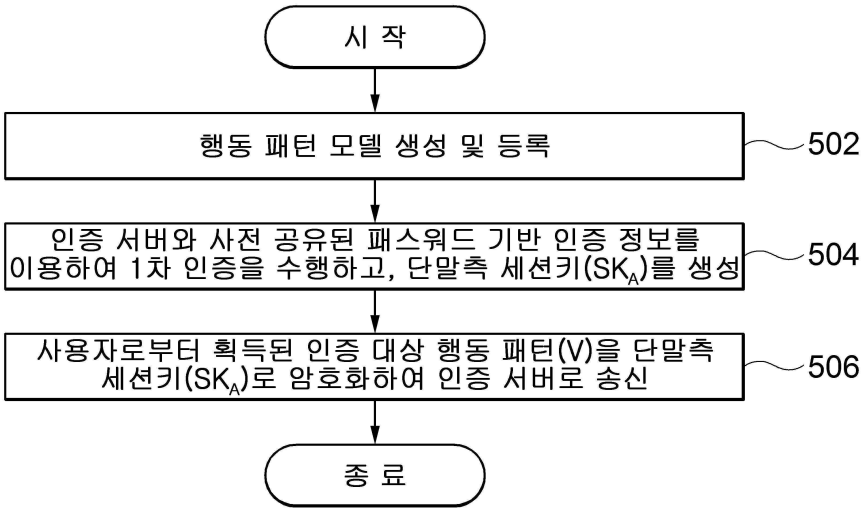
도면4

104

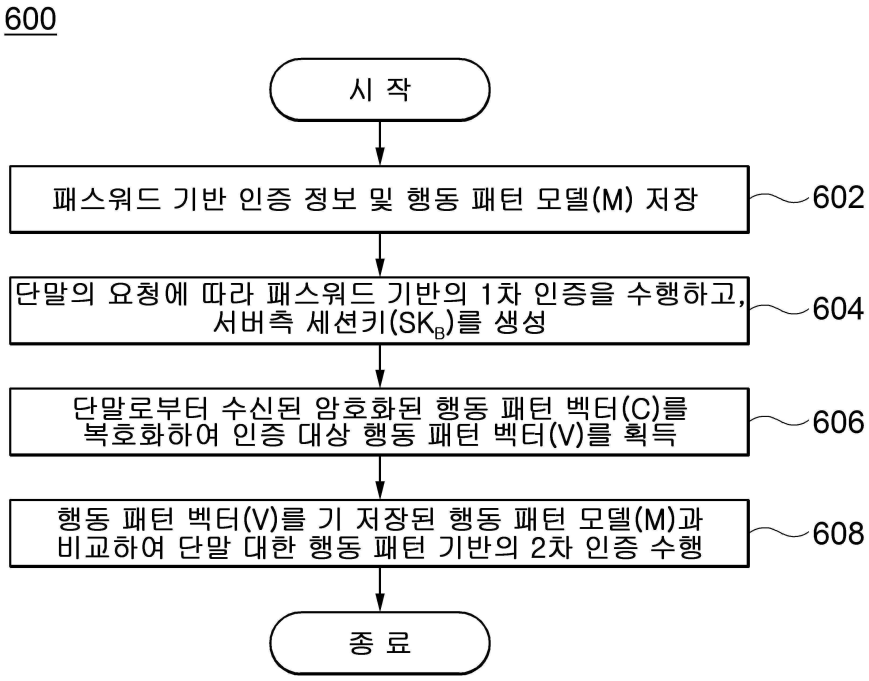


도면5

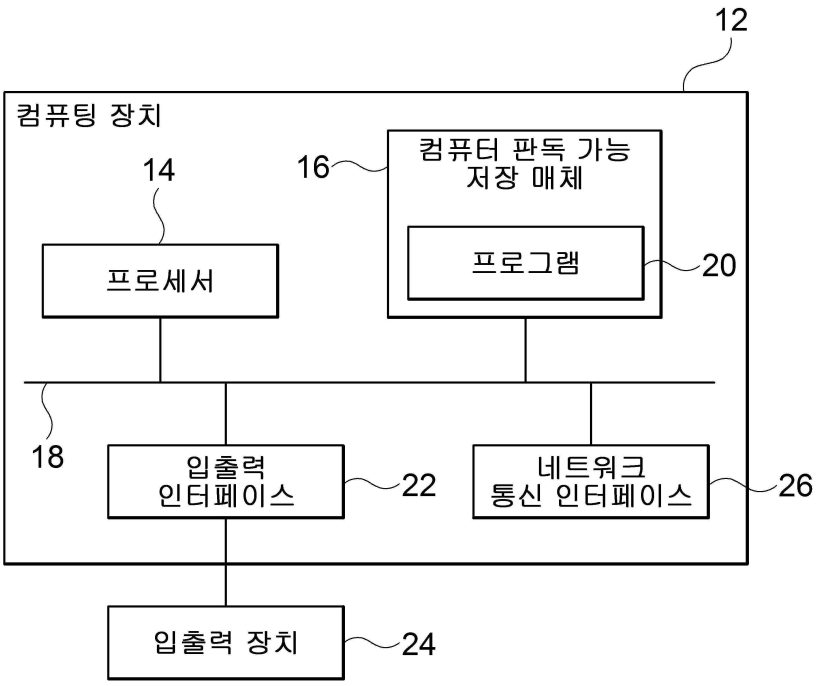
500



도면6


600
시 작
패스워드 기반 인증 정보 및 행동 패턴 모델(M) 저장
602
단말의 요청에 따라 패스워드 기반의 1차 인증을 수행하고, 서버측 세션키(SK_B)를 생성
604
단말로부터 수신된 암호화된 행동 패턴 벡터(C)를 복호화하여 인증 대상 행동 패턴 벡터(V)를 획득
606
행동 패턴 벡터(V)를 기 저장된 행동 패턴 모델(M)과 비교하여 단말 대한 행동 패턴 기반의 2차 인증 수행
608
종 료

도면7


10
12
컴퓨팅 장치
14
16
컴퓨터 판독 가능 저장 매체
프로세서
프로그램
20
18
입출력 인터페이스
22
네트워크 통신 인터페이스
26
입출력 장치
24