(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0092950
(43) 공개일자 2020년08월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3231 (2013.01)
H04L 63/0435 (2013.01)
(21) 출원번호 10-2020-7013863
(22) 출원일자(국제) 2018년11월14일
심사청구일자 없음
(85) 번역문제출일자 2020년05월14일
(86) 국제출원번호 PCT/SE2018/051169
(87) 국제공개번호 WO 2019/108111
국제공개일자 2019년06월06일
(30) 우선권주장
1751469-6 2017년11월29일 스웨덴(SE)

(71) 출원인
핑거프린트 카드즈 에이비
스웨덴 예테보리 411 19 쿵스가탄 20
(72) 발명자
게르만 크리스티안
스웨덴 227 38 룬드 후드베겐 2
포프 스티븐
덴마크 2840 홀테 콩 발데마스 바이 33
(74) 대리인
특허법인(유한)케이비케이

전체 청구항 수 : 총 30 항

(54) 발명의 명칭 **지문의 2단계 중앙 일치**

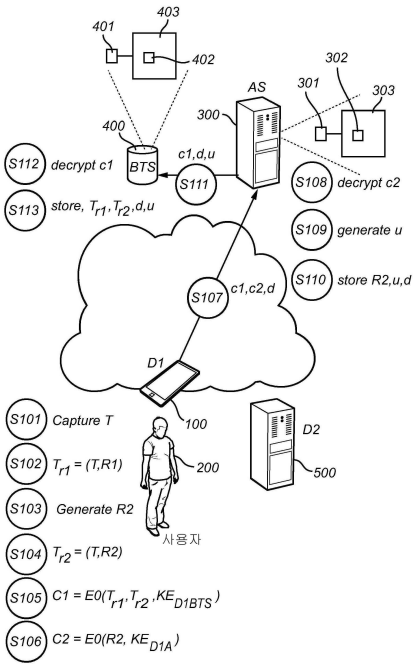
(57) 요 약

본 발명의 제 1 태양에서, 클라이언트 디바이스(100)가 보안 통신 채널을 통한 네트워크 노드(300)로 상기 클라이언트 디바이스의 사용자(200)의 생체 데이터를 등록하는 방법이 제공된다.

상기 방법은 사용자(200)의 생체 데이터를 캡처하는 단계(S101); 사용자(200)가 인증되는 임의의 다른 클라이언

(뒷면에 계속)

대 표 도 - 도4



트 디바이스(500)와 공유되는 제 1 특징 변환 키를 사용하여 생체 데이터를 변환된 제 1 생체 데이터 세트로 변환하는 단계(S102); 제 2 특징 변환 키를 생성하는 단계(S103); 제 2 특징 변환 키를 사용하여 생체 데이터를 변환된 제 2 생체 데이터 세트로 변환하는 단계(S104)를 포함한다. 상기 방법은 사용자(200)가 인증되는 생체 데이터 검증 노드(400)와 공유되는 암호화 키로 변환된 제 1 및 제 2 생체 데이터 세트를 암호화하는 단계(S105); 변환된 제 1 및 제 2 생체 데이터의 세트가 등록되는 네트워크 노드(300)와 공유되는 암호화 키로 제 2 특징 변환 키를 암호화하는 단계(S106); 및 암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 암호화된 제 2 특징 변환 키 및 사용자 프로파일 데이터를 포함하는 등록 요청을 네트워크 노드(300)에 제출하는 단계(S107)를 더 포함한다.

(52) CPC특허분류
H04L 63/0478 (2013.01)
H04L 63/061 (2013.01)
H04L 63/0861 (2013.01)
H04L 63/102 (2013.01)
H04L 63/123 (2013.01)
H04L 63/126 (2013.01)
H04L 9/0866 (2013.01)

명 세 서

청구범위

청구항 1

클라이언트 디바이스(100)가 보안 통신 채널을 통한 네트워크 노드(300)로 상기 클라이언트 디바이스의 사용자(200)의 생체 데이터를 등록하는 방법으로서,

사용자(200)의 생체 데이터를 캡처하는 단계(S101);

사용자(200)가 인증되는 임의의 다른 클라이언트 디바이스(500)와 공유되는 제 1 특징 변환 키를 사용하여 생체 데이터를 변환된 제 1 생체 데이터 세트로 변환하는 단계(S102);

제 2 특징 변환 키를 생성하는 단계(S103);

제 2 특징 변환 키를 사용하여 생체 데이터를 변환된 제 2 생체 데이터 세트로 변환하는 단계(S104);

사용자(200)가 인증되는 생체 데이터 검증 노드(400)와 공유되는 암호화 키로 변환된 제 1 및 제 2 생체 데이터 세트를 암호화하는 단계(S105);

변환된 제 1 및 제 2 생체 데이터의 세트가 등록되는 네트워크 노드(300)와 공유되는 암호화 키로 제 2 특징 변환 키를 암호화하는 단계(S106); 및

암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 암호화된 제 2 특징 변환 키 및 사용자 프로파일 데이터를 포함하는 등록 요청을 네트워크 노드(300)에 제출하는 단계(S107)를 포함하는 생체 데이터를 등록하는 방법.

청구항 2

제 1 항에 있어서,

변환된 제 1 및 제 2 생체 데이터 세트의 암호화 단계(S105)는:

변환된 생체 데이터의 제 1 및 제 2 세트에 생체 데이터 검증 노드(400)에 의해 검증될 인증을 제공하는 단계를 더 포함하는 생체 데이터를 등록하는 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서,

제 2 특징 변환 키의 암호화 단계(S105)는:

제 2 특징 변환 키에 네트워크 노드(300)에 의해 검증될 인증을 제공하는 단계를 더 포함하는 생체 데이터를 등록하는 방법.

청구항 4

네트워크 노드(300)가 보안 통신 채널을 통해 클라이언트 디바이스(100)의 사용자(200)의 생체 데이터를 등록하는 방법으로서,

클라이언트 디바이스(100)로부터, 사용자(200)의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 포함하는 등록 요청을 수신하는 단계(S107);

암호화된 제 2 특징 변환 키를 해독하는 단계(S108);

수신된 제 2 특징 변환 키에 대한 사용자 인덱스를 생성하는 단계(S109);

제 2 특징 변환 키, 사용자 프로파일 데이터 및 사용자 인덱스를 저장하는 단계(S110); 및

암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 사용자 프로파일 데이터 및 사용자 인덱스를 생체 데이터 검증 노드(400)에 제출하는 단계(S111)를 포함하고,

제 1 생체 데이터 세트는 제 1 특징 변환 키에 의해 변환되며, 암호화된 제 2 특징 변환 키는, 사용자 프로파일 데이터와 함께, 변환된 제 2 생체 데이터 세트를 변환하는데 사용되는 생체 데이터를 등록하는 방법.

청구항 5

생체 데이터 검증 노드(400)가 보안 통신 채널을 통해 클라이언트 디바이스(100)의 사용자(200)의 생체 데이터를 등록하는 방법으로서,

클라이언트 디바이스(100)와 통신하도록 구성된 네트워크 노드(300)로부터, 클라이언트 디바이스(100)의 사용자(200)의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 포함하는 등록 요청을 수신하는 단계(S111);

암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 해독하는 단계(S112); 및

변환된 제 1 및 제 2 생체 데이터 세트, 사용자 프로파일 데이터 및 사용자(200)의 후속 인증을 위한 사용자 인덱스를 저장하는 단계(S113)를 포함하고,

상기 생체 데이터 세트는 수신된 데이터와 관련된 생체 데이터 검증 노드(400), 사용자 프로파일 데이터 및 사용자 인덱스에 액세스될 수 없는 특징 변환 키에 의해 변환되는 생체 데이터를 등록하는 방법.

청구항 6

클라이언트 디바이스(500)가 생체 데이터에 기초한 보안 통신 채널을 통해 네트워크 노드(300)로 클라이언트 디바이스(500)의 사용자(200)의 인증을 가능하게 하는 방법으로서,

네트워크 노드(300)로부터 세션 값을 수신하는 단계(S202);

사용자(200)의 생체 데이터를 캡처하는 단계(S203);

인증이 수행될 등록된 생체 데이터를 갖는 클라이언트 디바이스(100)와 공유된 제 1 특징 변환 키를 사용하여 생체 데이터를 변환된 제 1 생체 데이터 세트로 변환하는 단계(S204);

사용자(200)가 인증될 생체 데이터 검증 노드(400)와 공유되는 암호화 키를 이용하여 변환된 제 1 생체 데이터 세트 및 수신된 세션 값을 암호화하는 단계(S205);

네트워크 노드(300)와 공유된 암호화 키로 세션 값을 암호화하는 단계(S206);

암호화된 변환된 제 1 생체 데이터 세트, 2 개의 암호화된 세션 값 및 사용자 프로파일 데이터를 네트워크 노드(300)에 제출하는 단계(S207);

적어도 하나의 암호화된 제 2 특징 변환 키 및 세션 값의 암호화된 사본을 수신하는 단계(S216);

상기 암호화된 적어도 하나의 제 2 특징 변환 키 및 상기 암호화된 세션 값을 해독하는 단계 및 상기 해독된 세션 값이 이전에 수신된 세션 값과 일치하는지 검증하는 단계(S217);

네트워크 노드(300)와 공유되는 적어도 하나의 제 2 특징 변환 키를 사용하여 생체 데이터를 적어도 하나의 변환된 제 2 생체 데이터 세트로 변환하는 단계(S218);

생체 데이터 검증 노드(400)와 공유된 키로 변환된 제 2 생체 데이터 세트 및 세션 값을 암호화하는 단계(S219); 및

암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값을 네트워크 노드에 제출하는 단계(S220)를 포함하고,

상기 적어도 하나의 제 2 특징 변환 키 및 상기 세션 값은 상기 네트워크 노드와 공유된 키로 암호화되며,

상기 네트워크 노드(300)는 제출된 데이터를 클라이언트 디바이스의 인증을 위해 생체 데이터 검증 노드(400)에 전달하는 사용자의 인증을 가능하게 하는 방법.

청구항 7

제 6 항에 있어서,

변환된 제 1 생체 데이터 세트와 수신된 세션 값을 암호화하는 단계(S205)는:

변환된 제 1 생체 데이터 세트 및 수신된 세션 값에 생체 데이터 검증 노드(400)에 의해 검증될 인증을 제공하는 단계를 더 포함하는 사용자의 인증을 가능하게 하는 방법.

청구항 8

제 6 항 또는 제 7 항에 있어서,

세션 값을 암호화하는 단계(S206)는:

네트워크 노드(300)에 의해 검증될 인증을 암호화된 세션 값에 제공하는 단계를 더 포함하는 사용자의 인증을 가능하게 하는 방법.

청구항 9

제 6 항 내지 제 8 항 중 어느 한 항에 있어서,

적어도 하나의 변환된 제 2 생체 데이터 세트와 세션 값을 암호화하는 단계(S219)는:

적어도 하나의 변환된 제 2 생체 데이터 세트 및 세션 값에 생체 데이터 검증 노드(400)에 의해 검증될 인증을 제공하는 단계를 더 포함하는 사용자의 인증을 가능하게 하는 방법.

청구항 10

네트워크 노드(300)가 생체 데이터에 기초한 보안 통신 채널을 통해 생체 데이터 검증 노드(400)로 클라이언트 디바이스(500)의 사용자(200)의 인증을 가능하게 방법으로서,

클라이언트 디바이스(500)에 세션 값을 제출하는 단계(S202);

클라이언트 디바이스로부터, 사용자의 암호화된 변환된 제 1 생체 데이터 세트를 수신하는 단계(S207);

수신된 암호화된 세션 값을 해독하고, 상기 해독된 세션 값이 이전에 전송된 세션 값과 일치하는지를 검증하는 단계(S208);

암호화된 변환된 제 1 생체 데이터 세트, 사용자 프로파일 데이터, 및 제 1 생체 데이터 세트 및 클라이언트 디바이스와 공유된 키로 암호화된 세션 값을 제출하는 단계(S209);

생체 데이터 검증 노드로부터, 생체 데이터 검증 노드에 미리 등록되어 있고 변환된 생체 데이터가 제출된 변환된 제 1 생체 데이터 세트와 일치하는 적어도 하나의 변환된 생체 데이터 세트 및 세션 값 각각과 관련된 사용자 인덱스를 수신하는 단계(S212);

세션 값이 생체 데이터 검증 노드로 이전에 전송된 세션 값과 일치하는지 확인하는 단계(S213);

수신된 각 사용자 인덱스에 대해, 이전에 등록된 제 2 특징 변환 키를 인출하는 단계(S214);

인출된 적어도 하나의 제 2 특징 변환 키 및 클라이언트 디바이스와 공유되는 키로 세션 값을 암호화하는 단계(S215);

암호화된 제 2 특징 변환 키 및 세션 값을 클라이언트 디바이스에 제출하는 단계(S216);

클라이언트 디바이스(500)로부터, 적어도 하나의 제 2 특징 변환 키로 변환된 적어도 하나의 변환된 암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값의 사본을 수신하는 단계(S220);

암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트, 세션 값 및 암호화된 세션 값을 생체 데이터 검증 노드(400)에 제출하는 단계(S221); 및

생체 데이터 검증 노드로부터, 각각의 적어도 하나의 이전에 등록된 제 2 특징 변환 키와 관련된 사용자 인덱스뿐만 아니라 생체 데이터 검증 노드가 적어도 하나의 변환된 제 2 생체 데이터 세트와 일치하는 경우의 세션 값을 수신하는 단계(S224)를 포함하고,

상기 제 1 생체 데이터 세트는 제 1 특징 변환 키에 의해 변환되고 클라이언트 디바이스와 생체 데이터 검증 노드 사이에서 공유된 키로 암호화되며, 상기 세션 값은 사용자 프로파일 데이터와 함께 클라이언트 디바이스와 생체 데이터 검증 노드간에 공유된 키로 암호화되고,

적어도 하나의 변환된 생체 데이터 세트와 세션 값은 클라이언트 디바이스(500)와 생체 데이터 검증 노드(400)

사이에서 공유되는 키로 암호화되며,

적어도 하나의 변환된 생체 데이터 세트는 사용자가 인증된 것으로 간주된 사용자 인덱스용으로 이전에 등록되었던, 사용자(200)의 인증을 가능하게 방법.

청구항 11

제 10 항에 있어서,

인출된 적어도 하나의 제 2 특징 변환 키 및 세션 값을 암호화하는 단계(S215)는:

상기 인출된 적어도 하나의 제 2 특징 변환 키 및 세션 값에 네트워크 노드에 의해 검증될 인증을 제공하는 단계(300)를 더 포함하는 사용자(200)의 인증을 가능하게 방법.

청구항 12

생체 데이터 검증 노드(400)가 생체 데이터에 기초한 보안 통신 채널을 통해 클라이언트 디바이스(500)의 사용자(200)의 인증을 가능하게 하는 방법으로서,

클라이언트 디바이스(500)와 통신하도록 구성된 네트워크 노드(300)로부터, 암호화된 변환된 제 1 생체 데이터 세트, 클라이언트 디바이스와 공유된 키로 암호화된 세션 값뿐만 아니라 및 사용자 프로파일 데이터를 수신하는 단계(S209)

암호화된 변환된 제 1 생체 데이터 세트 및 암호화된 세션 값을 해독하고, 해독된 세션 값이 수신된 세션 값과 일치하는지 검증하는 단계(S210);

해독된 변환된 제 1 생체 데이터 세트를 수신된 사용자 프로파일 데이터에 대해 미리 등록된 적어도 하나의 변환된 생체 데이터 세트에 매칭하는 단계(S211);

매칭이 있는 미리 등록된 적어도 하나의 변환된 생체 데이터 세트 각각과 관련된 사용자 인덱스 및 세션 값을 네트워크 노드(300)에 제출하는 단계(S212);

네트워크 노드로부터, 적어도 하나의 변환된 제 2 생체 데이터 세트, 암호화된 세션 값 및 상기 세션 값의 일반 텍스트 사본(clear-text copy)을 수신하는 단계(S221);

암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값을 해독하고, 해독된 세션 값이 일반 텍스트 세션 값과 일치하는지 검증하는 단계(S222);

해독된 적어도 하나의 변환된 제 2 생체 데이터 세트를 미리 등록된 적어도 하나의 변환된 생체 데이터 세트와 매칭시키는 단계(S223); 및

세션 값과 함께 사용자가 인증된 것으로 간주되는 매치가 있는 적어도 하나의 사용자 인덱스를 네트워크 노드에 제출하는 단계(S224)를 포함하는 사용자의 인증을 가능하게 하는 방법.

청구항 13

보안 통신 채널을 통해 네트워크 노드(300)로, 생체 데이터 센서(102) 및 처리유닛(103)을 포함하는 생체 데이터 감지 시스템(101)을 구비하는 클라이언트 디바이스(100)의 사용자(200)의 생체 데이터를 등록하도록 구성된 클라이언트 디바이스(100)로서,

생체 데이터 센서(102)는 사용자(200)의 생체 데이터를 캡처하도록 구성되고,

처리유닛(103)은:

사용자(200)가 인증될 임의의 다른 클라이언트 디바이스(500)와 공유되는 제 1 특징 변환 키를 사용하여 상기 생체 데이터를 변환된 제 1 생체 데이터 세트로 변환하고;

제 2 특징 변환 키를 생성하며;

상기 제 2 특징 변환 키를 사용하여 생체 데이터를 변환된 제 2 생체 데이터 세트로 변환하고;

사용자(200)가 인증될 생체 데이터 검증 노드(400)와 공유되는 암호화 키로 변환된 변환된 제 1 및 제 2 생체 데이터 세트를 암호화하며;

변환된 제 1 및 제 2 생체 데이터 세트가 등록될 네트워크 노드(300)와 공유되는 암호화 키로 제 2 특징 변환 키를 암호화하고;

암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 암호화된 제 2 특징 변환 키 및 사용자 프로파일 데이터를 포함하는 등록 요청을 네트워크 노드(300)에 제출하도록 구성되는 클라이언트 디바이스.

청구항 14

제 14 항에 있어서,

처리유닛(103)은 생체 데이터 검증 노드(400)에 의해 검증될 인증을 변환된 생체 데이터의 제 1 및 제 2 세트에 제공하도록 더 구성되는 클라이언트 디바이스.

청구항 15

제 14 항 및 제 15 항에 있어서,

처리유닛(103)은 네트워크 노드(300)에 의해 검증될 인증을 제 2 특징 변환 키에 제공하도록 더 구성되는 클라이언트 디바이스.

청구항 16

보안 통신 채널을 통해 클라이언트 디바이스(100)의 사용자(200)의 생체 데이터를 등록하도록 구성된 네트워크 노드(300)로서,

상기 네트워크 노드(300)는:

클라이언트 디바이스(100)로부터, 사용자(200)의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 포함하는 등록 요청을 수신하고;

암호화된 제 2 특징 변환 키를 해독하며;

수신된 제 2 특징 변환 키에 대한 사용자 인덱스를 생성하고;

제 2 특징 변환 키, 사용자 프로파일 데이터 및 사용자 인덱스를 저장하며;

암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 사용자 프로파일 데이터 및 사용자 인덱스를 생체 데이터 검증 노드(400)에 제출하도록 구성되고,

상기 제 1 생체 데이터 세트는 제 1 특징 변환 키에 의해 변환되며, 상기 암호화된 제 2 특징 변환 키는 사용자 프로파일 데이터와 함께 변환된 제 2 생체 데이터 세트를 변환하기 위해 사용되는 네트워크 노드.

청구항 17

보안 통신 채널을 통해 클라이언트 디바이스(100)의 사용자(200)의 생체 데이터를 등록하도록 구성된 생체 데이터 검증 노드(400)로서,

상기 생체 데이터 검증 노드(400)는:

클라이언트 디바이스(100)와 통신하도록 구성된 네트워크 노드(300)로부터, 클라이언트 디바이스(100)의 사용자(200)의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 포함하는 등록 요청을 수신하고,

암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 해독하며;

사용자(200)의 후속 인증을 위해 변환된 제 1 및 제 2 생체 데이터 세트, 사용자 프로파일 데이터 및 사용자 인덱스를 저장하도록 구성되고,

상기 생체 데이터 세트는 생체 데이터 검증 노드(400), 사용자 프로파일 데이터 및 수신된 데이터와 관련된 사용자 인덱스에 액세스할 수 없는 특징 변환 키에 의해 변환되는 처리유닛(401)을 포함하는 생체 데이터 검증 노드.

청구항 18

생체 데이터에 기초한 보안 통신 채널을 통해 네트워크 노드(300)로 생체 데이터 센서(102) 및 처리유닛(103)을

포함하는 생체 데이터 감지 시스템(101)을 구비하는 클라이언트 디바이스(500)의 사용자(200)의 인증을 가능하게 하도록 구성된 클라이언트 디바이스(500)로서,

상기 처리유닛(103)은 네트워크 노드(300)로부터 세션 값을 수신하도록 구성되고,

상기 생체 데이터 센서(102)는 사용자(200)의 생체 데이터를 캡처하도록 구성되며,

상기 처리유닛(103)은:

인증이 수행될 등록된 생체 데이터를 갖는 클라이언트 디바이스(100)와 공유되는 제 1 특징 변환 키를 사용하여 상기 생체 데이터를 변환된 제 1 생체 데이터 세트 세트로 변환하고;

사용자(200)가 인증될 생체 데이터 검증 노드(400)와 공유되는 암호화 키를 사용하여 변환된 제 1 생체 데이터 세트 및 수신된 세션 값을 암호화하며;

네트워크 노드(300)와 공유된 암호화 키로 세션 값을 암호화하고;

암호화된 변환된 제 1 생체 데이터 세트, 2개의 암호화된 세션 값 및 사용자 프로파일 데이터를 네트워크 노드(300)에 제출하며;

네트워크 노드와 공유된 키로 암호화된 적어도 하나의 암호화된 제 2 특징 변환 키 및 세션 값의 암호화된 사본을 수신하고,

암호화된 적어도 하나의 제 2 특징 변환 키 및 암호화된 세션 값을 해독하고, 상기 해독된 세션 값이 이전에 수신된 세션 값과 일치하는지 검증하며;

네트워크 노드(300)와 공유된 적어도 하나의 제 2 특징 변환 키를 사용하여 생체 데이터를 변환된 생체 데이터의 적어도 하나의 제 2 세트로 변환하고;

상기 생체 데이터 검증 노드(400)와 공유된 키로 상기 변환된 제 2 생체 데이터 세트 및 세션 값을 암호화하며;

암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값을 네트워크 노드에 제출하도록 구성되고,

상기 네트워크 노드(300)는 제출된 데이터를 클라이언트 디바이스의 인증을 위해 생체 데이터 검증 노드(400)에 전달하는 클라이언트 디바이스.

청구항 19

제 18 항에 있어서,

상기 처리유닛(103)은 변환된 제 1 생체 데이터 세트 및 수신된 세션 값에 생체 데이터 검증 노드(400)에 의해 검증될 인증을 제공하도록 더 구성되는 클라이언트 디바이스.

청구항 20

제 18 항 또는 제 19 항에 있어서,

처리유닛(103)은 네트워크 노드(300)에 의해 검증될 인증을 암호화된 세션 값에 제공하도록 더 구성되는 클라이언트 디바이스.

청구항 21

제 18 항 내지 제 20 항 중 어느 한 항에 있어서,

상기 처리유닛(103)은 적어도 하나의 변환된 제 2 생체 데이터 세트 및 세션 값에 생체 데이터 검증 노드(400)에 의해 검증될 인증을 제공하도록 더 구성되는 클라이언트 디바이스.

청구항 22

생체 데이터에 기초한 보안 통신 채널을 통해 생체 데이터 검증 노드(400)로 클라이언트 디바이스(500)의 사용자(200)의 인증을 가능하게 하도록 구성된 네트워크 노드(300)로서,

상기 네트워크 노드(300)는:

클라이언트 디바이스(500)에 세션 값을 제출하고;

클라이언트 디바이스로부터, 사용자의 암호화된 변환된 제 1 생체 데이터 세트 세트를 수신하며;

수신된 암호화된 세션 값을 해독하고 상기 해독된 세션 값이 이전에 전송된 세션 값과 일치하는지 검증하고;

암호화된 변환된 제 1 생체 데이터 세트, 사용자 프로파일 데이터 및 클라이언트 디바이스와 생체 데이터 검증 노드 사이에서 공유된 키로 암호화된 세션 값을 제출하며;

생체 데이터 검증 노드로부터, 생체 데이터 검증 노드에 미리 등록되어 있고 변환된 생체 데이터가 제출된 변환된 제 1 생체 데이터 세트와 일치하는 적어도 하나의 변환된 생체 데이터 세트 각각과 관련된 사용자 인덱스를 수신하고;

세션 값이 생체 데이터 검증 노드로 이전에 전송된 세션 값과 일치하는지 검증하며;

수신된 각 사용자 인덱스에 대해, 이전에 등록된 제 2 특징 변환 키를 인출하고;

인출된 적어도 하나의 제 2 특징 변환 키 및 세션 값을 클라이언트 디바이스와 공유된 키로 암호화하고;

암호화된 제 2 특징 변환 키 및 세션 값을 클라이언트 디바이스에 제출하고;

클라이언트 디바이스(500)로부터, 적어도 하나의 제 2 특징 변환 키로 변환된 암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트와 암호화된 세션 값의 사본을 수신하며;

암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트, 세션 값 및 암호화된 세션 값을 생체 데이터 검증 노드(400)에 제출하고;

생체 데이터 검증 노드로부터, 적어도 하나의 이전에 등록된 제 2 특징 변환 키 각각과 연관된 사용자 인덱스 뿐만 아니라 생체 데이터 검증 노드가 적어도 하나의 변환된 제 2 생체 데이터 세트와 일치하는 경우의 세션 값을 수신하도록 구성되는 처리유닛(301)을 포함하고,

상기 제 1 생체 데이터 세트는 클라이언트 디바이스와 생체 데이터 검증 노드 사이에서 공유된 키로 암호화된 제 1 특징 변환 키에 의해 변환되며, 상기 세션 값은 사용자 프로파일 데이터와 함께 클라이언트 디바이스와 공유된 키로 암호화되고, 상기 세션 값은 클라이언트 디바이스와 생체 데이터 검증 노드 사이에서 공유된 키로 암호화되며,

적어도 하나의 변환된 제 2 생체 데이터 세트와 세션 값은 클라이언트 디바이스(500)와 생체 데이터 검증 노드(400) 사이에서 공유되는 키로 암호화되고,

상기 적어도 하나의 변환된 생체 데이터 세트는 사용자가 인증된 것으로 간주되는 사용자 인덱스에 대해 미리 등록된 네트워크 노드.

청구항 23

제 22 항에 있어서,

처리유닛(301)은 인출된 적어도 하나의 제 2 특징 변환 키 및 세션 값에 네트워크 노드(300)에 의해 검증될 인증을 제공하도록 더 구성되는 네트워크 노드.

청구항 24

생체 데이터에 기초한 보안 통신 채널을 통해 클라이언트 디바이스(500)의 사용자(200)의 인증을 가능하게 하도록 구성된 생체 데이터 검증 노드(400)로서,

상기 생체 데이터 검증 노드(400)는:

클라이언트 디바이스(500)와 통신하도록 구성된 네트워크 노드(300)로부터, 암호화된 변환된 제 1 생체 데이터 세트 및 클라이언트 디바이스(500)와 공유된 키로 암호화된 세션 값 뿐만 아니라 사용자 프로필 데이터를 수신하고;

암호화된 변환된 제 1 생체 데이터 세트 및 암호화된 세션 값을 해독하고, 해독된 세션 값이 수신된 세션 값과 일치하는지 검증하며;

상기 해독된 변환된 제 1 생체 데이터 세트를 수신된 사용자 프로파일 데이터에 대해 미리 등록된 적어도 하나의 변환된 생체 데이터 세트와 매칭시키고;

일치하는 이전에 등록된 적어도 하나의 변환된 생체 데이터 세트 각각과 관련된 사용자 인덱스 및 세션 값을 네트워크 노드(300)에 제출하며;

네트워크 노드로부터, 적어도 하나의 변환된 제 2 생체 데이터 세트, 암호화된 세션 값 및 상기 세션 값의 일반 텍스트 사본을 수신하고;

암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값을 해독하고, 해독된 세션 값이 일반 텍스트 세션 값과 일치하는지 검증하며;

해독된 적어도 하나의 변환된 제 2 생체 데이터 세트를 미리 등록된 적어도 하나의 변환된 생체 데이터 세트와 매칭시키고;

사용자가 인증된 것으로 간주되는 세션 값과 함께 일치하는 하나 이상의 사용자 인덱스를 네트워크 노드에 제출하도록 구성되는 처리유닛(401)을 포함하는 생체 데이터 검증 노드.

청구항 25

컴퓨터 실행 가능 명령어가 생체 데이터 감지 시스템(101)에 포함된 처리유닛(103)에 실행될 경우, 생체 데이터 감지 시스템(101)이 제 1 항 내지 제 3 항 및/또는 제 6 항 내지 제 9 항 중 어느 한 항에 따른 단계를 수행하게 하는 컴퓨터 실행 가능 명령어를 포함하는 컴퓨터 프로그램(107).

청구항 26

제 25 항에 따른 컴퓨터 프로그램(107)을 수록한 컴퓨터 판독 가능 매체(105)를 포함하는 컴퓨터 프로그램 제품.

청구항 27

컴퓨터 실행 가능 명령어가 네트워크 노드(300)에 포함된 처리유닛(301)에 실행될 경우, 네트워크 노드(300)가 제 4 항, 제 10 항 및 제 11 항 중 어느 한 항에 따른 단계를 수행하게 하는 컴퓨터 실행 가능 명령어를 포함하는 컴퓨터 프로그램(302).

청구항 28

제 27 항에 따른 컴퓨터 프로그램(302)을 수록한 컴퓨터 판독 가능 매체(303)를 포함하는 컴퓨터 프로그램 제품.

청구항 29

컴퓨터 실행 가능 명령어가 생체 데이터 검증 노드(400)에 포함된 처리유닛(401)에서 실행될 경우, 생체 데이터 검증 노드(400)가 제 5 항 또는 제 12 항에 따른 단계를 수행하게 하는 컴퓨터 실행 가능 명령어를 포함하는 컴퓨터 프로그램(402).

청구항 30

제 29 항에 따른 컴퓨터 프로그램(402)을 수록한 컴퓨터 판독 가능 매체(403)를 포함하는 컴퓨터 프로그램 제품.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안 통신 채널을 통한 네트워크 노드로 사용자의 생체 데이터를 등록하는 방법 및 장치에 관한 것이다. 본 발명은 또한 등록된 생체 데이터에 기초하여 사용자의 인증을 가능하게 하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 생체 인식 기반 식별은 인간 사용자를 안전하게 인증할 수 있는 사용자 친화적인 방법이다. 분산 시스템에서 식별 목적으로 생체 데이터 사용시, 상기 생체 데이터에 대한 한 가지 주요 문제는 최종 사용자를 식별해야 하는 컴퓨터 시스템의 노드에서 템플릿 생체 데이터를 사용할 수 있어야 한다는 것이다. 이는 분산형 컴퓨터 시스템의 주요 보안 설계 문제를 이루는 데, 이는 일반적으로 원본의 일반 텍스트 생체 데이터가 중앙 노드에 저장되고 시스템에 분산되어야 하기 때문이다. 이러한 방안은 원본 생체 인식 데이터 손상에 매우 취약하며, 한 시스템에서 손상된 데이터는 다른 모든 시스템에서 또한 동일한 생체 인식 데이터가 손상될뿐만 아니라 생체 인식 데이터가 사용되는 상황으로 이어질 수 있다. 인증하는 동안 원격 위치에서 원본 생체 데이터를 사용할 수 있어야 하기 때문에 단순히 생체 데이터를 암호화해도 이 문제가 해결되지 않는다.

[0003] 따라서, 생체 인식에 기초한 원격 인증을 가능하게 하는 동시에 원본 생체 데이터의 보호를 제공하는 방안을 제공할 필요가 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은 해당 기술 분야에서 이러한 문제를 해결하거나 적어도 완화시키며, 따라서 사용자의 생체 데이터에 기초하여 생체 데이터 검증 노드에서 클라이언트 디바이스의 사용자의 원격 인증을 가능하게 하는 개선된 방법을 제공하는 것이다.

과제의 해결 수단

[0005] 이 목적은 본 발명의 제 1 태양에서 클라이언트 디바이스가 보안 통신 채널을 통한 네트워크 노드로 상기 클라이언트 디바이스의 사용자의 생체 데이터를 등록하는 방법에 의해 달성된다. 상기 방법은 사용자의 생체 데이터를 캡처하는 단계; 사용자가 인증되는 임의의 다른 클라이언트 디바이스와 공유되는 제 1 특징 변환 키를 사용하여 생체 데이터를 변환된 제 1 생체 데이터 세트로 변환하는 단계; 제 2 특징 변환 키를 생성하는 단계; 제 2 특징 변환 키를 사용하여 생체 데이터를 변환된 제 2 생체 데이터 세트로 변환하는 단계; 사용자가 인증되는 생체 데이터 검증 노드와 공유되는 암호화 키로 변환된 제 1 및 제 2 생체 데이터 세트를 암호화하는 단계를 포함한다. 상기 방법은 변환된 제 1 및 제 2 생체 데이터의 세트가 등록되는 네트워크 노드와 공유되는 암호화 키로 제 2 특징 변환 키를 암호화하는 단계; 및 암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 암호화된 제 2 특징 변환 키 및 사용자 프로파일 데이터를 포함하는 등록 요청을 네트워크 노드에 제출하는 단계를 더 포함한다.

[0006] 이 목적은 본 발명의 제 2 태양에서 보안 통신 채널을 통해 네트워크 노드로 클라이언트 디바이스의 사용자의 생체 데이터를 등록하도로 구성된 생체 데이터 센서와 처리유닛을 포함하는 생체 데이터 감지 시스템을 구비하는 클라이언트 디바이스에 의해 달성된다. 상기 생체 데이터 센서는 사용자의 생체 데이터를 캡처하도록 구성된다. 처리유닛은 사용자가 인증될 임의의 다른 클라이언트 디바이스와 공유되는 제 1 특징 변환 키를 사용하여 생체 데이터를 변환된 제 1 생체 데이터 세트로 변환하고, 제 2 특징 변환 키를 생성하며, 제 2 특징 변환 키를 사용하여 생체 데이터를 변환된 제 2 생체 데이터 세트로 변환하고, 사용자가 인증될 생체 데이터 검증 노드와 공유되는 암호화 키로 변환된 제 1 및 제 2 생체 데이터 세트를 암호화하도록 구성된다. 처리유닛은 변환된 제 1 및 제 2 생체 데이터 세트가 등록될 네트워크 노드(300)와 공유된 암호화 키로 제 2 특징 변환 키를 암호화하고, 암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 암호화된 제 2 특징 변환 키 및 사용자 프로파일 데이터를 포함하는 등록 요청을 네트워크 노드에 제출하도록 더 구성된다.

[0007] 이 목적은 본 발명의 제 3 태양에서 네트워크 노드가 보안 통신 채널을 통해 클라이언트 디바이스의 사용자의 생체 데이터를 등록하는 방법에 의해 달성된다. 상기 방법은, 클라이언트 디바이스로부터, 사용자의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 포함하는 등록 요청을 수신하는 단계; 암호화된 제 2 특징 변환 키를 해독하는 단계; 수신된 제 2 특징 변환 키에 대한 사용자 인덱스를 생성하는 단계; 제 2 특징 변환 키, 사용자 프로파일 데이터 및 사용자 인덱스를 저장하는 단계; 및 암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 사용자 프로파일 데이터 및 사용자 인덱스를 생체 데이터 검증 노드에 제출하는 단계를 포함하고, 제 1 생체 데이터 세트는 제 1 특징 변환 키에 의해 변환되며, 암호화된 제 2 특징 변환 키는, 사용자 프로파일 데이터와 함께, 변환된 제 2 생체 데이터 세트를 변환하는데 사용된다.

[0008] 이 목적은 본 발명의 제 4 태양에서 보안 통신 채널을 통해 클라이언트 디바이스의 사용자의 생체 데이터를 등록하도록 구성된 네트워크 노드에 의해 달성된다. 네트워크 노드는, 클라이언트 디바이스로부터, 사용자의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 포함하는 등록 요청을 수신하고; 암호화된 제 2 특징 변환 키를

해독하며; 수신된 제 2 특징 변환 키에 대한 사용자 인덱스를 생성하고; 제 2 특징 변환 키, 사용자 프로파일 데이터 및 사용자 인덱스를 저장하며; 암호화된 변환된 제 1 및 제 2 생체 데이터 세트, 사용자 프로파일 데이터 및 사용자 인덱스를 생체 데이터 검증 노드에 제출하도록 구성된 처리유닛을 포함하고, 제 1 생체 데이터 세트는 제 1 특징 변환 키에 의해 변환되며, 암호화된 제 2 특징 변환 키는, 사용자 프로파일 데이터와 함께, 변환된 제 2 생체 데이터 세트를 변환하는데 사용된다.

[0009] 이 목적은 본 발명의 제 5 태양에서 생체 데이터 검증 노드가 보안 통신 채널을 통해 클라이언트 디바이스의 사용자의 생체 데이터를 등록하는 방법에 의해 달성된다. 상기 방법은 클라이언트 디바이와 통신하도록 구성된 네트워크 노드로부터, 클라이언트 디바이스의 사용자의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 포함하는 등록 요청을 수신하는 단계; 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 해독하는 단계; 및 변환된 제 1 및 제 2 생체 데이터 세트, 사용자 프로파일 데이터 및 사용자의 후속 인증을 위한 사용자 인덱스를 저장하는 단계를 포함하고, 상기 생체 데이터 세트는 수신된 데이터와 관련된 생체 데이터 검증 노드, 사용자 프로파일 데이터 및 사용자 인덱스에 액세스될 수 없는 특징 변환 키에 의해 변환된다.

[0010] 이 목적은 본 발명의 제 6 태양에서 보안 통신 채널을 통해 클라이언트 디바이스 사용자의 생체 데이터를 등록하도록 구성된 생체 데이터 검증 노드에 의해 달성된다. 생체 데이터 검증 노드는 클라이언트 디바이스와 통신하도록 구성된 네트워크 노드로부터 클라이언트 디바이스 사용자의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 포함하는 등록 요청을 수신하고, 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 해독하며, 사용자의 후속 인증을 위한 변환된 제 1 및 제 2 생체 데이터 세트, 사용자 프로파일 데이터 및 사용자 인덱스 세트를 저장하도록 구성되는 처리유닛을 포함하고, 상기 생체 데이터 세트는 수신된 데이터와 관련된 생체 데이터 검증 노드, 사용자 프로파일 데이터 및 사용자 인덱스에 액세스될 수 없는 특징 변환 키에 의해 변환된다.

[0011] 이 목적은 본 발명의 제 7 태양에서 생체 데이터에 기초한 보안 통신 채널을 통해 네트워크 노드로 클라이언트 디바이스의 사용자의 인증을 가능하게 하는 클라이언트 디바이스에 의해 수행되는 방법에 의해 달성된다. 이 방법은 네트워크 노드로부터 세션 값을 수신하는 단계; 사용자의 생체 데이터를 캡처하는 단계; 인증이 수행될 등록된 생체 데이터를 갖는 클라이언트 디바이스와 공유된 제 1 특징 변환 키를 사용하여 생체 데이터를 변환된 제 1 생체 데이터 세트로 변환하는 단계; 사용자가 인증될 생체 데이터 검증 노드와 공유되는 암호화 키로 변환된 제 1 생체 데이터 세트 및 수신된 세션 값을 암호화하는 단계; 네트워크 노드와 공유된 암호화 키를 사용하여 세션 값을 암호화하는 단계; 암호화된 변환된 제 1 생체 데이터 세트, 2개의 암호화된 세션 값 및 사용자 프로파일 데이터를 네트워크 노드에 제출하는 단계; 및 적어도 하나의 암호화된 제 2 특징 변환 키 및 세션 값의 암호화된 사본을 수신하는 단계를 포함하고, 적어도 하나의 제 2 특징 변환 키 및 세션 값은 네트워크 노드와 공유된 키로 암호화된다. 이 방법은 암호화된 적어도 하나의 제 2 특징 변환 키 및 암호화된 세션 값을 해독하는 단계 및 해독된 세션 값이 이전에 수신된 세션 값을 준수하는지를 검증하는 단계; 네트워크 노드와 공유되는 적어도 하나의 제 2 특징 변환 키를 이용하여 생체 데이터를 적어도 하나의 변환된 제 2 생체 데이터 세트로 변환하는 단계; 생체 데이터 검증 노드와 공유된 키로 적어도 하나의 변환된 제 2 생체 데이터 세트와 세션 값을 암호화하는 단계; 및 암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트와 및 암호화된 세션 값을 네트워크 노드에 제출하는 단계를 포함하고, 네트워크 노드는 제출된 데이터를 클라이언트 디바이스의 인증을 위해 생체 데이터 검증 노드에 전달한다.

[0012] 이 목적은 본 발명의 제 8 태양에서 생체 데이터에 기초한 보안 통신 채널을 통해 네트워크 노드로 클라이언트 디바이스의 사용자를 인증할 수 있도록 구성된 클라이언트 디바이스에 의해 달성된다. 클라이언트 디바이스는 생체 데이터 센서 및 처리유닛을 포함하는 생체 데이터 감지 시스템을 포함한다. 처리유닛은 네트워크 노드로부터 세션 값을 수신하도록 구성된다. 생체 데이터 센서는 사용자의 생체 데이터를 캡처하도록 구성된다. 처리유닛은 인증이 수행될 등록된 생체 데이터를 갖는 클라이언트 디바이스와 공유되는 제 1 특징 변환 키를 이용하여 생체 데이터를 변환된 제 1 생체 데이터 세트 세트로 변환하고; 사용자가 인증될 생체 데이터 검증 노드와 공유된 암호화 키로 변환된 제 1 생체 데이터 세트와 수신된 세션 값을 암호화하며; 네트워크 노드와 공유된 암호화 키를 사용하여 세션 값을 암호화하고; 암호화된 변환된 제 1 생체 데이터 세트, 2개의 암호화된 세션 값 및 사용자 프로파일을 네트워크 노드에 제출하며; 적어도 하나의 암호화된 제 2 특징 변환 키 및 세션 값의 암호화된 사본을 수신하고; 암호화된 적어도 하나의 제 2 특징 변환 키와 암호화된 세션 값을 해독하고 상기 암호화된 세션 값이 이전에 수신한 세션 값과 일치하는지 검증하도록 구성되며, 적어도 하나의 제 2 특징 변환 키 및 세션 값은 네트워크 노드와 함께 공유된 키로 암호화된다. 처리유닛은 또한 네트워크 노드와 공유된 적어도 하나의 제 2 특징 변환 키를 사용하여 생체 데이터를 적어도 하나의 변환된 제 2 생체 데이터 세트로 변환하고, 생체 데이터 검증 노드와 공유된 키를 이용해 적어도 하나의 변환된 제 2 생체 데이터 세트 및 세션 값을

암호화하며, 암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값을 네트워크 노드에 제출하도록 구성되고, 네트워크 노드는 클라이언트 디바이스의 인증을 위해 제출된 데이터를 생체 데이터 검증 노드에 전달한다.

[0013] 이 목적은 본 발명의 제 9 태양에서 생체 데이터에 기초한 보안 통신 채널을 통해 클라이언트 디바이스의 사용자의 인증을 가능하게 하는 생체 데이터 검증 노드에 의해 수행되는 방법에 의해 달성된다. 이 방법은 클라이언트 디바이스와 통신하도록 구성된 네트워크 노드로부터, 암호화된 변환된 제 1 생체 데이터 세트 및 클라이언트 디바이스와 공유된 키로 암호화된 세션 값 뿐만 아니라 사용자 프로파일을 수신하는 단계; 암호화된 변환된 제 1 생체 데이터 세트 및 암호화된 세션 값을 해독하고, 해독된 세션 값이 수신된 세션 값과 일치하는지 검증하는 단계; 해독된 변환된 제 1 생체 데이터 세트를 수신된 사용자 프로파일 데이터에 대해 미리 등록된 적어도 하나의 변환된 생체 데이터 세트에 매칭하는 단계; 매칭이 있는 미리 등록된 적어도 하나의 변환된 생체 데이터 세트 각각과 관련된 사용자 인덱스 및 세션 값을 네트워크 노드에 제출하는 단계; 네트워크 노드로부터, 적어도 하나의 변환된 제 2 생체 데이터 세트, 암호화된 세션 값 및 상기 세션 값의 일반 텍스트 사본(clear-text copy)을 수신하는 단계를 포함한다. 상기 방법은 암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값을 해독하고, 해독된 세션 값이 일반 텍스트 세션 값과 일치하는지 검증하는 단계; 해독된 적어도 하나의 변환된 제 2 생체 데이터 세트를 미리 등록된 적어도 하나의 변환된 생체 데이터 세트와 매칭시키는 단계; 및 세션 값과 함께 사용자가 인증된 것으로 간주되는 매치가 있는 적어도 하나의 사용자 인덱스를 네트워크 노드에 제출하는 단계를 더 포함한다.

[0014] 이 목적은 본 발명의 제 10 태양에서 생체 데이터에 기초한 보안 통신 채널을 통해 클라이언트 디바이스의 사용자의 인증을 가능하게 하도록 구성된 생체 데이터 검증 노드에 의해 달성된다. 생체 데이터 검증 노드는, 클라이언트 디바이스와 통신하도록 구성된 네트워크 노드로부터, 암호화된 변환된 제 1 생체 데이터 세트, 클라이언트 디바이스와 공유된 키로 암호화된 세션 값 뿐만 아니라 사용자 프로파일 데이터를 수신하고; 암호화된 변환된 제 1 생체 데이터 세트를 해독하고 해독된 세션 값이 수신된 세션 값과 일치하는지 검증하며; 해독된 변환된 제 1 생체 데이터 세트를 수신된 사용자 프로파일 데이터에 대해 사전에 등록된 적어도 하나의 변환된 생체 데이터 세트에 매칭시키고; 사전에 등록된 각각의 사전에 등록된 적어도 하나의 변환된 생체 데이터 세트와 관련된 사용자 인덱스 및 세션 값을 네트워크 노드에 제출하며; 네트워크 노드로부터 암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트, 암호화된 세션 값 및 세션 값의 일반 텍스트 사본을 수신하도록 구성된 처리유닛을 포함한다. 처리유닛은 또한 암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값을 해독하고, 해독된 세션 값이 일반 텍스트 세션 값과 일치하는지 검증하며, 이전에 등록된 적어도 하나의 변환된 생체 데이터 세트와 해독된 적어도 하나의 변환된 제 2 생체 데이터 세트를 매칭시키고, 세션 값과 함께 사용자가 인증된 것으로 간주되는 일치하는 적어도 하나의 사용자 인덱스를 네트워크 노드에 제출하도록 더 구성된다.

[0015] 유리하게는, 본 발명은 매칭 백엔드 서버에 일반 텍스트 생체 인식을 나타내지 않으면서 대규모 사용자 그룹의 중앙 매칭을 가능하게 한다.

[0016] 간단히 말하면, 중앙 매칭 서버에 보관된 보호된 (예를 들어, 변환되거나 암호화된) 생체 템플릿 데이터가 애플리케이션 서버를 대신하여 식별 결정을 내리는 데 사용되는 방법이 개시된다.

[0017] 더욱이, 매칭은 다단계 접근법 및 변환/암호화된 공간 또는 환경에서 수행된다.

[0018] 본 발명은 제 1 변환을 사용한 사전매칭과 제 2 변환에 대한 최종 매칭을 조합함으로써 대규모 사용자 세트에 대해 효율적이고 고성능이며 매우 안전한 중앙 매칭을 가능하게 한다. 중앙 매칭 서버는 결코 일반 텍스트 생체 데이터를 처리하지 않지만, 최신 생체 매칭 기술을 사용하여 대규모 사용자 세트에 대해 효율적으로 일치시킬 수 있다.

[0019] 시스템을 공격하려는 공격자는 애플리케이션 서버와 매칭 서버를 모두 공격하여 일반 텍스트 생체 인식 데이터에 액세스해야 하며 일반 텍스트 생체 데이터는 최종 사용자로부터 생체 인식 정보를 읽는 노드를 제외한 모든 노드의 어떠한 타입의 메모리에도 결코 저장되지 않는다. 그러나, 최종 사용자는 자신의 데이터를 생체 리더기에 제시하는 것으로 가정하기 때문에, 이 데이터는 사용자가 식별되려고할 때 항상 해당 노드에 일시적으로 존재한다. 시스템의 어느 위치에서나 생체 데이터가 일반 텍스트로 영구히 저장되지 않는다.

[0020] 전체 생체 인식 템플릿 데이터는 개별 변환 키와 함께 저장되는 반면, 생체 인식 데이터의 일부만이 애플리케이션 와이브 변환 키를 사용하여 변환된다. 이 키 리포지토리만 공격해도 공격자가 개별 최종 사용자의 생체 데이터에 액세스하거나 시스템내 임의의 개인을 가장할 가능성은 없다. 일치하는 리포지토리만 공격하는 것은 임의

의 최종 사용자의 생체 데이터를 제공하지 않는다.

[0021] 전반적으로, 청구범위에 사용된 모든 용어는 달리 명시적으로 정의되지 않는 한, 기술 분야에서 일반적인 의미에 따라 해석되어야 한다. "a/an/the 요소, 장치, 구성 요소, 수단, 단계 등"에 대한 모든 참조는 달리 명시적으로 언급되지 않는 한, 요소, 장치, 구성 요소, 수단, 단계 등의 적어도 하나의 예를 언급하는 것으로서 공개적으로 해석되어야 한다. 기재된 임의의 방법의 단계는 명시적으로 언급되지 않는 한, 개시된 순서대로 수행될 필요는 없다.

발명의 효과

[0022] 본 발명의 내용에 포함됨.

도면의 간단한 설명

[0023] 이제 첨부도면을 참조로 본 발명을 예로서 설명한다:

도 1은 본 발명이 구현될 수 있는 스마트폰 형태의 전자장치를 도시한다.

도 2는 사용자가 손가락을 놓는 지문센서의 도면을 도시한다.

도 3은 일 실시예에 따른 지문감지 시스템의 일부인 지문센서를 도시한다.

도 4는 일 실시예에 따라 신뢰할 수 있는 서버에서 사용자의 변환된 생체 데이터를 등록하는 시그널링 다이어그램을 도시한다.

도 5는 다른 변형에 따라 등록된 변환된 생체 데이터에 기초하여 사용자를 인증하는 시그널링 다이어그램을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0024] 본 발명은 이제 본 발명의 특정 실시예가 도시된 첨부도면을 참조로 하기에서 보다 완전하게 설명될 것이다. 그러나, 본 발명은 많은 상이한 형태로 구현될 수 있으며, 제시된 실시예에 국한되는 것으로 해석되어서는 안된다; 오히려, 본 개시가 철저하고 완전하며, 본 발명의 범위를 당업자에게 완전히 전달하도록 이들 실시예는 예로서 제공된다. 명세서 전체에 걸쳐 동일한 참조부호는 동일한 구성요소를 지칭한다.

[0025] 도 1은 본 발명이 구현될 수 있는 스마트폰 형태의 클라이언트 디바이스(100)를 도시한다. 스마트폰(100)에는 지문센서(102) 및 터치 스크린 인터페이스(106)를 갖는 디스플레이 유닛(104)을 구비한다. 지문센서(102)는, 예를 들어, 이동전화(100)의 잠금을 해제하고/하거나 이동전화(100) 등을 이용해 수행되는 거래를 인증하는 데 사용될 수 있다. 지문센서(102)는 대안으로 이동전화(100)의 후면에 배치될 수 있다. 지문센서(102)는 디스플레이 유닛/터치 스크린에 통합되거나 스마트폰 홈 버튼의 일부를 형성할 수 있음이 주목된다.

[0026] 본 발명의 실시예에 따른 지문센서(102)는 랩탑, 리모트 컨트롤, 태블릿, 스마트 카드 등과 같은 다른 유형의 전자장치, 또는 지문 감지를 이용하는 임의의 다른 유형의 현재 또는 미래에 유사하게 구성된 장치에서 구현될 수 있음이 이해된다.

[0027] 도 2는 사용자가 손가락(201)을 위치시키는 지문센서(102)의 다소 확대된 도면을 도시한다. 용량성 감지기술을 사용하는 경우, 지문센서(102)는 복수의 감지소자를 포함하도록 구성된다. 단일 감지소자(또한 픽셀로 표시됨)는 도 2에서 참조번호 202로 표시되어 있다.

[0028] 도 3은 지문감지 시스템(101)의 일부인 지문센서(102)를 도시한다. 지문감지 시스템(101)은 지문센서(102) 및 상기 지문센서(102)를 제어하고 캡처된 지문을 분석하기 위한 마이크로 프로세서와 같은 처리유닛(103)을 포함한다. 지문감지 시스템(101)은 메모리(105)를 더 포함한다. 지문감지 시스템(101)은 일반적으로 도 1에 예시된 바와 같이 전자장치(100)의 일부를 형성한다.

[0029] 이제, 물체가 지문센서(102)와 접촉할 때, 센서(102)는 캡처된 지문을 메모리(105)에 미리 저장된 하나 이상의 인증된 지문 템플릿과 비교함으로써 물체가 허가된 사용자의 지문인지 아닌지를 처리유닛(103)이 판정하기 위해 물체의 이미지를 캡처할 것이다.

[0030] 지문센서(102)는 예를 들어 용량성, 광학, 초음파 또는 열감지 기술을 포함하는 임의의 종류의 현재 또는 미래의 지문 감지 원리를 사용하여 구현될 수 있다. 현재, 용량 감지는 특히 크기와 전력 소비가 중요한 응용 분야

에서 가장 일반적으로 사용된다. 용량성 지문센서는 다수의 감지소자(202)와 지문센서(102)의 표면 상에 위치된 손가락(201) 사이의 커패시턴스를 나타내는 측정치를 제공한다. 지문 이미지의 획득은 전형적으로 2차원 방식으로 배열된 복수의 감지소자(202)를 포함하는 지문센서(102)를 사용하여 수행된다

[0031] 대안으로, 사용자의 생체 데이터는 예컨대 홍채 또는 얼굴 인식 센서와 같이 지문센서와는 다른 장치를 사용하여 캡처될 수 있다. 홍채 또는 얼굴 인식 센서와 조합된 지문센서와 같은 센서의 조합이 사용되는 것도 또한 예상될 수 있다.

[0032] 일반적인 인증 프로세스에서, 지문센서가 사용되는 경우, 사용자는 센서가 사용자의 지문의 이미지를 캡처하도록 센서(102) 상에 손가락(201)을 둔다. 처리유닛(103)은 캡처된 지문을 평가하고 이를 메모리(105)에 저장된 하나 이상의 인증된 지문 템플릿과 비교한다. 기록된 지문이 사전 저장된 템플릿과 일치하면, 사용자는 인증되고 처리유닛(103)은 일반적으로 사용자가 스마트폰(100)에 액세스할 수 있는 잠금 모드에서 잠금 해제 모드로의 전환과 같은 적절한 동작을 수행하도록 스마트폰에 지시할 것이다.

[0033] 다시 도 3을 참조하면, (센서(102)에 의해 수행되는 이미지를 캡처하는 것을 제외하고) 지문감지 시스템(101)에 의해 수행되는 방법의 단계는 실제로 랜덤 액세스 메모리(RAM), 플래시 메모리 또는 하드 디스크 드라이브와 같은 마이크로 프로세서와 관련된 저장매체(105)에 다운로드된 컴퓨터 프로그램(107)을 실행하도록 구성된 하나 이상의 마이크로 프로세서의 형태로 구현된 처리유닛(103)에 의해 수행된다. 처리유닛(103)은 컴퓨터 실행가능 명령어를 포함한 적절한 컴퓨터 프로그램(107)이 저장매체(105)에 다운로드되어 처리유닛(103)에 의해 실행될 때 지문감지 시스템(101)이 실시예에 따른 방법을 수행하도록 구성된다. 저장매체(105)는 또한 컴퓨터 프로그램(107)을 포함하는 컴퓨터 프로그램 제품(103)에 의해 실행된다. 대안으로, 컴퓨터 프로그램(107)은 DVD(Digital Versatile Disc) 또는 메모리 스틱과 같은 적절한 컴퓨터 프로그램 제품에 의해 저장매체(105)로 전송될 수 있다. 다른 대안으로서, 컴퓨터 프로그램(107)은 네트워크를 통해 저장매체(105)로 다운로드될 수 있다. 처리유닛(103)은 대안으로 DSP(digital signal processor), ASIC(application specific integrated circuit), FPGA(field-programmable gate array), CPLD(complex programm logic device) 등의 형태로 구현될 수 있다. 처리유닛(103)에 의해 제공되는 기능의 전부 또는 일부는 지문센서(102)와 적어도 부분적으로 일체로 형성될 수 있음을 더 이해해야 한다.

[0034] 도 4는 애플리케이션 서버(AS)(300)라고 하는 네트워크 노드와의 보안 통신 채널을 통해 제 1 클라이언트 디바이스(100)의 사용자(200)의 생체 데이터를 등록하는 실시예를 도시한다. 애플리케이션 서버(300)는 차례로 생체 데이터 신뢰 노드(BTS)(400)라고 하는 생체 데이터 검증 노드에서의 사용자(200)의 생체 데이터 중 일부를 등록한다.

[0035] 간략하게, 예를 들어 스마트폰 형태로 구현된 제 1 클라이언트 디바이스(100)는 도 1-3을 참조하여 설명된 방식으로 사용자(200)의 생체 데이터를 캡처한다. 그런 다음 이 생체 데이터는 스마트폰에서 보호되고 (생체 데이터가 아니라) 수신된 데이터의 서브 세트를 저장하고 생체 데이터를 BTS(400)으로 전달하는 원격 위치된 신뢰할 수 있는 AS(300)으로 안전하게 기록 또는 등록된다. 이어서, 사용자(200)는 컴퓨팅 스테이션(500)이 사용자의 생체 데이터를 캡처하고, 캡처된 생체 데이터를 보호하며, (AS(300)을 통해) BTS(400)가 상기 BTS(400)로 이전에 등록된 보호된 생체 데이터와 보호된 생체 데이터를 매칭시킴으로써, 로컬 컴퓨팅 스테이션(500)에서, 즉, 제 2 클라이언트 디바이스에서 자신을 인증할 것이다.

[0036] 예를 들어, AS(300)는 사용자(200)가 전자 상거래 서비스를 통해 구매한 상품을 지불하기 위해 개인 식별 번호(PIN) 대신에 생체 데이터를 사용하여 자신을 인증하는 전자 상거래 서비스와 같이, 사용자(200)가 액세스하고자 하는 하나 이상의 서비스를 제공할 수 있다.

[0037] 이는 사용자가 원격 인증 절차를 지원하는 임의의 (신뢰된) 장치를 생체 정보에 제시함으로써 본 발명에 따른 로그인 절차를 제공하는 AS(300)에 의해 제공되는 원격 웹 서비스에 로그인할 수 있음을 의미한다. 따라서, 사용자는 사용자 이름 및/또는 비밀번호 또는 특정 하드웨어 토큰을 휴대하거나 로그인에 사용되는 클라이언트 디바이스에 특수용 식별 프로그램 또는 크리덴셜을 저장해야 한다는 임의의 요건을 기억할 필요가 없다.

[0038] 인증에 성공하면, 사용자(200)는 AS(300)에 의해 제공되는 서비스에 액세스할 수 있게 된다. 사용자(200)의 생체 데이터의 일반 텍스트 사본은 스마트폰(100) 또는 로컬 컴퓨팅 스테이션(500)을 결코 떠나지 않는다는 점이 주목된다. AS(300)는 복수의 서비스를 제공하고, 상이한 서비스가 상이한 식별된 사용자에게 제공될 수 있다는 것이 예상된다.

[0039] 대안으로, 사용자(200)에 대한 인증 프로세스는 제 1 클라이언트 디바이스(100), 즉, 사용자(200)의 생체 데이

터를 등록한 동일한 장치에서 수행될 수 있음에 유의한다.

[0040] 사용자는 스마트폰(100)을 사용하는 것에 대한 대안으로서 로컬 컴퓨팅 스테이션(500) 중 임의의 하나를 통해 AS(300)에 등록하는 것이 가능하다.

[0041] 다른 예에서, AS(300)는 렌터카 회사와 같은 서비스 제공자에 속하고, 제 2 클라이언트 디바이스(500)는 생체 인식 리더기를 구비한 자동차 키 디바이스의 형태로 구현될 수 있다. 이 애플리케이션에 사용될 때, 본 발명은 렌터카 회사가 고객을 완전히 온라인으로 처리할 수 있게 하고, 자동차 키가 실제로 특정한 차를 주문하고 지불한 사용자에게만 활성화될 수 있기 때문에, 자동차가 도난당할 높은 위험없이 안전하지 않은 장소(근무 시간외 및 원거리)에서도 고객이 이용할 수 있게 한다. 사용자는 생체 데이터가 렌터카 회사에 전송되더라도 사용자의 생체 데이터가 자동차 키 디바이스 외부의 렌터카 회사에 결코 제공될 수 없음을 보장하므로 시스템을 신뢰할 수 있어, 안전한 것으로 추정될 수 있다. 도 4를 참조하면, 스마트폰(100)은 예를 들어 도 1 내지 도 3을 참조하여 설명된 바와 같은 지문센서, 또는 예를 들어 홍채 또는 얼굴 인식 센를 이용해 단계(S101)에서 사용자(200)의 생체 데이터(T)를 캡처한다.

[0042] 단계(S102)에서, 스마트폰(100)은 적절한 특징 변환 방식을 사용하여, 즉, 원본 생체 템플릿 표현과 적절한 변환 파라미터를 입력 파라미터로 취하고 변환된 생체 인식 템플릿 정보를 출력으로 생성하는 "특징 변환(feature transform)" 기능을 선택하여, 캡처된 생체 데이터(T)를 변환된 제 1 생체 데이터 세트(Tr1)로 변환한다.

[0043] 이는 예를 들어 적절한 의사난수함수(PRF)에 의해 스마트폰(100)에서 생성된 비밀의 제 1 특징 변환 키(R1)를 사용하여 수행될 수 있다. 대안으로, 스마트폰(100)은 비밀의 제 1 특징 변환 키(R1)로 미리 구성되거나 AS(300)에 의해 비밀의 제 1 특징 변환 키(R1)와 함께 공급된다. 등록 동안 사용된 제 1 특징 변형 키(R1)는, 예를 들어, 가령, 로컬 컴퓨팅 스테이션(500)과 같이 사용자가 인증을 받는 임의의 다른 클라이언트 디바이스와 공유되어야 한다. 변환된 제 1 생체 데이터 세트는 따라서 Tr1 = F(R1, T)로 표시된다.

[0044] 이어서, 스마트폰(100)은 단계(S103)에서 제 2 특징 변환 키(R2)를 생성하고 단계(S104)에서 캡처된 생체 데이터(T)에 기초하여 변환된 제 2 생체 데이터 세트를 생성한다: Tr2 = F(R2, T).

[0045] 제 2 특징 변환 변환 키(R2)는 등록된 각각의 변환된 제 2 생체 데이터 세트(Tr2)마다 고유하며, 사용자는 복수의 캡처된 생체 데이터 세트(T)를 시스템에 등록할 수 있음에 유의해야 한다.

[0046] 단계(S105)에서, 변환된 제 1 및 제 2 생체 데이터 세트(Tr1, Tr2)는 BTS(400)와 공유된 암호화 키(KE_{D1BTS})로 암호화되며, 이는 c1 = EO(Tr1, Tr2, KE_{D1BTS})로 표시된다.

[0047] 실시예에서, c1에는 BTS(400)와 공유되는 대칭 키(KI_{D1BTS})에 의해 인증이 제공됨으로써, 메시지 인증 코드(MAC)를 제공하거나, 스마트폰(100)의 비대칭 개인 키를 제공함으로써, 디지털 서명을 제공한다(이는 BTS(400)에 스마트폰(100)의 대응하는 공개 키가 제공되어야 함을 의미한다).

[0048] 스마트폰은, 단계(S106)에서, 변환된 제 1 및 제 2 생체 데이터 세트 세트가 등록될 AS(300)와 공유된 암호화 키(KE_{D1A})를 갖는 제 2 특징 변환 키(R2)를 더 암호화하며, 이는 c2 = EO(R2, KE_{D1A})로 표시된다.

[0049] 실시예에서, c2에는 AS(300)와 공유되는 대칭 키(KI_{D1A})에 의해 인증을 제공함으로써, MAC을 제공하거나, 클라이언트 디바이스(200)의 또는 비대칭 개인 키를 제공함으로써, 디지털 서명을 제공한다(이는 AS(300)에 스마트폰(100)의 대응하는 공개 키가 제공되어야 함을 의미한다).

[0050] 마지막으로, 단계(S107)에서, 스마트폰(100)은 보안 채널, 즉, 기밀성 및 무결성 측면에서 보호되는 통신 채널을 통해, 예를 들어, 인터넷을 통해, 암호화된 변환된 제 1 및 제 2 생체 데이터 세트(c1), 암호화된 제 2 특징 변환 키(c2) 및 사용자 프로파일 데이터(d)를 포함하는 등록 요청을 AS(300)에 제출한다. 사용자 프로파일 데이터(d)는 예를 들어 최종 사용자 이름, 지리적 위치, 네트워크 등의 형태로 구현될 수 있다.

[0051] 일 실시예에서, 사용자 프로파일 데이터(d)는 제 2 특징 변환 키와 함께 암호화되고 따라서 c2 : c2 = EO(R2, d, KE_{D1A})에 포함된다.

[0052] 따라서, AS(300)는 암호화된 변환된 제 1 및 제 2 생체 데이터 세트(c1), 암호화된 제 2 특징 변환 키(c2) 및 사용자 프로파일 데이터(d)를 수신하고, 단계(S108)에서 암호화된 제 2 특징 변환 키(c2)를 해독하여 일반 텍스트로된 변환된 제 2 특징 키(R2)를 획득한다(그리고 가능하게는 제공된 c2의 인증 여부를 확인한다).

[0053] 이후, 단계(S109)에서, AS(300)는 수신된 제 2 특징 변환 키(R2)에 대한 고유 사용자 인덱스(u)를 생성하고, 단계(S110)에서 제 2 특징 변환 키(R2), 사용자 프로파일 데이터(d2) 및 사용자 인덱스(u)를 저장한다. 스마트폰(100)이 복수의 생체 템플릿을 등록하는 경우, 대응하여 수신된 각각의 제 2 특징 변환 키(R2)마다 고유 사용자 인덱스가 생성된다는 점이 주목된다.

[0054] AS(300)는 보안 통신 채널을 통해 단계(S111)에서 암호화된 변환된 제 1 및 제 2 생체 데이터 세트(c1), 사용자 프로파일 데이터(d) 및 사용자 인덱스(u)를 BTS(400)에 더 제출한다.

[0055] 등록 절차의 최종 단계에서, BTS(400)는, AS(300)로부터, 제 1 클라이언트 디바이스(100)의 사용자(200)의 암호화된 변환된 제 1 및 제 2 생체 데이터 세트(c1), 사용자 프로파일 데이터(d) 및 수신된 데이터와 관련된 사용자 인덱스(u)를 포함하는 등록 요청을 수신하고, 스마트폰(100)과 공유된 키(KE_{D1BTS})를 이용하여 단계(S112)에서 암호화된 변환된 제 1 및 제 2 생체 데이터 세트를 해독한다(그리고 가능하게는 c1의 임의의 제공된 인증을 검증한다).

[0056] 그 후, BTS(400)는 단계(S113)에서 변환된 제 1 및 제 2 생체 데이터 세트(Tr1, Tr2), 사용자 프로파일 데이터(d) 및 사용자 인덱스(u)를 저장한다

[0057] 결론적으로, BTS(400)는 제 1 및 제 2 특징 변환 키(R1, R2) 중 어느 하나에 액세스할 수 없으므로, 생체 데이터(T)의 일반 텍스트 사본을 얻는 것이 유리하지 않다.

[0058] 이제, 로컬 컴퓨팅 스테이션(500)을 통해 AS(300)의 상기 언급된 임의의 서비스에 액세스하고자 하는 사용자는 도 5의 시그널링 다이어그램을 참조로 도시된 바와 같이 AS(300)를 통해 자신이 이전에 등록한 BTS(400)를 통해 자신을 인증해야 한다.

[0059] 따라서, (이 특정 예에서 단계(S101-S107)에서 신뢰 서버에 등록된 사용자(200)인 것으로 가정되는) 사용자는 단계(S201)에서 제 2 클라이언트 디바이스, 즉, 로컬 컴퓨팅 스테이션(500)의 사용자(200)를 인증하기 위한 요청을 AS(300)에 제출할 수 있다.

[0060] 이에 응답하여, 로컬 스테이션(500)은 단계(S202)에서 AS(300)로부터 세션 값(q)를 수신하여 인증 프로세스 동안 보안을 개선하기 위해 사용된다. 인증 프로세스 동안, 세션 값(q)은 당사자 간의 각 통신 라운드에서 관련 당사자에 의해 검증되며, 어느 시점에서 q의 정확성을 검증할 수 없으면, 조작이 중단된다.

[0061] AS(300)에 인증 요청을 능동적으로 제출하는 것은 사용자가 아닐 수 있지만, 대신 AS(300)는 단계(S202)에서 세션 값(q)를 로컬 스테이션(500)에 제출함으로써 인증 세션을 시작한다. 이러한 시나리오에서, 단계(S201)는 생략된다.

[0062] 단계(S203)에서, (적절한 생체 센서가 장착된) 로컬 스테이션(500)은 사용자(200)의 생체 데이터(T')를 캡처하고, 단계(S204)에서 캡처된 생체 데이터(T') 를 변환된 제 1 생체 데이터 세트(Tr1)의 등록 동안 스마트폰(100)에 의해 사용되는 제 1 특징 변환 키(R1)을 이용하여 변환된 제 1 생체 데이터 세트(Tr1 : Tr1'= F(T', R1)')로 변환한다.

[0063] 또한, 단계(S205)에서, 로컬 스테이션(500)은 사용자(200)가 인증될 BTS(400)와 공유되는 키(KE_{D2BTS})로 변환된 제 1 생체 데이터(Tr1')및 세션 값(q)을 암호화하며, 이는 c3 = EO(Tr1', q, KE_{D2BTS})로 표시된다.

[0064] 예를 들어, c3에는 BTS(400)와 공유되는 대칭 키(KI_{D2BTS})에 의해 인증이 제공됨으로써, 메시지에 MAC을 제공하거나, 로컬 스테이션(500)의 비대칭 개인 키가 제공됨으로써 디지털 서명을 제공한다(즉, BTS(400)에는 로컬 스테이션(500)의 대응하는 공개 키가 제공되어야 함을 의미한다).

[0065] 또한, 단계(S206)에서, 로컬 스테이션(500)은 이 특정 사용자(200)에 대한 이미 등록된 사용자 프로파일 데이터(d)에 대응하는 사용자 프로파일 데이터(d')와 함께 단계(S207)에서 AS(300)에 c3 및 c4를 제출하기 전에 AS(300)과 공유된 키(KE_{D2A})로 세션 값(q): c4 = EO(q, KE_{D2A})을 암호화한다.

[0066] 실시예에서, c4에는 AS(300)와 공유되는 대칭 키(KI_{D2AS})에 의해 인증이 제공됨으로써, 메시지에 MAC을 제공하거나, 로컬 스테이션(500)의 비대칭 개인 키가 제공됨으로써, 디지털 서명을 제공한다(즉, AS(300)에는 로컬 스테이션(500)의 대응하는 공개 키가 제공되어야 함을 의미한다).

[0067] 따라서, AS(300)는 로컬 스테이션(500)과 BTS(400) 사이에서 공유되는 키(KE_{D2BTS})로 모두 암호화된, 사용자

(200)의 암호화된 변환된 제 1 생체 데이터 세트와 암호화된 세션 값뿐만 아니라 사용자 프로파일 데이터(d')와 함께 로컬 스테이션(500)과 AS(300)간에 공유된 키(KE_{D2A})로 암호화된 세션 값을 수신한다.

[0068] AS(300)은 단계(S208)에서 수신된 암호화된 세션 값 c4 = EO(q, KE_{D2A})을 해독하고, 해독된 세션 값이 단계(S202)에서 로컬 스테이션(500)으로 전송된 세션 값(q)를 일치하는지 검증한다(그리고 가능하게는 c4의 임의의 제공된 인증을 검증한다).

[0069] 이후, 단계(S209)에서, AS(300)는 암호화된 변환된 제 1 생체 데이터 세트 및 암호화된 세션 값, 즉, c3 = EO(Tr1', q, KE_{D2BTS}), 사용자 프로파일 데이터(d') 및 세션 값(q)를 BTS(400)에 제출한다.

[0070] BTS(400)는 단계(S210)에서 암호화된 변환된 제 1 생체 데이터 세트 및 암호화된 세션 값 c3 = EO(Tr1', q, KE_{D2BTS})을 해독하고, 해독된 세션 값이 수신된 세션 값(q)를 일치하는지 검증한다(그리고 가능하게는 c3의 임의의 제공된 인증을 검증한다).

[0071] 그 후, 단계(S211)에서, BTS(400)는 해독된 변환된 제 1 생체 데이터 세트(Tr1')를 수신된 사용자 프로파일 데이터(d')에 대해 미리 등록된 적어도 하나의 변환된 생체 데이터(Tr1) 세트, 즉, d'= d에 대해 매칭시킨다.

[0072] BTS(400)는 전형적으로 많은 수의 등록을 저장한다; 수천 명의 사용자들이 BTS(400)를 이용해 등록될 수 있다. 따라서, BTS(400)에 저장된 복수의 등록된 변환된 생체 데이터 세트(Tr1i)는 수신된 변환된 제 1 생체 데이터 세트(Tr1')와 일치하는 것으로 간주될 수 있다. 이를 후보 등록 세트라 한다.

[0073] 따라서, 후보 등록 세트를 구성하는 각각의 매칭 변환된 생체 데이터 세트에 대해, BTS(400)는 단계(S212)에서 세션 값(q)과 함께 연관된 사용자 인덱스(u_i)를 AS(300)에 반환한다.

[0074] 따라서, "사전 매칭"은 적절한 후보 등록 세트를 인출하기 위해 수신된 변환된 제 1 생체 데이터 세트(Tr1')를 이용하여 BTS(400)에서 유리하게 수행되어, 이후에 사전 매칭이 수행되지 않는 시나리오와 비해 컴퓨팅 스테이션(500)에 의해 크게 감소된 수의 후보 등록 세트가 필요하게 되는 효과를 갖는다.

[0075] 이제, 사용자 지수(u_i) 및 세션 값(q)을 수신하면, AS(300)는 단계(S213)에서 세션 값(q)이 단계(S209)에서 AS(400)에 이전에 전송된 세션 값과 일치하는지 검증한다.

[0076] 각각의 수신된 사용자 인덱스(u_i)에 대해, AS(300)는 단계(S214)에서 각각의 특정 사용자 인덱스(u_i)와 관련된 이전에 등록된 제 2 특징 변환 키($R2_i$)를 적절한 스토리지로부터 페치하고, 단계(S215)에서 로컬 스테이션(500)과 공유된 키(KE_{D2A})를 사용해 등록된 각각의 제 2 특징 변환 키(R2i) 및 세션 값(q): c5 = EO(R2i, q, KE_{D2A})을 암호화하고, 단계(S216)에서 c5를 로컬 스테이션(500)에 제출한다.

[0077] 실시예에서, c5에는 AS(300)와 공유되는 대칭 키(KI_{D2AS})를 통해 인증이 제공됨으로써, 메시지에 MAC을 제공하거나, 로컬 스테이션(500)의 비대칭 개인 키가 제공됨으로써 디지털 서명을 제공한다(즉, AS(300)에는 로컬 스테이션(500)의 대응하는 공개 키가 제공되어야 함을 의미한다).

[0078] 로컬 스테이션(500)은 단계(S217)에서 공유 키(KE_{D2A})를 사용하여 암호화된 적어도 하나의 제 2 특징 변환 키 및 암호화된 세션 값(c5)을 해독하고, 해독된 세션 값(q)이 단계(S202)에서 이전에 수신된 세션 값과 일치하는지를 검증한다(그리고 c5의 임의의 제공된 인증을 검증한다).

[0079] 로컬 스테이션(500)은 그 후 단계(S218)에서 각각의 수신된 제 2 특징 변환 키($R2_i$)를 이용하여 캡처된 생체 데이터(T')를 대응하는 개수(i)의 변환된 제 2 생체 데이터 세트로 변환하고: $Tr2_i'$=(T', $R2_i$), 단계(S219)에서, 변환된 제 2 생체 데이터 세트($Tr2_i'$)와 BTS(400)와 공유된 키 KE_{D2BTS}를 갖는 세션 값(q): c6 = EO($Tr2_i'$, q, KE_{D2BTS})을 암호화하며, 최종적 매칭을 위해 단계(S220)에서 c6를 AS(300)에 제출한다.

[0080] 실시예에서, c6에는 BTS(400)와 공유되는 대칭 키(KI_{D2BTS})에 의해 인증이 제공됨으로써, 메시지에 MAC을 제공하거나, 로컬 스테이션(500)의 비대칭 개인 키가 제공함으로써, 디지털 서명을 제공한다(즉, BTS(400)에는 로컬 스테이션(500)의 대응하는 공개 키가 제공되어야 함을 의미한다).

[0081] AS(300)는 최종 매칭을 위해 단계(S221)에서 c6 및 세션 값(q)을 BTS(400)로 차례로 전달할 것이다. AS(300)는

c6, 즉, 단계(S212)에서 후보 등록 세트가 BTS(400)로부터 수신된 순서와 동일한 순서로, 각각의 변환된 제 2 생체 데이터 세트(Tr2i')를 전달할 수 있다. 그렇다면, BTS(400)는 매칭을 수행할 때 각각의 변환된 제 2 생체 데이터 세트($Tr2_i'$)가 어떤 특정 사용자 인덱스(u_i)에 속하는지를 안다.

[0082] BTS(400)는 단계(S222)에서 암호화된 적어도 하나의 변환된 제 2 생체 데이터 세트 및 암호화된 세션 값(c6)을 해독하고, 해독된 세션 값(q)이 일반 텍스트 세션 값과 일치하는지 검증한다(그리고 가능하게는 c6의 임의의 제공된 인증을 검증한다).

[0083] 그 후, 단계(S223)에서, BTS(400)는 해독된 변환된 제 2 생체 데이터 세트($Tr2_i'$)를 이전에 사용자 인덱스(u_i)에 등록된 대응하는 변환된 제 2 생체 데이터 세트($Tr2_i$)와 매칭시킨다. 다시, 적어도 하나의 변환된 제 2 생체 데이터 세트(Tr2)가 각각의 사용자(수백 또는 수천에 이르는 사용자의 수)에 대해 등록되므로, 매칭은 데이터 처리 측면에서 부담스러운 작업일 수 있다.

[0084] 마지막으로, BTS(400)는 세션 값(q)과 함께 일치하는 적어도 하나의 사용자 인덱스(u_i)를 단계(S224)에서 AS(300)에 제출하고, 사용자(200)는 인증된 것으로 간주된다. 수신된 사용자 인덱스(또는 사용자 인덱스들)으로부터, AS(300)는 연관된 사용자 프로파일 데이터(d)로부터 사용자(200)를 식별할 수 있다.

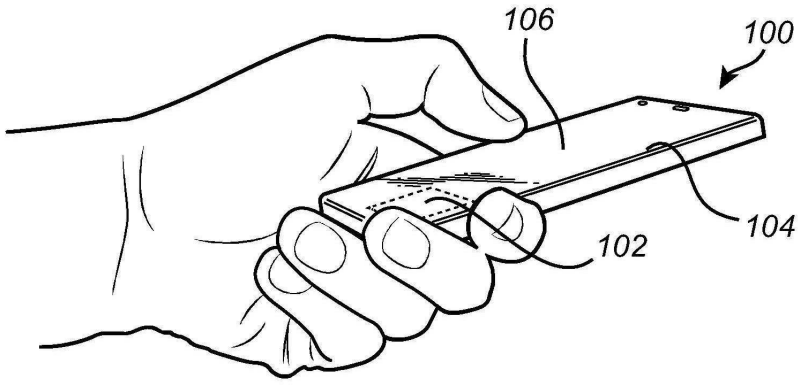
[0085] BTS(400)로부터 변환된 제 2 생체 데이터 세트(Tr2') 중 적어도 하나가 이전에 등록된 변환된 제 2 생체 데이터 세트(Tr2)와 매칭되었다는 확인을 수신하면, AS(300)는 로컬 스테이션(500)의 사용자(200)가 인증되었다고(임의의 수신된 사용자 인덱스(u)와 관련된 사용자 프로파일 데이터(d)에 의해 식별되었다고) 결론내리며, 단계(S225)에서 이에 따라 확인을 로컬 스테이션(500)에 전송할 수 있고, 이 경우 사용자(200)에게 예를 들어 컴퓨팅 스테이션(500)을 통해 AS(300)에 의해 제공되는 서비스에 대한 액세스가 주어진다.

[0086] 유리하게는, 상기에서 결론을 내릴 수 있는 바와 같이, 일반 텍스트 생체 데이터는 클라이언트 디바이스(100, 500)를 떠나지 않으면서, 안전한 인증이 여전히 제공되며, 이는 시스템 사용에 대한 사용자의 신뢰를 크게 증가시킬 수 있다.

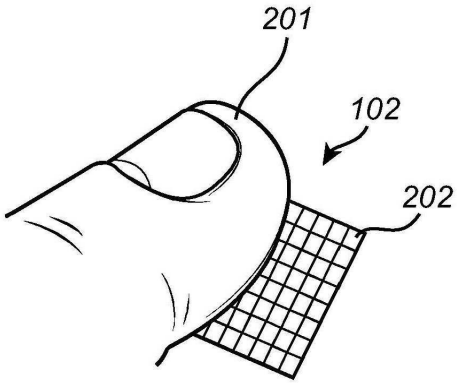
[0087] 본 발명은 주로 몇몇 실시예를 참조로 설명하였다. 그러나, 당업자가 쉽게 이해할 수 있는 바와 같이, 첨부된 특허 청구범위에 의해 정의된 바와 같이, 상기 개시된 것 이외의 다른 실시예들도 본 발명의 범위 내에서 동일하게 가능하다.

도면

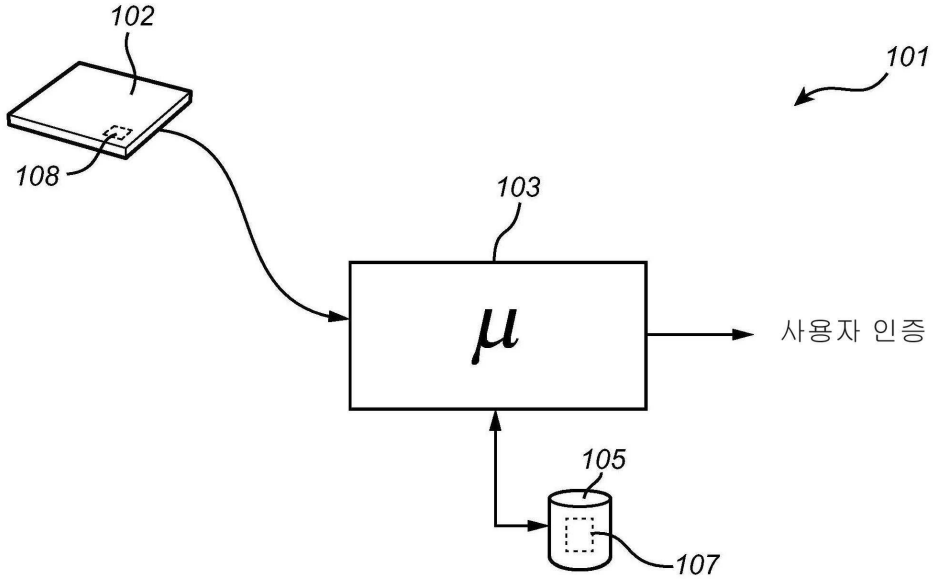
도면1



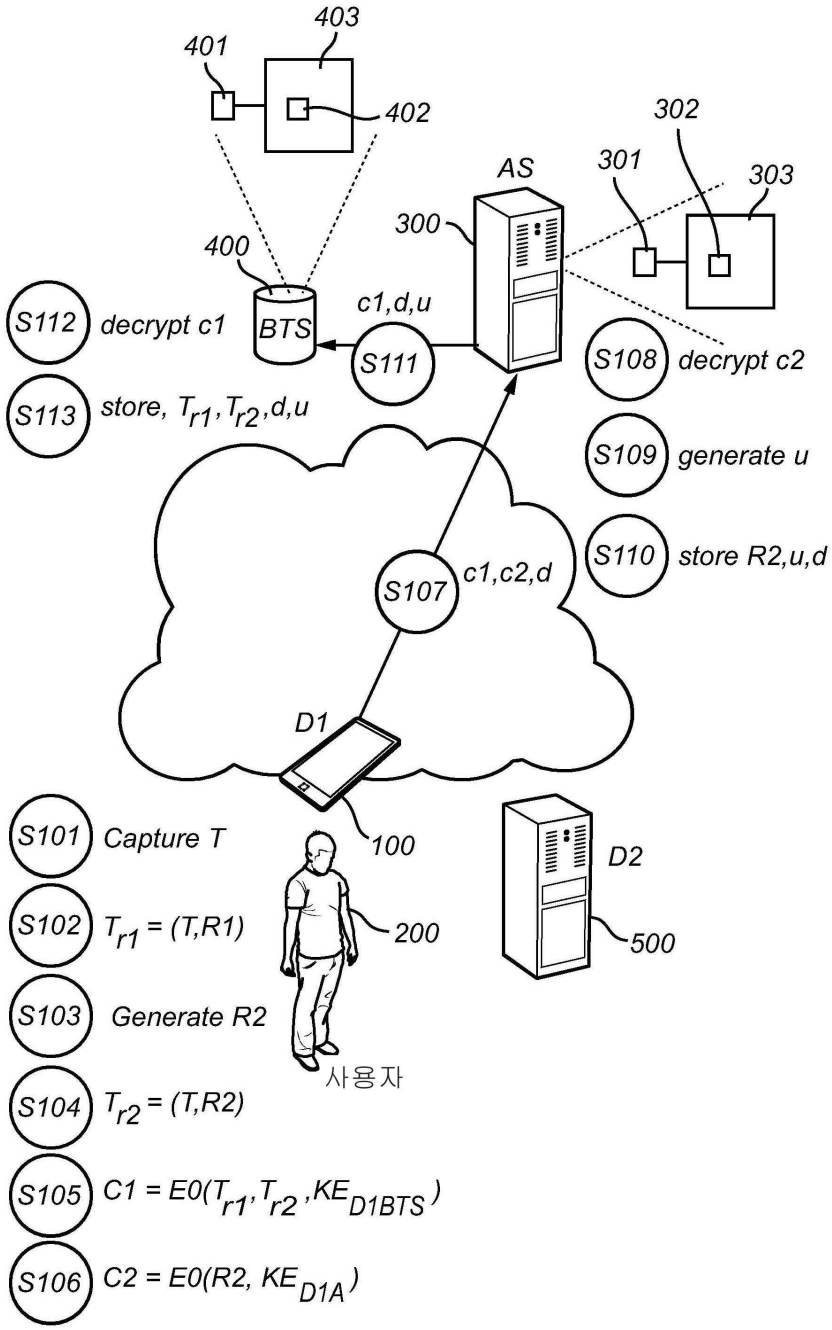
도면2



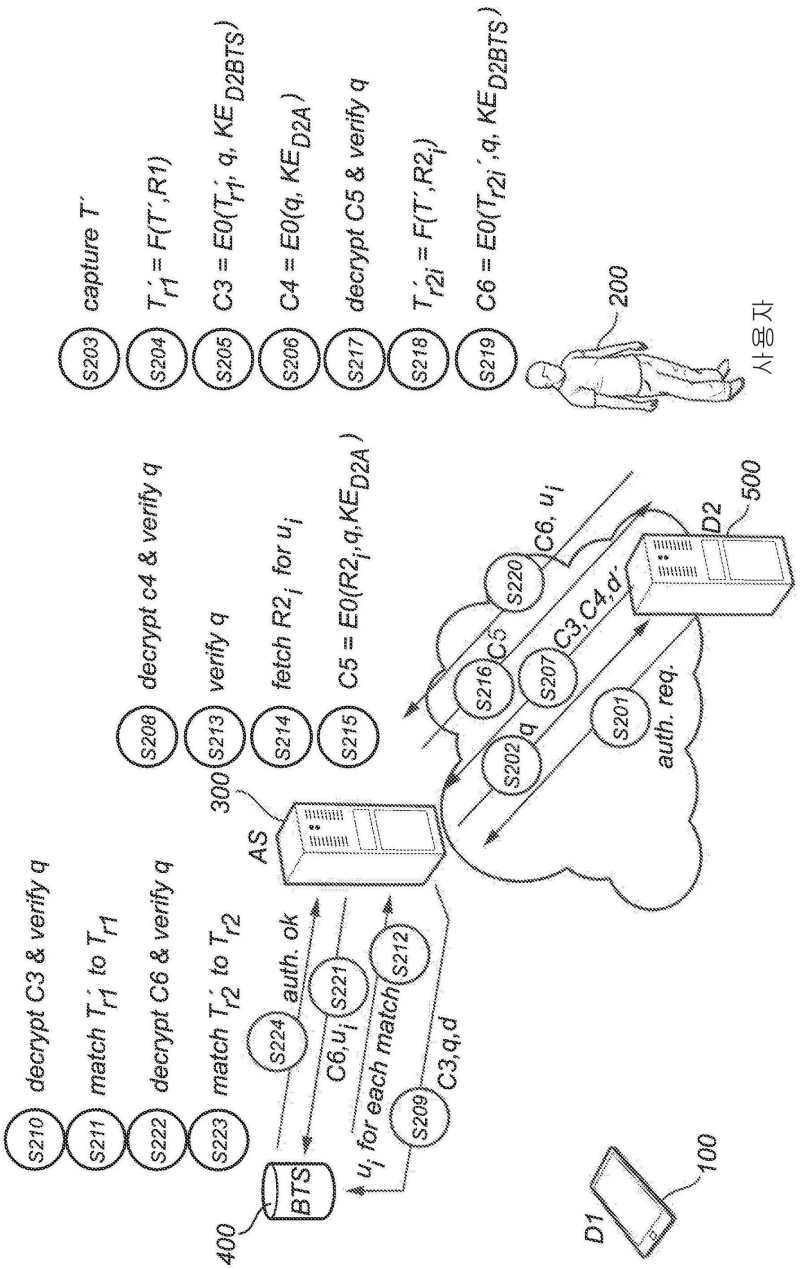
도면3



도면4


403
401
402
302
AS
301
303
300
400
BTS
c1,d,u
S112
decrypt c1
S111
S108
decrypt c2
S113
store, T_{r1},T_{r2},d,u
S109
generate u
S110
store R2,u,d
S107
c1,c2,d
D1
S101
Capture T
100
D2
S102
T_{r1} = (T,R1)
200
500
S103
Generate R2
사용자
S104
T_{r2} = (T,R2)
S105
C1 = E0(T_{r1},T_{r2},KE_{D1BTS})
S106
C2 = E0(R2, KE_{D1A})

도면5


S203 capture T´
S204 T´r1 = F(T´,R1)
S205 C3 = E0(T´r1, q, KE_D2BTS)
S206 C4 = E0(q, KE_D2A)
S217 decrypt C5 & verify q
S218 T´r2i = F(T´,R2i)
S219 C6 = E0(T´r2i ,q, KE_D2BTS)
200
사용자
S208 decrypt c4 & verify q
S213 verify q
S214 fetch R2i for ui
S215 C5 = E0(R2i,q,KE_D2A)
300
AS
S210 decrypt C3 & verify q
S211 match T´r1 to Tr1
S222 decrypt C6 & verify q
S223 match T´r2 to Tr2
S224 auth. ok
C6,ui S221
ui for each match S212
S209 C3,q,d
400
BTS
D1
100
S220 C6, ui
S216 C5
S207 C3,C4,d´
S202 q
S201 auth. req.
D2
500