http://dx.doi.org/10.15207/JKCS.2015.6.6.081

융합형 u-헬스케어 서비스에서 헬스 정보 교환을 위한 키 트리 기반 관리 체계 설계

김동현, 김석수*
한남대학교 멀티미디어학과

Design of Key Tree-based Management Scheme for Healthcare Information Exchange in Convergent u-Healthcare Service

Donghyun Kim, Seoksoo Kim*
Department of Multimedia, Hannam University

요 약 u-헬스케어에서는 무선 센서와 에드혹 네트워크를 통해 사용자의 건강 정보, 응급 정보를 수집, 분석하고 있으며 상호 운용이 가능한 전자 헬스 정보의 기록 및 전송을 위하여 동적인 액세스 제어를 수행하고 있다. 네트워크 시스템을 이용한 u-헬스케어의 경우 상호 운용 가능한 전자 건강 기록과 민감한 환자 의료 정보 전송은 개인 정보 보호 및 보안에 대한 문제점을 해결하기 위하여 키 관리 체계를 사용하고 있으나 동적인 액세스 제어에서는 그룹 키 관리가 어려우며 그룹에서 접근 맴버를 추가하거나 삭제할 경우에 매번 그룹 키를 변경해야하는 문제점을 가지고 있다. 따라서 본 논문에서는 유비쿼터스 헬스 케어의 동적 액세스를 수행하는 네트워크 환경에서 헬스 정보 교환을 위한 융합형 키 관리 체계방식을 제안한다.

• **주제어** : 키 관리, 헬스 정보, 유비쿼터스 헬스케어, 키 트리, 정보 보안

Abstract The threats to privacy and security have received increasing attention as ubiquitous healthcare applications over the Internet become more prevalent, mobile and universal. In particular, we address the communication security issues of access sharing of health information resources in the ubiquitous healthcare environment. The proposed scheme resolves the sender and data authentication problem in information systems and group communications. We propose a novel key management scheme for generating and distributing cryptographic keys to constituent users to provide form of data encryption method for certain types of data concerning resource constraints for secure communications in the ubiquitous healthcare domains.

• **Key Words** : Key Management, Health Information, Ubiquitous Healthcare, Key Tree, Information Security

1. 서론

정보통신기술의 발전으로 사회전반적인 활동들이 유비쿼터스(Ubiquitous) 환경으로 변화하고 있다. 의료 서비스 분야에서는 사용자의 상황을 언제, 어디에서든지 모니터링하여 응급상황에 대처하기 위한 u-헬스케어 서비스가 연구되고 있다.

u-헬스케어에서 실시간으로 환자의 상황을 모니터링하거나 응급상황에 대처하기 위해서는 사용자와 주변 환경에 따른 상황인식을 수행해야 한다[1].

*교신저자 : 김석수(sskim0123@naver.com)
접수일 2015년 10월 2일 수정일 2015년 11월 20일 게재확정일 2015년 12월 20일

사용자의 환경정보를 수집하기 위해서는 무선 센서와 에드혹 네트워크를 통해 효과적으로 사용자의 위치를 추적해야하며 사용자의 혈압, 맥박 등 다양한 신체 정보를 신체 센서를 통해 수집하고 수집된 정보를 분석하여 사용자를 진단하고 상황을 판단해야 한다.

이와 같은 u-헬스케어에 대한 관심이 증대되면서 최근 네트워크 컴퓨팅 시스템을 이용한 헬스케어 정보 시스템(HIS, Healthcare Information System)[2]의 사용자 헬스 정보 공유를 위한 시스템 접속에 대한 연구가 진행되고 있다[3].

헬스 정보 관리자들의 상호 운영이 가능한 헬스케어 정보 시스템들 간의 사용자 헤스 정보의 전송 및 데이터 기록은 네트워크 시스템을 통해 이루어지고 있다.

이와 같이 다양한 u-헬스케어 서비스들이 이용하는 헬스 정보가 네트워크 시스템을 통해 헬스케어 정보 시스템들끼리 교환되면서 개인 정보 및 사용자의 중요 신체정보를 포함하고 있는 u-헬스 정보에 대한 보안 및 보호 방안에 대한 문제점들이 나타나기 시작하였으며 무선 네트워크 기술의 발전으로 u-헬스케어 서비스들이 모바일 디바이스와 무선 네트워크를 이용한 방식으로 변경되면서 무선 네트워크 환경에서 안전한 헬스 정보 리소스 교환을 위한 방법이 중요한 이슈 상황으로 대두되고 있다.

무선 네트워크 환경의 u-헬스케어 서비스에서 개인정보 및 헬스정보를 보호하기 위해서는 헬스정보 리소스의 접근 인증을 위한 키 관리 체계를 만들어야 한다.

기존 유선 네트워크 시스템을 이용한 헬스케어 시스템들은 헬스케어 시스템을 통해 진료를 수행하는 의사, 의료 기관에서 데이터 공유, 교환을 통해 상호운영을 수행한다. 이를 위해서는 키 관리 방식을 이용한 보안 체계를 사용하였으며 이 방법은 데이터 접근 권한이 있는 사용자들 사이에서 공유할 수 있는 비밀 키를 그룹 단위로 설정하고 비밀키를 이용하여 그룹간의 통신을 암호화하고 이를 위한 그룹키를 생성함으로써 데이터 접근 권한을 가지지 못한 타그룹의 사용자들이 리소스 접근을 차단하여 보다 안전한 데이터 리소스 관리를 수행하기 위핸 보안 체계를 활성화 시키는 것에 목적을 두고 있다.

그러나 기존 키 관리 방식들은 유선 네트워크 또는 정적인 노드들이 리소스 접근에 최적화 되어 있기 때문에 무선 네트워크망과 같이 동적인 노드들을 사용하는 시스템에는 최적화되어 있지 않아 무선 네트워크를 이용하는 헬스케어 정보 시스템들은 데이터 접근 권한을 가진 그룹들의 통신이 가능한 그룹키를 관리하여야 하나 무선 네트워크 상의 노드들은 그룹변경, 탈퇴가 빈번히 발생하기 때문에 그룹 키 관리가 어렵다는 문제점을 가지고 있다.

또한 그룹 컨트롤러에서는 그룹에서 접근 맴버를 추가하거나 삭제할 경우에 매번 그룹 키를 변경해야하는 문제점을 가지고 있다[3].

따라서 본 논문에서는 상호 운용이 필요한 융합형 u-헬스케어 시스템을 이용하는 각 시스템들 간의 동적 액세스 제어 및 안정적인 헬스 정보 교환을 위한 키 트리 기반의 관리 체계를 설계하였다.

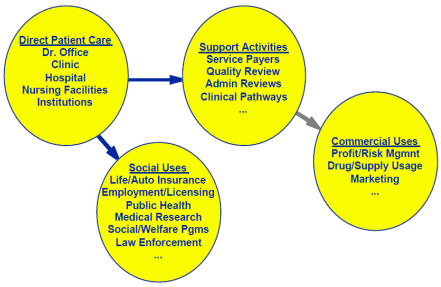
2. 관련 연구

기존 의료서비스 시스템들에서 이용하는 헬스 정보가 디지털화되면서 헬스 정보 교환 및 공유를 위한 네트워크 환경내 환자 정보 자원 공유 접속이 증가하게 되었다. 특히 u-헬스케어 시스템이 도입되면서 디지털화된 전자 헬스 정보에 대한 보안 위협이 대두되기 시작하였다[5].

Bohn[6] 은 u-헬스케어의 의료 서비스 환경을 구축하는 유비쿼터스 컴퓨팅에서 정보 보호를 위한 신뢰성 구축시 발생하는 문제에 관하여 연구를 수행하였다. 또한 Weis[7]등은 유비쿼터스 컴퓨팅의 신뢰성 문제를 해결하기 위하여 해쉬 기반 접속 컨트롤, 무작위 접속 컨트롤을 통한 개인 정보 보호 솔루션을 제안하였다.

u-헬스케어는 실시간으로 노드별로 데이터를 수집하고 수집된 데이터 리소스들을 노드 또는 시스템별로 공유하여야 하기 때문에 u-헬스케어에서 자원을 보호하기 위한 키 관리는 단순 정보보호이외에도 헬스정보 자원의 협력관계까지 고려해야 한다.

그러나 이와 같은 연구들은 단순히 u-헬스케어 시스템에서 개인 정보 보호에 목적을 둔 단순 보호 솔루션이기 때문에 각 노드, 시스템간의 정보 자원의 공유에 대한 QoS(Quality of Service)를 고려하지 않았으며 정적 노드들간의 헬스 정보 교환에 대해서만 키관리 체계를 설계하였기에 헬스정보 보호를 위한 키 관리 협력체계 구축이 어렵다.



[Fig. 1] Flow of Health Care Information in US System

[Fig. 2] Silent Tree Walking[7]

역할 기반 위임 프레임 워크는 네트워크상의 u-헬스케어 어플리케이션을 보호하고 의료 정보의 공유와 무분별한 데이터 전송을 차단하기 위한 보안 스키마이다[8].

보안 통신에서 데이터 기밀성을 보장하는 것은 일반적으로 수신자와 송신자 모두 대칭키를 사용하는 것이다.

키들은 키 관리 매커니즘을 통해 데이터 흐름을 관리하여 적절한 멤버들에 데이터에 접근하게 한다[4,9].

Razzi 등[11,12]은 웨어러블 어플리케이션의 WBAN (Wireless body area network)을 형성하기 위하여 효율적인 키 관리를 위한 새로운 아키텍처를 제안하였다.

그러나 위 개념은 일반적인 정적인 액세스 환경에서의 유비쿼터스 컴퓨팅 개념에 의해 설계되었기 때문에 상호운용이 필요한 융합형 u-헬스케어 시스템의 인증, 기밀성, 무결성 및 부인 방지에 대한 보안 문제를 해결할 수 없는 문제점을 가지고 있다.

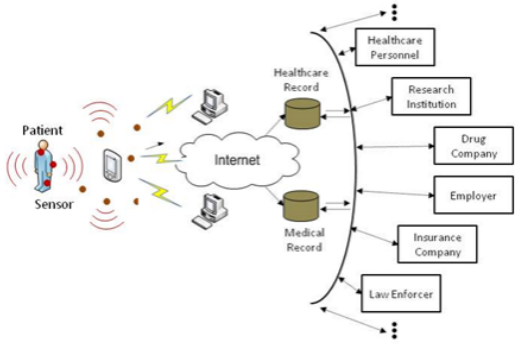
3. 헬스 정보 교환

u-헬스케어 시스템에서 네트워크 컴퓨팅은 환자 의료 기록의 접근과 레코딩 기능을 수행한다. 그러나 무선 단말기와 센서들의 발전으로 유선 기반의 u-헬스케어 시스템이 무선 네트워크를 기반으로 한 u-헬스케어 시스템 구조로 변화하면서 환자들이 자유로운 이동이 가능해지게 되어 모든 지역에서 환자의 의료 정보를 축적할 수 있게 되었다.

각 사용자에게 다양한 의료 정보를 제공하기 위해서 u-헬스케어 서비스는 서로 다른분야의 의료기관끼리 사용자의 헬스정보를 교환하고 협력해야한다.

헬스케어 서비스는 원격 워크스테이션과 복합 네트워크를 경유하여 하나 이상의 의료조직이 접속할 수 있도록 지원하며, 이는 국가 정보 인프라 중에 하나이다.

u-헬스케어 시스템의 사용자는 [Fig. 3]과 같이 헬스정보를 텍스트, 오디오, 비디오 메일과 같은 형태로 전달하는 수신자와 송신자로써 지정되어 있다[13].



[Fig. 3] Health Information Exchange

시스템에서 사용되는 부착형 생체 바이오 센서들은 가속도 센서와 같은 상황인식 센서들과 결합되어 사용되며 RF 송수신기 또한 센서 노드과 함께 환자의 활동과 위치를 추적한다.

4. 의사 결정 지원 시나리오

네트워크 환경에서 키 관리는 중요 이슈중 하나이다. 그룹 통신에서 데이터의 기밀성을 보장하기 위하여 송신자와 수신자 모두 대칭키를 소유하고 이를 통해 암호화 작업을 수행해야 한다.

서로 다른 데이터를 암호화 하는데 사용되는 키는 u-헬스케어에서 환경에서 자원을 사용할 수 있는 정당한 사용자가 데이터 액세스 및 교환을 할 수 있도록 한다.

키 생성 및 업데이트는 그룹 통신에서 키 관리에서 가장 중요하다. 키 생성 과정은 키 파라미터 생성과 보간 다항식 생성 두 단계의 과정을 거친다[14,15].

A. 키 파라미터 생성

① URG_i를 위한 무작위 수 $rand$을 생성

② $KM_i = E_s(rand)$을 통해 KM_i을 계산, s는 비밀 키, E는 안전한 대칭키 암호화 알고리즘

③ URG_i에 KM_i을 적용

B. 보간 다항식 생성

① 뉴튼의 보간 함수 $H_i(x)$를 통해 모든 URG_i 를 도출하고 URG_i를 통한 x,y에 대한 계산은 $x = (h(URG_i) \rightarrow KM_i)$와 $y = KM_i$,. 여기서 h는 일방향 암호화 함수

② URG_i에 시크릿 파라미터 KM_i과 H_i를 할당

키가 생성되면 키 생성에 대한 알림 메시지가 전송된다. 키 생성 알림 메시지가 수신되면 <Table 1>과 같이 사용자의 리소스 그룹 구성원들을 키 테이블에 추가한다. 키 생성 체계는 리소스 그룹에 구성원이 추가되거나 그룹을 탈퇴할 때 보안 상황을 고려하여 동시에 직간접적으로 결합한다.

〈Table 1〉 Evaluation results

Group	Key
2	KM2
3	KM3
5	KM5
6	KM6

이때 데이터의 기밀성을 보장하기 위해 송신자와 수신자가 그룹에 참여하거나 탈퇴할 때 키 갱신이 필요하다. 이와 같은 경우 새로운 구성원들은 키 갱신과정동안 다른 그룹 구성원들과 결합하기 전에 헬스 정보에 접근하는 것을 허용하지 않는다.

구성원 추가 및 탈퇴로 인한 키 갱신이 발생할 경우 후방 비밀의 요구 사항을 준수하여 새로운 그룹 구성원은 키 갱신이 완료되기 까지 헬스 정보 자원을 사용할 수 없다.

키 갱신 과정은 새로운 키가 생성되면 구성원 변경 전 가지 사용되던 현재 키를 통해 새로운 키를 암호화하여 기존 구성원들에게 전송한다, 그리고 개인키를 사용하여 새 그룹 구성원에게 별도의 사본을 전송하도록 구성된다.

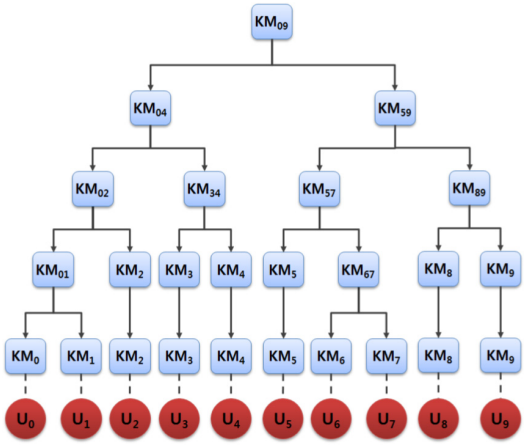
키 갱신을 위해서 헬스 정보 자원을 가지고 있는 최하위 노드(사용자)들을 그룹화하고 그룹회된 노드 세트들을 하나 노드 세트가 되도록 반복적으로 그룹화 한다. 그룹화된 노드 세트들 별로 각각 다른 키를 할당하는 분배 기술을 수행한 후 새로운 키를 배포하기 위한 키를 생성한다. 위 기술은 기존 기술보다 효율적으로 키 갱신이 가능하며 키 트리는 이를 위하여 사용된다.

키 관리에서 보안 요구사항을 충족하기 위해 본 논문에서 제안하는 새로운 키 관리 방식은 중앙 집중형 방식에서 사용되는 키 트리를 이용한다. 이 기술은 트리 구조의 하위 노드에서 모든 그룹 구성들을 포함하고 있는 중앙 집중형 키 트리를 구성한다. 키 트리는 노드에 의해 나타나며 비순환방식의 선형 그래프로써 키 들은 하위 노드를 나타내며 그룹화된 노드 세트의 키는 각 노드들의 개인키이다. 사용자는 상위에서 사용자의 개인키까지의 경로에 있는 모든 키들을 가지고 있다.

키 트리에 있는 노드들은 최상위부터 중간 노드의 모든 노드들의 키를 유지하고 있다. 중간 키들은 키 트리에서 헬스정보의 액세스에 대하여 관리하는데 사용된다. [Fig. 1]에 도시된 바와 같이. $u2$, $u3$, $u5$ 그리고 $u6$는 같은 그룹에 해당한다.

본 논문에서 제안하는 방식은 각 구성원 별로 자신이 액세스 할 수 있는 모든 헬스 정보에 대한 키를 보유한다.

사용자간의 헬스 정보를 교환은 텍스트, 음성, 비디오, 오디오, 메일 등의 형태로 이루어지며 본 논문의 모델에서는 식 (1)과 같이 각 사용자들 간에 헬스 정보 자원에 접근하기 위한 행렬을 사용하며 행렬의 결과 값이 1이면 사용자가 헬스 정보 자원에 접근하며, 결과값이 0이면 헬스 정보 자원을 가지고 있는 노드 세트 그룹에 접속할 수 없다.



[Fig. 4] Health Information Exchange

식 (1)에서 나타난 것처럼 사용자들은 그룹으로부터 해당 헬스 정보 자원에 대한 접근 권한을 가지게 된다.

사용자들은 사용자의 노드 세트 그룹으로부터 동일한 노드 세트의 하위 그룹에 대한 접근 권한을 가지게 된다.

$$URG = \begin{pmatrix} 0 & r1 & r2 & r3 & r4 \\ u1 & 0 & 0 & 0 & 0 \\ u2 & 1 & 0 & 0 & 1 \\ u3 & 1 & 0 & 0 & 0 \\ u4 & 0 & 0 & 0 & 1 \\ u5 & 1 & 1 & 0 & 0 \\ u6 & 1 & 0 & 1 & 1 \end{pmatrix} \quad (1)$$

5. 결론

유비쿼터스 컴퓨팅 환경은 개인, 가정, 의료 기관에 제공하는 기존의 의료서비스와 융합하여 보다 나은 의료서비스를 제공한다. u-헬스케어는 센서노드, RF 통신과 같은 다양한 유비쿼터스 컴퓨팅기술을 통해 사용자에게 큰 편의를 제공하나 이를 위한 헬스 정보, 개인 정보가 디지털화되어 있기 때문에 정보 보안에 대한 위험을 가지고 있다.

본 논문에서는 유비쿼터스 환경에서 의료 정보 교환을 위한 키 트리 기법을 융합한 진보된 키 관리 방식을 제안하였다. 제안한 키 관리 방식은 그룹 통신과 정보 시스템에서 데이터 전송과 인증에 대한 문제를 해결하였으며 기존 방식보다 통신, 연산, 저장에 관한 적은 성능을 필요하면서 보안을 보장한다. 본 논문에서 제안하는 키 관리 기법은 종단 노드간의 인증 및 기밀성만을 고려하였기 때문에 향후 보다 효율적인 u-헬스케어 적용을 위하여 무선 디바이스의 전원 연산 및 네트워크 주파수 대역폭을 감소에 대한 연구가 필요하다.

ACKNOWLEDGMENTS

본 논문은 2013년도 아산재단의 중진 • 공동연구 지원사업의 지원을 받아 작성되었습니다.

REFERENCES

[1] A. Berler, S. Pavlopoulos, D. Koutsouris, “Design of an interoperability framework in a regional healthcare system”, In:Proceedings of Engineering in Medicine and Biology Society, Vol. 2, pp. 3093-3096, 2004.

[2] R. Heeks, “Health information systems: Failure, success and improvisation”, International journal of medical informatics Vol. 75, No. 2, pp. 125-137, 2006.

[3] S.K. Katsikas, “Health care management and information systems security:awareness, training or education”, In:Int. J.Med. Informatics 60, pp. 129-135, 2000.

[4] S. Rafaeli, D. Hutchison, “A survey of key management for secure group communication”, In:ACM Computing Surveys 35, Vol. 3, pp. 309-329, 2003.

[5] T. Rindfleisch, “Privacy, information technology, and health care”, In:Communications of the ACM, Vol. 40, No. 8, pp. 92-100, 1997.

[6] J. Bohn, F. Gartner, H. Vogt, Dependability Issues of Pervasive Computing in a Healthcare Environment”, In:Security in Pervasive Computing, Lecture Notes in Computer Science, Vol.2802, pp.53-70, 2004.

[7] S. Weis, S. Sarma, R. Rivest, D. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, In:Security in Pervasive Computing, Lecture Notes in Computer Science, Vol. 2802, pp. 201-212, 2004.

[8] Y.B. Kim, M. Kim, Y.J. Lee, “COSMOS: a middleware platform for sensor networks and a u-healthcare service”, Proceedings of the 2008 ACM symposium on Applied computing. pp. 512-513, 2008.

[9] L. Zhang, B. Chu, “A Role-Based Delegation Framework for Healthcare Information Systems”, In:ACM Symposium on Access Control Models And Technologies(SACMAT), pp. 125-134, 2002.

[10] C. Wong, M. Gouda, S. Lam, “Secure group communications using key graphs, Networking”, IEEE/ACM Transactions on Networking, Vol. 8,

No. 1, pp. 16-30, 1998.

[11] S. Muhammad, K. Raazi, S. Lee, Y. Lee, “A Novel Architecture for Efficient Key Management in Humanware Applications”, In: Fifth International Joint Conference on INC, IMS and IDC, pp. 1918-1922, 2009.

[12] S. Muhammad, K. Raazi, S. Lee, Y. Lee, “TIMAR: an efficient key management scheme for ubiquitous health care environments”, In:Proceedings of the 5th International ICST Mobile Multimedia Communications Conference, London, United Kingdom, p. 33, 2009.

[13] J.S. Shapiro, G. Kuperman, Health information exchange.″ Medical informatics: An executive primer, (Ed. Ong, KR) Healthcare Information & Management Systems Society, pp. 147-16, 2011.

[14] M. Das, A. Saxena, V. Gulati, D. Phatak, “Hierarchical key management scheme using polynomial interpolation”, SIGOPS Operational Systematic Review, Vol. 39, No. 1, pp. 40-47, 2005.

[15] D. Dolev, A.C. Yao, On the security of public key protocols.″ Information Theory, IEEE Transactions on, Vol. 29, No. 2, pp. 198-208, 1983.

저자소개

김 동 현(Donghyun Kim) [정회원]

- 2012년 2월 : 한남대학교 멀티미디어공학전공(공학사)
- 2014년 2월 : 한남대학교 멀티미디어학과 (공학석사)
- 2003년 3월 ~ 현재 : 한남대학교 멀티미디어학과 박사과정

<관심분야> : 이미지 프로세싱, 증강현실, 정보보안

김 석 수(Seoksoo Kim) [정회원]

- 1989년 2월 : 경남대학교 컴퓨터 공학(공학사)
- 1991년 2월 : 성균관대학교 정보 공학(공학석사)
- 2002년 2월 : 성균관대학교 정보 공학(공학박사)
- 2003년 3월 ~ 현재 : 한남대학교 미디어영상전공 교수

<관심분야> : 멀티미디어 통신 시스템, 유헬스케어, 정보 보안, 컴퓨터 네트워크,