DBpia

바이오 정보 기반 실시간 키 생성 기법을 이용한 u-헬스케어 정보 보안에 관한 연구

정회원 김 창 복*, 김 남 일**

A Study On u-Healthcare Information Security Using Real-Time Technique of Key Generation Based Bio information

Kim Chang-Bok*, Kim Nam-il** ***Regular Members***

요 약

의료정보는 다수의 연구자나 의료인에 의해 무작위로 이용되는 경우에 개인의 사생활에 대한 중대한 침해가 될 수 있다. u-헬스케어는 기존의 무선 네트워크 기반 서비스에 의한 보안위협과 의료정보 시스템이 가진 개인 프라이버시 정보의 특성에 따른 보안위협이 있다. 본 논문은 u-헬스케어에서 모바일장비와 의료정보시스템과의 보안위협에 대해서 고찰하고, 바이오기반 실시간 비 대칭키 생성 방법에 대해서 제안하였다. 제안 알고리즘은 3개의 1024비트 지문 특징 정보를 SHA-1 해쉬 알고리즘의 입력값으로 하여 160비트의 해쉬값을 추출한다. 또한, 3개의 해쉬값은 RSA 알고리즘의 p, q, e 값을 생성하는 키값으로 사용하였다. 본 논문은 실시간으로 비대칭키를 생성함으로서 개인키의 분실과 Euler함수의 노출에 따른 문제점을 제거할 수 있다. 또한, 생성된 비대칭키는 WPKI 기반 전자서명 기법으로 의료정보에 대한 다양한 보안 위협을 제거할 수 있다.

Key Words : Key Generation, Bio information, u-Healthcare

ABSTRACT

If medical information is used numbers of researches and medical scientist by without permission, it can be seriously violated about personal privacy. The security weakness of ubiquitous healthcare has form similar to existing service based wireless network and has new security weakness by new mobile equipment and due to characteristic of medical information. This paper consider security threaten between mobile device and medical information system about ubiquitous healthcare. Then it propose real-time technique of asymmetric key generation based biometric. The algorithm The asymmetric key generation abstract 1024-bit characteristic information by three random fingerprint, which abstract hash code of 160-bit by use input value of SHA-1 hash algorithm. then three hash code use to generate p, q, e value of RSA algorithm. As a result, this paper can remove problem about private key loss and Euler function exposure by real-time asymmetric key generation. The generated asymmetric key can remove various security threaten about medical information by electronic signature technique based WPKI.

Ⅰ. 서 론

u-헬스케어는 대부분 개인 정보이기 때문에 정보 보안 서비스가 제공되지 않을 경우 악의적인 사용자에 의해 개인의 기밀정보가 악용될 수 있다. 그러나 u-헬스케어는 무선 네트워크와 밀접한 관계가 있

* 가천의과학대학교 정보기술학과(cbkim@gachon.ac.kr), ** 가천의과학대학교 정보기술학과(nikim@gachon.ac.kr)
논문번호 : 07086-1117, 접수일자 : 2007년 11월 17일

www.dbpia.co.kr

고, 개인의 의료정보에 대한 사용권한을 가진 다양한 이해 당사자에 의해 보안 및 프라이버시 측면에 많은 취약점과 위협을 보유한다[1].

특히 u-헬스케어의 핵심 장비인 모바일 단말기는 유선 네트워크 보다 보안위협이 높으며, 도난, 복제, 정보 유출 등에서 자유롭지 못하다. 개인 프라이버시 침해 가능성을 줄이고 신뢰성을 갖춘 u-헬스케어를 제공하기 위하여 무선상의 보안기능이 필수적이라 할 수 있다. 현재 무선상의 보안은 모바일 플랫폼용 공통 보안 핵심 모듈기술인 TPM(Trusted Platform Module)기술을 이용하고 있으며[2], WPKI (Wireless Public Key Infrastructure)기반의 전자서명 기법이 활용되고 있다. 전자서명(Electronic Signature)은 인증, 무결성, 기밀성, 부인봉쇄와 같은 4가지의 보안 요구사항을 보증하며, u-헬스케어에 적용할 경우, 사용 의료인의 신원확인, 진료내용의 위변조 방지, 진료정보 생성에 대한 부인방지를 보증한다[3,4]. 또한, 최근 개인 인식 및 검증을 위한 바이오인식(Biometric)이 발전하면서, 기존의 전자서명 알고리즘 등과 연계하여 바이오정보 기반의 인증시스템 및 서명키 생성 기술에 적용하려는 연구가 활발히 진행 중이다[5].

본 논문은 u-헬스케어에서 모바일장비와 의료정보시스템과의 보안위협에 대해서 고찰하고, 지문 특징정보를 이용하여 실시간으로 비 대칭키를 생성하는 방법에 대해서 제안한다. 제안알고리즘은 무작위 3개의 지문에 대해서 1024비트의 특징 정보 추출하여, SHA-1 알고리즘을 통해 3개의 160비트의 해쉬값(H_A, H_B, H_C)을 생성하였다. 또한, RSA 공개키 알고리즘에서 소수 p, q 및 공개키를 추출하였다.

본 논문은 실시간으로 개인키와 공개키를 생성함으로서 개인키의 분실에 따른 문제점을 제거할 수 있으며, RSA 알고리즘의 문제점인 Euler의 함수의 노출을 방지할 수 있다. 본 논문의 결과로서 실시간 비대칭키 생성에 따른 WPKI 기반 전자서명방식으로 안정적인 의료정보 보안이 가능할 것이다.

Ⅱ. 관련연구

2.1 u-헬스케어 보안위협

u-헬스케어는 m-헬스케어의 발전된 형태로서 무자각, 무구속적 의료 진단, 분석, 처방 등을 추구한다. 특히, u-헬스케어의 핵심 인프라는 무선 네트워크이며, 무선상의 보안은 유선상의 보안 보다 취약점이 더욱 많다. u-헬스케어의 보안 취약점은 기존의 유무선 네트워크 기반 서비스와 유사한 형태의 보안위협이 존재한다. 이러한 u-헬스케어 서비스의 보안 취약점을 노린 공격 유형은 다음과 같다[6].

① u-헬스케어를 지원하는 서버를 공격하는 DoS (Denial of Service) 공격 유형이다. 이것은 u-헬스케어 서버로의 사용자 접속을 막고 다른 위장 서버로 연결되도록 유도한 후 개인의 인증정보 등을 습득하여 악의적으로 이용하는 유형이다.
② 바이러스 및 웜 해킹 공격 유형이다. 이것은 u-헬스케어 서버에 정상적인 사용자로 위장하고 접속을 시도하여, 실제 사용자들의 정보를 변경하거나 삭제 하여 u-헬스케어 서비스 가입자들의 접속을 막는 유형이다.
③ 의료정보 도청 및 위변조 공격 유형이다. 의료 정보 및 서비스 결과 전송 시 의료 정보를 도청 및 감청 하여 정보를 수정하고 서비스 결과를 변조하여 전송하는 공격 유형이다.
④ 유·무선 인프라에서 가능한 여러 불법 접근 공격 유형이다. 특히 유·무선 인프라를 통한 게이트웨이나 다양한 서버들을 불법적으로 집중 공격하는 유형이다.

u-헬스케어 분야가 안정적으로 실현 및 성장하기 위해서는 환자 개인 및 의료 기관이 이와 같은 보안적 위협으로부터 안전을 보장 받을 수 있어야 한다.

u-헬스케어는 다른 유비쿼터스 정보화 서비스 영역과 달리, 생성 및 공유되는 정보들이 환자의 질병 및 생명과 관련된 정보들이 대부분이므로 데이터의 보호 및 무결성 보장, 불법적 액세스 방지 등은 의료 서비스의 신뢰성 및 안전성 보장을 위해 반드시 지원되어야할 기술이다. u-헬스케어 분야에서 의료정보 시스템의 특성상 검토해야할 위협요소들은 다음과 같다.

① 기밀성 : 환자가 의료 정보의 기밀에 대한 신뢰성을 인식하지 못하면 치료와 관련된 정보의 비밀로 인하여 부적절한 치료의 원인이 된다.
② 안전성 : 의료정보에 대한 기록들이 안전하다는 확신이 없으면 의사들은 의료 정보 시스템에 구축되어 있는 정보를 사용하지 않게 되므로 전자기록에대한 법적 보장이 선행되어야 한다.
③ 무결성 : 진료기록은 어떠한 경우에도 삭제되

www.dbpia.co.kr

어 서는 안된다. 오진의 경우가 발생 하였더라도 기록은 유지되어야 하며, 내용을 수정해야 한다면 추가사항으로 기록 되어야 한다.

④ 접근 동의 : 법적으로 인정하는 경우에만 제외하고 개인에 대한 기록 접근시 반드시 환자 혹은 대리인의 동의를 얻어야 한다.

⑤ 익명성 : 연구목적으로 환자의 의료정보를 접근할 경우 환자 개인에 대한 식별이 되지 않도록 해야 한다.

2.2 SHA-1 해쉬 알고리즘

해쉬 함수(hash function)는 임의의 유한 길이의 비트 스트링을 고정된 길이(n비트 길이)의 비트 스트링으로 변환하는 함수이다. 해쉬 함수의 기본 아이디어는 해쉬값이 입력 스트링의 축소된 대표 이미지의 역할을 하며, 그 스트링을 유일하게 표현한다. 해쉬 함수는 다음과 같은 4가지 특성을 가진다.

① compression - 임의의 유한 길이의 입력 비트 스트링 x를 고정된 길이의 출력 비트 스트링 $h(x)$로 변환한다.

② ease of computation - 주어진 h와 x에 대하여, $h(x)$를 계산하기 쉽다.

③ 2nd-preimage resistance - 주어진 입력에 대하여 같은 출력을 내는 또 다른 입력을 찾아내는 것이 계산상 불가능하다.

④ collision resistance - 같은 출력을 내는 임의의 서로 다른 두 입력 메시지를 찾는 것이 계산상 불가능하다.

해쉬함수의 대표적인 것들을 살펴보면, 1990년에 R.C Merkle에 의해 제안된 SNEFRU, 1989년 일본 NTT의 Miyaguchi 등이 발표한 N-HASH, 1990년과 1992년 Ron Rivest에 의해 개발된 MD4와 MD5, 1993년에 미국 NIST에 의해 개발된 SHA-1(Secure Hash Algorithm) 등이 있다. MD5와 SHA-1은 모두 MD4에 근거하고 있기 때문에 그 특성 및 암호화적 강도는 비슷하다. 안정성의 경우 암호 해독 공격에 대한 취약적 결점이 없다라고 가정할 경우 출력 길이가 더 긴 SHA-1이 더 강하다고 할 수 있으며, 32비트 구조를 가지고 있고 mod232상의 덧셈을 사용하고 있는 두 알고리즘은 80단계를 수행하고 버퍼의 크기가 160인 SHA-1이 더 빠르다. 또한 하나의 단일 구조와 버퍼로 운용되는 SHA-1이 더 간결하다.

SHA-1은 임의의 길이를 가지는 입력 메시지를 512비트 블록 단위로 처리하여 160비트의 출력을 낸다. 512비트 단위 블록을 처리하는 압축 함수는 모두 4라운드, 80단계로 구성되며, 해쉬코드를 계산하는 연쇄변수는 5개이다[7].

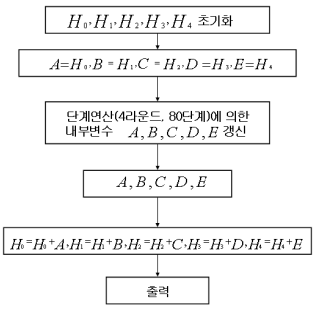

그림 1. SHA-1 알고리즘

SHA-1은 임의의 길이의 메시지 M이 입력으로 들어오면 패딩(padding) 과정을 통해 512비트의 배수로 만든 후, 512비트 블록 $M_i(1 \le i \le n)$로 나눈다. 각 블록 M_i를 그림 1과 같은 과정을 통해 압축하여 최종 블록 처리후의 연쇄변수 H_0, H_1, H_2, H_3, H_4를 연결시킨 것이 해쉬코드가 된다.

SHA-1 알고리즘에서 우선 다섯 개의 32비트 초기 연쇄변수와 각 라운드에서 사용될 상수를 다음과 같이 정의 한다.

h_0=0x67452301, h_1=0xefcdab89, h_2=0x98badcfe,
h_3 = 0x10325476, h_4 = 0xc3d2e1f0

K_t = 0x5a827999 (0 ≤t< 19)
K_t = 0x6ed9eba1 (20≤t< 39)
K_t = 0x8f1bbcdc (40≤t< 59)
K_t = 0xca62c1d6 (60≤t< 79)

다음은 논리함수(logical functions)를 정의한다. 각각의 $f_t(0 \le t \le 79)$는 3개의 32비트 워드를 입력으로 받아 32비트 워드를 출력하는 함수이다.

$f_t(B,C,D) = (B \wedge C) \vee (: B \wedge D)$ $(0 \le t \le 19)$
$f_t(B,C,D) = B \oplus C \oplus D$ $(20 \le t \le 39)$
$f_t(B,C,D) = (B \wedge C) \vee (B \wedge D) \wedge (C \vee D)$ $(40 \le t \le 59)$
$f_t(B,C,D) = B \oplus C \oplus D$ $(60 \le t \le 79)$

www.dbpia.co.kr

다음은 전처리(Preprocessing)과정으로서 메시지 M을 길이가 512의 배수가 되도록 패딩한다. 패딩과정은 메시지 끝에 "1"을 덧붙이고, 메시지 길이가 512의 배수보다 64비트 만큼 작아지도록 "0"을 덧붙인다. 마지막 64비트에는 메시지 M의 길이를 2^{64}를 법으로 하여 계산한 정수값이 채워진다. 512비트 메시지 블록은 16개의 32비트 워드열로 나누어지므로, n이 512비트 메시지 블록의 개수라 했을 때, 패딩된 메시지는 16n개의 워드들로 이루어지게 된다. 여기에서 16개의 32비트 워드 블록을 M_i라 하면 패딩된 메시지 전체는 M_1, M_2, L, M_n로 나누어진다. 또한, 연쇄변수 초기화를 한다.

$H_0 \leftarrow h_0,\ H_1 \leftarrow h_1,\ H_2 \leftarrow h_2,\ H_3 \leftarrow h_3,\ H_4 \leftarrow h_4$

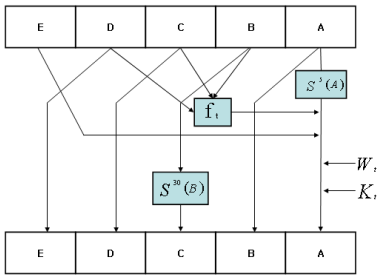

그림 2. t번째 단계영상

여기서 M_1, M_2, L, M_n을 다음과 같이 처리한다.

① M_i를 16개의 32비트 워드 W_0, W_1, …,W_{15}로 분할한다.
② (16≤t≤79)에 대해서는
$W_t=S^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16})$라 놓는다.
③ $A=H_0,\ B=H_1,\ C=H_2,\ D=H_3,\ E=H_4$
④ (0≤t≤79)에 대해 다음을 수행한다.
$TEMP=S^5(A) + F_t(B,C,D) + E + W_t + K_t$
$E=D,\ D=C,\ C=S^{30}(B),\ B=A,\ A$=TEMP
⑤ $H_0=H_0+A,\ H_1=H_1+B,\ H_2=H_2+C,\ H_3=H_3+D,$
$H_4 = H_4+E$

M_1 부터 M_n 까지 모두 처리한 후, 최종적으로 나타난 5개의 워드를 연접하여 160비트 해쉬 코드 H_0, H_1, H_2, H_3, H_4를 얻는다.

2.3 바이오 기반의 키 생성 기법

Janbandhu와 Siyal이 제안한 바이오 기반 전자서명 방식은 512 바이트의 바이오인식 데이터를 가정한다. 또한, 바이오 인식 샘플을 통한 정보가 충분한 오류정정을 통하여 결정적인 값으로 항상 복원될 수 있도록 가정하고 있다. 바이오 기반 RSA 알고리즘을 통한 키 생성은 다음과 같다[8,9].

① 각각 256바이트의 소수 p와 q 생성
② 법(modular) n=p×q와 오일러 함수
$\Phi(n)=(p-1)(q-1)$을 계산
③ 512바이트 바이오템플릿에서 개인 키 생성
④ $e=d^{-1} \bmod \Phi(n)$: 공개 키 생성

여기서 바이오 템플릿은 지문, 홍채, 망막 등 바이오 특징정보이다. RSA기반 키 생성은 법의 크기와 서명을 암호화 하여 전달하는 특징이 있으며, Φ(n)을 안전하게 소지해야 하는 부담이 있다.

바이오 기반 DSA 알고리즘을 통한 키 생성은 다음과 같다[7, 8].

① 64~128바이트 크기의 큰 소수 p를 구한다.
② 20바이트 크기를 갖는 p-1의 소인수 q를 구한다.
③ 서브그룹의 생성자 $g=h^{(p-1)/q} \bmod p$를 구한다.
이때 $h<(p-1)$이며 $h^{(p-1)q} \bmod p>1$이다.
④ 512바이트 크기의 바이오템플릿에 일방향 해쉬 함수를 적용하여 20바이트 크기의 해쉬값을 구한다. 그리고 이 값을 개인키 x로 정의한다.
⑤ 공개키 $y=g^x \bmod p$를 구한다.

서명 생성은 메시지의 해쉬값을 구하여 개인키로 서명한 후, 검증자와 공유하는 비밀키로 암호화하여 전달한다. 서명검증은 전달된 서명 메시지를 서명자와 공유하는 비밀키로 복호화하여, 메시지의 해쉬값을 구한 후 검증 한다. 그림 3에 바이오 기반 키 추출 및 전자서명에 대해서 나타냈다.

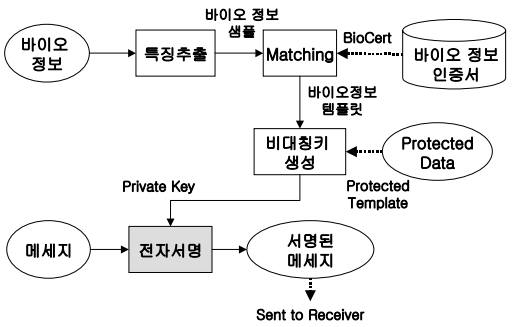

그림 3. 바이오 기반 키 추출 및 전자서명

www.dbpia.co.kr

RSA 전자서명은 원래의 메시지가 필요하나 DSA 전자서명은 원문이 불필요하며, yes/no로 서명 여부를 응답한다. 또한, DSA 알고리즘은 전자 서명을 통한 인증, 무결성, 부인방지 기능이 제공되며, RSA 알고리즘보다 복잡하여 기밀성 유지에는 사용되지 않는다.

Ⅲ. 제안 시스템

3.1 지문특징정보를 이용한 비대칭키 생성

본 논문에서 제안하는 지문 영상 특징 추출 알고리즘은 블록 FFT를 이용한 실시간 지문 인식 알고리즘으로 2차원 FFT를 수행하기 때문에 일반적으로 거치는 여러 전처리 과정이 생략되어 실시간 처리가 가능하다[10].

입력 지문영상은 256x256화소, 256그레이 레벨의 화상이며, 8x8화소의 단위 블록으로 분할하여, 1024 (32x32)개의 블록으로 분할한다. 단위블록에 대한 방향성을 8방향중의 하나로 결정하며, 방향이 정의되지 않는 블록 등은 특이점으로 구분한다. 또한, 8방향성을 이용하여 실제로 지문인식을 위한 중심점을 선정하고 중심점을 기준으로 하여 256(16x16)개의 유용한 블록 영역만을 선택한다. 방향성과 특이점 여부를 나타내고 있는 추출된 지문영상의 특징은 각각 블록에 나타난 특징을 4비트의 정형화된 표현 형식으로 나타내어, 최종적으로 1024(256×4)비트의 지문영상의 특징정보를 나타낼 수 있다[11].

지문영상은 조건에 따라 동일인의 지문이라 하더라도 약간의 오차를 가진다. 이러한 오차로 인해 전혀 다른 키가 생성되는 오류를 방지하기 위하여, 지문 등록시에 수평 및 수직 패리티를 사용하여, 추후에 입력되는 지문의 오류를 교정함으로서 약간의 오차로부터 동일한 결과 값을 유도해낼 수가 있다.

하나의 지문입력으로 부터 얻은 1024비트의 지문 특징정보는 512 단위의 두 블록(M_1, M_2)으로 나뉘어 처리되어, SHA-1 해시함수를 통해서 160비트의 해쉬값 H_A를 얻게 된다. 동일한 방법으로 지문입력에 의해 해쉬값 H_B, Hc를 얻게 된다. 여기서 H_A, H_B는 RSA공개키 암호 알고리즘의 두 소수 p, q를 계산하는데 사용되며, H_C는 공개키를 생성하는데 사용된다. 본 논문의 제안 알고리즘은 다음과 같다.

① 첫 번째 지문 영상을 SHA-1 해쉬함수를 통하여 얻어진 160비트의 해쉬값 H_A로부터 $\Phi(H_A+\delta_A) = H_A+\delta_A-1$을 만족하는 최소의 δ_A를 구한다

② 두 번째 지문 영상을 SHA-1 해쉬함수를 통하여 얻어진 160비트의 해쉬값 H_B로부터 $\Phi(H_B+\delta_B) = H_B+\delta_B-1$을 만족하는 최소의 δ_B를 구한다

③ 공개키에 필요한 두 소수 p와 q를 구한다. 단 p, q는 RSA 암호 방식의 안전성의 보장 조건에 만족되는 소수이어야 한다. 따라서 안정성을 위한 선택조건을 만족하지 못할 경우 δ_A, δ_B의 범위를 수정하여 새로운 p, q를 선택할 수 있다. 여기서 소수여부의 판정은 Euler의 함수(ϕ)에서 어떤 수 n이 소수 일 때 ϕ(n)이 n-1인 특성을 이용하였다.
$p = H_A+\delta_A$, $q = H_B+\delta_B$

③ 법 $n = p * q$ 와 오일러 함수
$\Phi(n) = (p-1) \times (q-1)$ 을 구한다.

④ 세 번째 지문 영상을 SHA-1 해쉬함수를 통하여 얻어진 160비트의 해쉬값 H_C로 부터 공개지수 e를 구하는데, 1씩 증가하여 Φ(n)과 서로 소가 되는 값을 선택한다.

⑤ 개인 비밀키 $d = e^{-1} \bmod \Phi(n)$를 구한다.

3.2 지문 검증 및 실시간 개인키 생성

초기 지문등록과정에서 입력 지문영상 특징으로부터 해시함수를 통해 얻어진 H_A, H_B, H_C에 대해서, SHA-1 해시함수를 재 적용해서 새로운 160비트 해쉬값 T를 계산하여 저장한다. 이렇게 생성된 T는 지문영상의 본인여부를 확인 하는데 사용된다. 비록 저장된 T가 노출되어도 이는 일방향으로 해시함수를 거친 결과이므로 T를 통해 H_A, H_B, H_C를 얻어 내는 것이 불가능하다. 따라서 지문특징이나 p, q를 찾아 낼 수 없으므로 개인키를 생성할 수가 없다.

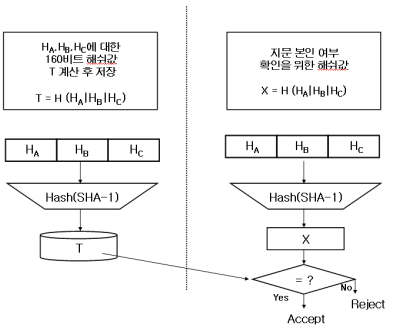

그림 4. 지문 검증과정

www.dbpia.co.kr

지문 검증과정에서 지문영상이 입력되고 지문영상 특징에 대한 해쉬값 H_A, H_B, H_C가 얻어지면 해시함수를 적용한 해쉬값 X가 이미 저장되어 있는 해쉬값 T와 일치하는지 비교 한다. 일치하면 본인의 지문으로 검증되며 본인의 개인키 생성할 수 있다.

비대칭키는 검증된 해쉬값(H_A, H_B, H_C)를 이용하여 본 논문에서 제안한 알고리즘으로 생성하게 된다. 즉, 개인키 생성을 위해서 지문영상이 입력되면 앞에서 제시된 해시함수를 통해서 지문영상특징에 대한 다이제스트 H_A, H_B, H_C를 얻는다. 먼저 지문 검증 과정을 거친 후 본인 지문으로 확인이 되면 H_A, H_B, H_C와 가지고 있던 δ_A, δ_B를 이용하여 간단히 p, q계산해 낸다. 이미 알고 있는 공개키 e와 p, q를 이용 개인키를 생성하게 된다.

Ⅳ. 제안 알고리즘 고찰

본 논문은 지문 인식을 기반으로 공개키 암호알고리즘인 RSA의 키를 생성하는 방법을 사용함에 따라 지문 자체 보안 특성에 의존한다. 본 논문에서 사용한 지문인식 알고리즘은 타인의 지문을 본인의 지문으로 잘못 인식하는 타인 접수율을 0%로 했을 때 자신의 지문을 타인의 지문으로 판단하는 본인 거부율이 2.2%로 실험결과 발표되었다[10]. 지문인식 알고리즘은 지속적으로 개발되고 있으며, 현재 본인 거부율이 0.1%미만 까지 줄일 수 있는 알고리즘이 개발된 상태이다. 또한, 본 논문에서 제시된 SHA-1 해시함수는 입력의 크기가 160 비트이상에 대해서는 안정성을 검증되어 있으며, 2차 해쉬값 T로부터 H_A, H_B, H_C를 알아내는 것이 거의 불가능하다. 따라서, 의료정보 시스템 사용자의 안전성이 높은 개인 인식 및 검증시스템으로도 사용할 수 있다. 본 알고리즘에 의해 생성된 해쉬값 H_A, H_B, H_C를 키 값으로 소수 p, q 의 크기를 조절할 수 있으며, 이를 통해 더욱 견고한 비 대칭키를 생성할 수 있다.

본 논문에서 제안하는 방법은 무선상의 보안서비스 뿐아니라, 개인의 의료정보를 사용하는 모든 이해 당사자들에 대한 인증및 검증을 가능하게 한다. 또한, 지문 특징 정보를 통해 실시간으로 비대칭키를 생성함으로써 개인키 관리상에 발생할 수 있었던 보안상의 문제점을 해결 하였으며, 개인 지문입력을 통한 일괄적인 전자서명 방식은 보안성 및 편리성을 향상시킬 수 있다. 이러한 특징은 관리상의 허점과 분실의 우려가 높은 u-헬스케어의 핵심 장비인 모바일 의료장비에 특히 효율적으로 적용 될 수 있을 것이다. 즉, 제안시스템에 의해 실시간으로 생성되는 비대칭키를 표준 WPKI 기반 전자서명에 응용함으로써, u-헬스케어 분야에서 의료정보 시스템의 특성상 검토해야할 위협요소인 기밀성, 안정성, 무결성, 접근 동의, 익명성 등을 제거할 수 있다. 그림 5.는 본 논문의 지문 특징정보를 이용한 전체 전자서명도에 대해서 나타내었다.

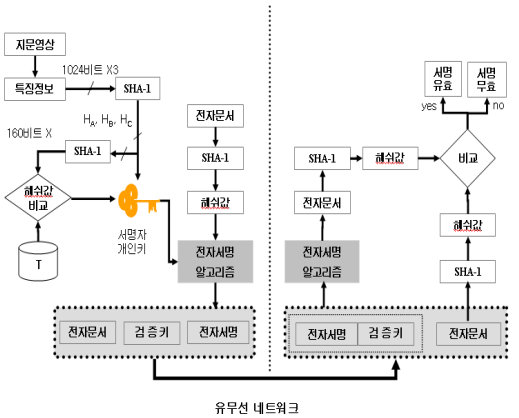

그림 5. 지문 특징 정보를 이용한 전자서명

본 제안알고리즘에서 지문영상 뿐 아니라 다른 바이오정보의 특징정보를 이용할 수 있다. 또한, 특징 정보를 키 값으로 하여, 다양한 암호알고리즘에 응용할 수 있을 것이다. 본 제안시스템을 무선단말기 환경에 적용한다면 기존의 전자 지불은 물론 은행창구와 ATM을 통한 은행업무 등 다양한 분야에서 적용할 수 있을 것이다.

Ⅴ. 결 론

최근 정보기술의 발전과 더불어, 경제발전으로 인한 고령화에 따른 의료 정보기술이 발전하면서, u-헬스케어의 연구 개발이 활발히 진행하고 있다. 이에따른 의료정보 서비스에 다양한 보안 위협이 발생하고 있다. 본 논문은 u-헬스케어에서 모바일장비와 의료정보시스템과의 보안위협에 대해서 고찰하고 지문 특징정보를 이용하여 실시간으로 비 대칭키를 생성하는 방법에 대해서 제안하였다. 제안 알고리즘은 무작위 3개의 지문에 대해서 특징 정보 추출하여, SHA-1 알고리즘을 통해 해쉬값을 생성하였고, RSA 공개키 알고리즘으로 실시간 비대칭키를 생성하는 방법을 제안하였다. 본 논문은 실시간으로 비대칭키를 생성함으로서 개인키의 분실과

www.dbpia.co.kr

Euler함수의 노출에 따른 문제점을 제거할 수 있다. 또한, 생성된 비대칭키는 WPKI 기반 전자서명 기법으로 의료정보에 대한 다양한 보안 위협을 제거할 수 있다. 본 알고리즘은 홍채, 손등 정맥, 망막, DNA 등 다른 바이오 정보에 대해서 응용할 수 있다. 앞으로 연구내용으로 각 의료정보 문서에 DRM (Digital right Management)을 이용하여, 워커마킹 및 핑거프린트 알고리즘을 적용하여 의료정보 문서를 사용한 사용자들에 대한 추적을 가능하게 하는 기술의 적용이 필요할 것이다.

참 고 문 헌

〔1〕 송지은, 김신효, 정명애, "u-헬스케어 서비스에서의 의료정보보호", 정보보호학회지, 제 17권 제 1호, pp. 47-55. 2007. 2.

〔2〕 김무섭, 신진아, 박영수, 전성익, "모바일 플랫폼용 공통보안핵심 모듈기술", 정보보호학회지, 제 16권 제 3호, pp. 7-17, 2006. 6.

〔3〕 성윤국 김현철, 정진욱, 김순철, 유원, "A Study on Wireless PKI Technology Standard", 정보 보증 논문지, 제 2권 제 2호, 2002.

〔4〕 김용국, 이윤배, "모바일 환경에서 의료 정보 특성을 고려한 디지털 서명", 한국해양 정보통신 학회 논문지, 제 9권 제 2호, pp.374-379, 2005.

〔5〕 이형우, 윤성현, 문기영, 정윤수, "바이오정보 기반 전자서명 및 디지털 키 생성기법", 한국콘텐츠 학회지, 제 5권 제 1호, pp.32-43, 2007.

〔6〕 김재성, 김영준, "바이오 정보를 이용한 U-Healthcare 인증방안 연구", 한국정보보호학회지, 17(1), pp.57-62, 2007.

〔7〕 하창승, 조익성, "SHA-1 방식을 이용한 제한된 웹 페이지에 접근하기 위한 서버 독립적인 패스워드 인정 방안", 한국컴퓨터정보학회논문지, 6(4), pp.146-153, 2001.

〔8〕 P. Janbandhu and M. siyal, "Novel biometric digital signature for Internet-based application", Information Management & Computer Security, vol. 9, No. 5, 2001, pp. 205-212.

〔9〕 R.Rivest, A Shamir, and L.Adleman, "A method for obtaining digital signatures and public-key crypto systems" Communication of the ACM, vol. 21 pp.120-126, 1978"

〔10〕 안도성, 김학일, "블럭 FFT를 이용한 실시간 지문인식 알고리즘", 전자공학회 논문지, 제 32권, B편, 제 6권, pp. 89-101, 1995.

〔11〕 차정희, 장석우, 김계영, "특징점의 연결정보를 이용한 지문인식", 한국정보처리학회논문지B, 10B(7), pp.815-822, 2003.

김 창 복 (Kim Chang-Bok) 정회원

1989년 2월 단국대학교 전자공학과 석사

2006년 3월~현재 인천대학교 컴퓨터공학과 박사과정

<관심분야>이동통신, 인터넷 보안, 임베디드시스템

김 남 일 (Kim Nam-il) 정회원

2000년 8월 건국대학교 전자공학과 박사

2008년 2월~현재 가천의과학대학교 IT학과 교수

<관심분야>컴퓨터네트워크,트래픽제어, 유비쿼터스,유헬스케어,BcN

www.dbpia.co.kr