디지털산업정보학회 논문지 제4권 제2호 - 2008년 6월

지문 인식 기반의 개인키 위탁 시스템의 설계

신 용 녀* · 이 용 준**

Design of a Private Key Escrow System based on the Fingerprint Identification

Shin, Yong-Nyuo · Lee, Yong-Jun

〈Abstract〉

There are some problems on the system that uses a password comprising a digital signature to identify the secret key owner under the public key infrastructure. For example, the password can be difficult to remember or easy to be disclosure, and users should make more complex password to protect it. A number of studies have been proceeded in order to overcome these defects using the fingerprint identification technologies, but they need to change the current standard of public key infrastructure. On the suggested private key escrow system, the private key can be withdrawn only through the enrollment and identification of a fingerprint template after it is saved to a reliable third system. Therefore, this new private key escrow system can remove previous inconveniences of managingthe private key on current public key infrastructure, and it exhibited superior results in terms of the evaluation items when compared with the integrated method of the existing fingerprint identification and public key infrastructure.

Key Words : Private key escrow system, PKI, Fingerprint Identification, Authentication, Digital signature password

Ⅰ. 서 론

공인인증서의 활성화에 따라서 금융거래시스템, 의료정보시스템, 전자입찰시스템 등 온라인 서비스 분야에 일반적인 인증 방식으로 사용되고 있다. 공인인증서가 법적 효력을 제공하는 장점에 반하여 사용자에게 안전한 하드웨어에 개인키를 관리해야 하는 불편함이 있다. 또한 사용자에 의한 고의적인 키 위임의 경우 법적 분쟁의 소지가 있으며 전자서명 비밀번호에 의한 보안강도가 약화되는 문제점이 있다[1].

지문 인식 기반의 인증은 시스템의 접근시 본인만이 접근할 수 있는 강한 보안강도를 가지고 있으며 신체적

* 한국정보보호 진흥원 산업지원팀 주임연구원
** LG CNS 기술연구부문 부책임연구원

특징을 이용하기 때문에 키 관리의 불편함이 없다. 그러나 지문 인식은 완벽한 인식률을 제공할 수 없으며 법적 효력을 제공하지 못하는 한계점을 가지고 있다.

따라서 공인인증서와 지문인식을 융합하는 방식의 연구가 수행되어 왔으며 이러한 연구는 지문 인식을 이용하여 개인키를 복원함으로써 사용자에게 편리함과 높은 보안강도를 제공할 수 있다.

본 논문에서는 개인키를 신뢰할 수 있는 제3의 시스템에 저장한 후, 지문 템플릿의 등록과 인식에 의해서만 개인키를 인출하는 지문인식 기반의 키 위탁 시스템을 제안한다. 제안하는 시스템은 기존의 공개키 기반 구조의 표준을 준용하면서 공인인증서 사용자에게 키 관리의 불편함을 해소하고 고의적인 키 위임을 방지하는 기능의 제공이 가능하다.

Ⅱ. 관련연구

2.1 공인인증서 기반의 인증

공인인증서 기반의 인증은 개인키의 소유자가 생성한 전자서명을 검증함으로써 신원을 확인한다. 개인키 소유자는 공인인증을 요청하는 시스템을 접근할 때 전자서명을 수행하며 시스템은 해당 인증서의 유효성, 인증서의 상태를 확인하고 전자서명을 검증한 후 인증여부를 판별한다[2].

공인인증서 기반의 인증은 다음과 같은 문제점을 가지고 있다.

첫 번째, 개인키의 보안 강도가 전자서명 비밀번호에 의존적이라는 문제가 있다. 개인키는 패스워드 기반 암호화 방식으로 저장되어 있는데 실제 보안강도는 패스워드 기반 암호 알고리즘이 아닌 개인키 소유자의 전자서명 비밀번호에 의해 결정된다. 개인키 소유자는 전자서명 비밀번호를 기억하기 쉬운 단순정보 또는 신상정보를 사용하는 경우가 많기 때문에 보안이 취약한 문제가 있다.

두 번째, 개인키 소유자는 키를 안전하게 관리해야 하는 불편함을 가지고 있다. 공인인증서 기반의 인증을 요구하는 시스템에 접근하기 위해서 사용자는 해당 개인키를 스마트카드 또는 토큰 등의 안전한 하드웨어에 보관하여 휴대해야 하는 불편함의 문제가 있다.

세 번째, 개인키 소유자는 키 위임을 할 수 있기 때문에 분쟁의 소지가 발생한다. 개인키의 분실 또는 고의적인 키 위임 행위에 대하여 확인할 수 있는 방법이 없다.

2.2 지문인식 기반의 인증

바이오 인식은 신체적 특징인 지문, 얼굴, 홍체, 정맥 등을 식별하는 방법과 사람의 행위나 형태적 특성을 이용한 음성, 서명 등의 방법이 있다. 이러한 생체 특징들을 이용한 인증방식 중 개인 내 변화가 적고 개개인별로 유일하기 때문에 지문 인식방식이 상대적으로 증가하고 있다[3, 4].

지문 인식은 등록과 검증의 2가지 단계로 구성된다. 등록 단계에서 지문 샘플이 획득되며 유일한 특징점을 추출하여 지문 템플릿을 생성하여 저장한 후 인식 단계에서 사용된다. 인식 단계에서 지문 샘플을 획득하여 특징점을 추출한 후 등록 단계에서 저장된 지문 템플릿과 비교하여 동일인 여부를 인식한다[5].

지문 인식은 식별과 인식의 2가지 주요 목적을 가지고 있다. 식별은 시스템 의 데이터베이스에 등록된 복수 템플릿과 비교하는 것이며 인식은 등록된 단일 템플릿과 비교하여 정합 여부를 판별하는 것이다[6].

지문 인식은 다음과 같은 문제점을 가지고 있다.

첫 번째, 지문 인식은 법적효력을 가지지 못하는 한계를 가지고 있다. 공인인증서 기반의 로그인, 전자문서에 대한 전자서명은 법률적으로 공식문서로써의 효력을 가진다. 그러나 지문 인식은 법률로 제정되지 않았기 때문 법적효력을 가지지 못하는 한계를 가지고 있다.두 번째, 지문인식은 완전한 인식률을 제공할 수 없다. 지문인식

알고리즘 개선에 대한 연구가 지속적으로 연구가 되었으나 완전한 인식률을 제공할 수 없으며 특히 지문이 손상되거나 변형되는 경우는 등록된 지문 템플릿을 사용할 수 없다[7].

Ⅲ. 기존 시스템의 분석

전자서명 기반의 인증은 키 관리의 불편함과 전자서명 비밀번호에 의해 보안강도가 약화되는 문제가 있으며 지문 인식은 법적 효력이 보장되지 않고 완벽한 인식률을 제공하지 못하는 한계를 가지고 있다. 이러한 문제를 해결하기 위해 다음과 같은 암호화와 지문인식을 융합하는 연구가 진행되었다[8].

첫 번째, 등록된 템플릿에서 비트 치환 알고리즘으로 암호키를 추출하는 방식이다. 암호키를 비트 단위로 템플릿의 특정 위치에 위치시키기 때문에 공격자가 비트 치환 알고리즘을 분석하게 되면 해당 시스템의 사용자의 암호키가 유출되는 문제점을 가지고 있다.

두 번째, 지문 샘플에서 추출한 정보를 암호키로써 직접 사용하는 방식이 있다. 이 방식은 지문 샘플이 환경 또는 신체적으로 변화가 일어나는 경우 동일한 템플릿이 추출되지 않아 암호키가 변경되는 문제가 발생한다. 또한 암호키가 일정 기간에 따라서 변경 또는 폐기되는 경우, 해당 지문을 사용할 수 없게 된다[9].

세 번째, 지문 샘플을 등록 및 검증 시 간접적인 정보를 사용하는 방식이 있다. 등록시, 암호키를 생성할 때 템플릿 정보를 간접적으로 연결하는 정보를 생성하고 검증시, 간접정보를 사용하여 암호를 복호하는 방식이다. 이 방식은 암호키가 일정 기간에 따라서 변경 또는 폐기되는 경우에는 유용하게 활용할 수 있으나 검증시 연결정보가 항상 요구되는 단점을 가지고 있다.

네 번째, 신뢰할 수 있는 제3의 시스템에 지문 템플릿과 암호키를 저장하는 방식이 있다. 지문 샘플을 획득한 후 안전하게 저장되어 있는 지문 템플릿과 비교하여 인증을 제공한다. 해당 사용자가 정상적이면 안전한 저장소에서 해당 암호키를 제공하는 방식이다.

Ⅳ. 지문인식 기반의 개인키 위탁 시스템

제안하는 지문인식 기반의 개인키 위탁 시스템은 위탁과정과 인출과정으로 구성된다. 공인인증기관으로부터 발급받은 개인키를 지문인식 기반으로 위탁하고 위탁자가 필요에 의해 개인키를 인출하여 사용함으로써 개인키를 관리해야 하는 불편함을 줄일 수 있다. 또한 사용자에 의해 고의적인 개인키 위임을 사전에 방지할 수 있다.

4.1 용어 정의

- KMS : 키 관리 서버
- $User$: 키 위탁자
- $Cert_{KMS}$: 키 관리 서버의 인증서
- FIE_{User} : 사용자의 등록 지문 이미지
- FIM_{User} : 사용자의 매칭 지문 이미지
- FTE_{User} : 사용자의 등록 지문 템플릿
- FTM_{User} : 사용자의 매칭 지문 템플릿
- ID_{User} : 사용자 아이디
- pri : 개인키
- PBE_{pri} : 암호화된 개인키
- PWD_{pri} : 전자서명 비밀번호
- $Envelop()$: 비대칭키 암호 함수
- $Develop()$: 비대칭키 복호 함수
- $Encrypt()$: 대칭키 암호 함수
- $Decrypt()$: 대칭키 복호 함수
- $TKE = (ID_{User} \| FTE_{User} \| PBE_{PRI} \| PWD_{PRI})$: 키 위탁 토큰
- $ETKE = Envelop_{KMS}(TKE)$: 키 위탁 토큰 암호봉투
- $TKM = (ID_{User} \| FTM_{User})$: 키 인출 토큰
- $ETKM = Encrypt_K(TKM)$: 암호화된 키 인출 토큰

· $EETKM = Envelop_{KMS}(K \| ETKM)$
: 키 인출 토큰 암호봉투

4.2 개인키 위탁 프로토콜

지문인식 기반의 개인키 위탁 과정을 [그림 1]에 나타내었다. 키 위탁 프로토콜을 수행하면 사용자는 지문인식을 이용하여 원하는 장소에서 개인키의 키를 복원하여 사용할 수 있다.

User		KMS
	(1) $Cert_{KMS}$ ←	
(2) FIE_{User} = Scan($User$)		
(3) FTE_{User} = Extract(FIE_{User})		
(4) $TKE = (ID_{User} \| FTE_{User} \| PBE_{PRI} \| PWD_{PRI})$		
(5) $ETKE = Envelop_{KMS}(TKE)$		
	(6) $ETKE$ →	
		(7) $TKE = Develop_{KMS}(ETKE)$
		(8) Save ID_{User}, FTE_{User}
		(9) Save PBE_{PRI}, PWD_{PRI}

[그림 1] 개인키 위탁 프로토콜

(1) 사용자는 키 관리 서버의 인증서($Cert_{KMS}$)를 획득한다. 사용자는 획득한 키 관리 서버 의 인증서에 대하여 유효성과 상태확인을 검증한다. 키 관리 서버의 인증서에서 추출한 공개키는 키 위탁 토큰을 비대칭키 암호화하는데 사용한다.

(2) 사용자는 지문 템플릿을 등록하기 위해 지문 이미지(FIE_{User})를 스캔한다. 스캔한 지문 이미지의 품을 확인하여 등록에 적합하지 않는 경우 재스캔을 요청한다.

(3) 스캔한 지문 이미지(FIE_{User})에서 특징점을 추출하여 등록 템플릿(FTE_{User})을 생성한다. 등록 템플릿을 생성한 이후 지문 이미지는 메모리에서 완전 폐기하여 프라이버시를 보호한다.

(4) 키 관리 서버에 등록할 키 위탁 토큰(TKE)을 생성한다. 키 위탁 토큰(TKE)은 사용자 아이디(ID_{User}), 등록 템플릿(FTE_{User}), 암호화된 개인키(PBE_{pri}), 전자서명 비밀번호(PWD_{pri})로 구성되어 있다.
$TKE = ID_{User} \| FTE_{User} \| PBE_{PRI} \| PWD_{PRI}$

(5) 키 관리 서버의 공개키로 키 위탁 토큰(TKE)를 비대칭키 암호화를 수행한다. 키 위탁 토큰 암호봉투는 키 관리 서버(KMS)의 개인키에 의해서만 복호화가 되기 때문에 토큰이 외부에 유출되지 않는다.
$ETKE = Envelop_{KMS}(TKE)$

(6) 사용자는 생성한 키 위탁 토큰 암호봉투(ETKE)를 키 관리 서버에 전송한다.

(7) 키 관리 서버는 전송받은 키 위탁 토큰 암호봉투(ETKE)를 키 관리 서버의 개인키로 복호화한다. 복호화가 정상적으로 수행되면 키 위탁 토큰이 복구된다.
$TKE = Develop_{KMS}(ETKE)$

(8) 키 관리 서버는 키 위탁 토큰(TKE)에서 사용자 아이디(ID_{User}), 등록 템플릿(FTE_{User})을 데이터베이스에 등록한다.

(9) 키 관리 서버는 등록된 사용자 계정과 구별된 테이블에 암호화된 개인키(PBE_{PRI}), 전자서명 비밀번호(PWD_{PRI})를 저장한다.

4.3 개인키 인출 프로토콜

지문인식 기반의 개인키 인출 프로토콜을 [그림 2]에 나타내었다. 키 인출 과정을 거치게 되면 사용자는 지문인식을 이용하여 원하는 장소에서 개인키를 인출하여 전자서명을 불편함 없이 사용할 수 있다.

(1) 사용자는 키 관리 서버의 인증서($Cert_{KMS}$)를 획득한다. 사용자는 획득한 키 관리 서버 의 인증서에 대하여 유효성과 상태확인을 검증한다. 키 관리 서버의 인증서에서 추출한 공개키는 키 인출 토큰을 비대칭키 암호화하는데 사용한다.

(2) 사용자는 사용자 아이디(ID_{User})를 입력한다. 사용자 아이디는 키 관리 서버의 데이터베이스에 등록

User		KMS
	← (1) $Cert_{KMS}$	
(2) Input(ID_{User})		
(3) FIM_{User} = Scan($User$)		
(4) FTM_{User} = Extract(FIM_{User})		
(5) $TKM = ID_{User} \| FTM_{User}$		
(6) Generate K		
(7) $ETKM = Encrypt_K(TKM)$		
(8) $EETKM = Envelop_{KMS}(K \| ETKM)$		
	→ (9) $EETKM$	
		(10) $K \| ETKM = Develop_{KMS}(EETKM)$
		(11) $TKM = Decrypt_K(ETKM)$
		(12) Research(ID_{User})
		(13) Authenticate(FTM_{User}, FTB_{User}
		(14) $pri = Decrypt_{PWD_{pri}}(PBE_{pri})$
		(15) $Epri = Encrypt_K(\mathrm{Pri})$
	← (16) $Epri$	
(17) $pri = Decrypt_K(Epri)$		

[그림 2] 개인 키 위탁 프로토콜

여부를 확인하는 정보로써 사용된다.

(3) 사용자는 지문을 인식하기 위해 지문 샘플(FIM_{User})을 스캔한다. 스캔한 지문 이미지의 품질을 확인하여 매칭에 적합하지 않는 경우 재스캔을 요청한다.

(4) 획득한 지문 이미지(FIM_{User})의 특징점을 추출하여 매칭 템플릿(FTM_{User})을 생성한다. 매칭 템플릿을 생성한 이후 지문 이미지는 메모리에서 완전 폐기하여 프라이버시를 보호한다.

(5) 키 관리 서버에 전송할 키 인출 토큰(TKM)을 생성한다. 키 인출 토큰은 사용자 아이디(ID_{User})와 매칭 템플릿(FTM_{User})으로 구성된다.

$TKM = ID_{User} \| FTM_{User}$

(6) 사용자는 키 관리 서버와 통신구간의 보안을 위해 세션키(K)를 생성한다.

(7) 사용자는 키 인출 토큰을 세션키로 대칭키 암호화를 수행한다.

$ETKM = Encrypt_K(TKM)$

(8) 키 관리 서버의 공개키로 세션키(K)와 암호화된 키 인출 토큰(ETKM)에 대하여 비대칭키 암호화를 수행한다. 키 인출 토큰 암호봉투(EETKM)는 키 관리 서버의 개인키만으로 복호화가 수행되기 때문에 토큰이 외부에 유출되지 않는다.

$EETKM = Envelop_{KMS}(K \| ETKM)$

(9) 사용자가 생성한 키 인출 토큰 암호봉투(EETKM)를 키 관리 서버에 전송한다.

(10) 키 관리 서버는 전송받은 키 인출 토큰 암호봉투(EETKM)를 키 관리 서버의 개인키로 복호화를 수행한다. 복호화가 정상적으로 수행되면 세션키(K)와 암호화된 키 위탁 토큰(ETKM)을 복구한다.

$K \| ETKM = Develop_{KMS}(EETKM)$

(11) 키 관리 서버는 복호화한 세션키로 암호화된 키 위탁 토큰(ETKM)을 복호화한다.

$TKM = Decrypt_K(ETKM)$

(12) 키 관리 서버는 키 인출 토큰의 사용자 아이디로 데이터베이스 검색하여 해당하는 사용자 아이디에 해당하는 정보를 추출한다.

(13) 키 관리 서버는 사용자의 매칭 템플릿과 사용자의 등록 템플릿을 1:1 비교하여 본인 여부를 판별한다.

(14) 키 관리 서버는 1:1 지문비교가 정합의 결과를 제공하면 해당 인출자의 별도 테이블에 암호화된 개인키(PBE_{pri}), 전자서명 비밀번호(PWD_{pri})을 인출하여 암호화된 개인키를 전자서명 비밀번호로 복호화한다.

$pri = Decrypt_{PWD_{pri}}(PBE_{pri})$

(15) 키 관리 서버는 사용자와 교환된 세션키로 개인키를 대칭키 암호화한다.

$Epri = Encrypt_K(\mathrm{Pri})$

(16) 키 관리 서버는 세션키로 암호화한 암호화된 개인키를 사용자에게 전송한다.

(17) 사용자는 프로토콜 초기에 생성한 세션키로 전송받은 암호화된 개인키를 복호화한다. 사용자는 복구된 개인키(pri)로 전자서명을 수행할 수 있다.

$pri = Decrypt_K(Epri)$

Ⅴ. 제안하는 시스템의 비교분석

제안하는 지문인식 기반의 개인키 위탁 시스템은 기존의 연구와 비교하기 위한 평가항목은 다음과 같다.

- 키 무결성 : 지문 정보로부터 유도된 개인키가 항상 결정적이어야 무결성이 보장된다. 지문 정보로부터 실시간으로 유도된 개인키 정보가 항상 동일하지 않는 경우 보장되지 않는다.
- 키 유효성 : 지문 정보로 부터 유도된 개인키는 충분한 복잡도가 보장되어야 한다. 지문 정보의 용량에 의해 복잡도가 결정되는 경우는 복잡도가 충분하게 보장되지 않는다.
- 통신부하 : 지문 정보로부터 유도된 개인키로 전자서명을 수행하고 검증하는 과정에서 부가정보가 요구되는 경우 통신부하가 발생한다. 현재 공개키 기반 구조에서 사용되는 인증서, 인증서 폐지 목록 이외에 추가적인 부가정보가 요구되는 경우 통신부하가 발생한다.
- 확장성 : 제안하는 시스템이 공개키 기반 구조의 표준에 대한 변경이 없이 확장성을 제공해야 한다. 제안하는 시스템이 지문인식이 공개키 기반 구조에 접목되는 과정에서 표준을 변경해야하는 경우 확장성을 보장하지 못한다.
- 보안강도 : 키 무결성, 키 유효성, 통신부하, 확장성을 고려하는 시스템이 제공하는 전체 보안강도로써 말한다.

제안하는 시스템과 기존의 3가지 지문인식과 공개키 기반 구조의 접목 기술을 비교분석한 결과를 <표 1>에 나타내었다.

<표 1> 제안시스템 비교 분석

방식 / 항목	템플릿 은닉	지문이미지 직접입력	부가정보 간접입력	제안 시스템
키 무결성	보장	보장 불가	보장	보장
키 유효성	보장 불가	보장 불가	보장	보장
통신부하	부하 없음	부하 없음	부하	부하 없음
확장성	보장 불가	보장 불가	보장 불가	보장
보안강도	낮음	중간	높음	높음

키 무결성은 템플릿 은닉 방식은 템플릿 정보에 개인키 정보를 은닉하기 때문에 지문인식에서 성공하는 경우 항상 동일한 개인키 정보를 생성할 수 있다. 부가정보 간접입력 방식과 제안 시스템은 지문인식과정과 전자서명 과정이 분리되어 있기 때문에 지문인식의 성공하는 경우 항상 동일한 개인키 정보를 생성할 수 있다. 그러나 지문이미지 직접입력 방식의 경우는 아날로그인 지문이미지 정보이기 때문에 항상 동일한 개인키를 생성할 수 없기 때문에 무결성을 제공하지 못한다.

키 유효성은 템플릿 은닉방식, 지문이미지 직접입력 방식은 지문이미지 정보량에 의해 복잡도가 의존됨으로써 공개키 기반 구조에 적합하지 않는 저수준의 복잡도를 제공한다. 부가정보 간접입력 방식과 제안하는 시스템은 지문인식과 개인키 정보가 별도로 수행되기 때문에 공개키 기반 구조가 요구하는 복잡도를 제공한다.

통신부하는 템플릿 은닉 방식, 지문이미지 직접입력 방식, 제안 시스템은 인증서와 인증서 폐지목록 이외에 부가정보를 요구하지 않는다. 그러나 부가정보 간접입력 방식은 검증하는 과정에서 부가적인 정보를 요구함으로써 통신부하를 발생시킨다.

확장성은 템플릿 은닉 방식, 지문이미지 직접입력 방식, 부가정보 간접입력 방식은 현재의 공개키 기반 구조와 표준을 변경하도록 설계되어 있다. 따라서 이러한 시스템을 도입하기 위해서는 정책 및 시스템 변경사항이 요구된다. 제안 시스템은 현재의 공개키 기반 구조를 준용하기 때문에 확장성을 제공한다.

보안강도는 키 무결성, 키 유효성 및 시스템의 전체

보안을 고려할 때 부가정보 간접입력 방식과 제안 시스템은 보안강도가 높은 반면, 템플릿 은닉 방식과 지문이미지 직접입력 방식은 낮다.

Ⅵ. 결론

통신과 컴퓨터 기술이 비약적으로 발전하면서 금융권을 중심으로 인터넷을 이용한 전자상거래가 활성화 되고 있으며 이러한 전자상거래는 전통적인 상거래를 대체하거나 보조하면서 급속도로 확산되고 있다. 전자상거래의 안전성과 신뢰성을 확보하기 위해서는 공인인증의 도입이 요구되며 공인인증은 전자서명의 안전한 운용으로써 공개키 기반 구조를 의미한다. 현재 공개키 기반 구조에서는 비밀키 소유자의 인증을 위하여 전자서명 비밀번호를 사용하고 있으나 이러한 방식은 타인에게 노출되거나 기억하기 어려운 문제점을 가지고 있다. 비밀키 소유자가 개인키를 관리해야 하며 소유자에 의한 고의적인 키 위임의 방지가 어려우며 근본적으로 전자서명 비밀번호의 복잡도에 의해 보안강도가 결정되는 문제점이 있다.

따라서 이러한 단점을 보완하기 위해 공개키 기반 구조와 지문 인식기술을 접목시키려는 연구가 활발히 진행되고 있다. 기존의 지문인식과 공개키 기반 구조를 접목하는 기술로는 템플릿 은닉 방식, 지문이미지 직접입력 방식, 부가정보 간접입력 방식이 제안되었다. 그러나 기존 방식은 지문인식과 공개키 기반 구조의 접목과정에서 전체시스템의 보안강도가 낮아지는 문제와 무엇보다 현재 운용되고 있는 공개키 기반 구조의 표준을 변경해야 하는 문제점을 가지고 있다.

본 논문에서는 개인키를 신뢰할 수 있는 제3의 시스템에 저장한 후, 지문 템플릿의 등록과 인식에 의해서만 개인키를 인출하는 지문인식 기반의 키 위탁 시스템을 제안한다. 제안하는 시스템은 현재의 공개키 기반 구조를 유지한 상태에서 개인키 관리의 불편함을 해소하고 전자서명 비밀번호 인증 방식의 보안성을 강화하기 위해 설계하였다. 본 논문에서 제안하는 시스템은 기존의 지문인식과 공개키 기반 구조의 접목 방식과 비교하여 보안강도, 키 유효성, 키 무결성, 표준 준용성 등의 항목에서 우수한 결과를 나타내었다.

향후 연구과제로는 본 논문이 제안하는 방식이 제2의 서버 방식으로 개인의 모든 정보가 서버에 집중되며 이를 유지하고 관리하는데 해킹의 위험, 프라이버시의 침해 문제를 해결하기 위해 바이오 정보에 대한 불법적인 접근을 방지할 수 있는 접근 통제 메커니즘의 연구가 요구된다.

참고문헌

[1] Andrew Nash, William Duane, Celia Joseph, Derek Brink, "PKI: Implementing and Managing E-Security", 2001, pp. 41-48.

[2] OECD, OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, 2001.

[3] B.Miller, Everything you need to know about biometric identification. Personal Identification News 1988 Biometric Industry Directory, Warfel&Miller,Inc., Washington DC, January. 1988.

[4] J.Wayman, A definition of biometrics National Biometric Test Center Collected Works 1997-2000, San Jose State University, 2000.

[5] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, "Handbook of Fingerprint Recognition", Springer, 2003.

[6] Colin soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, Biometric Encryption, Bioscrypt Inc, 1999.

[7] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, Biometric

Encryption - Enrollment and Verification Procedures" Proc. SPIE3386, 1998, pp. 24-35.

[8] MANSFILED, A.J., KELLY, G.P., CHANDLER, D.J. and KANE, J. Biometric Product Testing Final Report. 2002.

[9] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, Biometric Encryption using image Processing Proc. SPIE3314, 1998, pp. 178-188.

■ 저자소개 ■

신용녀
Shin, Yong-nyuo

2002년~현재 한국정보보호 진흥원 산업지원팀 주임연구원
2008년 고려대학교 컴퓨터 학과(이학박사)
2001년 고려대학교 컴퓨터학과 (이학석사)
1999년 승실대학교 컴퓨터학과(이학사)

관심분야 : 생체인식, 정형기법, 정보보호
E-Mail : ynshin@kisa.or.kr

이 용 준
Lee Yong Joon

2006년~현재 LG CNS 기술연구부문 부책임연구원
2005년 승실대학교 컴퓨터학과 박사
2001년 승실대학교 컴퓨터학과 석사
1999년 강남대학교 전자계산학과 졸업

관심분야 : 컨텐츠 보호, 바이오인식, PKI
E-Mail : bigman@lgcns.com

논문접수일 : 2008년 2월 29일, 수 정 일 : 2008년 4월 20일(1차)
게재확정일 : 2008년 5월 1일