(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년01월30일
(11) 등록번호 10-2493744
(24) 등록일자 2023년01월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
H04L 9/40 (2022.01)
(52) CPC특허분류
H04L 9/3231 (2013.01)
H04L 63/0861 (2013.01)
(21) 출원번호 10-2018-7003347
(22) 출원일자(국제) 2016년06월23일
심사청구일자 2020년03월24일
(85) 번역문제출일자 2018년02월02일
(65) 공개번호 10-2018-0026508
(43) 공개일자 2018년03월12일
(86) 국제출원번호 PCT/CN2016/086868
(87) 국제공개번호 WO 2017/000829
국제공개일자 2017년01월05일
(30) 우선권주장
201510394393.3 2015년07월02일 중국(CN)
(56) 선행기술조사문헌
US20080172725 A1*
(뒷면에 계속)

(73) 특허권자
어드밴스드 뉴 테크놀로지스 씨오., 엘티디.
케이만 군도, 그랜드 케이만 케이와이1-9008, 조지 타운, 27 하스피탈 로드, 케이만 코포레이트 센터
(72) 발명자
린 준세이
중국 항저우 310099 완탕 로드 넘버 18 후앙롱 타임스 플라자 빌딩 비 17층 앤츠 패튼 팀 내
(74) 대리인
김태홍, 김진희

전체 청구항 수 : 총 17 항 심사관 : 양종필

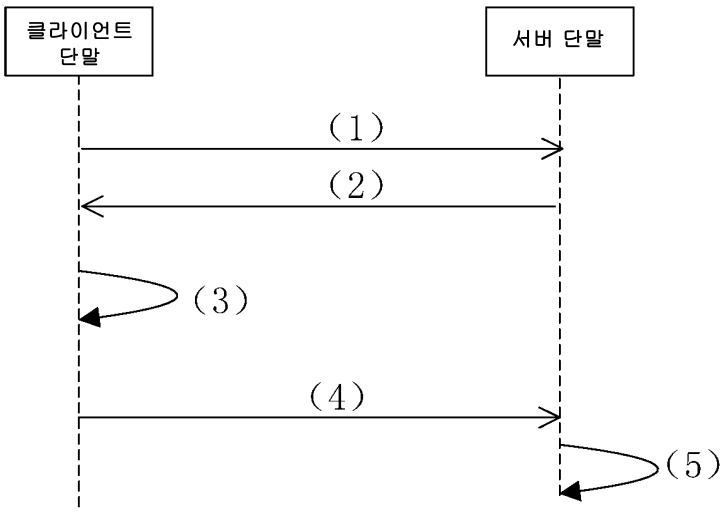
(54) 발명의 명칭 **생체 특징에 기초한 보안 검증 방법, 클라이언트 단말, 및 서버**

(57) 요 약

본 발명은 생체 특징에 기초한 보안 검증 방법, 클라이언트 단말, 및 서버를 개시한다. 클라이언트 단말은 인증 요청을 전송한다. 서버 단말은 인증 요청을 수신하고, 그 후 인증 요청 답신 메시지를 회신한다. 클라이언트 단말은 사용자에 의해 입력되고 검증에 이용되는 지문 이미지를 수신하고, 대응하는 생체 특징 템플릿 ID를 획득하

(뒷면에 계속)

대 표 도 - 도2



고, 획득된 생체 특징 템플릿 ID와 국부적으로 저장된 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교하며, 획득된 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 생성하고, 이 인증 응답 메시지를 서버 단말에 전송한다. 서버 단말은 인증 응답 메시지를 수신하고, 이 인증 응답 메시지 내에 포함된 생체 특징 템플릿 ID와 서버 단말에 국부적으로 저장된 대응하는 사용자 레코드 내의 생체 특징 템플릿 ID를 비교한다. 생체 특징 템플릿 ID들이 일치하면, 검증이 성공된 것이며, 그렇지 않은 경우에는 오류가 보고된다. 본 발명은 전술한 방법에 대응하는 클라이언트 단말 및 서버를 더 제공한다. 본 발명은 네트워크를 통한 개인 생체 특징의 송신을 회피하고, 유출 위험성을 회피하며, 네트워크 송신 동안에 소모되는 네트워크 트래픽을 더욱 감소시킬 수 있다. 따라서, 본 발명은 보다 높은 보안성을 달성한다.

(52) CPC특허분류
H04L 9/0825 (2013.01)
H04L 9/3247 (2013.01)
H04L 9/3271 (2013.01)

(56) 선행기술조사문헌
US20100223663 A1*
T. Dierks 외 1명, The TLS Protocol Version 1.0, Request for Comments : 2246 (1999.01.)*
US20110083170 A1
US20070016777 A1
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

컴퓨터 구현(computer-implemented) 방법에 있어서,

클라이언트로부터 서버로, 생체 특징(biometric feature)을 인에이블(enable)하기 위한 인에이블 요청을 전송하는 단계;

상기 서버로부터 그리고 상기 인에이블 요청에 응답하여, 인에이블 요청 답신(reply) 메시지를 수신하는 단계;

생체 특징 검증 인에이블 프로세스 동안, 사용자에 의해 입력된 상기 생체 특징을 수신하는 단계 - 상기 생체 특징은 상기 사용자의 검증을 위해 제공됨 -;

상기 수신된 생체 특징에 대응하는 생체 특징 템플릿 식별자(ID)를 획득하는 단계;

상기 생체 특징 템플릿 ID를 포함하는 인에이블 레코드(enable record)를 생성하고 저장하는 단계;

상기 생체 특징 템플릿 ID를 포함하는 인에이블 응답(response) 메시지를 생성하고, 사용자 레코드의 생성과 저장을 위해 상기 인에이블 응답 메시지를 상기 서버에 전송하는 단계 - 상기 사용자 레코드는 생체 특징 검증을 위해 사용되는 생체 특징 템플릿 ID를 포함함 -;

상기 서버에 인증 요청을 전송하는 단계;

상기 서버로부터 그리고 상기 인증 요청에 응답하여, 인증 요청 답신 메시지를 수신하는 단계;

상기 사용자에 의해 입력된 상기 생체 특징을 수신하는 단계;

상기 수신된 생체 특징을 사용하여, 상기 수신된 생체 특징에 대응하는 상기 생체 특징 템플릿 ID를 획득하는 단계 - 상기 획득된 생체 특징 템플릿 ID는 복수의 저장된 생체 특징 템플릿 ID로부터 선택되는 것임 - ;

상기 획득된 생체 특징 템플릿 ID와, 상기 인에이블 레코드 내에 포함되어 있는, 저장된 생체 특징 템플릿 ID를 비교하는 단계; 및

상기 획득된 생체 특징 템플릿 ID와 상기 저장된 생체 특징 템플릿 ID가 일치한 경우, 상기 획득된 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 생성하고, 검증을 위해 상기 인증 응답 메시지를 상기 서버에 전송하는 단계

를 포함하고,

상기 서버에 의한 검증은, 상기 인증 응답 메시지 내의 상기 획득된 생체 특징 템플릿 ID와, 저장된 사용자 레코드 내의 생체 특징 템플릿 ID의 비교를 포함하며,

상기 획득된 생체 특징 템플릿 ID와 상기 저장된 사용자 레코드 내의 생체 특징 템플릿 ID가 일치한다고 결정한 것에 기초하여 상기 검증은 성공된 것인 컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 클라이언트가 상기 인증 요청 답신 메시지를 수신한 후, 합의된 제1 공개키(agreed-to first public key)를 사용하여 상기 수신된 인증 요청 답신 메시지를 검증하는 단계 - 상기 검증이 성공이었다고 결정한 것에 기초하여 후속 응답이 행해지고, 상기 검증이 실패였다고 결정한 것에 기초하여 오류가 보고됨 -; 및

상기 클라이언트가 상기 인에이블 요청 답신 메시지를 수신한 후, 상기 합의된 제1 공개키를 사용하여 상기 수신된 인에이블 요청 답신 메시지를 검증하는 단계 - 상기 검증이 성공이었다고 결정한 것에 기초하여 후속 응답이 행해지고, 상기 검증이 실패였다고 결정한 것에 기초하여 오류가 보고됨 -

를 더 포함하며,

상기 인증 요청 답신 메시지와 상기 인에이블 요청 답신 메시지는 합의된 제1 개인키(agreed-to first private key)를 사용하여 상기 서버에 의해 서명(sign)되는 것인 컴퓨터 구현 방법.

청구항 3

제1항에 있어서,

사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 상기 사용자 개인키를 저장하는 단계;

상기 인에이블 요청 답신 메시지 내에 포함된 챌린지 값(challenge value)에 따라 서명 알고리즘(signature algorithm)을 선택하는 단계;

상기 선택된 서명 알고리즘 및 합의된 제2 개인키를 사용하여 상기 생성된 인에이블 응답 메시지에 서명하는 단계; 및

상기 서명된 인에이블 응답 메시지를 상기 서버에 전송하는 단계

를 더 포함하며,

상기 인에이블 응답 메시지는 상기 사용자 공개키를 포함하고,

상기 서버는 합의된 제2 공개키를 사용하여 상기 인에이블 응답 메시지를 검증하며,

상기 사용자 공개키는 상기 서버에 저장되는 것인 컴퓨터 구현 방법.

청구항 4

제3항에 있어서,

상기 인증 요청 답신 메시지 내에 포함된 챌린지 값에 따라 서명 알고리즘을 선택하는 단계; 및

상기 선택된 서명 알고리즘 및 상기 사용자 개인키를 사용하여 상기 인증 응답 메시지에 서명하는 단계

를 더 포함하고,

상기 서버는, 상기 인증 응답 메시지를 수신한 후에 상기 챌린지 값에 따라 서명 알고리즘을 선택하고, 상기 서명 알고리즘과 상기 사용자 공개키를 사용하여 상기 인증 응답 메시지를 검증하며,

상기 검증은, 상기 서명 알고리즘과 상기 사용자 공개키를 사용하여 상기 인증 응답 메시지에 대한 서명을 검증하는 것을 포함한 것인 컴퓨터 구현 방법.

청구항 5

제1항에 있어서,

상기 인에이블 요청 답신 메시지는 사용자 ID를 더 포함하고,

상기 컴퓨터 구현 방법은, 상기 인에이블 요청 답신 메시지를 수신한 후, 상기 사용자 ID를 상기 인에이블 레코드 내에 저장하는 단계를 더 포함하고,

상기 인에이블 응답 메시지는 상기 사용자 ID를 더 포함하며,

상기 서버는, 상기 인에이블 응답 메시지를 수신한 후, 상기 사용자 ID를 획득하고, 상기 사용자 ID를 상기 사용자 레코드 내에 저장하는 것인 컴퓨터 구현 방법.

청구항 6

제5항에 있어서,

상기 인에이블 응답 메시지는 클라이언트 디바이스 ID를 더 포함하고,

상기 서버는, 상기 인에이블 요청 답신 메시지를 수신한 후, 상기 클라이언트 디바이스 ID를 획득하고, 상기 클라이언트 디바이스 ID를 상기 사용자 레코드 내에 저장하는 것인 컴퓨터 구현 방법.

청구항 7

제5항에 있어서,

상기 인증 요청 답신 메시지는 상기 사용자 ID를 더 포함하고,

상기 컴퓨터 구현 방법은, 사용자에 의해 입력된 상기 생체 특징을 수신하고 상기 생체 특징에 대응하는 상기 생체 특징 템플릿 ID를 획득한 후, 상기 사용자 ID에 따라 대응하는 인에이블 레코드를 검색하며, 상기 획득된 생체 특징 템플릿 ID와, 찾아낸 상기 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교하는 단계를 더 포함하고,

상기 생성된 인증 응답 메시지는 상기 사용자 ID를 더 포함하며,

상기 서버는, 상기 인증 응답 메시지를 수신한 후, 상기 사용자 ID를 획득하고, 상기 사용자 ID에 따라 대응하는 사용자 레코드를 검색하는 것인 컴퓨터 구현 방법.

청구항 8

제6항에 있어서,

상기 인증 응답 메시지는 상기 클라이언트 디바이스 ID를 더 포함하고,

상기 서버는, 상기 인증 응답 메시지를 수신한 후, 상기 클라이언트 디바이스 ID를 획득하고, 상기 클라이언트 디바이스 ID에 따라 대응하는 사용자 레코드를 검색하는 것인 컴퓨터 구현 방법.

청구항 9

동작들을 수행하도록 컴퓨터 시스템에 의해 실행가능한 하나 이상의 명령어를 저장한 컴퓨터 판독가능 비일시적 기록 매체에 있어서, 상기 동작들은,

클라이언트로부터 서버로, 생체 특징을 인에이블하기 위한 인에이블 요청을 전송하는 동작;

상기 서버로부터 그리고 상기 인에이블 요청에 응답하여, 인에이블 요청 답신 메시지를 수신하는 동작;

생체 특징 검증 인에이블 프로세스 동안, 사용자에 의해 입력된 생체 특징을 수신하는 동작 - 상기 생체 특징은 상기 사용자의 검증을 위해 제공됨 -;

상기 수신된 생체 특징에 대응하는 생체 특징 템플릿 식별자(ID)를 획득하는 동작;

상기 생체 특징 템플릿 ID를 포함하는 인에이블 레코드를 생성하고 저장하는 동작;

상기 생체 특징 템플릿 ID를 포함하는 인에이블 응답 메시지를 생성하고, 사용자 레코드의 생성과 저장을 위해 상기 인에이블 응답 메시지를 상기 서버에 전송하는 동작 - 상기 사용자 레코드는 생체 특징 검증을 위해 사용되는 생체 특징 템플릿 ID를 포함함 -;

상기 서버에 인증 요청을 전송하는 동작;

상기 서버로부터 그리고 상기 인증 요청에 응답하여, 인증 요청 답신 메시지를 수신하는 동작;

상기 사용자에 의해 입력된 상기 생체 특징을 수신하는 동작;

상기 수신된 생체 특징을 사용하여, 상기 수신된 생체 특징에 대응하는 상기 생체 특징 템플릿 ID를 획득하는 동작 - 상기 획득된 생체 특징 템플릿 ID는 복수의 저장된 생체 특징 템플릿 ID로부터 선택되는 것임 - ;

상기 획득된 생체 특징 템플릿 ID와, 상기 인에이블 레코드 내에 포함되어 있는, 저장된 생체 특징 템플릿 ID를 비교하는 동작; 및

상기 획득된 생체 특징 템플릿 ID와 상기 저장된 생체 특징 템플릿 ID가 일치한 경우, 상기 획득된 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 생성하고, 검증을 위해 상기 인증 응답 메시지를 상기 서버에 전송하는 동작

을 포함하고,

상기 서버에 의한 검증은, 상기 인증 응답 메시지 내의 상기 획득된 생체 특징 템플릿 ID와, 저장된 사용자 레

코드 내의 생체 특징 템플릿 ID의 비교를 포함하며,

상기 획득된 생체 특징 템플릿 ID와 상기 저장된 사용자 레코드 내의 생체 특징 템플릿 ID가 일치한다고 결정한 것에 기초하여 상기 검증은 성공된 것인 컴퓨터 판독가능 비일시적 기록 매체.

청구항 10

제9항에 있어서,

상기 동작들은,

상기 클라이언트가 상기 인증 요청 답신 메시지를 수신한 후, 합의된 제1 공개키를 사용하여 상기 수신된 인증 요청 답신 메시지를 검증하는 동작 - 상기 검증이 성공이었다고 결정한 것에 기초하여 후속 응답이 행해지고, 상기 검증이 실패였다고 결정한 것에 기초하여 오류가 보고됨 -; 및

상기 클라이언트가 상기 인에이블 요청 답신 메시지를 수신한 후, 상기 합의된 제1 공개키를 사용하여 상기 수신된 인에이블 요청 답신 메시지를 검증하는 동작 - 상기 검증이 성공이었다고 결정한 것에 기초하여 후속 응답이 행해지고, 상기 검증이 실패였다고 결정한 것에 기초하여 오류가 보고됨 -

을 더 포함하고,

상기 인증 요청 답신 메시지와 상기 인에이블 요청 답신 메시지는 합의된 제1 개인키를 사용하여 상기 서버에 의해 서명되는 것인 컴퓨터 판독가능 비일시적 기록 매체.

청구항 11

제9항에 있어서,

상기 동작들은,

사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 상기 사용자 개인키를 저장하는 동작;

상기 인에이블 요청 답신 메시지 내에 포함된 챌린지 값에 따라 서명 알고리즘을 선택하는 동작;

상기 선택된 서명 알고리즘 및 합의된 제2 개인키를 사용하여 상기 생성된 인에이블 응답 메시지에 서명하는 동작; 및

상기 서명된 인에이블 응답 메시지를 상기 서버에 전송하는 동작

을 더 포함하며,

상기 인에이블 응답 메시지는 상기 사용자 공개키를 포함하고,

상기 서버는 합의된 제2 공개키를 사용하여 상기 인에이블 응답 메시지를 검증하며,

상기 사용자 공개키는 상기 서버에 저장되는 것인 컴퓨터 판독가능 비일시적 기록 매체.

청구항 12

제11항에 있어서,

상기 동작들은,

상기 인증 요청 답신 메시지 내에 포함된 챌린지 값에 따라 서명 알고리즘을 선택하는 동작; 및

상기 선택된 서명 알고리즘 및 상기 사용자 개인키를 사용하여 상기 인증 응답 메시지에 서명하는 동작

을 더 포함하고,

상기 서버는, 상기 인증 응답 메시지를 수신한 후에 상기 챌린지 값에 따라 서명 알고리즘을 선택하고, 상기 서명 알고리즘과 상기 사용자 공개키를 사용하여 상기 인증 응답 메시지를 검증하며,

상기 검증은, 상기 서명 알고리즘과 상기 사용자 공개키를 사용하여 상기 인증 응답 메시지에 대한 서명을 검증하는 것을 포함한 것인 컴퓨터 판독가능 비일시적 기록 매체.

청구항 13

제9항에 있어서,

상기 인에이블 요청 답신 메시지는 사용자 ID를 더 포함하고,

상기 동작들은, 상기 인에이블 요청 답신 메시지를 수신한 후, 상기 사용자 ID를 상기 인에이블 레코드 내에 저장하는 동작을 더 포함하고,

상기 인에이블 응답 메시지는 상기 사용자 ID를 더 포함하며,

상기 서버는, 상기 인에이블 응답 메시지를 수신한 후, 상기 사용자 ID를 획득하고, 상기 사용자 ID를 상기 사용자 레코드 내에 저장하는 것인 컴퓨터 판독가능 비일시적 기록 매체.

청구항 14

컴퓨터 구현 시스템에 있어서,

하나 이상의 컴퓨터; 및

상기 하나 이상의 컴퓨터와 상호동작가능하게 결합되고, 하나 이상의 명령어를 저장한 유형의 머신 판독가능 비일시적 기록 매체를 갖는 하나 이상의 컴퓨터 메모리 디바이스

를 포함하고, 상기 하나 이상의 명령어는, 상기 하나 이상의 컴퓨터에 의해 실행될 때, 하나 이상의 동작을 수행하고,

상기 하나 이상의 동작은,

클라이언트로부터 서버로, 생체 특징을 인에이블하기 위한 인에이블 요청을 전송하는 동작;

상기 서버로부터 그리고 상기 인에이블 요청에 응답하여, 인에이블 요청 답신 메시지를 수신하는 동작;

생체 특징 검증 인에이블 프로세스 동안, 사용자에 의해 입력된 상기 생체 특징을 수신하는 동작 - 상기 생체 특징은 상기 사용자의 검증을 위해 제공됨 -;

상기 수신된 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하는 동작;

상기 생체 특징 템플릿 ID를 포함하는 인에이블 레코드를 생성하고 저장하는 동작;

상기 생체 특징 템플릿 ID를 포함하는 인에이블 응답 메시지를 생성하고, 사용자 레코드의 생성과 저장을 위해 상기 인에이블 응답 메시지를 상기 서버에 전송하는 동작 - 상기 사용자 레코드는 생체 특징 검증을 위해 사용되는 생체 특징 템플릿 ID를 포함함 -;

상기 서버에 인증 요청을 전송하는 동작;

상기 서버로부터 그리고 상기 인증 요청에 응답하여, 인증 요청 답신 메시지를 수신하는 동작;

상기 사용자에 의해 입력된 상기 생체 특징을 수신하는 동작;

상기 수신된 생체 특징을 사용하여, 상기 수신된 생체 특징에 대응하는 상기 생체 특징 템플릿 ID를 획득하는 동작 - 상기 획득된 생체 특징 템플릿 ID는 복수의 저장된 생체 특징 템플릿 ID로부터 선택되는 것임 -;

상기 획득된 생체 특징 템플릿 ID와, 상기 인에이블 레코드 내에 포함되어 있는, 저장된 생체 특징 템플릿 ID를 비교하는 동작; 및

상기 획득된 생체 특징 템플릿 ID와 상기 저장된 생체 특징 템플릿 ID가 일치한 경우, 상기 획득된 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 생성하고, 검증을 위해 상기 인증 응답 메시지를 상기 서버에 전송하는 동작

을 포함하고,

상기 서버에 의한 검증은, 상기 인증 응답 메시지 내의 상기 획득된 생체 특징 템플릿 ID와, 저장된 사용자 레코드 내의 생체 특징 템플릿 ID의 비교를 포함하며,

상기 획득된 생체 특징 템플릿 ID와 상기 저장된 사용자 레코드 내의 생체 특징 템플릿 ID가 일치한다고 결정한 것에 기초하여 상기 검증은 성공된 것인 컴퓨터 구현 시스템.

청구항 15

제14항에 있어서,

상기 하나 이상의 동작은,

상기 클라이언트가 상기 인증 요청 답신 메시지를 수신한 후, 합의된 제1 공개키를 사용하여 상기 수신된 인증 요청 답신 메시지를 검증하는 동작 - 상기 검증이 성공이었다고 결정한 것에 기초하여 후속 응답이 행해지고, 상기 검증이 실패였다고 결정한 것에 기초하여 오류가 보고됨 -; 및

상기 클라이언트가 상기 인에이블 요청 답신 메시지를 수신한 후, 상기 합의된 제1 공개키를 사용하여 상기 수신된 인에이블 요청 답신 메시지를 검증하는 동작 - 상기 검증이 성공이었다고 결정한 것에 기초하여 후속 응답이 행해지고, 상기 검증이 실패였다고 결정한 것에 기초하여 오류가 보고됨 -

을 더 포함하고,

상기 인증 요청 답신 메시지와 상기 인에이블 요청 답신 메시지는 합의된 제1 개인키를 사용하여 상기 서버에 의해 서명되는 것인 컴퓨터 구현 시스템.

청구항 16

제14항에 있어서,

상기 하나 이상의 동작은,

사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 상기 사용자 개인키를 저장하는 동작;

상기 인에이블 요청 답신 메시지 내에 포함된 챌린지 값에 따라 서명 알고리즘을 선택하는 동작;

상기 선택된 서명 알고리즘 및 합의된 제2 개인키를 사용하여 상기 생성된 인에이블 응답 메시지에 서명하는 동작; 및

상기 서명된 인에이블 응답 메시지를 상기 서버에 전송하는 동작

을 더 포함하며,

상기 인에이블 응답 메시지는 상기 사용자 공개키를 포함하고,

상기 서버는 합의된 제2 공개키를 사용하여 상기 인에이블 응답 메시지를 검증하며,

상기 사용자 공개키는 상기 서버에 저장되는 것인 컴퓨터 구현 시스템.

청구항 17

제16항에 있어서,

상기 하나 이상의 동작은,

상기 인증 요청 답신 메시지 내에 포함된 챌린지 값에 따라 서명 알고리즘을 선택하는 동작; 및

상기 선택된 서명 알고리즘 및 상기 사용자 개인키를 사용하여 상기 인증 응답 메시지에 서명하는 동작

을 더 포함하고,

상기 서버는, 상기 인증 응답 메시지를 수신한 후에 상기 챌린지 값에 따라 서명 알고리즘을 선택하고, 상기 서명 알고리즘과 상기 사용자 공개키를 사용하여 상기 인증 응답 메시지를 검증하며,

상기 검증은, 상기 서명 알고리즘과 상기 사용자 공개키를 사용하여 상기 인증 응답 메시지에 대한 서명을 검증하는 것을 포함한 것인 컴퓨터 구현 시스템.

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 신원 인증 기술의 분야에 관한 것이며, 특히, 신원 인증 프로세스에서 이용하기 위한, 생체 특징(biological feature)에 기초한 보안 검증 방법, 클라이언트 단말, 및 서버에 관한 것이다.

배 경 기 술

[0002] 전통적인 패스워드 검증 프로세스에서는 패스워드가 입력될 필요가 있다. 패스워드가 입력될 때마다, 키로거 트로이 목마(keylogger Trojan), 물리적 엿보기(physical peep) 등과 같은 유출 위험이 있다. 지문은 높은 안정성, 개별 고유성, 및 높은 알고리즘 정확성과 같은 특징을 가지고 있기 때문에, 최근 해에 많은 디바이스들이 지문 검증 기능을 이용하기 시작한다. 예를 들어, 온라인 결제가 지문 검증을 통해 구현되어, 사용자 경험을 개선하고 결제 보안을 강화할 수 있다.

[0003] 종래에, 온라인 지문 검증 프로세스에서는, 클라이언트 단말이 사용자의 지문 데이터(지문 이미지 또는 지문 특징 데이터)를 서버 단말에 전송한다. 서버 단말은 사용자의 원래 지문 데이터와 수신된 지문 데이터를 비교하여, 검증을 완료한다. 지문 데이터를 서버 단말에 송신할 필요가 있기 때문에, 업로드 프로세스에서 지문 데이터를 유출시킬 위험성이 존재한다. 지문 데이터는 개인 데이터이므로, 사용자는 지문 데이터를 업로드하는 것에 합의(agreed)하지 않을 수 있다. 또한, 지문 데이터가 유출되면 평판 위험(reputational risk)이 발생할 수 있다. 사용자가 지문 데이터를 업로드하는 것에 합의하더라도, 데이터 업로드 동안 네트워크 트래픽이 소모될 필요가 있다. 서버 단말은 또한 지문 데이터를 비교할 필요가 있고, 이에 따라 추가적인 컴퓨팅 리소스와 저장 리소스를 소모한다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은 종래의 검증 프로세스에서의 전술한 네트워크 트래픽 소모 및 개인 지문 데이터의 유출 위험의 기술적 문제점을 방지하고, 보안성을 더욱 강화시키기 위해, 생체 특징에 기초한 보안 검증 방법, 클라이언트 단말, 및 서버를 제공하는 것이다.

과제의 해결 수단

[0005] 전술한 목적을 달성하기 위해, 본 발명의 기술적 해결책은 다음과 같다:

[0006] 생체 특징에 기초한 보안 검증 방법은 신원 인증 시스템에서의 클라이언트 단말에 적용되며, 신원 인증 시스템은 서버 단말을 더 포함하고, 클라이언트 단말은 인에이블 레코드(enable record)를 저장하고, 인에이블 레코드는 생체 특징 검증에 이용되고 생체 특징 검증을 인에이블시키는 프로세스에서 획득되는 생체 특징 템플릿(template) ID를 포함하며, 보안 검증 방법은,

[0007] 서버 단말에 인증 요청을 전송하고, 서버 단말에 의해 회신된 인증 요청 답신 메시지를 수신하는 단계; 및

[0008] 사용자에 의해 입력되는 생체 특징을 수신하고, 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하고, 획득된 생체 특징 템플릿 ID와 저장된 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교하고, 상기 두 개의 생체 특징 템플릿 ID들이 일치하면 획득된 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 생성하며, 서버 단말이 인증 응답 메시지를 수신하여 검증을 수행할 수 있도록, 인증 응답 메시지를 서버 단말에 전송하는 단계를 포함한다.

[0009] 생체 특징 검증을 인에이블시키는 프로세스는,

[0010] 생체 특징 검증을 인에이블시키기 위한 인에이블 요청을 서버 단말에 전송하고, 서버 단말에 의해 회신된 인에이블 요청 답신 메시지를 수신하는 단계;

[0011] 검증에 이용되고 사용자에 의해 입력되는 생체 특징을 수신하고, 검증에 이용되는 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하며, 인에이블 레코드를 생성하고 저장하는 단계; 및

[0012] 생체 특징 템플릿 ID를 포함하는 인에이블 응답 메시지를 생성하고, 인에이블 응답 메시지를 서버 단말에 전송하는 단계를 포함함으로써, 서버 단말이 인에이블 응답 메시지를 수신하고, 이 메시지에 포함된 생체 특징 템플릿 ID를 획득하며, 사용자 레코드를 생성하고 저장할 수 있도록 한다.

[0013] 또한, 서버 단말은 합의된 제1 개인키를 이용하여 인증 요청 답신 메시지 또는 인에이블 요청 답신 메시지에 서명하고, 클라이언트 단말이 인증 요청 답신 메시지를 수신한 후, 본 방법은,

[0014] 합의된 제1 공개키를 이용하여 상기 수신된 인증 요청 답신 메시지를 검증하는 단계를 더 포함하고, 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고되고;

[0015] 클라이언트 단말이 인에이블 요청 답신 메시지를 수신한 후, 본 방법은,

[0016] 합의된 제1 공개키를 이용하여 상기 수신된 인에이블 요청 답신 메시지를 검증하는 단계를 더 포함하고, 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고된다.

[0017] 이 단계는 인에이블 프로세스에서 보안을 더욱 강화하고 인에이블 프로세스의 위조를 방지할 수 있다.

[0018] 또한, 인에이블 요청 답신 메시지는 챌린지 값(challenge value)을 운반하며, 생체 특징 검증을 인에이블시키는 프로세스는,

[0019] 사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 사용자 개인키를 저장하는 단계; 및

[0020] 인에이블 요청 답신 메시지에서의 챌린지 값에 따라 서명 알고리즘(signature algorithm)을 선택하고, 선택된 서명 알고리즘 및 합의된 제2 개인키를 이용하여 상기 생성된 인에이블 응답 메시지에 서명한 후, 서명된 인에이블 응답 메시지를 서버 단말에 전송하는 단계를 더 포함하며, 여기서, 인에이블 응답 메시지는 사용자 공개키를 포함하여, 서버 단말이 인에이블 응답 메시지를 수신하고, 합의된 제2 공개키를 이용하여 인에이블 응답 메시지를 검증할 수 있도록 하며, 사용자 공개키는 서버 단말에 저장된다.

[0021] 또한, 인증 요청 답신 메시지는 챌린지 값을 운반하며, 보안 검증 방법은,

[0022] 챌린지 값에 따라 서명 알고리즘을 선택하고, 선택된 서명 알고리즘과 사용자 개인키를 이용하여 인증 응답 메시지에 서명하는 단계를 더 포함함으로써, 서버 단말이 또한 인증 응답 메시지를 수신한 후에 챌린지 값에 따라 서명 알고리즘을 선택하고, 서명 알고리즘과 사용자 공개키를 이용하여 인증 응답 메시지를 검증할 수 있도록 한다.

[0023] 사용자 키 쌍은 생체 특징 검증을 인에이블시키는 프로세스에서 생성되고, 인증 프로세스에서, 선택된 서명 알고리즘과 사용자 키 쌍을 이용하여 검증이 수행되며, 이에 따라 보안이 강화되고 위조 메시지로부터의 재생 공격(replay attack)을 방지할 수 있다.

[0024] 또한, 인에이블 요청 답신 메시지에는 사용자 ID가 더 포함되고, 클라이언트 단말이 인에이블 요청 답신 메시지를 수신한 후, 본 방법은,

[0025] 사용자 ID를 인에이블 레코드에 저장하는 단계를 더 포함하며, 여기서, 클라이언트 단말에 의해 생성된 인에이블 응답 메시지에는 사용자 ID가 더 포함되어, 서버 단말이, 인에이블 응답 메시지를 수신한 후, 인에이블 응답 메시지 내에서 사용자 ID를 획득하고 이 사용자 ID를 사용자 레코드에 저장할 수 있도록 한다.

[0026] 인에이블 응답 메시지에는 클라이언트 단말 디바이스 ID가 더 포함되어, 서버 단말이, 인에이블 요청 답신 메시지를 수신한 후, 인에이블 요청 답신 메시지 내에서 클라이언트 단말 디바이스 ID를 획득하고 이 클라이언트 단말 디바이스 ID를 사용자 레코드에 저장할 수 있도록 한다.

[0027] 인증 요청 답신 메시지에는 사용자 ID가 더 포함되고, 사용자에 의해 입력되는 생체 특징을 수신하고 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득한 후, 본 방법은,

[0028] 사용자 ID에 따라 대응하는 인에이블 레코드를 검색하여, 획득된 생체 특징 템플릿 ID와 찾아낸 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교하는 단계를 더 포함하며,

[0029] 여기서, 클라이언트 단말에 의해 생성된 인증 응답 메시지에는 사용자 ID가 더 포함되어, 서버 단말이, 인증 응답 메시지를 수신한 후, 인증 응답 메시지 내에서 사용자 ID를 획득하고 사용자 ID에 따라 대응하는 사용자 레코드를 검색할 수 있도록 한다.

[0030] 인증 응답 메시지에는 클라이언트 단말 디바이스 ID가 더 포함되어, 서버 단말이, 인증 응답 메시지를 수신한 후, 인증 응답 메시지 내에서 상기 클라이언트 단말 디바이스 ID를 획득하고 상기 클라이언트 단말 디바이스 ID에 따라 대응하는 사용자 레코드를 검색할 수 있도록 한다.

[0031] 전술한 단계들을 이용함으로써, 하나의 단말 디바이스가 복수의 사용자들을 지원하거나 또는 하나의 사용자가 복수의 단말 디바이스들을 갖는 상황이 지원될 수 있다. 비교 및 검증을 수행하기 위해, 대응하는 인에이블 레코드 또는 사용자 레코드가 사용자 ID 또는 디바이스 ID에 따라 검색된다.

[0032] 본 발명은 생체 특징에 기초한 보안 검증 방법을 더 제공한다. 본 방법은 신원 인증 시스템에서의 서버 단말에 적용되고, 여기서, 신원 인증 시스템은 클라이언트 단말을 더 포함하며, 서버 단말은 사용자 레코드를 저장하며, 사용자 레코드는 생체 특징 검증에 이용되고 생체 특징 검증을 인에이블시키는 프로세스에서 획득되는 생체 특징 템플릿 ID를 포함한다. 보안 검증 방법은,

[0033] 클라이언트 단말로부터 인증 요청을 수신하고, 인증 요청 답신 메시지를 클라이언트 단말에 전송하는 단계;

[0034] 클라이언트 단말로부터 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 수신하는 단계; 및

[0035] 인증 응답 메시지 내의 생체 특징 템플릿 ID와 상기 저장된 사용자 레코드 내의 생체 특징 템플릿 ID를 비교하여 검증을 수행하는 단계를 포함하며, 여기서, 이 두 개의 생체 특징 템플릿 ID들이 일치하면 검증은 성공된 것이며, 그렇지 않은 경우에는 오류가 보고된다.

[0036] 생체 특징 검증을 인에이블시키는 프로세스는,

[0037] 클라이언트 단말로부터 생체 특징 검증을 인에이블시키기 위한 인에이블 요청을 수신하고, 클라이언트 단말에게 인에이블 요청 답신 메시지를 전송함으로써, 클라이언트 단말이, 검증에 이용되고 사용자에 의해 입력되는 생체 특징에 따라, 검증에 이용되는 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하고, 인에이블 레코드를 생성하고 저장할 수 있도록 하는 단계; 및

[0038] 클라이언트 단말로부터 인에이블 응답 메시지를 수신하고, 인에이블 응답 메시지에 포함된 생체 특징 템플릿 ID를 획득하며, 사용자 레코드를 생성하고 저장하는 단계를 포함한다.

[0039] 또한, 보안 검증 방법은,

[0040] 합의된 제1 개인키를 이용하여 인증 요청 답신 메시지 또는 인에이블 요청 답신 메시지에 서명하는 단계를 더 포함함으로써, 클라이언트 단말이, 합의된 제1 공개키를 이용하여 상기 수신된 인증 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 할 수 있도록 하거나; 또는 클라이언트 단말이, 합의된 제1 공개키를 이용하여 상기 수신된 인에이블 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 할 수 있도록 한다. 이 단계는 인에이블 프로세스에서 보안을 더욱 강화하고 인에이블 프로세스의 위조를 방지할 수 있다.

[0041] 또한, 인에이블 요청 답신 메시지는 챌린지 값을 운반하고; 클라이언트 단말은 사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 사용자 개인키를 저장하며; 생체 특징 검증을 인에이블시키는 프로세스는,

[0042] 선택된 서명 알고리즘 및 합의된 제2 개인키를 이용하여 클라이언트 단말에 의해 서명된 인에이블 응답 메시지를 수신하고 - 여기서 서명 알고리즘은 인에이블 요청 답신 메시지 내의 챌린지 값에 따라 클라이언트 단말에 의해 선택되고, 인에이블 응답 메시지는 사용자 공개키를 포함함 -, 그리고 또한 챌린지 값에 따라 서명 알고리즘을 선택하며, 제2 공개키를 이용하여 인에이블 응답 메시지를 검증하는 단계를 더 포함하며, 사용자 공개키는 서버 단말에 저장된다.

[0043] 또한, 보안 검증 방법은,

[0044] 선택된 서명 알고리즘 및 사용자 개인키를 이용하여 클라이언트 단말에 의해 서명된 인증 응답 메시지를 수신하

고 - 여기서 서명 알고리즘은 인증 요청 답신 메시지 내의 챌린지 값에 따라 클라이언트 단말에 의해 선택됨 -, 그리고 또한 챌린지 값에 따라 서명 알고리즘을 선택하며, 서명 알고리즘 및 사용자 공개키를 이용하여 인증 응답 메시지 상의 서명을 검증하는 단계를 더 포함한다.

[0045] 사용자 키 쌍은 생체 특징 검증을 인에이블시키는 프로세스에서 생성되고, 인증 프로세스에서, 선택된 서명 알고리즘과 사용자 키 쌍을 이용하여 검증이 수행되며, 이에 따라 보안이 강화되고 위조 메시지로부터의 재생 공격(replay attack)을 방지할 수 있다.

[0046] 또한, 인에이블 요청 답신 메시지에는 사용자 ID가 더 포함되어, 클라이언트 단말이 인에이블 요청 답신 메시지를 수신한 후에 인에이블 레코드에 사용자 ID를 저장할 수 있도록 하고; 클라이언트 단말에 의해 생성된 인에이블 응답 메시지에는 사용자 ID가 더 포함되며; 서버 단말이 인에이블 응답 메시지를 수신한 후, 본 방법은,

[0047] 인에이블 응답 메시지로부터 사용자 ID를 획득하고, 사용자 레코드에 사용자 ID를 저장하는 단계를 더 포함한다.

[0048] 인에이블 응답 메시지에는 클라이언트 단말 디바이스 ID가 더 포함되며; 서버 단말이 인에이블 응답 메시지를 수신한 후, 본 방법은,

[0049] 인에이블 응답 메시지로부터 디바이스 ID를 획득하고, 사용자 레코드에 디바이스 ID를 저장하는 단계를 더 포함한다.

[0050] 인증 요청 답신 메시지에는 사용자 ID가 더 포함되어, 클라이언트 단말이 사용자 ID에 따라 대응하는 인에이블 레코드를 검색하고, 획득된 생체 특징 템플릿 ID와 찾아낸 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교할 수 있도록 하며; 클라이언트 단말에 의해 생성된 인증 응답 메시지에는 사용자 ID가 더 포함되며; 서버 단말이 인증 응답 메시지를 수신한 후, 본 방법은,

[0051] 인증 응답 메시지로부터 사용자 ID를 획득하고, 사용자 ID에 따라 대응하는 사용자 레코드를 검색하는 단계를 더 포함한다.

[0052] 인증 응답 메시지에는 클라이언트 단말 디바이스 ID가 더 포함되며, 서버 단말이 인증 응답 메시지를 수신한 후, 본 방법은,

[0053] 인증 응답 메시지로부터 클라이언트 단말 디바이스 ID를 획득하고, 클라이언트 단말 디바이스 ID에 따라 대응하는 사용자 레코드를 검색하는 단계를 더 포함한다.

[0054] 본 발명은 신원 인증 시스템에 적용되는 클라이언트 단말을 더 제공하고, 여기서, 신원 인증 시스템은 서버 단말을 더 포함하며, 클라이언트 단말은 인에이블 레코드를 저장하며, 인에이블 레코드는 생체 특징 검증에 이용되고 생체 특징 검증을 인에이블시키는 프로세스에서 획득되는 생체 특징 템플릿 ID를 포함하며; 클라이언트 단말은,

[0055] 서버 단말에 인증 요청을 전송하고, 서버 단말에 의해 회신된 인증 요청 답신 메시지를 수신하도록 구성된 요청 모듈; 및

[0056] 사용자에 의해 입력되는 생체 특징을 수신하고, 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하고, 획득된 생체 특징 템플릿 ID와 저장된 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교하고, 상기 두 개의 생체 특징 템플릿 ID들이 일치하면 획득된 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 생성하며, 서버 단말이 인증 응답 메시지를 수신하고 검증을 수행할 수 있도록 인증 응답 메시지를 서버 단말에 전송하도록 구성된 응답 모듈을 포함한다.

[0057] 더 나아가, 요청 모듈은 또한, 생체 특징 검증을 인에이블시키기 위한 인에이블 요청을 서버 단말에 전송하고, 서버 단말에 의해 회신된 인에이블 요청 답신 메시지를 수신하도록 구성되고; 응답 모듈은 또한, 검증에 이용되고 사용자에 의해 입력되는 생체 특징을 수신하고, 검증에 이용되는 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하고, 인에이블 레코드를 생성하고 저장하고, 생체 특징 템플릿 ID를 포함하는 인에이블 응답 메시지를 생성하고, 인에이블 응답 메시지를 서버 단말에 전송하도록 구성됨으로써, 서버 단말이 인에이블 응답 메시지를 수신하고, 인에이블 응답 메시지에 포함된 생체 특징 템플릿 ID를 획득하며, 사용자 레코드를 생성하고 저장할 수 있도록 한다.

[0058] 또한, 서버 단말은 합의된 제1 개인키를 이용하여 인증 요청 답신 메시지 또는 인에이블 요청 답신 메시지에 서명하고, 인증 요청 답신 메시지를 수신한 후, 요청 모듈은 또한, 합의된 제1 공개키를 이용하여 상기 수신된 인

증 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 하도록 구성되고; 인에이블 요청 답신 메시지를 수신한 후, 요청 모듈은 또한, 합의된 제1 공개키를 이용하여 상기 수신된 인에이블 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 하도록 구성된다.

[0059] 본 발명에서, 인에이블 요청 답신 메시지는 챌린지 값을 운반하고, 응답 모듈은 또한, 사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 사용자 개인키를 저장하며; 인에이블 요청 답신 메시지에서의 챌린지 값에 따라 서명 알고리즘을 선택하고, 선택된 서명 알고리즘 및 합의된 제2 개인키를 이용하여 상기 생성된 인에이블 응답 메시지에 서명한 후, 서명된 인에이블 응답 메시지를 서버 단말에 전송하도록 구성되며, 여기서, 인에이블 응답 메시지는 사용자 공개키를 포함하여, 서버 단말이 인에이블 응답 메시지를 수신하고, 합의된 제2 공개키를 이용하여 인에이블 응답 메시지를 검증할 수 있도록 하며, 사용자 공개키는 서버 단말에 저장된다.

[0060] 또한, 인증 요청 답신 메시지는 챌린지 값을 운반하고, 응답 모듈은 또한 챌린지 값에 따라 서명 알고리즘을 선택하고, 선택된 서명 알고리즘과 사용자 개인키를 이용하여 인증 응답 메시지에 서명하도록 구성됨으로써, 서버 단말이 또한 인증 응답 메시지를 수신한 후에 챌린지 값에 따라 서명 알고리즘을 선택하고, 서명 알고리즘과 사용자 공개키를 이용하여 인증 응답 메시지를 검증할 수 있도록 한다.

[0061] 본 발명은 신원 인증 시스템에 적용되는 서버를 더 제공하고, 신원 인증 시스템은 클라이언트 단말을 더 포함하고, 서버는 사용자 레코드를 저장하며, 사용자 레코드는 생체 특징 검증에 이용되고 생체 특징 검증을 인에이블시키는 프로세스에서 획득되는 생체 특징 템플릿 ID를 포함하며; 서버는,

[0062] 클라이언트 단말로부터 인증 요청을 수신하고, 인증 요청 답신 메시지를 클라이언트 단말에 전송하도록 구성된 답신 모듈; 및

[0063] 클라이언트 단말로부터 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 수신하며; 인증 응답 메시지 내의 생체 특징 템플릿 ID와 상기 저장된 사용자 레코드 내의 생체 특징 템플릿 ID를 비교하여 검증을 수행하도록 구성된 검증 모듈을 포함하며, 여기서, 이 두 개의 생체 특징 템플릿 ID들이 일치하면 검증은 성공된 것이며, 그렇지 않은 경우에는 오류가 보고된다.

[0064] 더 나아가, 답신 모듈은 또한, 클라이언트 단말로부터 생체 특징 검증을 인에이블시키기 위한 인에이블 요청을 수신하고, 클라이언트 단말에게 인에이블 요청 답신 메시지를 전송하도록 구성됨으로써, 클라이언트 단말이, 검증에 이용되고 사용자에 의해 입력되는 생체 특징에 따라, 검증에 이용되는 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하고, 인에이블 레코드를 생성하고 저장할 수 있도록 하며; 검증 모듈은 또한, 클라이언트 단말로부터 인에이블 응답 메시지를 수신하고, 인에이블 응답 메시지에 포함된 생체 특징 템플릿 ID를 획득하며, 사용자 레코드를 생성하고 저장하도록 구성된다.

[0065] 더 나아가, 답신 모듈은 또한, 합의된 제1 개인키를 이용하여 인증 요청 답신 메시지 또는 인에이블 요청 답신 메시지에 서명하도록 구성됨으로써, 클라이언트 단말이, 합의된 제1 공개키를 이용하여 상기 수신된 인증 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 할 수 있도록 하거나; 또는 클라이언트 단말이, 합의된 제1 공개키를 이용하여 상기 수신된 인에이블 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 할 수 있도록 한다.

[0066] 본 발명에서, 인에이블 요청 답신 메시지는 챌린지 값을 운반하고; 클라이언트 단말은 사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 사용자 개인키를 저장하며; 검증 모듈은 또한, 선택된 서명 알고리즘 및 합의된 제2 개인키를 이용하여 클라이언트 단말에 의해 서명된 인에이블 응답 메시지를 수신하고 - 여기서 서명 알고리즘은 인에이블 요청 답신 메시지 내의 챌린지 값에 따라 클라이언트 단말에 의해 선택되고, 인에이블 응답 메시지는 사용자 공개키를 포함함 -; 그리고 또한 챌린지 값에 따라 서명 알고리즘을 선택하고, 제2 공개키를 이용하여 인에이블 응답 메시지를 검증하며, 사용자 공개키를 저장하도록 구성된다.

[0067] 더 나아가, 검증 모듈은 또한, 선택된 서명 알고리즘 및 사용자 개인키를 이용하여 클라이언트 단말에 의해 서명된 인증 응답 메시지를 수신하고 - 여기서 서명 알고리즘은 인증 요청 답신 메시지 내의 챌린지 값에 따라 클라이언트 단말에 의해 선택됨 -; 그리고 또한 챌린지 값에 따라 서명 알고리즘을 선택하며, 서명 알고리즘 및 사용자 공개키를 이용하여 인증 응답 메시지 상의 서명을 검증하도록 구성된다.

발명의 효과

[0068] 본 발명의 생체 특징에 기초한 보안 검증 방법, 클라이언트 단말, 및 서버는, 클라이언트 단말이 신뢰성 있는 실행 환경(trusted execution environment; TEE)에서 지문 검증, 지문 템플릿 저장, 및 검증 프로세스를 수행하는 것을 구현한다. 이러한 구현은 보통의 하드웨어와 완전히 분리되므로 프라이버시 유출 위험을 방지할 수 있다. 또한, 네트워크 트래픽이 지문 데이터 송신 프로세스에서 감소된다. 게다가, 서버 단말은 지문 템플릿 ID만을 비교하므로, 서버 단말의 연산 오버헤드와 저장 오버헤드를 감소시킨다. 지문 검증이 인에이블되면 특정 지문 템플릿이 결속(bind)된다. 검증이 인에이블된 후에 추가되는 새로운 지문 템플릿은 검증에 이용될 수 없으므로, 보안을 향상시킨다. 선택된 서명 알고리즘을 이용함으로써, 검증 프로세스에서 보안이 더욱 강화되고 위조 메시지로부터의 네트워크 공격이 방지된다.

도면의 간단한 설명

[0069] 도 1은 본 발명에 따른 생체 특징 검증을 인에이블시키는 프로세스의 흐름도이다.

도 2는 본 발명에 따른 생체 특징에 기초한 보안 검증 방법의 흐름도이다.

도 3은 본 발명에 따른 클라이언트 단말의 개략적인 구조도이다.

도 4는 본 발명에 따른 서버의 개략적인 구조도이다.

발명을 실시하기 위한 구체적인 내용

[0070] 아래에서는, 첨부된 도면과 실시예들을 참조하여 본 발명의 기술적 해결책을 상세히 설명하며, 아래의 실시예들은 본 발명을 제한시키지 않는다.

[0071] 생체 특징에 기초한 검증을 위해, 지문 인식, 음성 인식, 얼굴 인식, 및 홍채 인식과 같은 기술적 수단에 의해 신원 인증을 수행하는 것이 점차 보편화되고 있다. 이러한 생체 특징 검증은, 예를 들어, 출입 통제 시스템이나 인터넷 결제에 널리 적용된다. 이 실시예는 본 발명에 따른 생체 특징에 기초한 보안 검증 방법을 상세하게 설명하기 위한 예시로서 인터넷 결제 시의 지문 검증을 이용한다.

[0072] 본 실시예의 인터넷 결제에서의 지문 검증은, 온라인 지문 검증과는 달리, 사용자의 클라이언트 단말에서 지문 비교를 완료하고, 또한 서버 단말에서 결과를 검증한다. 이러한 이중 보호는 지문 검증의 효율성을 보장한다. 이 실시예에서의 클라이언트 단말은 일반적으로 애플리케이션 프로그램이며, 이동 단말, 컴퓨터, 또는 사용자의 다른 지능형 디바이스 상에 설치된다. 일부 클라이언트 단말들은 서비스 제공자에 의해 제공되는 직접적 웹페이지 결합형 지문 스캐닝 단말이다.

[0073] 이 실시예의 지문 검증 방법은, 이하에서 별도로 설명하는 지문 검증 인에이블링 프로세스 및 검증 프로세스를 포함한다.

[0074] 실시예 1: 지문 검증 인에이블링 프로세스

[0075] 인터넷 결제 시의 지문 검증을 위해서는, 먼저 지문 검증 기능이 인에이블될 필요가 있다. 도 1에서 도시된 바와 같이, 본 프로세스는 다음의 단계들을 포함한다:

[0076] ① 클라이언트 단말이 서버 단말에게 지문 검증을 인에이블시키기 위한 인에이블 요청을 전송한다.

[0077] 지문 검증 기능을 인에이블시킨 경우, 사용자는 먼저 서버 단말에 대한 인에이블 요청을 개시한다.

[0078] ② 서버 단말은, 지문 검증을 인에이블시키기 위한 인에이블 요청을 수신한 후, 클라이언트 단말에게 인에이블 요청 답신 메시지를 전송한다.

[0079] ③ 클라이언트 단말은, 인에이블 요청 답신 메시지를 수신한 후, 사용자에 의해 입력되고 검증에 이용되는 지문 이미지를 수신하고, 검증에 이용되는 지문 이미지에 대응하는 지문 템플릿 ID를 획득한다.

[0080] 지문 검증이 인에이블되기 전에, 사용자의 클라이언트 단말 디바이스는 사용자에 의해 입력되는 복수의 지문 템플릿들을 저장한다. 지문 템플릿은 지문 이미지로부터 추출된 지문 특징이다. 지문 검증 기능이 인에이블되면, 사용자는 지문 검증을 위한 손가락의 지문 이미지를 클라이언트 단말에 입력한다. 예를 들어, 사용자는 지문 스캐닝 디바이스 상에 손가락을 올려놓는다. 지문 이미지가 획득되고, 지문 특징이 추출된다. 그 후, 대응하는 지문 템플릿 ID를 획득하기 위해, 지문 특징이 클라이언트 단말에 저장된 지문 템플릿과 비교된다.

[0081] 지문 검증이 인에이블되기 전에 사용자의 클라이언트 단말 디바이스가 사용자의 어떠한 지문 템플릿도 저장하지 않은 경우, 지문 검증을 위해 사용자에 의해 이용되는 지문 이미지가 사용자의 클라이언트 단말 디바이스에 직접 입력되어, 지문 템플릿과 지문 템플릿 ID를 생성하고, 지문 템플릿 ID를 획득하도록 한다.

[0082] ④ 클라이언트 단말은 인에이블 레코드를 저장하며, 인에이블 레코드에는 지문 템플릿 ID가 포함된다.

[0083] 인에이블 레코드는 클라이언트 단말 디바이스에 저장된 레코드이며, 지문 검증의 인에이블링 동안 지문 검증을 위해 사용자에 의해 이용되는 지문 템플릿 ID를 포함한다. 후속 지문 검증 단계에서 지문 템플릿 ID는 입력되는 지문 템플릿 ID와 비교되어, 입력되는 지문 템플릿 ID가 검증의 인에이블 동안에 이용되는 원래의 지문 템플릿 ID와 일치하는지 여부를 판단한다. 즉, 검증의 인에이블 동안에 입력되는 지문 템플릿 ID만이 후속 검증에서 이용될 수 있다. 검증에 이용되는 지문 템플릿 ID는 사용자의 구동 패스워드를 크래킹(cracking)하여 수정될 수 없다. 따라서, 사용자의 클라이언트 단말 디바이스가 분실된 경우에도, 사용자는 패스워드가 크래킹되고 디바이스가 불법적인 사람에 의해 사기 목적으로 이용되는 것을 걱정할 필요가 없다.

[0084] ⑤ 클라이언트 단말은 인에이블 레코드 내의 지문 템플릿 ID를 포함한 인에이블 응답 메시지를 생성하고, 이 인에이블 응답 메시지를 서버 단말에 전송한다.

[0085] 이 실시예에서, 인에이블 레코드 내의 지문 템플릿 ID는 인에이블 응답 메시지로 운반되고 서버 단말에 전송되어, 서버 단말이 이 정보를 저장할 수 있도록 한다.

[0086] ⑥ 서버 단말은 인에이블 응답 메시지를 수신하고, 사용자의 지문 템플릿 ID를 포함한 사용자 레코드를 생성하고 저장한다.

[0087] 이러한 방식으로, 클라이언트 단말에 의해 전송된 인에이블 응답 메시지를 수신한 후, 서버 단말은 사용자 레코드를 생성하고 저장한다. 사용자 레코드에는 사용자의 지문 템플릿 ID가 포함된다. 서버 단말은 후속 검증 프로세스에서의 결과를 검증하기 위해, 사용자 레코드를 저장한다.

[0088] 바람직하게는, 인에이블 프로세스에서의 보안을 더욱 강화하기 위해, 이 실시예의 단계 ②는 다음의 서브단계를 더 포함한다:

[0089] 서버 단말에 의해, 제1 개인키를 이용하여 인에이블 요청 답신 메시지를 암호화하는 단계.

[0090] 이러한 방식으로, 인에이블 요청 답신 메시지를 수신한 후, 클라이언트 단말은 인에이블 요청 답신 메시지를 검증할 필요가 있다. 일반적으로 말해서, 제1 공개키와 제1 개인키를 포함하는 서버 공개키 및 개인키 쌍은 클라이언트 단말과 서버 단말에 의해 합의된 것이다. 제1 공개키는 클라이언트 단말에 저장되고 제1 개인키는 서버 단말에 저장된다. 서버 단말은 제1 개인키를 이용하여 인에이블 요청 답신 메시지를 암호화하고, 그 후, 암호화된 메시지를 클라이언트 단말에 전송한다. 클라이언트 단말은 제1 공개키를 이용하여 이 메시지를 암호해제하고 검증을 수행한다. 검증이 성공된 경우 후속 단계가 수행되고, 그렇지 않으면 오류가 보고된다. 여기서 이용되는 암호화 알고리즘은 대칭 알고리즘, 비대칭 알고리즘, 추상화 알고리즘 등일 수 있다.

[0091] 따라서, 이 실시예의 단계 ③은 다음의 서브단계를 더 포함한다:

[0092] 클라이언트 단말에 의해, 제1 공개키를 이용하여 인에이블 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 하는 단계.

[0093] 즉, 인에이블 요청 답신 메시지를 수신한 후, 클라이언트 단말은 제1 공개키를 이용하여 이 메시지를 암호해제하고 검증을 수행한다. 검증이 성공된 경우 후속 단계가 수행되고, 그렇지 않으면 오류가 보고된다. 보안 요구사항이 높지 않은 일반적인 경우, 인에이블 요청 답신 메시지를 검증하는 프로세스는 또한 생략될 수 있음에 유의해야 한다. 제1 공개키와 제1 개인키는 어떠한 클라이언트 단말에 대해서도 변하지 않는다.

[0094] 이 실시예에서, 복수의 사용자가 클라이언트 단말에 등록하는 경우, 예를 들어, 복수의 사용자가 하나의 클라이언트 단말을 공유하는 경우, 인에이블 레코드는, 상이한 사용자들의 인에이블 레코드들을 구별하기 위해, 사용자 ID를 포함할 필요가 있다. 그러나, 해커가 클라이언트 단말을 공격하여 사용자 ID를 변조하는 것이 쉽기 때문에, 이 실시예에서 인에이블 요청 답신 메시지는 사용자 ID를 포함한다. 인에이블 요청 답신 메시지는 암호화되고 서명되며, 이에 따라, 인에이블 요청 답신 메시지가 송신 프로세스에서 변조되는 것을 효과적으로 방지한다. 인에이블 요청 답신 메시지는 사용자 ID를 포함하고, 인에이블 레코드는 사용자 ID를 이용하여 생성되므로, 인에이블 레코드가 올바른 사용자 ID 및 대응하는 지문 템플릿 ID를 레코딩하는 것을 효과적으로 보장한다. 따라서, 후속 단계들에서의 검증 정확도가 보장된다.

[0095] 따라서, 이 실시예의 인에이블 요청 답신 메시지에는 사용자 ID가 더 포함되고, 인에이블 레코드에는 사용자 ID 및 지문 템플릿 ID가 포함된다. 인에이블 응답 메시지에는 또한 사용자 ID 및 지문 템플릿 ID가 포함된다. 따라서, 서버 단말은, 인에이블 응답 메시지를 수신한 후, 사용자 ID 및 지문 템플릿 ID를 획득하고, 사용자 레코드를 생성하고 저장한다. 사용자 레코드에는 사용자 ID 및 지문 템플릿 ID가 포함된다.

[0096] 이러한 방식으로, 사용자가 사용자 ID를 이용하여 클라이언트 단말에 로그온한 후, 사용자 ID에 따라 대응하는 인에이블 레코드가 검색된다. 인에이블 레코드 내의 지문 템플릿 ID와 사용자 ID간의 매칭이 수행될 수 있다. 복수의 사용자들에 의한 하나의 클라이언트 단말의 공유가 지원될 수 있다. 마찬가지로, 서버 단말에서, 사용자 ID에 따라 사용자 레코드가 또한 검색되고, 대응하는 지문 템플릿 ID를 비교하여 검증이 수행된다.

[0097] 또한, 사용자가 복수의 단말 디바이스들을 갖는 경우, 상이한 단말 디바이스들을 구별하기 위해, 인에이블 응답 메시지에는, 사용자의 상이한 디바이스들을 더 구별하기 위한 디바이스 ID가 더 포함된다. 따라서, 서버 단말은 사용자 ID, 디바이스 ID, 및 지문 템플릿 ID를 포함하는 사용자 레코드를 저장한다. 사용자가 복수의 디바이스들을 갖는 경우, 서버 단말은 인식 및 검증을 구현하기 위해, 사용자의 상이한 디바이스들에 대응하는 상이한 사용자 레코드들을 저장한다. 마찬가지로, 사용자가 상이한 단말 디바이스들을 이용하는 경우, 본 발명의 전술한 단계들에 기초하여, 사용자의 상이한 단말 디바이스들이 서로 구별되어 검증이 수행될 수 있다. 즉, 비교 동안, 대응하는 인에이블 레코드 및 사용자 레코드가 디바이스 ID에 따라 더 검색되고, 지문 템플릿 ID를 매칭된 인에이블 레코드 및 사용자 레코드 내의 지문 템플릿 ID와 비교함으로써 검증이 수행된다.

[0098] 바람직하게는, 검증 프로세스에서 재생 공격을 더 방지하기 위해, 이 실시예의 인에이블 프로세스에서, 챌린지 응답(challenge-response) 방식이 또한 보안을 강화시키기 위해 이용된다. 즉, 단계 ②에서, 인에이블 요청 답신 메시지는 챌린지 값을 더 운반한다. 챌린지 응답 방식은 신원 인증에서 자주 이용되는 방법 중 하나이다. 따라서, 클라이언트 단말로부터 인에이블 요청을 수신한 후, 서버 단말은 챌린지 값을 생성하고, 챌린지 값을 운반하는 인에이블 요청 답신 메시지를 클라이언트 단말에 전송한다. 후속 단계에서, 응답 값을 검증함으로써 검증이 수행된다. 챌린지 값은 랜덤 알고리즘(random algorithm)을 이용하여 신원 인증 프로세스에서 생성된다. 난수의 생성을 위해, 의사 랜덤 알고리즘(pseudo-random algorithm) 및 스트롱 랜덤 알고리즘(strong random algorithm)이 종래 기술에서 제공된다. 이 실시예에서는, 스트롱 랜덤 알고리즘이 이용되고, 획득된 난수는 보다 균일하게 분포된다. 인에이블 요청 답신 메시지를 수신한 후, 클라이언트 단말은 또한 응답 값을 생성할 필요가 있다. 인에이블 응답 메시지는 응답 값을 운반하고 응답 값은 서버 단말에 전송된다. 서버 단말은 인에이블 응답 메시지를 검증할 필요가 있다.

[0099] 단계 ③ 이후, 이 실시예는 다음의 단계들을 더 포함한다:

[0100] 클라이언트 단말에 의해, 인에이블 요청 답신 메시지에 포함된 챌린지 값에 따라 서명 알고리즘을 선택하고, 사용자 공개키 및 개인키 쌍을 생성하는 단계 - 여기서, 상기 저장된 인에이블 레코드는 사용자 개인키를 포함함 -;

[0101] 선택된 서명 알고리즘 및 합의된 제2 개인키를 이용하여 인에이블 응답 메시지에 서명하는 단계 - 여기서, 인에이블 응답 메시지는 상기 생성된 사용자 공개키를 포함함 -; 및

[0102] 마찬가지로, 챌린지 값에 따라 선택된 서명 알고리즘과 합의된 제2 공개키를 이용하여 인에이블 응답 메시지를 검증하고, 검증이 성공된 후 사용자 공개키를 포함하는 사용자 레코드를 저장하거나 또는 검증이 실패한 경우 오류를 보고하는 단계.

[0103] 수신된 챌린지 값에 따라 서명 알고리즘이 선택되는 경우, 예를 들어, 서명 알고리즘 1, 서명 알고리즘 2, 서명 알고리즘 3, 및 서명 알고리즘 4의 4개의 서명 알고리즘들이 선택될 수 있다. 상기 알고리즘은 챌린지 값의 나누기 후에 얻어지는 나머지 값에 따라 선택될 수 있다. 챌린지 값을 4로 나눈 후에 나머지 값이 0이면, 서명 알고리즘 1이 선택된다. 나머지 값이 1이면, 서명 알고리즘 2가 선택된다. 나머지 것들은 유추하여 도출될 수 있다.

[0104] 특정 서명 알고리즘은 RAS-SHA1 또는 RSA-SHA256과 같은 보안 해시 알고리즘(Secure Hash Algorithm)일 수 있다. 전술한 서명 알고리즘은 균일한 사용자 공개키 및 개인키 생성 알고리즘에 대응한다. 검증 기능이 인에이블될 때 사용자 공개키 및 개인키의 쌍이 생성되며, 후속 지문 검증 시 암호화 및 암호해제에 이용된다. 따라서, 각 사용자는 자신의 사용자 공개키 및 개인키 쌍을 가지며, 여기서 사용자 공개키 및 개인키 쌍은 사용자 개인키 및 사용자 공개키를 포함한다.

[0105] 인에이블 응답 메시지가 전송되기 전에, 이 실시예에서, 인에이블 응답 메시지는 선택된 서명 알고리즘 및 합의된 제2 개인키를 이용하여 서명된다. 여기서, 제2 개인키는 클라이언트 단말의 하드웨어에 의해 결정된다. 이에 대응하여, 서버 단말은 대응하는 제2 공개키를 갖는다.

[0106] 알고리즘은 이 실시예에서 챌린지 값의 나누기 후에 얻어지는 나머지 값에 따라 선택된다는 점에 유의해야 한다. 알고리즘은 챌린지 값의 1자리 숫자 및 10자리 숫자에 따라 또는 챌린지 값을 4로 나눈 후에 얻어지는 값에 따라 직접 선택될 수도 있다. 본 발명은 특정 선택 방식으로 제한되지 않는다.

[0107] 서버에 의해 인에이블 응답 메시지를 검증하는 프로세스는 다음의 두 개의 검증 단계들을 포함한다:

[0108] 1) 제2 공개키와 서명 알고리즘을 이용하여 서명이 검증된다.

[0109] 서버 단말에서, 챌린지 값은 나머지 값을 얻기 위해 클라이언트 단말에 의해 이용된 것과 동일한 방법을 이용하여 나누기된다. 대응하는 서명 알고리즘이 선택되고, 서명된 응답 메시지는 합의된 제2 공개키에 따라 검증된다.

[0110] 2) 클라이언트 단말에 의해 이용된 것과 동일한 알고리즘을 이용하여 응답 값이 계산되고, 획득된 응답 값을 응답 메시지 내의 응답 값과 비교하여 검증이 수행된다.

[0111] 지문 검증 프로세스에서, 클라이언트 단말은, 인에이블 요청 답신 메시지를 수신한 후, 응답할 필요가 있고 서버 단말에게 응답 메시지를 회신한다. 응답 메시지에는 챌린지 값에 따라 고정 알고리즘을 이용하여 계산된 응답 값이 포함되어, 서버 단말이 동일한 알고리즘에 따라 응답 값을 계산하고, 그 후 응답 값들을 비교하여 검증을 수행할 수 있도록 한다.

[0112] 이러한 방식으로, 검증이 성공된 후, 서버 단말은 대응하는 사용자 레코드를 저장한다. 서버 단말에 의해 저장된 사용자 레코드에는 사용자 ID, 디바이스 ID, 사용자 공개키, 및 지문 템플릿 ID가 포함되어, 후속 검증 프로세스에서 결과 검증이 수행될 수 있도록 한다.

[0113] 이 실시예에서, 인에이블 요청 답신 메시지에는 사용자 ID 및 챌린지 값이 포함된다. 인에이블 레코드에는 사용자 개인키, 사용자 ID, 및 지문 템플릿 ID가 포함된다. 인에이블 응답 메시지에는 사용자 공개키, 사용자 ID, 디바이스 ID, 및 지문 템플릿 ID가 포함된다. 서버 단말에 의해 저장된 사용자 레코드는 사용자 ID, 디바이스 ID, 지문 템플릿 ID, 및 사용자 공개키가 포함된다.

[0114] 실시예 2: 사용자에 의한 이용 동안의 지문 인증 프로세스

[0115] 사용자가 인터넷 결제를 이용할 때, 사용자의 지문은 검증될 필요가 있다. 도 2에서 도시된 바와 같이, 다음의 단계들이 수행된다:

[0116] (1) 클라이언트 단말은 서버 단말에게 인증 요청을 전송하고, 서버 단말은 클라이언트 단말로부터 인증 요청을 획득한다.

[0117] (2) 인증 요청을 수신한 후, 서버 단말은 인증 요청 답신 메시지를 클라이언트 단말에게 전송한다.

[0118] (3) 클라이언트 단말은, 인증 요청 답신 메시지를 수신한 후, 사용자에 의해 입력되고 검증에 이용되는 지문 이미지를 수신하고, 검증에 이용되는 지문 이미지에 대응하는 지문 템플릿 ID를 획득하며, 이 지문 템플릿 ID를, 클라이언트 단말에 의해 저장된 인에이블 레코드 내의 지문 템플릿 ID와 비교한다. 이 두 개의 지문 템플릿 ID들이 일치하면 다음 단계가 수행되고, 그렇지 않으면 오류가 보고된다.

[0119] 결제 프로세스에서의 지문 검증 동안, 사용자는 프롬프트 인터페이스에 따라 결제에 이용되는 손가락을 지문 스캐너 상에 올려놓고, 검증에 이용되는 지문 이미지를 입력할 필요만 있을 뿐이다. 클라이언트 단말은 저장된 지문 템플릿들로부터 대응하는 지문 템플릿을 찾고, 지문 템플릿 ID를 획득하고, 사용자 ID에 따라 대응하는 인에이블 레코드를 찾고, 이 획득된 지문 템플릿 ID를 인에이블 레코드 내의 지문 템플릿과 비교한다. 획득된 지문 템플릿 ID가 인에이블 레코드 내의 것과 일치하면, 검증은 성공된 것이며, 그렇지 않은 경우에는 오류가 보고되고 검증은 실패로 끝난다.

[0120] 예를 들어, 지문 검증 기능이 인에이블될 때 사용자가 검지 손가락을 이용하면, 인에이블 레코드는 "검지 손가락"의 지문 템플릿 ID를 저장한다. 검증 동안, 사용자에 의해 단말에 입력되는 지문에 대응하는 지문 템플릿 ID가 "검지 손가락"의 지문 템플릿 ID인지의 여부, 즉, 지문 템플릿 ID가 인에이블 레코드 내에 저장된 지문 템플릿 ID와 일치하는지의 여부가 먼저 식별된다.

[0121] 이 실시예에서, 지문 템플릿 ID는 클라이언트 단말에서 국부적으로 비교된다. 네트워크를 통해 사용자의 지문을 송신할 필요가 없으므로, 사용자의 생체 특징의 유출을 방지할 수 있다.

[0122] (4) 클라이언트 단말은 획득된 지문 템플릿 ID를 포함하는 인증 응답 메시지를 생성하고, 이 인증 응답 메시지를 서버 단말에 전송한다.

[0123] (5) 서버 단말은 인증 응답 메시지를 수신하고, 이 메시지에 포함된 지문 템플릿 ID를, 국부적으로 저장된 대응하는 사용자 레코드 내의 지문 템플릿 ID와 비교한다. 지문 템플릿 ID들이 일치하면 검증은 성공된 것이며, 그렇지 않은 경우에는 오류가 보고된다.

[0124] 이 실시예의 지문 인증 프로세스에서, 지문 검증을 수행한 후, 클라이언트 단말은 지문 템플릿 대신에 지문 템플릿 ID를 서버 단말에 전송할 필요만 있을 뿐이다. 서버 단말은 지문 템플릿 ID를, 사용자 레코드 내의 지문 템플릿 ID와 다시 비교한다. 지문 인증은 두 번의 비교들을 통해 심화적으로 수행되므로, 보다 높은 보안이 달성된다. 또한, 지문 템플릿 ID의 송신은 송신 프로세스에서 낮은 송신 트래픽을 소모하며, 서버 단말의 연산량도 작다.

[0125] 실시예 1과 마찬가지로, 사용자들을 구별하고 사용자들의 단말 디바이스들을 구별하기 위해, 인증 요청 답신 메시지에는 사용자 ID가 포함된다. 따라서, 클라이언트 단말은 사용자 ID에 따라 대응하는 인에이블 레코드를 국부적으로 검색하고, 획득된 지문 템플릿 ID를 인에이블 레코드 내의 지문 템플릿 ID와 비교한다. 또한, 인증 응답 메시지에는 디바이스 ID, 사용자 ID, 및 지문 템플릿 ID가 포함된다. 서버 단말은 인증 응답 메시지에 따라 대응하는 사용자 레코드를 찾고, 지문 템플릿 ID와 국부적으로 저장된 대응하는 사용자 레코드 내의 지문 템플릿 ID를 비교한다. 지문 템플릿 ID가 일치하면, 검증이 성공한 것으로 간주되어, 검증 프로세스는 종료되며; 그렇지 않은 경우에는, 오류가 보고되고 검증은 실패로 끝난다.

[0126] 실시예 1과 마찬가지로, 실시예 2에서, 인증 요청 답신 메시지는 제1 개인키를 이용하여 암호화될 수도 있다. 그 후, 클라이언트 단말은 이 메시지를 암호해제하고 제1 공개키를 이용하여 이 메시지를 검증한다.

[0127] 지문 검증의 인증 프로세스에서, 이 실시예는 여전히 챌린지 응답 방식에 기초하여 검증을 수행한다는 것을 유의해야 한다. 마찬가지로, 인증 요청 답신 메시지에는 챌린지 값이 포함된다. 클라이언트 단말은 챌린지 값에 따라 서명 알고리즘을 선택한다. 서명 알고리즘에서 이용되는 키는 제2 개인키일 수 있다. 이 경우, 서버 단말은 제2 공개키를 이용하여 검증을 수행한다.

[0128] 바람직하게는, 인증 응답 메시지는 인에이블 레코드 내의 사용자 개인키를 이용하여 서명된다. 서버 단말은 또한 챌린지 값에 따라 서명 알고리즘을 선택하고, 사용자 레코드 내의 사용자 공개키를 이용하여 인증 응답 메시지를 검증한다. 검증 프로세스는 실시예 1에서의 응답 메시지의 검증 프로세스와 동일하되, 이용되는 키들만이 다르다. 실시예 1에서는, 제2 공개키를 이용하여 검증을 수행하는 반면에, 실시예 2에서는, 사용자 공개키를 이용하여 검증을 수행한다. 사용자 공개키 및 개인키 쌍은 각 사용자마다 고유하기 때문에, 인증 프로세스에서의 보안이 더욱 보장된다.

[0129] 즉, 클라이언트 단말은 챌린지 값에 따라 서명 알고리즘을 선택하고, 선택된 서명 알고리즘과 사용자 개인키를 이용하여 인증 응답 메시지에 서명한다. 서버 단말은, 인증 응답 메시지를 수신한 후에, 챌린지 값에 따라 서명 알고리즘을 선택하고, 서명 알고리즘 및 사용자 공개키를 이용하여 인증 응답 메시지를 검증한다.

[0130] 실시예 1과는 달리, 이 단계에서 인증 요청 답신 메시지는 서비스 정보를 더 포함하여, 클라이언트 단말이 인증 요청 답신 메시지를 수신한 후에 이 서비스 정보를 디스플레이할 수 있도록 한다. 사용자는, 디스플레이된 서비스 정보에 따라, 본 서비스가 사용자가 현재 수행하고 있는 지문 검증에 대응하는 서비스인지 여부를 판단할 수 있다. 이에 해당하는 경우, 사용자는 작업을 계속하는 것을 선택하며, 그렇지 않은 경우에는, 사용자는 지문 인증을 포기할 수 있다.

[0131] 인에이블 프로세스 및 후속 검증 프로세스 둘 다에서, 본 발명은 난수에 따라 서명 알고리즘을 선택한다. 그러나, 서명을 행하기 위해 선택된 서명 알고리즘의 개수는 하나로 국한되지 않으며, 서명 연산을 수행하기 위해 다중 알고리즘들의 조합이 또한 선택될 수 있으며, 이에 따라 알고리즘들의 다양성을 증가시킨다. 예를 들어, 임의의 숫자의 1자리 숫자와 10자리 숫자에 따라 두 개의 서명 알고리즘들이 선택된다. 서명 보안은 두 번의 연속적인 서명 작업들을 통해 더욱 강화된다. 이 실시예에서, 응답 메시지에 대한 서명 검증을 위해 랜덤 서명 알고리즘이 이용되기 때문에, 사용자 개인키가 유출되더라도 공격자는 서명 알고리즘을 알지 못하고, 응답 메시지를 위조할 수 없다.

[0132] 종래 기술에서, FIDO(Fast Identity Online) 연맹에 의해 제안된 검증 해결책은 패스워드, 웹페이지 플러그인, 및 검증 하드웨어를 포함한다. 다양한 검증 하드웨어, 예를 들어, USB 플래시 디스크(또는 USB 키), NFC(Near Field Communication) 칩, TPM(Trusted Platform Module) 칩, 및 지문 스캐너, 음성 인식 하드웨어, 얼굴 인식 하드웨어, 및 홍채 인식 하드웨어와 같은 생체 인식 하드웨어가 존재한다. FIDO 연맹에 의해 제안된 검증 방법을 이용함으로써, 사용자 패스워드는 발송되지 않을 것이지만, 휴대 전화 또는 컴퓨터와 같은 디바이스 내부에서 소프트웨어를 이용하여 처리된다. 검증이 성공된 후, 소프트웨어는 로그인 서버에 키를 전송하고, 로그인 정보는 저장되지 않는다. 동시에, 로그인 서버는 "인증을 통과했다"는 것을 통지하기 위해 사용자 장비에 키를 전송한다. 기업이 FIDO 연맹의 인증 방식을 이용하려는 경우, 서버 상에 검증 소프트웨어를 설치한 다음, 고객 또는 직원의 디바이스들 상에 대응하는 플러그인 또는 애플리케이션 프로그램을 설치하는 것만이 필요할 뿐이다. 그러나, 지문 검증을 예로 들면, FIDO 연맹에 의해 제안된 지문 검증의 인에이블링은 디바이스에만 결속될 수 있다. 즉, 지문 검증이 인에이블된 후, 디바이스 상의 모든 지문 템플릿들을 이용하여 지문 검증을 완료할 수 있다. 지문 검증이 인에이블된 후에 추가된 지문 템플릿을 이용하여 검증을 완료할 수도 있다. 그러나, 일반적으로, 지문 템플릿을 추가하려면 간단한 패스워드(예컨대, 4자리 패스워드)만을 입력하면 된다. 이것은 보안 취약점이 되어, 보안 허점을 야기시킨다. 또한, 서버 단말로부터의 메시지에는 서명이 없으므로, 디바이스 단말에서의 모듈들은 위조 메시지를 통해 공격받을 수 있다. 그러나, 본 발명에서는, 인에이블 프로세스에서 인에이블 레코드 및 사용자 레코드가 저장되고, 지문 검증에 이용되는 지문 템플릿 ID가 추후에 수정될 수 없음에 따라, 지문 검증이 인에이블된 후에 지문 템플릿이 추가되는 것을 방지할 수 있다. 또한, 챌린지 값을 이용하여 서명 알고리즘이 선택되고, 검증 프로세스에서 서명이 추가됨에 따라, 위조 메시지를 통한 공격을 방지한다.

[0133] 도 3에서 도시된 바와 같이, 본 발명은 신원 인증 시스템에 적용되는 클라이언트 단말을 더 제공한다. 신원 인증 시스템은 서버 단말을 더 포함한다. 클라이언트 단말은 인에이블 레코드를 저장하고, 서버 단말은 사용자 레코드를 저장한다. 인에이블 레코드 및 사용자 레코드 둘 다는 생체 특징 검증에 이용되고 생체 특징 검증을 인에이블시키는 프로세스에서 획득되는 생체 특징 템플릿 ID를 포함한다. 클라이언트 단말은,

[0134] 서버 단말에 인증 요청을 전송하고, 서버 단말에 의해 회신된 인증 요청 답신 메시지를 수신하도록 구성된 요청 모듈; 및

[0135] 사용자에 의해 입력되는 생체 특징을 수신하고, 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하고, 획득된 생체 특징 템플릿 ID와 국부적으로 저장된 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교하고, 상기 두 개의 생체 특징 템플릿 ID들이 일치하면 획득된 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 생성하며, 인증 응답 메시지를 서버 단말에 전송하여, 서버 단말이 인증 응답 메시지를 수신하고 생체 특징 템플릿 ID를 국부적으로 저장된 사용자 레코드 내의 생체 특징 템플릿 ID와 비교하여 검증을 수행하도록 하거나, 또는 상기 두 개의 생체 특징 템플릿 ID들이 불일치하면 오류를 보내도록 구성된 응답 모듈을 포함한다.

[0136] 더 나아가, 요청 모듈은 또한, 생체 특징 검증을 인에이블시키기 위한 인에이블 요청을 서버 단말에 전송하고, 서버 단말에 의해 회신된 인에이블 요청 답신 메시지를 수신하도록 구성된다. 응답 모듈은 또한, 사용자에 의해 입력되고 검증에 이용되는 생체 특징을 수신하고, 검증에 사용되는 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하고, 인에이블 레코드를 생성하고 저장하고, 생체 특징 템플릿 ID를 포함하는 인에이블 응답 메시지를 생성하고, 서버 단말이 인에이블 응답 메시지를 수신하고, 이 메시지에 포함된 생체 특징 템플릿 ID를 획득하며, 사용자 레코드를 생성하고 저장할 수 있도록, 인에이블 응답 메시지를 서버 단말에 전송하도록 구성된다.

[0137] 또한, 서버 단말은 합의된 제1 개인키를 이용하여 인증 요청 답신 메시지 또는 인에이블 요청 답신 메시지에 서명하고, 그 후 인증 요청 답신 메시지를 수신한 후, 요청 모듈은 또한, 합의된 제1 공개키를 이용하여 상기 수신된 인증 요청 답신 메시지를 검증하도록 구성되고, 여기서 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우 오류가 보고된다. 인에이블 요청 답신 메시지를 수신한 후, 요청 모듈은 또한, 합의된 제1 공개키를 이용하여 상기 수신된 인에이블 요청 답신 메시지를 검증하도록 구성되고, 여기서 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우 오류가 보고된다.

[0138] 본 발명에서, 인에이블 요청 답신 메시지는 챌린지 값을 운반한다. 응답 모듈은 또한, 사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 사용자 개인키를 저장하며; 인에이블 요청 답신 메시지에서의 챌린지 값에 따라 서명 알고리즘을 선택하고, 선택된 서명 알고리즘 및 합의된 제2 개인키를 이용하여 상기 생성된 인에이블 응답 메시지에 서명한 후, 서명된 인에이블 응답 메시지를 서버 단말에 전송하도록 구성된다. 인에이블 응답 메시지는 사용자 공개키를 포함하여, 서버 단말이 인에이블 응답 메시지를 수신하고, 합

의된 제2 공개키를 이용하여 인에이블 응답 메시지를 검증할 수 있도록 하며, 사용자 공개키는 서버 단말에 저장된다.

[0139] 또한, 인증 요청 답신 메시지는 챌린지 값을 운반한다. 응답 모듈은 또한 챌린지 값에 따라 서명 알고리즘을 선택하고, 선택된 서명 알고리즘과 사용자 개인키를 이용하여 인증 응답 메시지에 서명하도록 구성됨으로써, 서버 단말이 또한 인증 응답 메시지를 수신한 후에 챌린지 값에 따라 서명 알고리즘을 선택하고, 서명 알고리즘과 사용자 공개키를 이용하여 인증 응답 메시지를 검증할 수 있도록 한다.

[0140] 또한, 인에이블 요청 답신 메시지에는 사용자 ID가 더 포함된다. 응답 모듈은 또한 사용자 ID를 인에이블 레코드에 저장하도록 구성된다. 생성된 인에이블 응답 메시지에는 사용자 ID가 더 포함되어, 서버 단말이, 인에이블 응답 메시지를 수신한 후, 인에이블 응답 메시지 내에서 사용자 ID를 획득하고 이 사용자 ID를 사용자 레코드에 저장할 수 있도록 한다.

[0141] 또한, 인에이블 응답 메시지에는 클라이언트 단말 디바이스 ID가 더 포함되어, 서버 단말이, 인에이블 요청 답신 메시지를 수신한 후, 인에이블 요청 답신 메시지 내에서 클라이언트 단말 디바이스 ID를 획득하고 이 디바이스 ID를 사용자 레코드에 저장할 수 있도록 한다.

[0142] 또한, 인증 요청 답신 메시지에는 사용자 ID가 더 포함된다. 사용자에 의해 입력되는 생체 특징을 수신하고 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득한 후, 응답 모듈은 또한, 사용자 ID에 따라 대응하는 인에이블 레코드를 검색하여, 획득된 생체 특징 템플릿 ID와 찾아낸 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교하도록 구성된다.

[0143] 응답 모듈에 의해 생성된 인증 응답 메시지에는 사용자 ID가 더 포함되어, 서버 단말이, 인증 응답 메시지를 수신한 후, 인증 응답 메시지 내에서 사용자 ID를 획득하고 사용자 ID에 따라 대응하는 사용자 레코드를 검색할 수 있도록 한다.

[0144] 또한, 인증 응답 메시지에는 클라이언트 단말 디바이스 ID가 더 포함되어, 서버 단말이, 인증 응답 메시지를 수신한 후, 인증 응답 메시지 내에서 상기 클라이언트 단말 디바이스 ID를 획득하고 상기 클라이언트 단말 디바이스 ID에 따라 대응하는 사용자 레코드를 검색할 수 있도록 한다.

[0145] 도 4에서 도시된 바와 같이, 본 발명은 전술한 서버 단말에 대응하는 서버를 더 제공한다. 서버는 신원 인증 시스템에 적용된다. 신원 인증 시스템은 클라이언트 단말을 더 포함한다. 클라이언트 단말은 인에이블 레코드를 저장하고, 서버는 사용자 레코드를 저장한다. 인에이블 레코드 및 사용자 레코드 둘 다는 생체 특징 검증에 이용되고 생체 특징 검증을 인에이블시키는 프로세스에서 획득되는 생체 특징 템플릿 ID를 포함한다. 서버 단말은,

[0146] 클라이언트 단말로부터 인증 요청을 수신하고, 인증 요청 답신 메시지를 클라이언트 단말에 전송하도록 구성된 답신 모듈; 및

[0147] 클라이언트 단말로부터 생체 특징 템플릿 ID를 포함하는 인증 응답 메시지를 수신하며; 인증 응답 메시지 내의 생체 특징 템플릿 ID와 상기 저장된 사용자 레코드 내의 생체 특징 템플릿 ID를 비교하여 검증을 수행하도록 구성된 검증 모듈을 포함하며, 여기서, 이 두 개의 생체 특징 템플릿 ID들이 일치하면 검증은 성공된 것이며, 그렇지 않은 경우에는 오류가 보고된다.

[0148] 더 나아가, 답신 모듈은 또한, 클라이언트 단말로부터 생체 특징 검증을 인에이블시키기 위한 인에이블 요청을 수신하고, 클라이언트 단말에게 인에이블 요청 답신 메시지를 전송하도록 구성됨으로써, 클라이언트 단말이, 검증에 이용되고 사용자에 의해 입력되는 생체 특징에 따라, 검증에 이용되는 생체 특징에 대응하는 생체 특징 템플릿 ID를 획득하고, 인에이블 레코드를 생성하고 인에이블 레코드를 저장할 수 있도록 한다. 검증 모듈은 또한, 클라이언트 단말로부터 인에이블 응답 메시지를 수신하고, 인에이블 응답 메시지에 포함된 생체 특징 템플릿 ID를 획득하며, 사용자 레코드를 생성하고 저장하도록 구성된다.

[0149] 더 나아가, 답신 모듈은 또한, 합의된 제1 개인키를 이용하여 인증 요청 답신 메시지 또는 인에이블 요청 답신 메시지에 서명하도록 구성됨으로써, 클라이언트 단말이, 합의된 제1 공개키를 이용하여 상기 수신된 인증 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 할 수 있도록 하거나; 또는 클라이언트 단말이, 합의된 제1 공개키를 이용하여 상기 수신된 인에이블 요청 답신 메시지를 검증 - 상기 검증이 성공된 경우에만 후속 응답이 행해지고, 그렇지 않은 경우에는 오류가 보고됨 - 할 수 있도록 한다.

[0150] 본 발명에서, 인에이블 요청 답신 메시지는 챌린지 값을 운반한다. 클라이언트 단말은 사용자 개인키와 사용자 공개키를 포함하는 사용자 공개키 및 개인키 쌍을 생성하고, 사용자 개인키를 저장한다. 검증 모듈은 또한, 선택된 서명 알고리즘 및 합의된 제2 개인키를 이용하여 클라이언트 단말에 의해 서명된 인에이블 응답 메시지를 수신하고 - 여기서 서명 알고리즘은 인에이블 요청 답신 메시지 내의 챌린지 값에 따라 클라이언트 단말에 의해 선택되고, 인에이블 응답 메시지는 사용자 공개키를 포함함 -; 그리고 또한 챌린지 값에 따라 서명 알고리즘을 선택하고, 제2 공개키를 이용하여 인에이블 응답 메시지를 검증하도록 구성된다. 사용자 공개키는 서버 단말에 저장된다.

[0151] 더 나아가, 검증 모듈은 또한, 선택된 서명 알고리즘 및 사용자 개인키를 이용하여 클라이언트 단말에 의해 서명된 인증 응답 메시지를 수신하고 - 여기서 서명 알고리즘은 인증 요청 답신 메시지 내의 챌린지 값에 따라 클라이언트 단말에 의해 선택됨 -; 그리고 또한 챌린지 값에 따라 서명 알고리즘을 선택하며, 서명 알고리즘 및 사용자 공개키를 이용하여 인증 응답 메시지 상의 서명을 검증하도록 구성된다.

[0152] 또한, 인에이블 요청 답신 메시지에는 사용자 ID가 더 포함되어, 클라이언트 단말이 인에이블 요청 답신 메시지를 수신한 후에 인에이블 레코드에 사용자 ID를 저장할 수 있도록 한다. 클라이언트 단말에 의해 생성된 인에이블 응답 메시지에는 사용자 ID가 더 포함된다. 검증 모듈은 또한, 인에이블 응답 메시지를 수신한 후, 인에이블 응답 메시지로부터 사용자 ID를 획득하고 사용자 레코드에 사용자 ID를 저장하도록 구성된다.

[0153] 또한, 인에이블 응답 메시지에는 클라이언트 단말 디바이스 ID가 더 포함된다. 검증 모듈은 또한, 인에이블 응답 메시지를 수신한 후, 인에이블 응답 메시지로부터 클라이언트 단말 디바이스 ID를 획득하고 사용자 레코드에 클라이언트 단말 디바이스 ID를 저장하도록 구성된다.

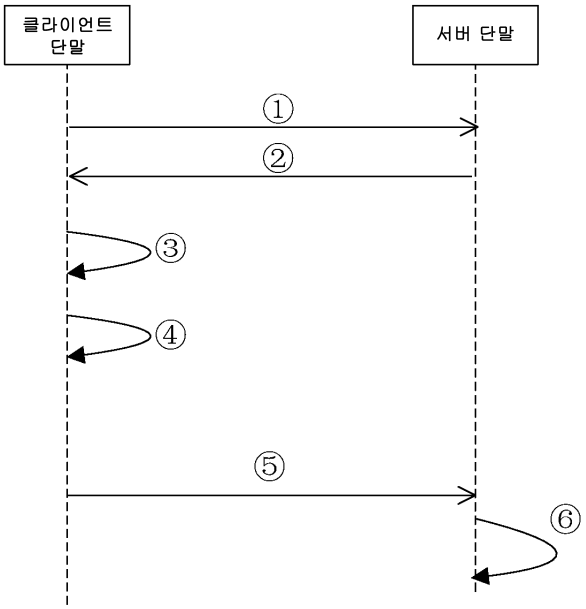
[0154] 또한, 인증 요청 답신 메시지에는 사용자 ID가 더 포함되어, 클라이언트 단말이 사용자 ID에 따라 대응하는 인에이블 레코드를 검색하고, 획득된 생체 특징 템플릿 ID와 찾아낸 인에이블 레코드 내의 생체 특징 템플릿 ID를 비교할 수 있도록 한다. 클라이언트 단말에 의해 생성된 인증 응답 메시지에는 사용자 ID가 더 포함된다. 검증 모듈은 또한, 인증 응답 메시지를 수신한 후, 인증 응답 메시지에서 사용자 ID를 획득하고, 사용자 ID에 따라 대응하는 사용자 레코드를 검색하도록 구성된다.

[0155] 또한, 인증 응답 메시지에는 클라이언트 단말 디바이스 ID가 더 포함된다. 검증 모듈은 또한, 인증 응답 메시지를 수신한 후, 인증 응답 메시지에서 클라이언트 단말 디바이스 ID를 획득하고, 클라이언트 단말 디바이스 ID에 따라 대응하는 사용자 레코드를 검색하도록 구성된다.

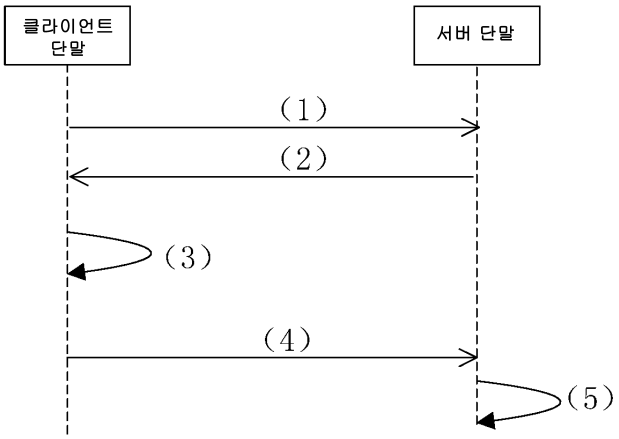
[0156] 전술한 실시예들은 단지 본 발명의 기술적 해결책을 설명하기 위해 이용된 것일 뿐이지, 본 발명을 제한하고자 하는 것은 아니다. 본 업계의 당업자들은 본 발명의 사상과 본질을 벗어나지 않고서 본 발명에 따라 다양한 대응하는 변형 및 수정을 취할 수 있다. 이러한 대응하는 변형 및 수정은 본 발명의 첨부된 청구범위의 보호 범위에 속해야 한다.

도면

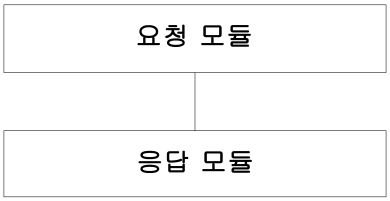
도면1



도면2



도면3



도면4