모바일 환경에서 의료 정보 특성을 고려한 디지털서명

김용국* · 이윤배*

Digital Signature Considering the Medical Information Property on Mobile Environment

Yong-Gug Kim* · Yeun-Bae Lee*

요 약

의료 정보가 데이터베이스에 집적되고 다수의 연구자 혹은 의료인에 의해 무작위로 이용되는 경우에는 개인의 사생활에 대한 중대한 침해가 될 수 있다. 의료 정보 서비스는 시간의 경과에 따라 통합 의료 정보 시스템으로 발전할 것이고 전체적 및 부분적으로 정보 보안의 요구는 필연적으로 대두될 것이다. 본 연구는 의료 정보 시스템에서 보안 위협 요소를 고찰하고 PDA 등의 모바일 디바이스를 통한 의료 정보 서비스 모델을 제시한다. 제안된 모델을 중심으로 처방전 전자 서명 관리에 중심을 둔 보안 구조를 제안하였다. 제안된 구조는 의료진의 책임 있는 처방을 유도하며, 신뢰성 있는 의료 시스템의 구성, 의료 분쟁 발생 시 적절한 데이터로써 활용될 수 있을 것이다.

ABSTRACT

In the most of medical institution medical information is totally stored in a database and many number of researchers and staffs of the hospital access these information anytime. This can be caused patient's privacy to be violated. Introducing a tool for security should be considered as one of the most important requirement especially in the case that today's medical information service expands into an integrated one.
In this paper we review the matters of security threat on a medical information system and propose a secure medical information service model equipped on mobile device such as PDA. Also we propose a security architecture employing a digital signature mechanism to protect the personal information on the model. Proposed architecture can lead the doctor to diagnose with high responsibility, help to build a reliable medical information system. and through the signed data, we can get some useful information against medical strife.

키워드

Medical information system, Medical information security, ID 기반 암호기법, Mobile Medical information system, Digital signature

*조선대학교 대학원 전자계산학과

접수일자 2005. 3. 23

Ⅰ. 서 론

대부분의 시장이 공급자 중심에서 소비자 중심으로 전환된 것과 마찬가지로 의료서비스 시장도 편의 시설, 친절도, 진료의 질에 따른 각종 정보를 바탕으로 의료 서비스 소비자에 의하여 선택 되는 시대가 되었다.

의료계는 1990년대 중반, 행정 업무 전산화를 시작으로 1990년대 후반에 소비자에 대한 서비스와 원가 절감을 위한 정보 처리 기술(IT)을 선택하여 의료 정보화를 추진하였다. 그 후 IT 기술은 의료 서비스 질을 향상시키고, 병원의 경영 성과를 높이는 방법으로 인식되어 가고 있다[1].

이에 따라 OCS(Order Communication System, 처방 전달 시스템), PACS(Picture Archiving and Communication System, 의료 영상 저장 전송 시스템), EMR(Electronic Medical Record, 전자 의무 기록 시스템), Tele-Medicine(원격 진료),EDI(Electronic Data Interchange, 전자 자료 교환), HIS(Hospital Information System, 병원 정보 시스템), 통합 의사 결정 시스템, 그리고 인공 지능 전문가 문진 시스템 등의 수많은 의료 서비스를 위한 IT 기술의 개념들이 도입되었거나 도입이 고려되고 있다. 이러한 시스템들과 함께 최근 관심이 집중 되고 있는 것 중의 하나가 모바일 디바이스(mobile device)에 의한 서비스의 제공이다. 조만간 장비의 제약성이 극복 되고 패러다임 변화에 대한 인식이 확산 되면 유비쿼터스(Ubiquitous) 의료 서비스 진화로의 자연스러운 변환이 이루어질 것이다. 이러한 시스템의 도입은 의료 서비스 소비자 입장에서 본다면 [3]에서 제시한 의료 서비스 질 구성 차원에서 심리성, 반응성, 고객이해성, 신뢰성 등에서 효과적인 접근이 될 것이다.

또한 의료 서비스 제공자 입장에서는 의료 정보의 관리 및 전달 체계의 효율성을 확보할 수 있을 것이다. 이러한 의료 정보 시스템은 의료 서비스 품질 향상과 효율성 향상을 기대할 수 있는 반면 취급 되는 의료 정보는 궁극적으로 개인에 대한 정보이기 때문에 사생활 보호의 차원에서 합법적으로 보호 받아야 한다. 특히, 의료 정보가 데이터베이스에 집적되고 다수의 연구자 혹은 의료인에 의해 무작위로 이용되는 경우에는 개인의 사생활에 대한 중대한 침해가 될 수 있다는 점에 주의 하여야 한다[4].

시간의 경과에 따라 의료 정보 서비스는 [5]에서 제안된 바와 같은 통합 의료 정보 시스템으로 발전할 것이고 전체적 및 부분적으로 정보 보안의 요구는 필연적으로 대두될 것으로 예측된다.

본 연구는 PDA 등의 모바일 디바이스를 통한 의료 정보 서비스 모델을 제시하고 그 모델을 중심으로 고려할 수 있는 보안 사항을 처방전 관리의 전자 서명 관리에 중심을 둔 적합한 보안 구조를 제안한다. 제안된 구조는 의료진의 책임 있는 처방을 유도하며, 신뢰성 있는 의료 시스템의 구성, 의료 분쟁 발생 시 적절한 데이터로써 활용될 수 있을 것이다.

Ⅱ. 의료 정보 시스템의 정보 보안

개인 정보의 중요성은 정보 자체가 갖는 가치만으로도 그 중요성이 크다 할 수 있으나, 정보의 노출로 인해 본질적인 부분인 프라이버시를 위협할 수 있다. 특히, 의료 정보는 개인 정보 중에서 변경, 수정할 수 없는 부분이 많으므로 가장 중요한 정보라고 할 수 있으며, 프라이버시에 대한 가장 핵심적인 요소라고 할 수 있다[6]. 본 장에서는 의료 정보 시스템에서 고려하여야 할 정보 보안 요소들을 고찰한다.

2.1 의료 정보 보호 원칙

첫째, 의료 정보는 건강 증진의 목적으로만 이용되어야 한다.

둘째, 진료 정보는 환자의 동의 없이는 공개되어서는 안 되며, 진료 정보를 획득한 자는 반드시 비밀을 지켜야 할 의무를 가진다.

셋째, 개인은 자신의 의료 정보에 접근할 권리를 가지며, 자신에 대한 의무 기록을 열람한 후 변경을 요구할 수 있어야 하고, 정보 이용과 관련된 사항들에 대해 고지를 받을 권리가 있다.

넷째, 의료 정보를 부당하게 취급하는 자는 법적 책임을 진다.

다섯째, 의료 정보에 관한 개인의 비밀은 국민 건강, 의학 연구, 건강 보험 등의 필요성에 의하여 침해되어서는 안 된다.

2.2 의료 정보의 보안

보안의 정의는 정보의 보안성, 무결성, 가용성을 모두 포함하는 의미로써 정보가 실수나 고의로 공개되지 않도록 하는 한편, 변조되지 않고 언제나 접근이 용이하도록 하는 일련의 활동이라고 할 수 있다. 특히, 진료 정보의 보안 체계에서는 다음과 같은 요소를 고려해야 한다[7].

1) 완전성(Completeness)

의료 현장에서는 일반적으로 비정상적인 내용만 기록되므로 어떤 데이터가 환자의 기록에서

발견되지 않을 때는 이상이 없는 것을 뜻할 수도 있고 이러한 데이터가 이용될 수 없거나 수집되지 않은 것을 뜻할 수도 있다.

2) 정확성(Accuracy)

판독이나 치료 및 약물 처방을 위한 데이터가 잘못 전달되거나 뒤바뀐 경우 적절치 못한 조치가 이루어질 수 있으므로 정확한 데이터가 정확한 송신자에게 전달되고 정확히 해독되어야 한다.

3) 정밀성(Precision)

의료 정보에서 나오는 데이터들 중 특히 수치 데이터는 환자의 생명과 직접적인 연관이 있는 데이터이므로 측정치, 투약량 등 수치의 전송에 있어 정밀성 또한 중요한 문제이다.

데이터의 안전한 전송을 보장하기 위해서는 상대방을 확인함과 동시에 정보의 복제에 의한 정보의 부당한 누출이나 손상을 방지하는 적절한 대책이 요구된다.

즉, 전송 당사자들에 대한 인증을 수행하고 데이터에 부정이 없다는 것을 증명하는 구조가 갖추어져 있어야 하며 이러한 데이터들이 다른 사람들에게 노출되어 손상 입는 일이 없이 기밀성을 보장하는 암/복호화가 필요하다. 그림 1은 의료 정보 서비스와 정보 보호 시스템과의 관계를 나타낸 것이다[8].

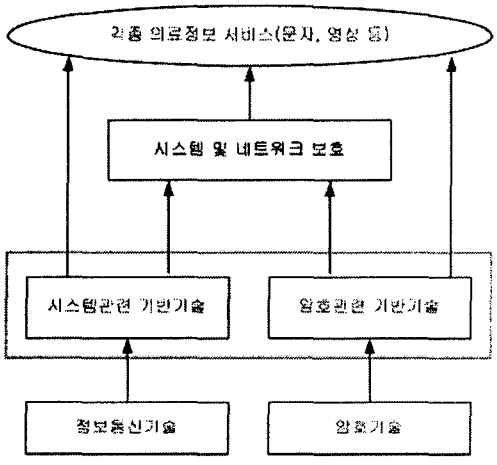


그림 4. 의료정보서비스와 정보보호

2.3 의료정보 특성에 따른 위협 요소

다른 정보 시스템과는 다른 몇 가지 특수한 요소를 포함하게 된다. 의료 업무 특성상 검토해야 할 위협 요소들은 표 1과 같다[9].

표 1. 의료정보 특성에 따른 위협요소

구분	위협요소
기밀 보존에 대한 인식	환자가 의료 정보의 기밀에 대한 신뢰성을 인식하지 못하면 치료와 관련된 정보의 비밀로 인하여 다른 환자에 대한 부적절한 치료의 원인이 되어 다른 환자의 위험이 증가된다.
정보에 대한 안전성 인식	의료 정보에 대한 기록들이 시스템 상에서 안전하다는 확신이 없으면 의사들은 의료 정보 시스템에 구축되어 있는 정보에 대한 사용을 꺼리게 되므로 전자 기록에 대한 법적 보장이 선행되어야 한다.
기록 변경에 따른 문제	진료 기록은 어떠한 경우에도 삭제되어서는 안 된다. 오진의 경우가 발생 하였더라도 기록은 유지되어야 한다. 허가된 사람이 내용을 수정해야 한다면 추가사항으로 기록 되어야 한다.
동의의 원칙	법적으로 인정하는 경우에만 제외하고 개인에 대한 기록 접근 시 반드시 환자 혹은 대리인의 동의를 얻어야 한다.
개인정보의 식별	통계를 얻기 위한 연구목적으로 환자의 기록 열람을 요청할 경우 관련된 환자의 모든 기록에 접근할 수 있는데 이때 개인에 대한 식별이 되지 않도록 해야 한다.
정보의 보존 및 유지	진료 기록에 대한 보존 기간과 의무가 명확히 명시되어 유지되도록 해야 한다.
정보의 보고 문제	법으로 정해진 특정 질병의 경우 반드시 보고 되어야 하는 의무가 있다.

2.4 의료 정보의 보호 방안

의료 정보를 보호할 수 있는 방안으로써 법제도적인 방법과 기술적인 방법으로 나누어 볼 수 있다.

1) 법제도적인 방법

보건 의료 기본법 제 12조에 보건 의료 서비스에 대한 국민의 자기 결정권, 13조에 보건 의료 정보의 비밀 보호에 관한 규정, 의료법/전염병예방법/정신 보건법에 의료 정보 보호에 관한 조항이 있다. 최근에 원격 의료, 전자 의무 기록 등 전자적인 방법으로 기록되는 의료 정보에 대해서도 개정 의료법에 정보 보호를 명시하고 있다. 공공기관의 개인 정보 보호에 관한 법률에도 공공 기관에 저장되어 있는 개인 정보로서 개인 의료 정보에 대한 보호를 명시하고 있는 상황이다. 이처럼 법적으로 보호되어야 할 의료 정보는 보호 문서, 절차, 조직, 등 전반적이고 총체적인 운영 및 유지를 위한 제도로서 실시되어야 한다.

2) 기술적인 방법

접근 통제, 자연 재해로부터의 보호와 정보를 저장하고 있는 시설에 대한 보호와 같은 물리적으로 보호하는 방법이 있다. 또, 네트워크, 시스템, 데이터베이스, 응용 소프트웨어, 데이터 등을 보호하기 위한 다양한 기술을 사용할 수 있다.

III. 모바일 의료정보시스템 모델

의료 정보의 범위는 의사와 환자를 중심으로 또는 그와 연관되어 발생되는 모든 데이터 즉, 환자 기록, 진료 기록, 환자와 관련된 검사 자료, 영상 자료, 투약관련 자료, 뿐만 아니라 치료와 관련 되어 지불해야 하는 진료비 및 의약품비 등 임상에서 다루어지는 모든 데이터들을 말한다[7]. 의료 정보 시스템의 모바일 디바이스 시스템으로의 진화는 진료 차트(또는 진단보고서)의 디지털화를 의미하기 하고 이는 의료 정보의 멀티미디어화를 의미하고 있다.

3.1 멀티미디어 의료 정보

의료 진단 보고서는 현재 병원에서 사용 중인 진료 차트와 유사한 서식으로 작성 되며, 환자의 기본적인 사항(성별, 성명, 주민등록번호, 연령, 신장, 체중, 혈액형, 혈압 등)과 기본적인 문진 결과 및 환자의 증세 등이 기록 된다 . 의료 진단 보고서는 담당 진료 과목에 따른 상세 진단 정보가 진료 단계에 따라 추가 된다. PACS 등의 다양한 의료 정보 시스템의 등장에 따라 취급 되어지는 정보는 표 2와 같다.

표 2. 멀티미디어 의료 정보

정보매체 구분	정보
영상정보	-흉부, 손, 발, 팔, 다리, 두부, 소화기 및 비뇨기 등의 일반 X-ray 영상 -유방 등의 특수 X-ray 영상 -심혈관, 뇌혈관 척수 등의 혈관 조형 영상 -CT 영상 -MRI영상 -초음파 진단 영상 -소화기 및 호흡기 계통의 내시경영상 -병리학적 검사에 따른 현미경 영상
생체전기적 계측신호 판독 파형정보	-심전도(일반 심전도, 부하 심전도, 24 시간 심전도) -신경전도(근전도, 시각 뇌 유발 전위, 청각 뇌 유발 전위, 망막 전위 등) -뇌파
문자 정보	-과거 병력 -문진 내용 -병리 검사 결과
음성정보	-방사선 판독 소견 -병리학적 검사 소견 -현미경 판독 소견

3.2 모바일 의료 정보 시스템

PDA, 임베디드 기기 등의 모바일 디바이스가 의료 정보 시스템에 접목되는 것은 기존의 시스템과는 다른 개념으로 해석될 수 있다. 기존 시스템이 행정, 정보 전달의 효율성에 기반하고 있었다면 모바일 의료 정보 시스템은 의료 수요자 중심적 시스템으로서의 기능을 제공할 것으로 보인다.

모바일 의료 정보 시스템은 부분적/통합적 적용에 따라 서비스 범주가 달라질 수 있겠으나 이면에서 병원 간 보건 의료 정보 표준프로토콜(HL7)이 도입되어 있고 통합 의료 정보 시스템이 구축된 경우 그림 2와 같이 모바일 진료 차트 부분을 도입함으로써 병원 내 종이 차트 없는 병원을 구현할 수 있을 것이다. 그림 2의 모바일 진료 차트를 통해 3.1절에서 기술된 멀티미디어 의료 정보들을 열람하고 진료 결과를 기록할 것이다.

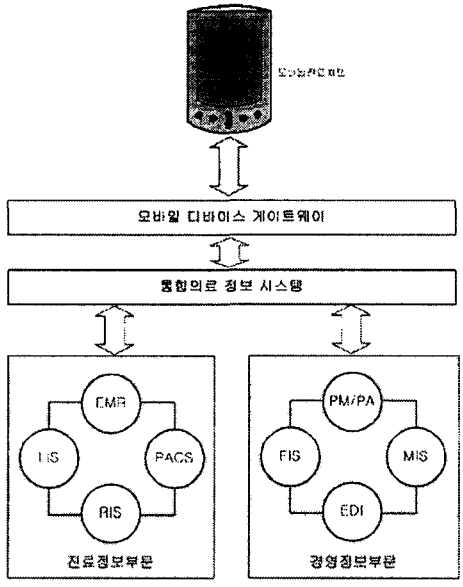


그림 5. 모바일 의료 정보 시스템 모델

모바일 의료 정보 시스템은 운영되는 시스템 의료 정보의 공유가 병원 어느 곳에서나 가능해져 보다 빠르고 정확한 진료를 수행하며 각종 검사 자료

와 이미지 정보를 환자나 의료진에게 신속하게 제공할 수 있다. 또한 의료진의 과중한 문서 작업과 반복 업무 시간을 줄여 업무 효율성을 향상 시킬 수 있는 장점이 있다.

IV. 의료 정보 특성을 고려한 디지털 서명

본 논문에서는 멀티미디어 의료정보를 취급할 수 있는 모바일 의료 정보 시스템에서 표 1에 제시된 바와 같은 위협 요소를 제거할 수 있는 기술적인 보호 방법을 제시하고자 한다. 위협 요소들은 보안 고려 요소인 디지털 서명에 의하여 제거될 수 있는 부분으로 진료자인 의사가 의료 진단 보고서에 디지털 서명하도록 하였다. ID 기반 공개키 암호 기법은 사용자의 식별 정보가 바로 공개키로 사용될 수 있기 때문에 PKI(Public Key Infrastructure) 기반의 기존의 공개키 암호 시스템에서의 인증서 관리보다 복잡성이 적다는 장점을 가지고 있다. 따라서 [10]에 제안된 방법을 응용하여 모바일 진료차트를 가진 의사가 사전의 의료 진단 보고서를 검증하여 신뢰 할 수 있도록 하였다.

표 3. 표기법

M = 의료정보(메세지)
f,h = 공개된 일방향 함수
D_1 = 최초의 의료 차트 작성자/보관자
D_i = 의사 i의 ID
(이름, 주민번호, 의사번호, 사원번호 등)
$D_{cm} = D_1 \| D_2 \| \ldots \| D_m$

4.1 키 발생 및 배포

진료자인 의사 및 의료 정보 발생자는 의료 정보 시스템의 신뢰센터인 KGC(Key Generation Center)에 ID를 등록하고 키를 발급 받는다.

다음은 KGC의 키 발생 과정이다.

1) N = p * q (큰 소수 p, q)
2) Iij = f(Di, j), j=1,2,...,k
   Iij-1 = Sij2 mod N
3) (N, f, h, Si1,...,Sik) 배포

4.2 최초의 차트 작성자(D1)의 서명

최초의 의료 차트 작성자는 자신이 만든 차트에 다음과 같은 알고리즘을 거쳐 서명한다.

1) D1은 랜덤(random) 수 R1 ∈ ZN 을 선택
   X1 = R12 mod N
   (e11,...,e1k) = h(M, Dcm, X1)
   $Y1 = R1 \prod_{e1j=1} S1j \bmod N, \quad j=1,2,...,k$
2) 다음, 진료자인 의사에게 (M, Dcm, X1,Y1) 전송
3) D1은 차트의 전체적인 검증이 요구되는 경우, 다음과 같이 검증할 수 있다.

수신된 ((e21,...,e2k),...,(em1,...,emk), Y2,...,Ym)을 바탕으로 (M, Dcm, (e11,...,e1k),...,(em1,...,emk),Y2,...,Ym)을 검증자에게 보내 4.5절과 같이 검증을 수행한다.

4.3 진료자 n의 서명 발생

진료자인 의사는 (M, Dcm, X1, Y1)을 받으면

4.4절의 단계를 거쳐 검증을 수행한다.

진료자 n의 서명과정 알고리즘은 다음과 같다.

1) 랜덤수 R1 ∈ ZN 을 선택
   Xn = Rn2X1 mod N
   (en1,...,enk) = h(M, Dcm, Xn)
   $Yn = Y1Rn \prod_{enj=1} Snj \bmod N, \quad j=1,2,...,k$
2) n은 (en1,...,enk)와 Yn을 D1에게 전송

4.4 서명자 n의 검증 단계

1) (e11,...,e1k) = h(M,Dcm,X1)
2) I1j = f(D1, j), j = 1,2,...,k
3) $Z1 = Y12 \prod_{e1j=1} I1j \bmod N$
4) Z1 = X1 이면 유효
   Z1 ≠ X1이면 무효

4.5 검증자의 서명 검증 단계

검증자는 D1에게서

(M, Dcm, (e11,...,e1k),...,(em1,...,emk),Y2,...,Ym)을 수신하여 다음 단계를 거쳐 검증을 수행 한다.

1) Iij = f(Di, j), i = 1,2,...,m, j = 1,2,...,k
2) $Zi = Yi2 \prod_{e1j=1} I1j \prod_{eij=1} Iij \bmod N$
3) (ei1,...,eik) = h(M, Dcm, Zi) 유효검증

4.6 적용된 디지털서명 기법의 분석

적용된 디지털서명 기법은 적절한 암호 기법을 사용하여 기밀성을 보장함으로써 표 1에서 언급한 위협 요소들을 제거할 수 있다. 제안된 방법만으로도 진료자인 의사들은 자신이 진료하기 전에 어떤 의사가 어떻게 진료하였는지를 알 수 있으며, 보고의 의무, 의료 사고 시에 적절한 책임의 한계를 규정지을 수 있는 장점이 있다. 또한 최초의 차트 작성자 또는 보관자로서 D1은 진료기록의 유지, 전체적인 검증을 수행할 수 있다.

V. 결 론

정보화는 종래의 의사 위주였던 환자-의사와의 의료 서비스 관계에서 의사는 환자에게 정보를 제공, 분석해 주고, 환자는 이 치료 과정에 적극 협조함으로써 수직적인 관계에서 수평적인 동반자적 관계로 발전할 것으로 보인다. 각종 의료 정보 제공 및 고객 만족 시스템 구축, 각종 모바일 디바이스를 통한 개인 의무 정보 조회 및 예약 서비스 등이 머지않아 정착되어질 것으로 보인다. 의료 정보화의 정착은 시스템의 안정성(reliability)과 보안성(security)를 전제로 한다. 본 논문에서는 모바일 의료 정보 시스템 환경에서 의료 정보 특성의 위협요소를 제거할 수 있는 기술적인 보호 방법을 제시하였다. 제시된 방법은 ID 기반 공개키 암호 기법을 응용한 것으로써 PKI 방식에서 보다 인증서 관리가 단순하다는 장점을 가진다. 위협요소들은 보안 고려 요소인 디지털 서명에 의하여 제거될 수 있는 부분으로 진료자인 의사가 의료 진단 보고서에 디지털 서명을 하도록 하였다. 그러나 제안된 방법은 기밀성을 보장을 위한 구체적인 방법과 멀티미디어 의료 정보의 원본 데이터의 보장을 위한 방법에 대하여는 언급되지 않았기 때문에 향후 추가적인 연구가 필요하다.

참고문헌

[1] "미래의료산업은 정보화가 좌우한다," Network Times. pp.122-132. 2004.9.

[2] 박영훈, PDA를 이용한 이동형 진료 정보 시스템 개발:MobileMed, 보건복지부, 보건의료기술연구개발사업최종보고서, 2003.9

[3] 박주희,"의료서비스의 구매평가에 관한 연구", 동아대학교 대학원, 박사학위논문, 1994

[4] 강성원, "진료정보 공동활용을 위한 한국형 표준 모델링 방안에 관한 연구", 연세대학교 보건대학원, 석사학위논문, 2003.

[5] 이원희, "통합의료정보시스템의 효율적인 설계 및 구축에 대한 연구", 청주대학교 산업경영대학원, 석사학위논문, 2002

[6] 진태영, "의학적 검사 및 의무기록과 관련된 사생활의 비밀보호", 연세대학교 보건대학원, 석사학위논문, 2003.

[7] 정혜명, "의료 정보 보안을 위한 MISec 암호 알고리즘의 설계 및 차분 해독", 숭실대학교 대학원 박사학위논문, 2001

[8] 정혜명, 전문석, "의료정보 보안을 위한 블록 암호 알고리즘의 설계", 정보처리학회논문지 C 제8-C권 제3호. pp.253-262. 2001.6

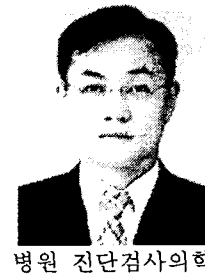
[9] 김봉희, 박진섭, "의료정보 특성을 고려한 보안 정책과 메커니즘", 한국멀티미디어학회 춘계학술발표논문집 pp.168-179. 1999.

[10] 강창구, "디지털 다중서명 방식과 응용에 관한 연구", 충남대학교 대학원, 박사학위논문, 1993.

저자소개

이윤배(Yeun-Bae Lee)

1997 - 1999. 조선대 정보과학대 학장.
2003 - 2005.현 한국정보 처리학회 부회장
2001 - 2005. 현 한국해양 정보통신학회 학술이사
2004 - 2005. 현 (국무총리) 한국청소년보호위원회 인터넷정책분과위원
※ 관심분야 : 인공지능, 데이터베이스, 전문가시스템, 무선인터넷.



김용국(Yong-Gug Kim)

1992 - 1994. 조선대 대학원 석사학위.
1996 - 현재. 조선대 대학원 박사수료.
1988 - 현재. 서강정보대학 외래강사.
1988 - 현재. 조선대학교부속병원 진단검사의학과.
※ 관심분야 : 영상처리, 무선인터넷보안, 멀티미디어, 원격진료.