(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년06월17일
(11) 등록번호 10-1528112
(24) 등록일자 2015년06월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2014-0162852
(22) 출원일자 2014년11월20일
심사청구일자 2014년11월20일
(56) 선행기술조사문헌
WO2013139221 A1
KR101460541 B1
US20100106964 A1
김현성 외 1명, 클라우드 컴퓨팅 보안을 위한 준동형 암호 기법 개발 및 응용들, 보안공학연구논문지 제10권 제2호 (2013.04.)

(73) 특허권자
중앙대학교 산학협력단
서울 동작구 흑석동 221
(72) 발명자
허준범
경기도 용인시 기흥구 보정로 30, 116동 1102호 (보정동, 행원마을 동아솔레시티아파트)
한창희
인천광역시 남동구 호구포로 924, 109동 2204호 (만수동, 햇빛마을벽산아파트)
(74) 대리인
송인호, 민영준, 최관락

전체 청구항 수 : 총 5 항 심사관 : 양종필

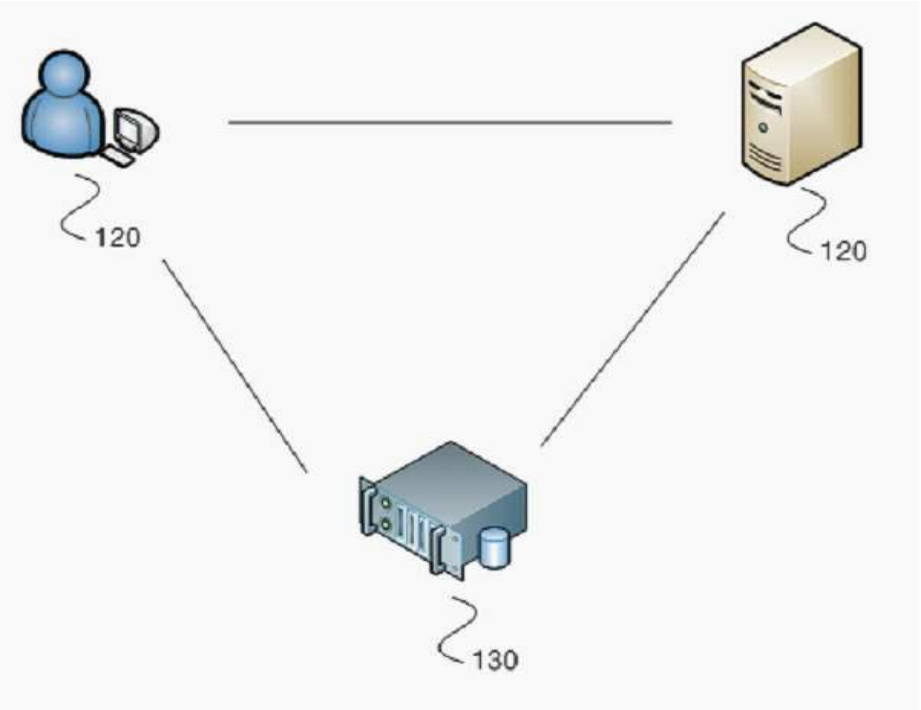
(54) 발명의 명칭 **생체 특성에 기반해 데이터 서버로 액세스하고자 하는 사용자를 인증하기 위한 클라우드 서버**

(57) 요 약

생체 특성에 기반해 데이터 서버로 액세스하고자 하는 사용자를 인증하기 위한 클라우드 서버가 개시된다. 개시된 클라우드 서버는 준동형 암호화 기법을 이용하여, 생체 특성에 기반해 데이터 서버로 액세스하고자 하는 사용자를 인증하기 위한 클라우드 서버로서, n(2 이상의 정수)개의 사용자의 등록을 위해, 상기 n개의 사용자와 대응

(뒷면에 계속)

대 표 도 - 도1



되는 암호화된 등록용 생체 특성 데이터인 n개의 제1 암호문을 저장하는 등록부; 및 인증 받고자 하는 사용자에 대한 인증용 생체 특성 데이터를 암호화한 제2 암호문와 상기 n개의 제1 암호문을 이용하여 상기 인증 받고자 하는 사용자를 인증하는 인증부;를 포함하되, 상기 인증부는, 상기 n개의 제1 암호문 전체에 대하여, 상기 제1 암호문과 상기 제2 암호문 사이의 가감산 연산을 수행함으로써, n개의 제3 암호문들을 생성하는 연산부; 및 상기 n개의 제3 암호문의 복호화를 수행함으로써, 상기 등록용 생체 특성 데이터와 상기 인증용 생체 특성 데이터를 뺀 값인 생체 특성 차이 데이터를 n개 산출하는 차이 데이터 산출부;를 포함하고, 상기 n개의 생체 특성 차이 데이터 중 최소값이 기 설정된 임계값 이상인 경우, 상기 인증 받고자 하는 사용자를 정당한 사용자로 인증한다.

이 발명을 지원한 국가연구개발사업
과제고유번호 ITAH0301140110440001000100100
부처명 산업통상자원부
연구관리전문기관 정보통신산업진흥원
연구사업명 지식경제기술혁신사업
연구과제명 산업기밀 정보유출 방지를 위한 융합보안 SW 연구 및 전문인력양성
기 여 율 1/3
주관기관 중앙대학교 산학협력단
연구기간 2014.06.01 ~ 2017.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 2014029608
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 이공분야기초연구사업
연구과제명 분산 클라우드컴퓨팅을 위한 보안 및 프라이버시 계층 연구 및 개발
기 여 율 1/3
주관기관 중앙대학교 산학협력단
연구기간 2013.06.01 ~ 2016.05.31
이 발명을 지원한 국가연구개발사업
과제고유번호 2014011250
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 이공분야기초연구사업
연구과제명 클라우드 컴퓨팅 환경에서의 스마트 기기 및 서비스 보안
기 여 율 1/3
주관기관 중앙대학교 산학협력단
연구기간 2012.05.01 ~ 2015.04.30

명 세 서

청구범위

청구항 1

준동형 암호화 기법을 이용하여, 생체 특성에 기반해 데이터 서버로 액세스하고자 하는 사용자를 인증하기 위한 클라우드 서버에 있어서,

n(2 이상의 정수)개의 사용자의 등록을 위해, 상기 n개의 사용자와 대응되는 암호화된 등록용 생체 특성 데이터인 n개의 제1 암호문을 저장하는 등록부; 및

인증 받고자 하는 사용자에 대한 인증용 생체 특성 데이터를 암호화한 제2 암호문와 상기 n개의 제1 암호문을 이용하여 상기 인증 받고자 하는 사용자를 인증하는 인증부;를 포함하되,

상기 인증부는, 상기 n개의 제1 암호문 전체에 대하여, 상기 제1 암호문과 상기 제2 암호문 사이의 가감산 연산을 수행함으로써, n개의 제3 암호문들을 생성하는 연산부; 및 상기 n개의 제3 암호문의 복호화를 수행함으로써, 상기 등록용 생체 특성 데이터와 상기 인증용 생체 특성 데이터를 뺀 값인 생체 특성 차이 데이터를 n개 산출하는 차이 데이터 산출부;를 포함하고,

상기 n개의 생체 특성 차이 데이터 중 최소값이 기 설정된 임계값 이상인 경우, 상기 인증 받고자 하는 사용자를 정당한 사용자로 인증하는 것을 특징으로 하는 클라우드 서버.

청구항 2

제1항에 있어서,

상기 n개의 제1 암호문을 아래의 수학식과 같이 표현되는 것을 특징으로 하는 클라우드 서버.

$$Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_1),$$
$$Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_2),$$
$$\vdots$$
$$Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_n).$$

여기서, k_i는 n개의 사용자 각각에서 생성된 랜덤 키, (k_{sn}, k'_{sn}) 는 n번째 사용자 등록 시 상기 데이터 서버에서 생성된 키 쌍, m_1 내지 m_n은 상기 n개의 사용자 각각의 등록용 생체 특성 데이터, Enc( )는 준동형 암호화 함수를 각각 의미함.

청구항 3

제2항에 있어서,

최초의 등록 사용자인 제1 사용자를 등록하는 경우, 상기 등록부는 상기 데이터 서버에서 수신된 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$(= $Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_1)$, n=1)를 상기 제1 암호문으로서 저장하고 있되,

상기 데이터 서버는 상기 제1 사용자로부터 암호문 $Enc_{k_1}(m_1)$를 수신하고, 상기 제1 사용자의 등록 시 생

성되는 키 쌍 (k_{s1}, k'_{s1})를 이용하여 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$를 생성하는 것을 특징으로 하는 클라우드 서버.

청구항 4

제3항에 있어서,

상기 제1 사용자를 제외한 차후의 제k(2≤k≤n) 사용자를 등록하는 경우, 상기 등록부는,

제1 사용자 내지 제k-1 사용자 각각의 제1 암호문을 갱신하되, 제k-1 사용자 등록 시 저장되어 있던 제1 암호문과, 키 $k_k - (k_{s(k-1)} + k'_{s(k-1)}) + (k_{sk} + k'_{sk})$를 이용하여 0를 암호화한 암호문 $Enc_{k_k - (k_{s(k-1)} + k'_{s(k-1)}) + (k_{sk} + k'_{sk})}(0)$를 합을 통해 갱신을 수행하고,

상기 제k-1 사용자 등록 시 저장되어 있던 상기 클라우드 서버의 암호키 $\sum_{i=1}^{k} k_i + k_{sk}$를 이용하여 0를 암호화한 암호문 $Enc_{\sum_{i=1}^{k} k_i + k_{sk}}(0)$과, 상기 제k 사용자에서 전송된 암호문 $Enc_{k_k}(m_k)$와, 키 $(k_{sk} + k'_{sk}) - k_{s(k-1)}$를 이용하여 0을 암호화한 암호문 $Enc_{(k_{sk} + k'_{sk}) - k_{s(k-1)}}(0)$를 이용하여 상기 제k 사용자의 제1 암호문을 저장하는 것을 특징으로 하는 클라우드 서버.

청구항 5

제4항에 있어서,

상기 연산부는 아래의 수학식을 이용하여 상기 n개의 제3 암호문들을 생성하고, 상기 차이 데이터 산출부는 상기 제k 사용자 등록 시 저장된 상기 클라우드 서버의 암호키 $\sum_{i=1}^{k} k_i + k_{sk}$를 이용하여 상기 n개의 제3 암호문의 복호화를 수행하는 것을 특징으로 하는 클라우드 서버.

$$
\begin{aligned}
&Enc_{\sum_{i=1}^{n} k_i+k_{sn}+k'_{sn}}(m_1) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i+k_{sn}}(m_1 - m_c), \\
&Enc_{\sum_{i=1}^{n} k_i+k_{sn}+k'_{sn}}(m_2) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i+k_{sn}}(m_2 - m_c), \\
&\vdots \\
&Enc_{\sum_{i=1}^{n} k_i+k_{sn}+k'_{sn}}(m_n) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i+k_{sn}}(m_n - m_c).
\end{aligned}
$$

여기서, m_c는 인증 받고자 하는 사용자의 인증용 생체 특성 데이터를 의미함.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 준동형 암호화 기법을 이용하여, 생체 특성에 기반해 데이터 서버로 액세스하고자 하는 사용자를 인증하기 위한 클라우드 서버에 관한 것이다.

배 경 기 술

[0002] IT 환경이 기존의 컴퓨팅 환경에서 클라우드 컴퓨팅 환경으로 점차 변하고 있다. 기존의 컴퓨팅 환경에서는 개인이 자신의 저장매체와 디지털 데이터를 관리하였지만, 클라우드 컴퓨팅 환경에서는 서비스 제공자가 고객들에게 스토리지와 같은 IT 자원을 제공하고, 고객들은 스마트폰, 태블릿 PC 등의 다양한 매체를 이용하여 인터넷이 가능한 모든 곳에서 데이터, 네트워크, 콘텐츠 등을 사용할 수 있도록 서비스를 제공한다

[0003] 하지만, 클라우드 컴퓨팅의 이러한 도입을 활성화하기 위해서는 선결되어야 하는 큰 문제가 있다. 최근 빈번히 발생하는 기업체의 고객 정보 유출 및 개인 사용자들의 위치 정보를 비롯한 여러 개인정보 유출 등의 일련의 사건들을 통해서 현재 서버가 제공하는 데이터 보호 기술에 한계가 있다는 것을 알 수 있다

[0004] 특히, 생체 특성(biometric trait), 일례로, 지문, 홍채 등은 사람들을 식별할 수 있는 가장 신뢰할 수 있는 방법 중 하나이지만, 생체 특성이 노출되는 경우, 치명적인 문제가 발생하는 단점이 존재한다.

[0005] 예를 들어, 사용자 A가 사용자 B로 지문을 사용한 인증을 수행하는 경우를 가정하면, 사용자 B는 미리 사용자 A의 지문을 알고 있다. 이 때, 사용자 A가 사용자 B에게 액세스하려는 경우, 사용자 A는 먼저 지문을 이용하여 인증을 수행한다. 만약, 사용자 A의 지문 데이터가 대중에게 공개되면, 누구나 간단히 사용자 A의 지문 데이터를 획득하여 사용자 A로 위장할 수 있다. 이는 사용자의 프라이버시를 침해하고 전체 시스템을 무효화할 수도 있는 문제점이 있다.

발명의 내용

해결하려는 과제

[0006] 상기한 바와 같은 종래기술의 문제점을 해결하기 위해, 본 발명에서는 준동형 암호화 기법을 이용하여, 생체 특

성을 노출시키기 않으면서 데이터 서버로 액세스하고자 하는 사용자를 인증하기 위한 클라우드 서버를 제안하고자 한다.

[0007] 본 발명의 다른 목적들은 하기의 실시예를 통해 당업자에 의해 도출될 수 있을 것이다.

과제의 해결 수단

[0008] 상기한 목적을 달성하기 위해 본 발명의 바람직한 일 실시예에 따르면, 준동형 암호화 기법을 이용하여, 생체 특성에 기반해 데이터 서버로 액세스하고자 하는 사용자를 인증하기 위한 클라우드 서버에 있어서, n(2 이상의 정수)개의 사용자의 등록을 위해, 상기 n개의 사용자와 대응되는 암호화된 등록용 생체 특성 데이터인 n개의 제1 암호문을 저장하는 등록부; 및 인증 받고자 하는 사용자에 대한 인증용 생체 특성 데이터를 암호화한 제2 암호문와 상기 n개의 제1 암호문을 이용하여 상기 인증 받고자 하는 사용자를 인증하는 인증부;를 포함하되, 상기 인증부는, 상기 n개의 제1 암호문 전체에 대하여, 상기 제1 암호문과 상기 제2 암호문 사이의 가감산 연산을 수행함으로써, n개의 제3 암호문들을 생성하는 연산부; 및 상기 n개의 제3 암호문의 복호화를 수행함으로써, 상기 등록용 생체 특성 데이터와 상기 인증용 생체 특성 데이터를 뺀 값인 생체 특성 차이 데이터를 n개 산출하는 차이 데이터 산출부;를 포함하고, 상기 n개의 생체 특성 차이 데이터 중 최소값이 기 설정된 임계값 이상인 경우, 상기 인증 받고자 하는 사용자를 정당한 사용자로 인증하는 것을 특징으로 하는 클라우드 서버가 제공된다.

[0009] 상기 n개의 제1 암호문을 아래의 수학식과 같이 표현될 수 있다.

$$
\begin{aligned}
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_1),\\
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_2),\\
&\vdots\\
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_n).
\end{aligned}
$$

[0010]

[0011] 여기서, k_i는 n개의 사용자 각각에서 생성된 랜덤 키, (k_{sn}, k'_{sn}) 는 n번째 사용자 등록 시 상기 데이터 서버에서 생성된 키 쌍, m_1 내지 m_n은 상기 n개의 사용자 각각의 등록용 생체 특성 데이터, Enc( )는 준동형 암호화 함수를 각각 의미함.

[0012] 최초의 등록 사용자인 제1 사용자를 등록하는 경우, 상기 등록부는 상기 데이터 서버에서 수신된 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$ (= $Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_1)$, n=1)를 상기 제1 암호문으로서 저장하고 있되, 상기 데이터 서버는 상기 제1 사용자로부터 암호문 $Enc_{k_1}(m_1)$를 수신하고, 상기 제1 사용자의 등록 시 생성되는 키 쌍 (k_{s1}, k'_{s1})를 이용하여 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$를 생성할 수 있다.

[0013] 상기 제1 사용자를 제외한 차후의 제k(1≤k≤n) 사용자를 등록하는 경우, 상기 등록부는, 제1 사용자 내지 제k-1 사용자 각각의 제1 암호문을 갱신하되, 제k-1 사용자 등록 시 저장되어 있던 제1 암호문과, 키 $k_k - (k_{s(k-1)} + k'_{s(k-1)}) + (k_{sk} + k'_{sk})$를 이용하여 0를 암호화한 암호문 $Enc_{k_k - (k_{s(k-1)} + k'_{s(k-1)}) + (k_{sk} + k'_{sk})}(0)$를 합을 통해 갱신을 수행하고, 상기 제k-1 사용자 등록

시 저장되어 있던 상기 클라우드 서버의 암호키 $\sum_{i=1}^{k} k_i + k_{sk}$ 를 이용하여 0를 암호화한 암호문 $Enc_{\sum_{i=1}^{k} k_i + k_{sk}}(0)$ 과, 상기 제k 사용자에서 전송된 암호문 $Enc_{k_k}(m_k)$ 와, 키 $(k_{sk} + k'_{sk}) - k_{s(k-1)}$ 를 이용하여 0을 암호화한 암호문 $Enc_{(k_{sk} + k'_{sk}) - k_{s(k-1)}}(0)$ 를 이용하여 상기 k번째 사용자의 제1 암호문을 저장할 수 있다.

[0014] 상기 연산부는 아래의 수학식을 이용하여 상기 n개의 제3 암호문들을 생성하고, 상기 차이 데이터 산출부는 상기 제k 사용자 등록 시 저장된 상기 클라우드 서버의 암호키 $\sum_{i=1}^{k} k_i + k_{sk}$ 이용하여 상기 n개의 제3 암호문의 복호화를 수행할 수 있다.

$$
\begin{aligned}
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_1) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i + k_{sn}}(m_1 - m_c), \\
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_2) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i + k_{sn}}(m_2 - m_c), \\
&\vdots \\
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_n) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i + k_{sn}}(m_n - m_c).
\end{aligned}
$$

[0015]

[0016] 여기서, m_c는 인증 받고자 하는 사용자의 인증용 생체 특성 데이터를 의미함.

발명의 효과

[0017] 본 발명에 따른 클라우드 서버는 준동형 암호화 기법을 이용하여, 생체 특성을 노출시키기 않으면서 데이터 서버로 액세스하고자 하는 사용자를 인증할 수 있는 장점이 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일 실시예에 따른 생체 정보 기반 식별 시스템의 개략적인 구성을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 클라우드 서버(130)의 개략적인 구성을 도시한 도면이다.

도 3 내지 도 8는 본 발명의 일 실시예에 따른 생체 정보 기반 식별 방법의 전체적인 흐름도를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0020] 첨부된 도면을 참조하여 본 발명을 설명하기에 앞서, 다음과 같은 기술들이 본 발명에 사용될 수 있다.

[0021] 1. 핑거코드 기반의 인증(Fingercode-based Identification)

[0022] 핑거코드는 지문 이미지를 스캔하여 정수 데이터로 변환한 지문 데이터를 의미한다. 사용자는 자신의 지문 이미지를 스캔하여 핑거코드를 추출한다. 핑거코드는 N개의 독립된 특징 코드의 체인으로 구성된다. 일례로, 핑거코드는 8비트의 정수 벡터일 수 있다.

[0023] 만약, 두 개의 핑거코드 $m_1=[x_{11},x_{12},...,x_{1N}]$ 과 $m_2 = [x_{21},x_{22},...,x_{xN}]$ 가 있는 경우, 두 개의 핑거코드의 유사도는 유클리드 거리를 이용하여 산출될 수 있으며, 이는 수학식 1과 같이 표현될 수 있다.

수학식 1

[0024] $$dist_1 = \sqrt{(m_1 - m_2)^2}$$

[0025] 여기서, $dist_1$는 유클리드 거리를 의미하고, $(m_1 - m_2)^2$는 $(x_{11} - x_{21})^2 + (x_{12} - x_{22})^2 + ... + (x_{1N} - x_{2N})^2$를 의미한다. 만약, 유클리드 거리가 기 설정된 임계값 이하인 경우, 두 개의 핑거코드는 동일한 것으로 가정한다.

[0026] 2. 대칭 준동형 암호화 기법(Symmetric Homomorphic Encryption)

[0027] 준동형 암호화 기법은 암호화된 데이터에 대해 복호화하지 않고 연산을 수행할 수 있는 기법을 의미한다. Enc( )가 준동형 암호화 함수인 경우, 주어진 암호키 k에 대해 암호화 함수는 아래의 수학식 2와 같은 연산이 수행된다.

수학식 2

[0028] $$Enc_k(m_1 \ \triangle \ m_2) \quad \longleftarrow \quad Enc_k(m_1) \ \triangledown \ Enc_k(m_2)$$

[0029] 여기서, $\triangle$ 와 $\triangledown$ 는 오퍼레이터를 나타낸다.

[0030] 특히, 대칭 준동형 암호화 기법은 덧셈 연산, 뺄셈 연산 및 곱셈 연산을 지원한다. 즉, 두 개의 암호문 $Enc_{k_1}(m_1)$ 및 $Enc_{k_2}(m_2)$가 있는 경우, 아래의 수학식 3과 같은 연산이 수행된다.

수학식 3

[0031] $$Enc_{(k1+k2)}(m_1 + m_2) = Enc_{k1}(m_1) + Enc_{k2}(m_2)$$

[0032] 공유 키 기반의 준동형 암호화 기법에서, 암호문은 같은 키를 이용하여 암호화되지만, 대칭 준동형 암호화 기법은 동일한 키를 이용하여 암호화하여 암호문을 생성하지 않으며, 각각의 암호문은 개인 비밀 키를 사용하여 암호화된다.

[0033] 이하, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0034] 도 1은 본 발명의 일 실시예에 따른 생체 정보 기반 식별 시스템의 개략적인 구성을 도시한 도면이다.

[0035] 도 1을 참조하면, 본 발명의 일 실시예에 따른 생체 특성 기반 식별 시스템(100)는 사용자 단말(110), 데이터 서버(120) 및 클라우드 서버(130)를 포함한다.

[0036] 사용자(110)는 생체 정보 기반 식별 시스템(100)의 일반적인 사용자와 대응되며, 사용자의 생체 특성 데이터(biometric trait), 일례로, 지문 데이터를 이용하여 데이터 서버(120)로 액세스를 위한 식별 내지 인증을 수행한다. 한편, 설명의 편의를 위해, 생체 특성 데이터를 지문 데이터로 가정하여 설명하지만 본 발명이 이에 한정되는 것은 아니다.

[0037] 클라우드 서버(130)는 사용자 식별 내지 인증을 위한 동작들을 아웃소싱(outsourcing)한다. 즉, 데이터 서버(120)에서 수행하는 사용자 식별 내지 인증을 위한 동작들 중 적어도 일부는 클라우드 서버(130)가 대신 수행한다. 이에 따라, 식별 내지 인증 동작이 빨라지는 장점이 있다.

[0038] 한편, 외부에 있는 공격자가 사용자(110)에서 전송되는 생체 특성 데이터를 도청하는 것으로 가정하면, 공격자는 노출된 생체 특성 데이터를 이용하여 식별 과정을 바이패스하고, 데이터 서버(120)에 성공적으로 접근할 수 있다. 이 때, 생체 특성들이 누출되는 경우 이는 폐기될 수 없게 되므로, 생체 정보가 공격자로부터 비밀로 유지되어야 하는 것이 중요하다. 또한, 클라우드 서버(130)가 불법적인 수익을 얻기 위해 외부의 악의적인 사용자와 결탁하여 사용자의 생체 특성 데이터를 추출하는 경우인 내부 공격이 있을 수도 있다. 따라서, 생체 특성 데이터는 소유자인 사용자만이 접근 가능한 것이 합리적이다.

[0039] 따라서, 본 발명에서는 사용자(110)의 생체 특성 데이터를 노출시키지 않으면서 사용자의 식별 내지 인증을 수행하는 생체 특성 기반 식별 시스템(100)을 제공하고자 한다.

[0040] 도 2를 참조하면, 클라우드 서버(130)는 등록부(131) 및 인증부(132)를 포함하며, 인증부(132)는 연산부(1321) 및 차이 데이터 산출부(1322)를 포함한다.

[0041] 등록부(131)는 n(2 이상의 정수)개의 사용자의 등록을 위해, n개의 사용자와 대응되는 암호화된 등록용 생체 특성 데이터인 n개의 제1 암호문을 저장한다.

[0042] 본 발명의 일 실시예에 따르면, n개의 제1 암호문은 아래의 수학식 4과 같이 표현될 수 있다.

수학식 4

[0043]
$$
\begin{aligned}
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_1),\\
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_2),\\
&\vdots\\
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_n).
\end{aligned}
$$

[0044] 여기서, k_i는 n개의 사용자 각각에서 생성된 랜덤 키, (k_{sn}, k'_{sn}) 는 n번째 사용자 등록 시, 데이터 서버(120)에서 생성된 키 쌍, m_1 내지 m_n은 n개의 사용자 각각의 등록용 생체 특성 데이터, Enc()는 준동형 암호화 함수를 각각 의미한다.

[0045] 이 때, 최초의 사용자(Initial Client)의 등록과 차후의 사용자(Subsequent Client)의 등록은 서로 다른 방식을 통해 이루어질 수 있다.

[0046] 본 발명의 일 실시예에 따르면, 최초의 등록 사용자인 제1 사용자를 등록하는 경우, 등록부(131)는 데이터 서버(120)에서 수신된 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$ (= $Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_1)$, n=1)를 제1 암호문으로서 저장할 수 있다. 이 때, 데이터 서버(120)는 제1 사용자로부터 암호문 $Enc_{k_1}(m_1)$를 수신하고, 제1 사용자의 등록 시 생성되는 키 쌍 (k_{s1}, k'_{s1})를 이용하여 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$를 생성할 수 있다.

[0047] 또한, 본 발명의 다른 실시예에 따르면, 제1 사용자를 제외한 차후의 제k(1≤k≤n) 사용자를 등록하는 경우, 등록부(131)는 제1 사용자 내지 제k-1 사용자 각각의 제1 암호문을 갱신하고, k번째 사용자의 제1 암호문을 저장할 수 있다.

[0048] 이 때, 제1 사용자 내지 제k-1 사용자의 제1 암호문 갱신의 경우, 등록부(131)는 제k-1 사용자 등록 시 저장되어 있던 제1 암호문과, 키 $k_k - (k_{s(k-1)} + k'_{s(k-1)}) + (k_{sk} + k'_{sk})$를 이용하여 0를 암호화한 암호문 $Enc_{k_k - (k_{s(k-1)} + k'_{s(k-1)}) + (k_{sk} + k'_{sk})}(0)$를 합을 통해 갱신을 수행할 수 있다.

[0049] 또한, k번째 사용자의 제1 암호문을 저장의 경우, 등록부(131)는 제k-1 사용자 등록 시 저장되어 있던 클라우드 서버(130)의 암호키 $\sum_{i=1}^{k} k_i + k_{sk}$를 이용하여 0를 암호화한 암호문 $Enc_{\sum_{i=1}^{k} k_i + k_{sk}}(0)$과, 제k 사용자에서 전송된 암호문 $Enc_{k_k}(m_k)$와, 키 $(k_{sk} + k'_{sk}) - k_{s(k-1)}$를 이용하여 0을 암호화한 암호문 $Enc_{(k_{sk} + k'_{sk}) - k_{s(k-1)}}(0)$를 이용하여 k번째 사용자의 제1 암호문을 저장할 수 있다.

[0050] 그리고, 인증부(132)는 인증 받고자 하는 사용자에 대한 인증용 생체 특성 데이터를 암호화한 제2 암호문와 n개의 제1 암호문을 이용하여 인증 받고자 하는 사용자를 인증한다.

[0051] 보다 상세하게, 인증부(132) 내의 연산부(1321)는, n개의 제1 암호문 전체에 대하여, 제1 암호문과 제2 암호문 사이의 가감산 연산을 수행함으로써, n개의 제3 암호문들을 생생할 수 있다. 그리고, 차이 데이터 산출부(1322)는 n개의 제3 암호문의 복호화를 수행함으로써, 등록용 생체 특성 데이터와 상기 인증용 생체 특성 데이터를 뺀 값인 생체 특성 차이 데이터를 n개 산출한다.

[0052] 따라서, n개의 생체 특성 차이 데이터 중 최소값이 기 설정된 임계값 이상인 경우, 인증 받고자 하는 사용자를 정당한 사용자로 인증한다.

[0053] 본 발명의 일 실시예에 따르면, 연산부(1321)는 아래의 수학식 5를 이용하여 n개의 제3 암호문들을 생성하고, 차이 데이터 산출부(1322)는 상기 제k 사용자 등록 시 저장된 상기 클라우드 서버의 암호키 $\sum_{i=1}^{k} k_i + k_{sk}$ 이용하여 n개의 제3 암호문의 복호화를 수행할 수 있다.

수학식 5

$$
\begin{aligned}
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_1) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i + k_{sn}}(m_1 - m_c), \\
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_2) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i + k_{sn}}(m_2 - m_c), \\
&\vdots \\
&Enc_{\sum_{i=1}^{n} k_i + k_{sn} + k'_{sn}}(m_n) + Enc_{-k'_{sn}}(-m_c) \\
&= Enc_{\sum_{i=1}^{n} k_i + k_{sn}}(m_n - m_c).
\end{aligned}
$$

[0054]

[0055] 여기서, m_c는 인증 받고자 하는 사용자의 인증용 생체 특성 데이터를 의미한다.

[0056] 도 3 내지 도 8는 본 발명의 일 실시예에 따른 생체 정보 기반 식별 방법의 전체적인 흐름도를 도시한 도면이다.

[0057] 이하, 도 3 내지 도 8를 참조하여, 각 구성 요소 별 기능 및 각 단계별로 수행되는 과정을 상세하게 설명한다.

[0058] 단계(310)에서, 사용자(110)는 암호화된 등록용 지문 데이터를 전송하여 사용자 등록을 수행한다. 앞서 설명한 바와 같이, 최초의 사용자의 등록과 차후의 사용자의 등록은 서로 다른 방식을 통해 이루어진다.

[0059] 이하, 도 4 내지 도 7을 참조하여, 사용자 등록을 상세하게 설명한다.

[0060] 도 4는 최초의 사용자인 제1 사용자의 등록의 세부적인 단계를 도시한 도면이고, 도 5는 도 4에서 전송되는 메시지의 흐름을 나타내는 도면이다.

[0061] 단계(402)에서, 제1 사용자는 자신의 지문을 스캔하여 등록용 지문 데이터 즉, 핑거코드를 추출한다.

[0062] 본 발명의 일 실시예에 따르면, 제1 사용자의 지문 데이터 m_1는 아래의 수학식 6과 같이 표현될 수 있다.

수학식 6

[0063] $$m_1 = [x_{11}, x_{12}, ..., x_{1N}]$$

[0064] 여기서, x_{1k}는 고정된 크기의 정수($1 \le k \le N$)를 나타낸다.

[0065] 그리고, 단계(404)에서 제1 사용자는 등록용 지문 데이터 m_1를 제1 랜덤 키 k_1로 암호화하여 데이터 서버(120)로 전송한다. 제1 랜덤 키 k_1는 영구적인 것이 아니며, 1회용 키이다. 즉, 제1 사용자가 데이터 서버(120)에 액세스를 원하는 경우, 새로운 암호화 키가 등록용 지문 데이터를 암호화하기 위해 생성된다.

[0066] 본 발명의 일 실시예에 따르면, 등록용 지문 데이터 m_1의 암호화는 아래의 수학식 7과 같이 표현될 수 있다.

수학식 7

[0067] $$Enc_{k_1}(m_1) = [x_{11} + k_{11} \pmod M, x_{12} + k_{12} \pmod M, ..., x_{1N} + k_{1N} \pmod M],$$
$$k_1 = [k_{11}, k_{12}, ..., k_{1N}]$$

[0068] 여기서, $Enc_{k_1}(m_1)$는 등록용 지문 데이터 m_1를 암호화한 암호문, M는 기 설정된 큰 정수를 각각 의미한다.

[0069] 그 후, 단계(406)에서, 데이터 서버(120)는 암호문 $Enc_{k_1}(m_1)$를 재암호화($Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$)하여 클라우드 서버(130)로 전송한다. 이에 따라, 제1 사용자, 데이터 서버(120) 및 클라우드 서버(130)는 단순한 키-교환 프로토콜(simple key-exchange protocol)을 수행하기 위해 그들 사이의 보안 채널을 확립할 수 있다.

[0070] 본 발명의 일 실시예에 따르면, 데이터 서버(120)는 제1 키 쌍 (k_{s1}, k'_{s1})를 이용하여 등록용 지문 데이터 m_1를 재암호화하여, 암호문 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$를 생성할 수 있다. 여기서, 제1 키 쌍 (k_{s1}, k'_{s1})은 $k_{s1} = [k_{s11}, k_{s12}, ..., k_{s1N}]$ 및 $k'_{s1} = [k'_{s11}, k'_{s12}, ..., k'_{s1N}]$를 의미하는 것으로서, 영구적일 수 있으며, 제1 사용자의 등록 과정에만 사용될 수 있다.

[0071] 계속하여, 단계(408)에서, 제1 사용자는 제1 랜덤 값 r_1($r_1 = [r_{11}, r_{12}, ..., r_{1N}]$)을 생성하고, 제1 랜덤 키 k_1와 제1 랜덤 값 r_1의 합인 키 $k_1 + r_1$를 데이터 서버(120)로 전송한다. 그리고, 단계(410)에서 데이터 서버(120)는 키 쌍 중 하나인 키 k_{s1}에 키 $k_1 + r_1$를 더하여 키 $k_1 + k_{s1} + r_1$를 클라우드 서버(130)로 전송하며, 단계(412)에서 제1 사용자는 제1 랜덤 값 r_1를 직접 클라우드 서버(130)로 전송한다.

[0072] 그 후, 단계(414)에서 클라우드 서버(120)는 데이터 서버(120)에서 전송된 키 $k_1 + k_{s1} + r_1$에서 제1 사용자로부터 전송된 제1 랜덤 값 r_1를 뺄셈하여 키 $k_1 + k_{s1}$를 획득한다. 이 때, 클라우드 서버(130)는 개인 키

들을 알지 못한다.

[0073] 상기의 과정을 통해 제1 사용자의 등록이 완료되며, 클라우드 서버(130)는 클라우드 암호키 $k_1 + k_{s1}$, 제1 암호문인 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$ 및 암호문 $Enc_{k_1+k_{s1}}(0)$를 획득한다. 여기서, 클라우드 암호키 $k_1 + k_{s1}$는 제1 사용자의 인증 과정에서 클라우드 서버(130)가 사용하는 키를 의미한다. 이 때, 클라우드 암호키 $k_1 + k_{s1}$는 다음 사용자 등록 과정에서 폐지되고, 새로운 사용자가 등록되는 경우 업데이트된다. 또한, 제1 암호문 $Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$는 등록용 지문 데이터 m_1의 암호문이며, 암호문 $Enc_{k_1+k_{s1}}(0)$는 다음 사용자 등록에 사용된다.

[0074] 도 6는 차후의 사용자인 제2 사용자 내지 제n 사용자의 등록의 세부적인 단계를 도시한 도면이고, 도 7는 도 6에서 전송되는 메시지의 흐름을 나타내는 도면이다.

[0075] 보다 상세하게, 도 6 및 도 7에서는 제2 사용자에 대한 등록 과정의 개념을 설명하고 있으며, 이는 제n 사용자의 경우에까지 확장된다. 즉, 제2 사용자에 대한 등록 과정은 제3 사용자 내지 제n 사용자의 등록 과정과 동일하게 적용될 수 있다.

[0076] 단계(602)에서, 제2 사용자는 자신의 지문을 스캔하여 등록용 지문 데이터 즉, 핑거코드를 추출한다.

[0077] 본 발명의 일 실시예에 따르면, 제2 사용자의 등록용 지문 데이터 m_2는 아래의 수학식 8과 같이 표현될 수 있다.

수학식 8

[0078] $$m_2 = [x_{21}, x_{22}, ..., x_{xN}]$$

[0079] 여기서, x_{2k}는 고정된 크기의 정수($1 \le k \le N$)를 나타낸다.

[0080] 그리고, 단계(604)에서 제2 사용자는 등록용 지문 데이터 m_2를 제2 랜덤 키 k_2로 암호화하여($Enc_{k_2}(m_2)$) 직접 클라우드 서버(130)로 전송한다. 제2 랜덤 키 k_2($k_2 = [k_{21}, k_{22}, ..., k_{2N}]$)역시 영구적인 것이 아니며, 1회용 키이다.

[0081] 본 발명의 일 실시예에 따르면, 등록용 지문 데이터 m_2의 암호화, 즉 암호문 $Enc_{k_2}(m_2)$의 생성은 상기의 수학식 7과 유사하게 수행될 수 있다.

[0082] 그 후, 단계(606)에서, 제2 사용자는 제2 랜덤 값 r_2($r_2 = [r_{21}, r_{22}, ..., r_{2N}]$)를 선택하여 데이터 서버(120)로 전송한다.

[0083] 계속하여, 단계(608)에서, 데이터 서버(120)는 새로운 제2 키 쌍 (k_{s2}, k'_{s2})를 생성하고, 제1 키 쌍 (k_{s1}, k'_{s1})을 이용하여 키 $r_2 - (k_{s1} + k'_{s1}) + (k_{s2} + k'_{s2})$ 및 키 $(k_{s2} + k'_{s2}) - k_{s1}$를 산출한다. 그 후, 단계(610)에서, 데이터 서버(120)는 직접 제2 사용자에게로 키 $r_2 - (k_{s1} + k'_{s1}) + (k_{s2} + k'_{s2})$를 전송하고, 클라우드 서버(130)로 키 $(k_{s2} + k'_{s2}) - k_{s1}$를 전송한다.

[0084] 그리고, 단계(612)에서, 제2 사용자는 키 $k_2 - (k_{s1} + k'_{s1}) + (k_{s2} + k'_{s2})$를 산출하고, 이를 클라우드

서버(130)로 전송한다. 이에 따라, 단계(614)에서, 클라우드 서버(130)는 제2 사용자로부터 수신한 정보와 데이터 서버(120)에서 수신한 정보를 이용하여 등록용 지문 데이터 데이터베이스를 아래의 수학식 9와 같이 업데이트한다.

수학식 9

$$Enc_{\sum_{i=1}^{2} k_i + k_{s2} + k'_{s2}}(m_1) = Enc_{k_1 + k_{s1} + k'_{s1}}(m_1) + Enc_{k_2 - (k_{s1} + k'_{s1}) + (k_{s2} + k'_{s2})}(0)$$

$$Enc_{\sum_{i=1}^{2} k_i + k_{s2} + k'_{s2}}(m_2) = Enc_{k_1 + k'_{s2}}(0) + Enc_{k_2}(m_2) + Enc_{(k_{s2} + k'_{s2}) - k_{s1}}(m_2)$$

[0085]

[0086] 여기서, $Enc_{\sum_{i=1}^{2} k_i + k_{s2} + k'_{s2}}(m_1)$ 는 제1 사용자를 위한 암호문이고, $Enc_{\sum_{i=1}^{2} k_i + k_{s2} + k'_{s2}}(m_2)$ 는 제2 사용자를 위한 암호문이다. 따라서, 등록용 지문 데이터 m_1 및 등록용 지문 데이터 m_2는 서로 다른 키를 통해 첫번째로 암호화되었지만, 현재는 같은 키로 암호화됨을 확인할 수 있다.

[0087] 한편, 등록용 지문 데이터 데이터베이스가 업데이트된 후에, 클라우드 서버(130)는 업데이트된 키를 통해 안전 채널(secure channel)를 개시한다. 먼저, 클라우드 서버(130)는 랜덤 값 $r_c = [r_{c1}, r_{c2}, ..., r_{cN}]$ 를 생성하고, 정보 $k_1 + k_{s1} + r_c$ 를 데이터 서버(120)로 전송한다. 그리고, 데이터 서버(120)는 키 k_{s1}를 삭제하고, 키 k_{s2} 를 추가한다. 그 후, 키 k_{s2} 는 키 $k_1 + k_{s2} + r_c$ 를 제2 사용자에게로 전송한다. 제2 사용자는 키 k_2를 더하여, 최종적인 결과인 키 $(k_1 + k_2) + k_{s2} + r_c$ 를 클라우드 서버(130)로 전송한다. 클라우드 서버(130)는 r_c 를 뺌으로써 키를 업데이트한다.

[0088] 동시에, 데이터 서버(120)는 제1 사용자 등록 과정에서 생성된 제1 키 쌍 (k_{s1}, k'_{s1})을 폐지한다. 그리고, 클라우드 서버(130)는 $\sum_{i=1}^{2} k_i + k_{s2} + k'_{s2}$ 를 키로서 사용한다.

[0089] 제3 사용자의 등록 과정은 제2 사용자 등록의 과정과 동일한 방식으로 수행된다. 예를 들어, n번째 사용자가 등록용 지문 데이터 m_n를 등록하는 경우, 데이터 서버(120)는 제n 키 쌍 (k_{sn}, k'_{sn})를 이용하고, 클라우드 서버(130)는 클라우드 암호키 $\sum_{i=1}^{n} k_i + k_{sn}$ 를 이용한다. 따라서, 등록용 지문 데이터 데이터베이스는 상기의 아래의 수학식 4와 같이 업데이트된다. 이 때, k번째 사용자의 등록 과정에서, 데이터 서버(120)는 k-1번째 사용자의 키 쌍 및 k번째 사용자의키 키 쌍만을 저장하고, 그 이전 키 쌍을 제거한다.

[0090] 한편, 클라우드 암호키 $\sum_{i=1}^{n} k_i + k_{sn}$ 의 크기는 n이 증가함에 따라 계속 증가되지 않는다. 변조 동작에서,

$[\sum_{i=1}^{n} k_i + k_{sn} + m_n \ (mod\ M)]$ 와 $[\{\sum_{i=1}^{n} k_i + k_{sn} \ (mod\ M) + m_n\} \ (mod\ M)]$ 는 동일하다.

그러므로, $\sum_{i=1}^{n} k_i + k_{sn}$ 는 $\sum_{i=1}^{n} k_i + k_{sn} \ (mod\ M)$ 과 동일하다.

[0091] 다시, 도 3를 참조하여 생체 정보 기반 식별 방법을 설명한다.

[0092] 단계(320)에서, 클라우드 서버(130)는 인증 받고자 하는 사용자의 인증용 생체 특성 데이터를 이용하여 사용자를 인증한다.

[0093] 도 8는 인증 받고자 하는 사용자의 인증의 세부적인 단계를 도시한 도면이다.

[0094] 단계(802)에서, 인증 받고자 하는 사용자 u_c는 자신의 지문 이미지를 스캔하여 인증용 지문 데이터 m_c를 추출한다. 그리고, 단계(804)에서, 사용자 u_c는 새로운 랜덤 키 k_c를 생성하고, 이를 이용하여 인증용 지문 데이터 m_c를 암호화하여 암호문 $Enc_{k_c}(-m_c)$를 생성하여 직접 클라우드 서버(130)로 전송한다.

[0095] 계속하여, 단계(806)에서, 클라우드 서버(130)는 새로운 랜덤 값 r를 $Enc_{k_c}(-m_c)$에 추가하여 암호문 $Enc_{k_c}(r - m_c)$를 생성하여 데이터 서버(120)로 전송한다(additive homomorphism 알고리즘).

[0096] 그 후, 단계(808)에서, 데이터 서버(120)는 암호문 $Enc_{k_c}(r - m_c)$를 수신하여 사용자 u_c로 전달하고, 단계(810)에서, 사용자 u_c는 암호문 $Enc_{-k'_{sn}}(r - m_c)$ 를 생성하여 직접 클라우드 서버(130)로 전송한다. 이 결과, 상기의 수학식 5와 같은 n개의 제3 암호문들이 생성된다.

[0097] 그리고, 단계(812)에서, 클라우드 서버(130)는 클라우드 서버의 암호키 $\sum_{i=1}^{k} k_i + k_{sk}$ 를 이용하여 n개의 제3 암호문을 복호화한다. 이에 따라, n개의 지문 차이 데이터인 $(m_1 - m_c)$, $(m_2 - m_c)$, ... $(m_n - m_c)$가 생성된다.

[0098] 그 후, 단계(814)에서, 클라우드 서버(130)는 n개의 지문 차이 데이터 각각에 대한 유클리드 거리를 산출하고 ($dist_k = \sqrt{(m_k - m_c)^2}$), 단계(816)에서, 클라우드 서버(130)는 n개의 지문 차이 데이터의 유클리드 거리 중 최소값을 산출하여 데이터 서버(120)로 전송한다. 그리고, 단계(818)에서, 데이터 서버(120)는 유클리드 거리 중 최소값이 기 설정된 임계값 이상인 경우, 상기 인증 받고자 하는 사용자를 정당한 사용자로 인증한다.

[0099] 정리하면, 본 발명에 따른 생체 특성 기반 식별 시스템(100)에서는, n개의 지문 차이 데이터를 이용하여 사용자 인증을 수행하되, 지문 차이 데이터를 통해서는 지문이 노출될 수 없으므로, 사용자의 프라이버시를 보호할 수 있는 장점이 있다.

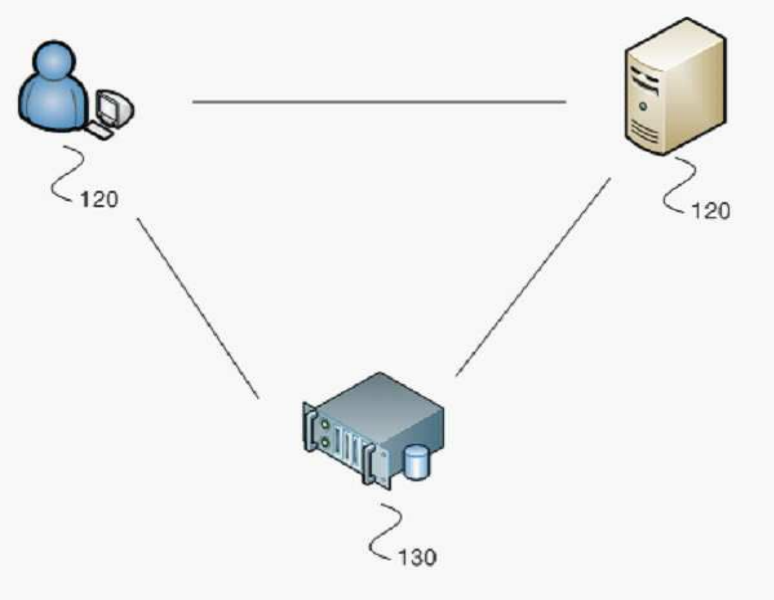
[0100] 또한, 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 일 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0101] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되

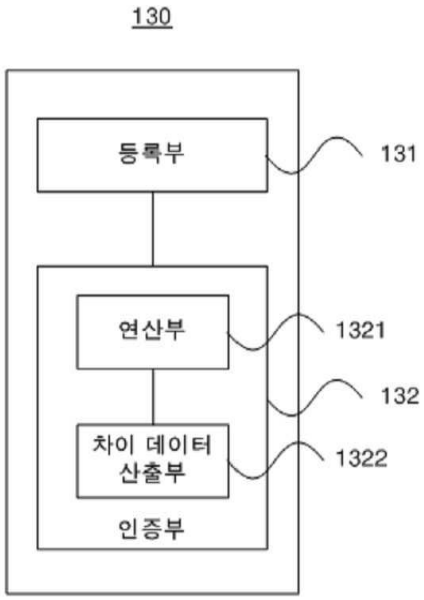
었으나 이는 본 발명의 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

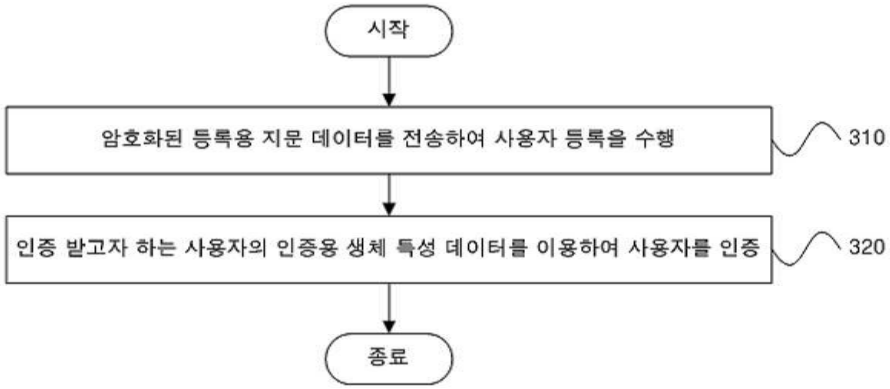
도면1



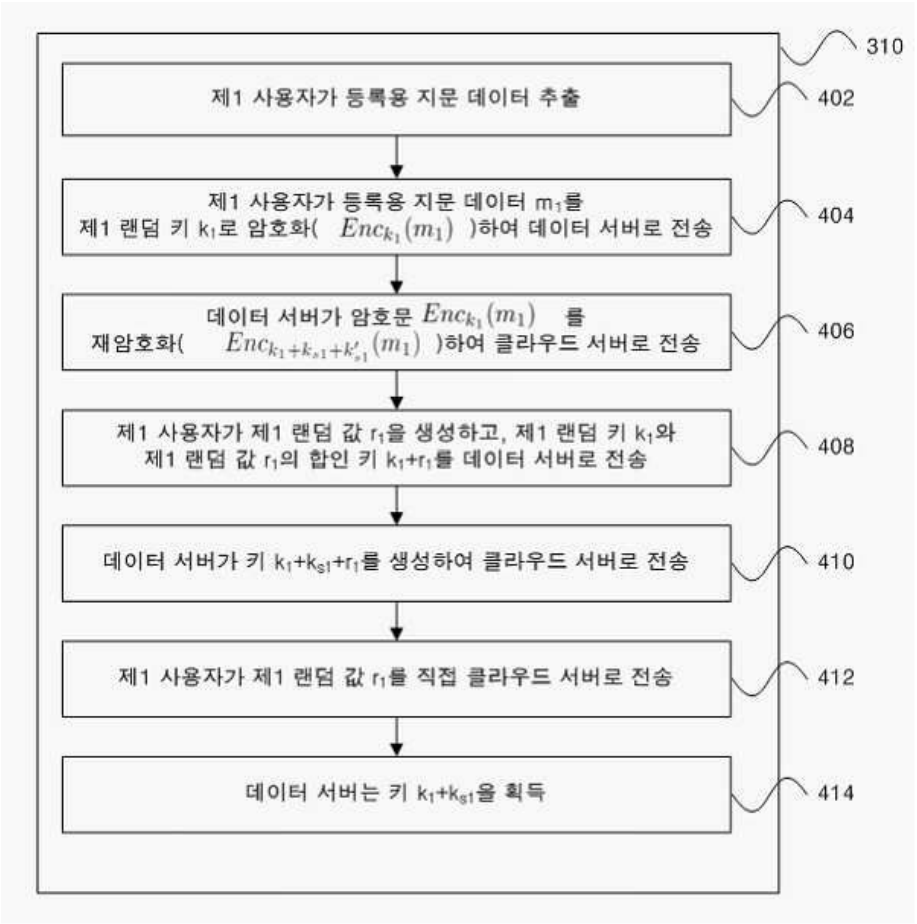
도면2



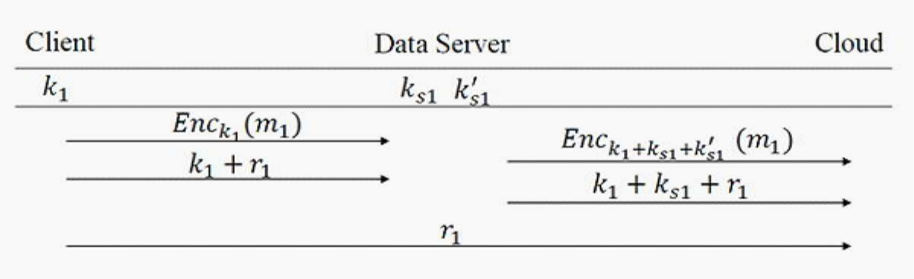
도면3


시작
암호화된 등록용 지문 데이터를 전송하여 사용자 등록을 수행
310
인증 받고자 하는 사용자의 인증용 생체 특성 데이터를 이용하여 사용자를 인증
320
종료

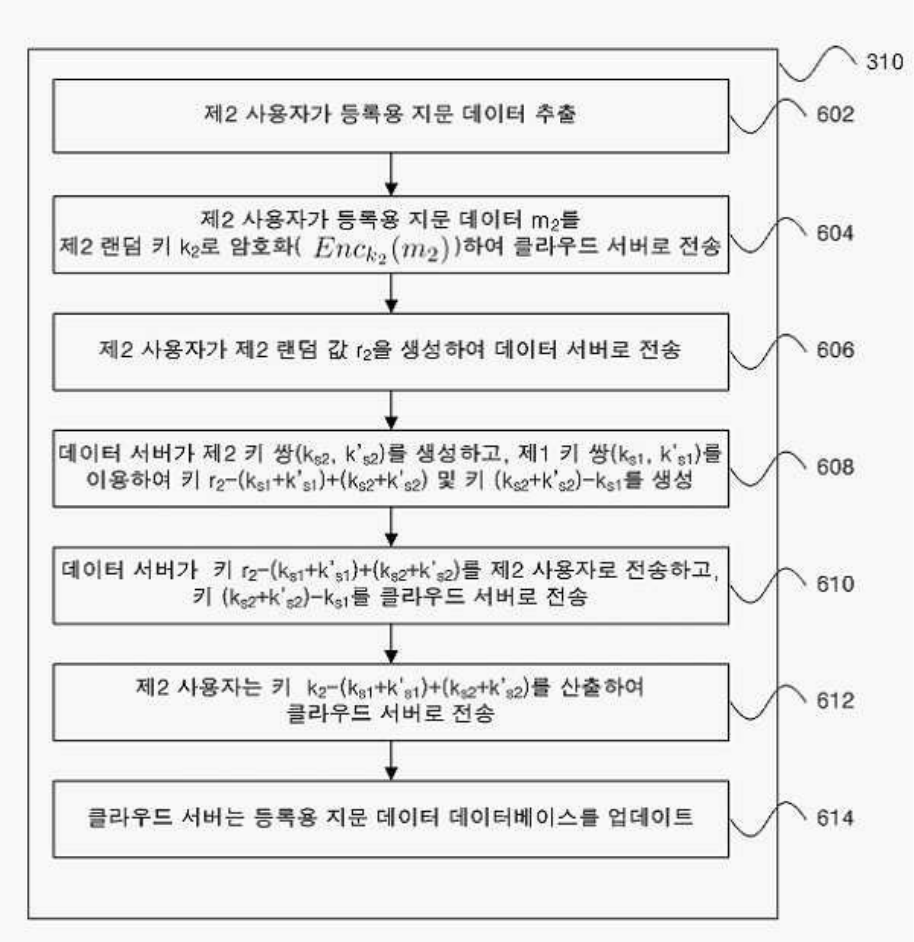
도면4


310
제1 사용자가 등록용 지문 데이터 추출
402
제1 사용자가 등록용 지문 데이터 m_1를
제1 랜덤 키 k_1로 암호화($Enc_{k_1}(m_1)$)하여 데이터 서버로 전송
404
데이터 서버가 암호문 $Enc_{k_1}(m_1)$ 를
재암호화($Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$)하여 클라우드 서버로 전송
406
제1 사용자가 제1 랜덤 값 r_1을 생성하고, 제1 랜덤 키 k_1와
제1 랜덤 값 r_1의 합인 키 k_1+r_1를 데이터 서버로 전송
408
데이터 서버가 키 $k_1+k_{s1}+r_1$를 생성하여 클라우드 서버로 전송
410
제1 사용자가 제1 랜덤 값 r_1를 직접 클라우드 서버로 전송
412
데이터 서버는 키 k_1+k_{s1}을 획득
414

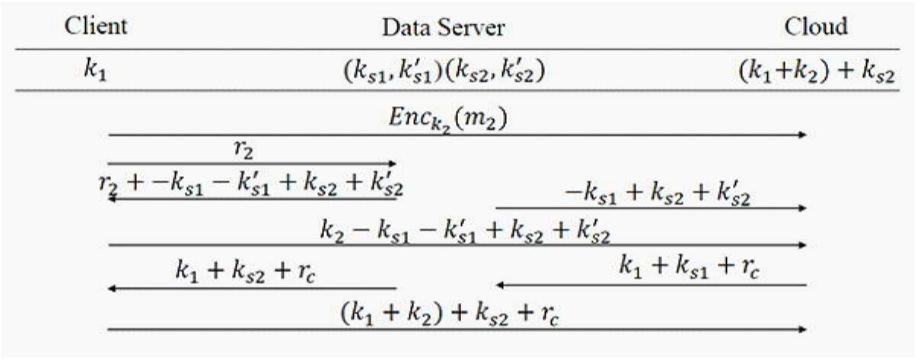
도면5


Client
Data Server
Cloud
k_1
k_{s1} k'_{s1}
$Enc_{k_1}(m_1)$
$k_1 + r_1$
$Enc_{k_1+k_{s1}+k'_{s1}}(m_1)$
$k_1 + k_{s1} + r_1$
r_1

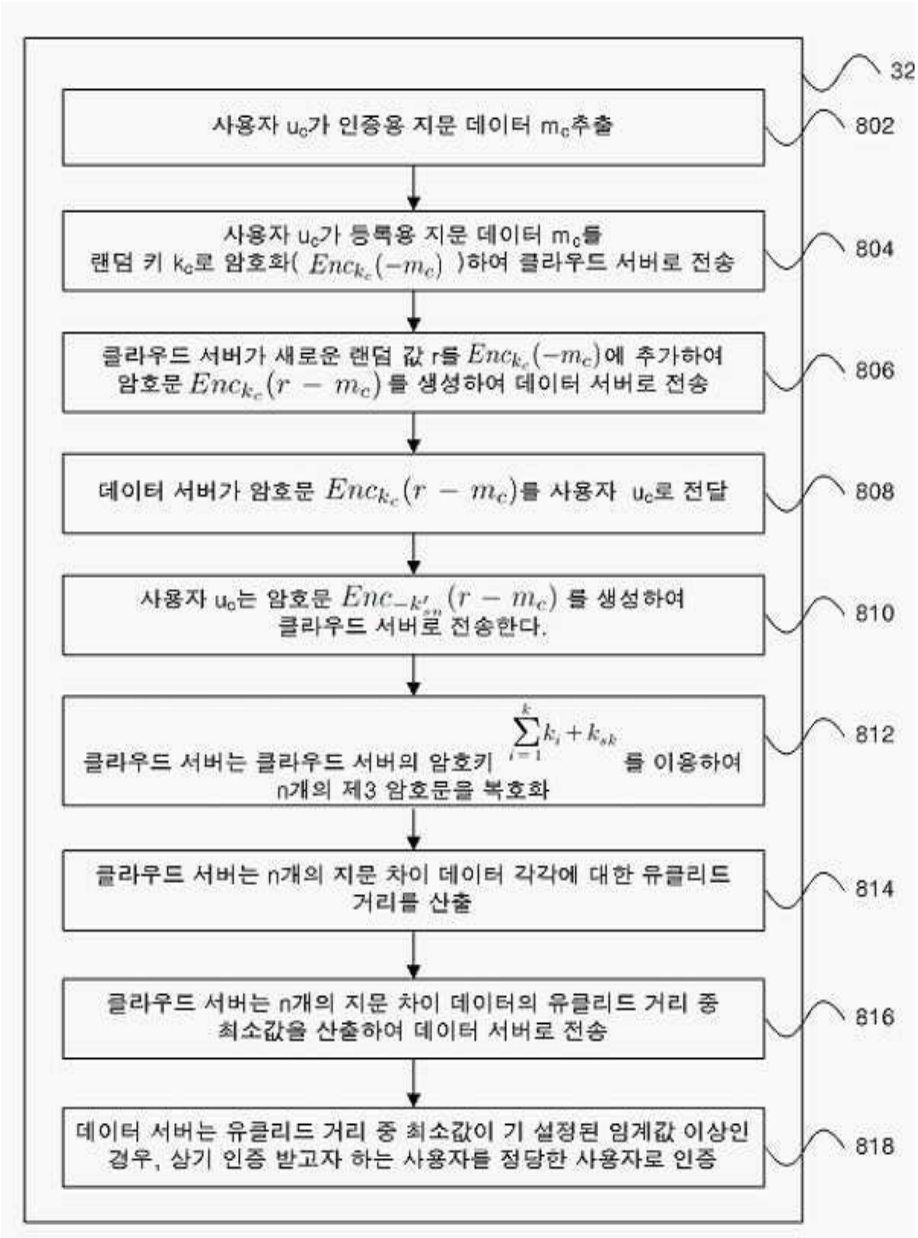
도면6


310
제2 사용자가 등록용 지문 데이터 추출
602
제2 사용자가 등록용 지문 데이터 m_2를 제2 랜덤 키 k_2로 암호화($Enc_{k_2}(m_2)$)하여 클라우드 서버로 전송
604
제2 사용자가 제2 랜덤 값 r_2을 생성하여 데이터 서버로 전송
606
데이터 서버가 제2 키 쌍(k_{s2}, k'_{s2})를 생성하고, 제1 키 쌍(k_{s1}, k'_{s1})를 이용하여 키 $r_2-(k_{s1}+k'_{s1})+(k_{s2}+k'_{s2})$ 및 키 $(k_{s2}+k'_{s2})-k_{s1}$를 생성
608
데이터 서버가 키 $r_2-(k_{s1}+k'_{s1})+(k_{s2}+k'_{s2})$를 제2 사용자로 전송하고, 키 $(k_{s2}+k'_{s2})-k_{s1}$를 클라우드 서버로 전송
610
제2 사용자는 키 $k_2-(k_{s1}+k'_{s1})+(k_{s2}+k'_{s2})$를 산출하여 클라우드 서버로 전송
612
클라우드 서버는 등록용 지문 데이터 데이터베이스를 업데이트
614

도면7


Client
Data Server
Cloud
k_1
$(k_{s1}, k'_{s1})(k_{s2}, k'_{s2})$
$(k_1+k_2)+k_{s2}$
$Enc_{k_2}(m_2)$
r_2
$r_2 + -k_{s1} - k'_{s1} + k_{s2} + k'_{s2}$
$-k_{s1} + k_{s2} + k'_{s2}$
$k_2 - k_{s1} - k'_{s1} + k_{s2} + k'_{s2}$
$k_1 + k_{s2} + r_c$
$k_1 + k_{s1} + r_c$
$(k_1 + k_2) + k_{s2} + r_c$

도면8


32
사용자 u_c가 인증용 지문 데이터 m_c추출
802
사용자 u_c가 등록용 지문 데이터 m_c를 랜덤 키 k_c로 암호화($Enc_{k_c}(-m_c)$)하여 클라우드 서버로 전송
804
클라우드 서버가 새로운 랜덤 값 r를 $Enc_{k_c}(-m_c)$에 추가하여 암호문 $Enc_{k_c}(r - m_c)$를 생성하여 데이터 서버로 전송
806
데이터 서버가 암호문 $Enc_{k_c}(r - m_c)$를 사용자 u_c로 전달
808
사용자 u_c는 암호문 $Enc_{-k'_{s2}}(r - m_c)$ 를 생성하여 클라우드 서버로 전송한다.
810
클라우드 서버는 클라우드 서버의 암호키 $\sum_{i=1}^{k} k_i + k_{sk}$ 를 이용하여 n개의 제3 암호문을 복호화
812
클라우드 서버는 n개의 지문 차이 데이터 각각에 대한 유클리드 거리를 산출
814
클라우드 서버는 n개의 지문 차이 데이터의 유클리드 거리 중 최소값을 산출하여 데이터 서버로 전송
816
데이터 서버는 유클리드 거리 중 최소값이 기 설정된 임계값 이상인 경우, 상기 인증 받고자 하는 사용자를 정당한 사용자로 인증
818

【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 제4항

【변경전】

상기 k번째 사용자

【변경후】

상기 제k 사용자

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 제4항

【변경전】

제1 사용자를 제외한 차후의 제k(1 <= k <= n) 사용자

【변경후】

제1 사용자를 제외한 차후의 제k(2 <= k <= n) 사용자