Journal of The Korea Knowledge Information Technology Society

ISSN 1975-7700

http://www.kkits.or.kr

A Cloud-Based Security Model Designed to Prepare Deployment Nationwide The Regional Public Hospitals Telemedicine Clusters

Chang-Ho An[1], Hyun-Chul Baek[2], Jae-Heung Park[1], Sang-Bok Kim[*1]

[1]*Department of Computer Science, Gyeongsang National University*
[2]*Department of Smart Convergence Information, Gyeongnam Provincial Namhae College*

ABSTRACT

Today, the government health policies and plans to introduce telemedicine system for the care of the Environment based on the upcoming ubiquitous. Remote medical system, from the standpoint of the patient utilizing the medical institution, means away from constraints of time and space. However, these policies have sparked strong opposition from private institutions, such as when subjected to pharmacists. In particular, the cause of repulsion for each individual security policies, lack of medical information has become an important factor in the rebound. and there is a limit to convince its medical institutions. This paper is a multifaceted network configuration for future cloud-based medical facilities for individual survival in relation to telemedicine enforcement. In addition, this individual will be clustered environment, telemedicine among national institutions are organized by the Gyeonggi Province Hospital Medical Center area as the model was constructed virtually. However, since the concentration of the individual critical information are clustered attack for unauthorized collection of personal information can also be increased dramatically. Therefore, this paper, in preparation for the ubiquitous care environment will emerge in our society in the future, illegal information gathering attack occurs configure a remote medical cluster system sharing a mutual infringement of the information and the encryption scheme service availability and proactively using which it was designed for defense cooperation model.

KEYWORDS: Big data, Big data securities, Cloud Computing, Encryptions, Tracebacks, Telemedicine

ARTICLE INFO: Received 22 March 2016, Revised 11 April 2016, Accepted 11 April 2016.

[*]Corresponding author is with the Department of Computer Science, Gyeongsang National University, 501, Jinju-*Gajwa-Dong*, Jinju-si, Gyeongsangnam-do, 52828, KOREA. *E-mail address*: sbkim@gnu.ac.kr

1. 서 론

오늘날 급속하게 발전하고 있는 네트워크 기술은 우리 사회에 많은 변화를 이끌어 내고 있다. 그 중 정부에서 시행하려는 원격진료정책은 향후 유비쿼터스 진료환경에 대비한 기초정책이라고 할 수 있다.

네트워크 환경은 초기의 단순한 정보의 송/수신 서비스에서 시작하여 현재 클라우드 컴퓨팅 환경으로 발전하고 있다. 빅데이터 서비스란 방대한 양의 서비스 처리 환경이 일반적으로 클라우드 컴퓨팅 환경을 기반으로 이루어지는 것을 의미한다[1][2]. 이러한 클라우드 컴퓨팅 환경은 현재 정부에서 추진하고자 하는 원격진료 서비스 정책에 반드시 필요한 기반 기술이라고 할 수 있다. 즉 원격진료가 시행되면 의료기관을 찾는 환자들이 시간과 공간의 제약에서 벗어나 언제든지 자신의 현재 위치에서 필요한 기본적인 진료를 받을 수 있기 때문이다. 아울러 원격진료 신청 과정에서 환자들이 동네의 의원급이나 지역의 일반 종합병원보다 규모나 질적인 면에서 앞서는 대학병원급 이상의 진료 기관을 선호하여 원격진료를 선택할 가능성이 아주 높아지는 결과도 수반할 수 있다. 그러므로 의원급 의료기관이나 일반 종합병원들은 이러한 경쟁 구도에서 생존하기 위한 전략으로 일반 종합병원과 의원급 의료기관들이 연합하여 원격진료 의료 클러스터를 형성할 가능성이 높아지는 것이다. 이렇게 형성되는 원격진료를 위한 의료 클러스터는 환자들의 진료정보 공유를 통하여 빠르고 정확한 진단을 할 수 있는 클라우드 컴퓨팅 환경 구축이 반드시 필요한 것이다. 즉 원격진료 의료 클러스터를 구성하는 의료기관들은 다음과 같은 기본적인 의료 정보들을 공유할 수 있을 것이다. 먼저 동일 환자에 대한 각 의료기관의 진료 정보를 공유할 수 있다. 다음은 동일 질병의 검사 결과에 대한 다양한 정보를 공유할 수 있다. 이렇게 클라우드 컴퓨팅 환경을 통하여 수집되는 환자들의 진료 정보는 대규모 의료기관들이 가지고 있는 진료의 다양성과 정확도를 가질 수 있으며, 또한 짧은 진료대기로 대규모 의료기관의 문제점인 환자 대기 시간에 대한 개선 효과를 가지고 올 수 있다. 그러므로 소규모 의료기관들을 위한 클라우드 컴퓨팅 환경 구축은 향후 시행하게 될 원격진료 환경에 대비하여 반드시 필요하다고 할 것이다. 그렇지만 이렇게 구축되는 원격진료를 위한 원격진료 클러스터는 환자들의 소중한 개인 정보나 진료 정보를 다량으로 보유하고 있기 때문에 경쟁 의료 기관 또는 악의적인 목적을 가진 공격자들의 집중적인 공격 대상이 될 수 있다.

본 논문에서는 원격진료를 위하여 상호 협력하에 구축한 원격진료 클러스터의 불법적인 진료정보 유출에 대비하여 경기도에서 운영하고 있는 지방의료원을 선정하여 다음과 같은 보안 모델을 제안하였다. 먼저 IP Spoofing를 이용한 공격자들의 불법적인 원격진료 클러스터 접근에 대비하여 트레이스 백 정보를 이용하여 초기 접근 관련 인증 정보로 사용하였다. 그 다음 정상 사용자의 로그인 정보를 단순한 아이디와 패스워드만 이용하지 않고 원격 진료를 담당하고 있는 의사들의 ID, 진료 처방 정보, 상병 정보 중 일부를 추가 인증 정보로 활용하여 강화된 인증 방식을 채택하였다.

본 논문의 구성은 다음과 같다. 2장에서 클라우드 컴퓨팅 환경과 빅데이터의 개념에 대해 알아보고, 이러한 환경의 공격에 많이 이용되는 IP Spoofing 공격과 이에 대응하기 위하여 본 논문에서 사용하고 있는 트레이스 백 정보에 대하여 알아본다. 3장에서는 클라우드 컴퓨팅 환경에서의 보안 모델을 제안하고 그 동작 과정을 설명하였다. 4장에서는 이에 대한 시뮬레이션과 제안 모델의 보안 레벨에 대한 단계별 보안 정책을 수행하였다. 그리고 결론에서 향후 본 논문의 응용 가능성에 대한 언급을 하였다.

2. 관련연구

2.1 원격진료

원격진료란 일반적으로 '상호작용하는 정보통신 기술을 이용하여 원거리에서 의료정보와 의료서비스를 전달하는 모든 활동'으로 정의할 수 있다. 즉 환자 및 진료정보가 먼 거리에 떨어져 있거나 시간적인 여러 가지 문제로 인해 직접 방문 진료가 어려운 경우 의료정보 및 전문적 조언을 원격으로 제공하는 시스템을 뜻한다. 이는 환자 진료뿐만 아니라 의료행정, 의학교육, 자문과 의뢰 등을 포함하는 포괄적인 개념으로 사용되고 있다. 그러므로 원격진료의 포괄적인 의미는 컴퓨터와 데이터 통신 기술을 이용하여 의학영상, 동영상, 환자기록 등 각종 데이터를 주고받고 의료서비스를 전달하는 기술을 통칭한다고 할 수 있다. 현재 국내에서는 충청북도 충주의료원을 효시로 일부 의료원에서 인근 보건진료소와 초보적인 원격진료를 시행하고 있다[3][4][5].

2.2 클라우드 컴퓨팅의 개념

클라우드 컴퓨팅에 대한 정의는 연구기관이나 학자들이 해석하는 관점에 따라 그 차이가 있다. 그렇지만 그 중 공통된 견해를 찾아보면 '네트워크 환경에서 이용자의 요구에 따라 실시간으로 소프트웨어, 플랫폼, 인프라 등 IT 자원이 필요한 만큼 공급받고, 그에 따른 비용을 지불하는 서비스' 라는 공통된 견해가 있다. 본 논문에서는 향후 원격진료 시행에 대비하여 소규모 의료기관들과 일반 종합 병원간의 의료 클러스터 구축을 위하여 일부이지만 정보 공유가 가능한 지방의료원 환경을 가상화시킨 클라우드 컴퓨팅 환경을 이용하였다.

2.3 빅 데이터의 개념

빅 데이터에 대한 일반적인 정의는 기존의 분석 도구나 시스템 체계의 처리 범위를 넘어선 방대한 양의 데이터 환경을 빅 데이터로 일컫는다. 아울러 또 다른 시각의 빅 데이터 개념으로는 다양한 종류의 대규모 데이터로부터 저렴한 비용으로 가치 추출이 가능하고, 필요 데이터에 대한 빠른 수집과 발굴 및 분석을 할 수 있는 차세대 기술 또는 아키텍처를 의미하기도 한다[6][7][8].

본 논문에서는 이상과 같이 원격진료 클러스터를 구성하는 의료기관들의 정보를 빅 데이터화 하여 정부의 질병관리에도 이용할 수 있는 환경을 구축하였다. 그렇지만 이러한 정보 운영은 클라우드 컴퓨팅 기반의 환경 특성상, 고도의 해킹 기술을 가진 공격자들이 주로 사용하는 IP Spoofing 공격에 대하여 그 취약점을 노출할 수 있다.

2.4 IP Spoofing 공격

IP Spoofing이란 자신의 IP를 속여 불법적인 접근을 시도하는 것을 의미한다. IP Spoofing 공격은 TCP/IP의 구조상의 문제점을 이용한 공격 방법으로 패킷이 가지고 있는 시퀀스 번호, 출발지 경로 정보, 출발지 IP 주소 등을 이용하여 <그림 1>과 같이 타겟 서버가 공격자 시스템을 신뢰하도록 하는 공격 기법이다. IP Spoofing 공격 과정은 먼저 공격자가 타겟 서버에 접속하기 위해 타겟 서버와 신뢰 관계를 가지고 있는 임의의 신뢰 호스트 정보를 획득한 후 최종 접속을 시도하기 전에 해당 신뢰호스트로 DoS나 DDoS 공격을 가하여 신뢰 호스트를 다운시킨다. 그 다음 타겟 서버와 해당 신뢰 호스간의 네트워크 연결이 해제되면, 공격자가 해당 신뢰 호스트의 IP 주소를 자신에게 재설정하고 타겟 서버로 접속한 후 정보를 빼내가는 것이다.

이렇듯 상호 IP 주소만으로 신뢰 관계를 이용하여 공격을 시도하기 때문에 원격진료 클러스터를 형성하고 있는 환경에서는 접속에 대한 엄격한 인증 과정이 더욱 요구된다고 할 수 있다[9][10].

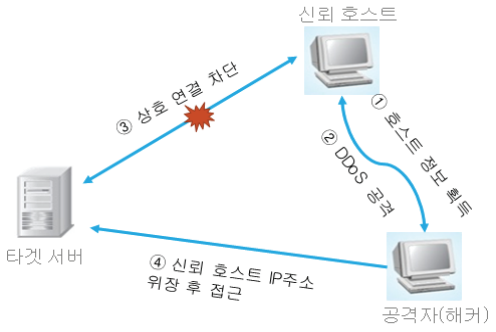

그림 1. IP Spoofing 공격의 예
Figure 1. Example of IP Spoofing Attack

2.5 트레이스 백 정보의 개념

송신자와 수신자의 일반적인 송/수신 과정은 여러 개의 경로를 거쳐 최종 목적지까지 연결되는 과정을 가진다. 트레이스 백이란 이러한 네트워크 과정에 경로를 분석할 수 있도록 사용하는 프로그램이다. 즉, 특정 송신자의 정보가 최종 수신자까지 도달하기 위해서는 여러 개의 라우터를 경유하게 되는데 이때 경유하는 각 구간의 정보를 분석할 수 있는 것이다. 본 논문에서는 트레이스 백 정보를 이용하여 원격진료 클러스터에 참여하고 있는 의료기관들의 트레이스 백 정보를 미리 구축한 후 원격진료 클러스터 사용자들의 초기 인증 과정 정보로 이용하고 있다[11].

3. 제안 모델 설계

3.1 제안 모델

본 논문에서 제안하는 원격진료 클러스터에 대한 구조는 네트워크를 이용한 다양한공격에 단일 보안시스템의 수동적인 대응 보다 클러스터를 구성하고 있는 시스템들의 실시간 공격 정보 공유와 이를 통하여 능동적인 대응을 할 수 있도록 <그림 2>와 같이 구성하였다. 아울러 클러스터 내 의료기관 상호 진료 정보 참조 관리와 공격정보 공유를 위하여 클러스터 본부에서 이들 자료를 관리하도록 하였다.

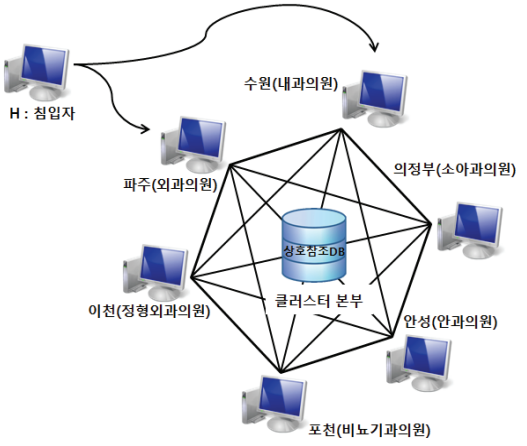

그림 2. 원격진료 클러스터 구성도
Figure 2. block diagram for telemedicine cluster

<그림 2>에서 수원의료원 또는 개인의원 각각은 원격진료 클러스터를 구성하는 의료기관들로서 가상적인 클라우드 컴퓨팅 환경으로 구축되어 있음을 보여주는 것이다. <그림 2>의 원격진료 클러스터를 구성하는 의료기관들은 상호 정보 공유가 가능하다. H는 IP Spoofing을 이용하여 원격진료 클러스터를 불법적으로 접근하는 공격자로 가정하였다. <그림 2>에서 원격진료 클러스터를 구성하는 시스템들은 자신을 제외한 다른 원격진료 클러스터 시스템의 상호 트레이스 백 정보와 <표 1>과 <표 2>를 통하여 각 시스템들의 정보를 공유하여 인증 정보로 사용할 수 있도록 한다[12][13].

표 1. 접근자(의료진) 별 인증을 위한 정보 목록
Table 1. information list for accessor(doctor) to authentication

클러스터 소속코드	의료진 코드	본인인증 Key(암호화)	
		특정진료코드	상병코드
A_01	A01_im_1	특정약품코드	S05
	A01_im_2	특정검사코드	A11
	A01_im_3	특정처치코드	D10
B_01	B01_ur_1	특정약품코드	L50
	B01_ur_2	특정검사코드	G32
	B01_ur_3	특정처치코드	H03
C_01	C01_pd_1	특정약품코드	B60
	C01_pd_2	특정검사코드	F21
	C01_pd_3	특정처치코드	I33
·	·	·	·
·	·	·	·
N_n	N01_Im_n	특정코드_n	Mn

표 2. 접근자(환자) 클러스터 내 진료 정보 제공 목록
Table 2. Information list for accessor(patient) to authentication

병록번호	클러스터 소속코드	의료진 코드	본인인증 OTP_n
A01_1	A_01	A01_im_1	A01_1_n
A01_2	A_01	A01_gs_1	A01_2_n
A01_3	A_01	A01_os_1	A01_3_n
B01_1	B_01	B01_im_2	B01_1_n
B01_2	B_01	B01_ds_1	B01_2_n
B01_3	B_01	B01_ur_1	B01_3_n
C01_1	C_01	C01_im_1	C01_1_n
C01_2	C_01	C01_pd_1	C01_2_n
C01_3	C_01	C01_og_1	C01_3_n
·	·	·	·
·	·	·	·
N01_m	N_n	N01_m_n	N01_m_n

본 논문에서는 <표 1>, <표 2>의 정보를 이용하여 IP Spoofing 공격이 발생하게 되면 적절한 인증 과정을 거치도록 한다.

표 3. 환자별 클러스터 내 진료 정보 제공 목록
Table 3. medicine information list for service in the cluster

병록번호	환자정보		
	개인 기본정보	기본 진료정보	진료 정보
A01_1	A01_1_P	A01_1_B	A01_1_C
A01_2	A01_2_P	A01_2_B	A01_2_C
A01_3	A01_3_P	A01_3_B	A01_3_C
B01_1	B01_1_P	B01_1_B	B01_1_C
B01_2	B01_2_P	B01_2_B	B01_2_C
B01_3	B01_3_P	B01_3_B	B01_3_C
C01_1	C01_1_P	C01_1_B	C01_1_C
C01_2	C01_2_P	C01_2_B	C01_2_C
C01_3	C01_3_P	C01_3_B	C01_3_C
·	·	·	·
·	·	·	·
N01_m	N01_m_P	N01_m_B	N01_m_C

먼저 접근자가 의료진의 접근 요청인지 일반 환자의 접근 요청인지를 구분하고 접근 여부와 정보 제공 수준을 결정한다. 환자의 진료 정보에 대한 서비스 요청은 <표 3>을 이용하여 다음 두 가지 경우를 고려하였다. 여기에는 의료진이 진료를 하기 위하여 내원한 환자의 진료 정보를 원격진료 클러스터에 참여하고 있는 타 의료기관으로 참조할 경우와 환자 본인의 필요에 의해 자신이 직접 진료 정보를 참조하는 경우이다. 첫 번째 의료진이 진료를 위하여 정보 참조를 요청하면 환자의 개인 정보, 진료 정보가 모두 제공되어야 할 것이다. 두 번째 환자가 직접 자신의 진료 정보를 참조하는 경우에는 자신의 개인 정보와 기본 진료정보만 참조할 수 있도록 한다.

3.2 제안 모델 동작과정

본 논문의 원격진료 클러스터를 위한 제안 모델의 사용자 접근 처리 과정은 <그림 3>과 같다. 클

라우드 컴퓨팅 기반의 정보 서비스 환경은 그 특성상 IP Spoofing 공격이 발생할 가능성이 높다. 그러므로 사용자 접근이 발생하면 엄격한 인증 과정을 거치도록 하는데, 먼저 원격진료를 신청하는 환자의 경우 그 처리과정은 다음과 같다.

1. 초기 사용자 정보를 이용한 접근 요청이 발생하면 보유하고 있는 정상 사용자들의 접근 정보와 트레이스 백 정보를 이용하여 1차 인증 과정을 수행한다. 이 과정에서 트레이스 백 정보 비교는 먼저 경로상의 전체 홉의 개수를 비교한 후 각 홉 별로 IP를 비교하였다.

2. 이때 트레이스 백 정보가 일치하지 않으면 해당 접근에 대하여 OTP를 발생시켜 재 인증 과정을 정상적으로 수행한 사용자 접근만 접근을 허용한다.

3. OTP 인증 과정을 정상적으로 수행하면 해당 경로 정보를 정상적인 트레이스 백 정보로 신규 등록하고, 그렇지 않은 경우는 차단과 동시에 공격자의 트레이스 백 정보로 등록한다.

4. 원격진료 환자의 정상적인 접근으로 판정되면 초기 접근 정보로 추정 가능한 의료진 또는 일반 환자에 대한 판별 작업을 수행한다.

5. 진료를 위한 일반 환자의 접근이면 기존 원격진료 클러스터에 존재하는 환자인지, 처음으로 접속한 신규 환자인지 분석을 한다.

6. 신규 환자이면 진료 대기 큐에 저장하고, 신규 환자가 아니고 원격진료 클러스터로 추가 진료 정보를 제공받아 진료를 시작한다.

7. 정상적으로 진료가 끝나면 해당 환자의 정보를 저장하고 모든 진료를 종료한다.

다음은 원격진료 클러스터내 의료진이 환자의 진료 정보를 참조할 경우 그 처리 과정이다.

1. 의료진의 자료 요청에 대한 서비스 수행 과정은 앞의 1에서 4번까지의 환자 처리과정과 동일하다.

2. 접근자 정보가 원격진료를 위한 의료진의 접근으로 판정되면 <표 3>의 환자 개인정보와 진료정보 모두를 제공한다.

3. 정상적으로 진료가 끝나면 해당 환자의 정보를 저장하고 모든 진료를 종료한다.

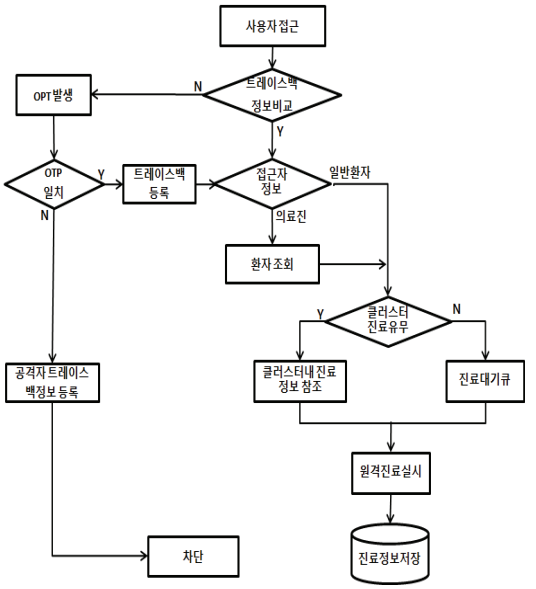

그림 3. 제안모델 동작과정
Figure 3. Operational process of proposed model

다음은 접근자 정보분석을 수행한 후 클러스터내 진료 정보에 대한 서비스 요구가 발생할 경우 그 처리 과정을 <그림 3>으로 나타낸 것이다.

1. 정보요청이 발생하면 클러스터 내에서 보안기능을 수행하는 탐지데이터베이스에 해당 접근자 정보를 등록한다. 이때 등록에 필요한 자료는 정보요청자의 ID, 해당 의료기관의 ID, 정보요청 횟수를 등록 해 둔다.

2. 정보요청자에 대하여 의료진 또는 환자 여부를 판별할 수 있는 작업 수행을 한다.

3. 정보요청자 분석이 완료되면 클러스터내 정보요청에 대한 횟수를 분석한다.

3-1-1 환자가 동일 의료기관에 대한 참조이면

원격진료 서비스를 실시한 후 그 결과를 진료정보 데이터베이스에 저장한다.

3-1-2 동일 환자가 동일 의료기관의 정보를 2회 이상 요구하는 경우는 원격진료 서비스를 바로 실행하도록 하였다. 그렇지만 의료진이 해당 환자의 정보를 2회 이상 요청할 경우에는 암호화를 수행한 후 요청 자료를 제공한다.

3-2-1 특정환자 또는 의료진이 타의료기관에 존재하는 자신이나 환자의 정보를 참조하는 경우에는 반드시 암호화 과정을 수행하도록 한다.

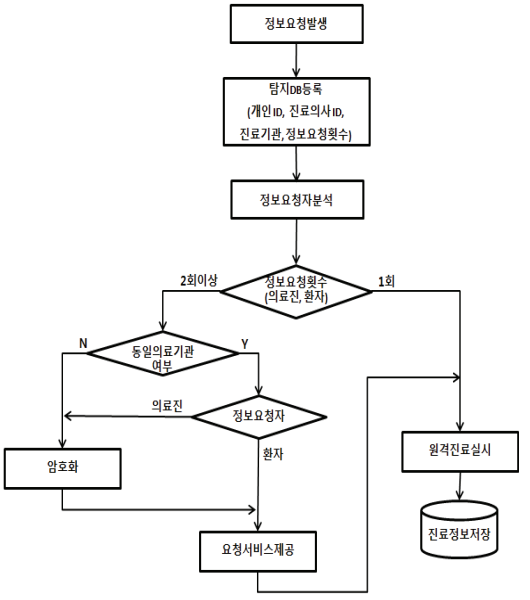

그림 4. 정보요구 발생시 처리 과정
Figure 4. Treatment process to information request

진료정보의 제공은 환자일 경우 <표 3>의 환자 개인정보와 기본 진료 정보만 제공하지만 이 경우는 두 곳 이상의 참조이므로 서비스 정보를 암호화 시켜 전송한다. 그리고 의료진의 정보요청의 판정되어도 <표 3>의 모든 진료 정보를 암호화 한 후 제공하게 된다. 이러한 제반 과정은 IP Spoofing을 이용한 공격자가 원격진료 클러스터 내의 의료기관으로 불법적인 접근을 시도할 수 있기 때문에 트레이스 백 정보, 접근자 정보, 요청 자료 정보를 조합하여 실시간 능동적으로 대응할 수 있도록 한 것이다.

본 논문의 암호화 과정은 다음과 같다. 먼저 암호화 모듈을 이용하여 첫 번째 암호화 과정을 수행하고 이를 K_E1으로 한다. 그 다음 의료진과 환자에게 제공하는 정보 중에서 특정 위치의 자료 값들을 이용하여 두 번째 암호화 과정을 수행하게 되고 이를 K_E2로 정의하여 사용한다. 본 논문에서 사용하고 있는 암호화 과정에 필요한 정보는 의료진 요청 자료에 대한 암호화와 복호화 과정에 <표 1>의 의료진 코드, 특정진료 코드, 상병코드를 동시에 만족해야만 원래의 진료 정보를 알 수 있도록 하였다. 의료진의 대부분이 진료 특성상 특정 상병에 대하여 자신만의 특정 진료코드를 가지고 있기 때문에 이는 의료진 본인만 알고 있다. 반면에 환자에게 제공하는 자료는 <표 2>에서 본인 인증 OTP 정보를 이용하여 암호화 시켜 전송하도록 하였다[14][15].

4. 실험 및 평가

4.1 시뮬레이션 환경

본 논문에서 제안하고 있는 원격진료 클러스터에 대한 불법적인 정보 수집에 대응 가능한 방어 시스템의 시뮬레이션 환경은 다음과 같다. 먼저 사용된 응용 소프트웨어는 jdk1. 8.0_45, Eclipse 4.3.2 SR2, 구현언어는 Java를 사용하였다. 시뮬레이션을 위한 운영 체제는 Windows 7 Professional K64비트이고, 시스템 사양은 8G B 메모리를 채택한 Core(TM)i5 2.67GHz Syst em으로 구성하였다.

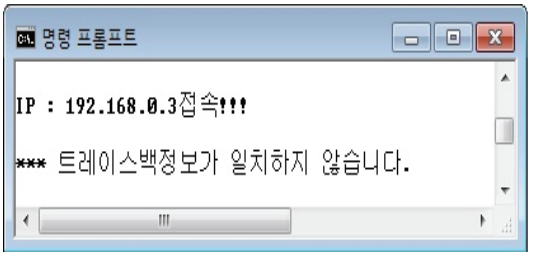

그림 5. 서버에서 트레이스 백 정보 처리과정
Figure 5. Traceback information processing in the server

<그림 5>는 사용자 접근이 발생하여 원격진료 클러스터의 각 협력시스템에 구축해 놓은 상호신뢰시스템의 트레이스 백 정보와 비교하여 일치하지 않을 경우 이를 차단하는 경우이다.

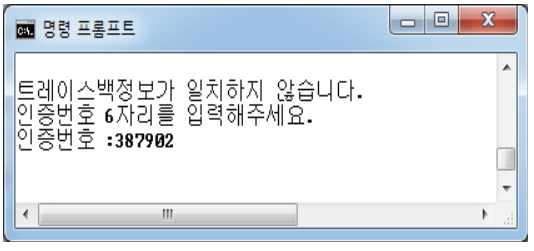

그림 6. 클라이언트에서 OTP 인증 과정
Figure 6. Authentication processing for OTP in the client

<그림 6>은 원격진료를 위하여 접속을 시도한 접근자의 트레이스 백 정보가 일치하지 않아 OTP 수행을 통하여 재인증 과정을 정상적으로 수행한 결과를 보여 주고 있다.

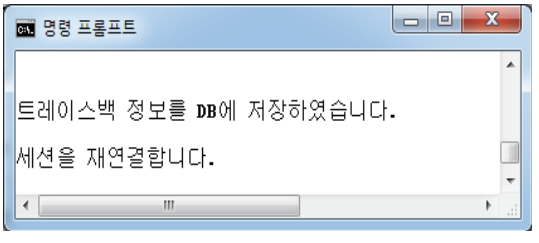

그림 7. 서버에서 OTP 인증과정이 성공한 경우
Figure 7. Successful to OTP authentication in the server

<그림 7>의 경우는 <그림 6>의 인증 과정을 정상적으로 수행한 사용자 트레이스 백 정보를 서버에 신규 트레이스백 인증 정보로 등록하는 과정을 보여 주고 있다.

그림 8. 클러스터별 환자 진료 등록 정보
Figure 8. Patient care properties in the cluster

<그림 8>은 원격진료를 위하여 클러스터 내에서 상호 제공하는 환자 진료 등록 정보를 보여 주고 있다.

그림 9. 환자가 직접 자신의 정보 참조
Figure 9. Direct reference to patient's information in the detection DB

<그림 9>는 탐지DB에 개인ID, 진료의사ID, 진료기관, 정보요청횟수를 저장하고 있는 것을 보여주고 있다.

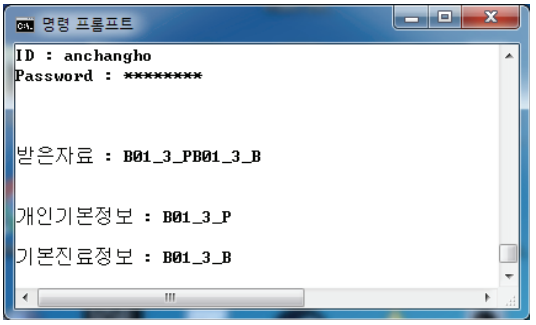

그림 10. 환자가 직접 자신의 정보 참조
Figure 10. An example of direct reference to patient's own information

<그림 10>은 환자가 직접 자신의 진료 정보를 참조할 경우 본인의 개인 기본정보와 기본 진료정보를 제공하게 된다.

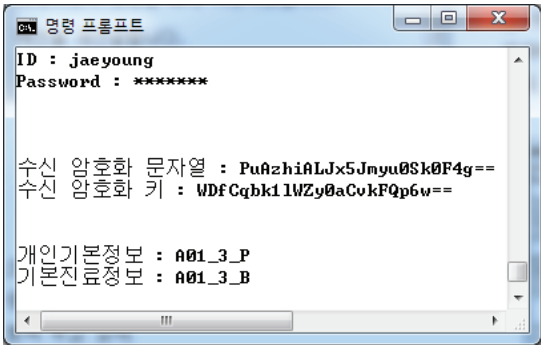

그림 11. 환자가 타 의료기관에서 정보 요청
Figure 11. patient information requested another medical facility

<그림 11>은 정보요청 횟수가 2회 이상이면서 타 의료기관에서 정보를 요청한 경우로 해당 서비스 자료에 대하여 암호화 과정을 수행한 후 서비스 하는 과정을 보인 것이다.

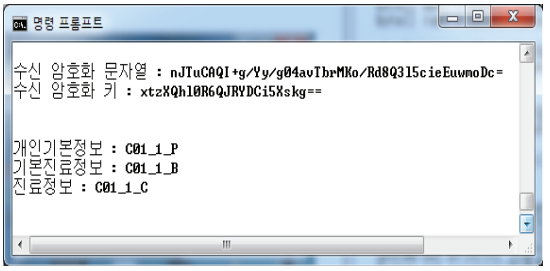

그림 12. 의료진 참조
Figure 12. request information of doctor

<그림 12>는 의료진이 진료를 위하여 클러스터 내 다른 시스템의 자료를 참조할 경우 환자의 개인기본정보, 기본진료정보, 진료정보를 암호화하여 전송한 후 해당 자료를 복호화 한 결과를 보여주고 있다.

<그림 11>의 암호화 과정은 <그림 13 >의 과정을 수행하고, <그림 12>의 복호화는 그 역과정을 수행한다.

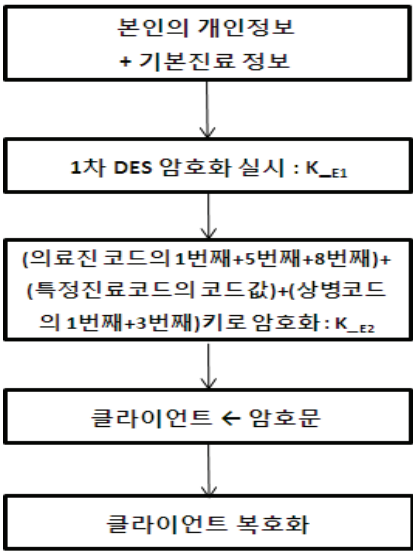

그림 13 서비스 자료 암/복호화 과정
Figure 13. data encryption/decryption process for service

5. 결 론

본 논문은 향후 우리사회에 대두하게 될 유비쿼터스 진료환경에 대비한 원격진료 시행에서 나타나게 될 문제점을 찾아보고 이를 해결하기 위하여 그 대안을 연구한 것이다. 원격진료를 시행하게 되면 소규모 의료기관들의 생존 여부는 즉각적인 문제가 될 수 있다. 이는 환자들의 특성상 시간과 공간의 제약이 사라지면 대형병원에 대한 원격진료 신청의 쏠림 현상이 한층 증가할 것이기 때문이다. 그러므로 소규모 의료기관들은 주위의 종합병원들과 원격진료를 위한 클러스터를 형성하려고 할 것이다. 그렇지만 이렇게 개인 진료정보의 집단적인 네트워크 구성은 보안에 대한 심각한 우려를 가지고 올 수 있다. 본 논문은 이러한 클라우드 환경을 기반으로 구축하게 될 원격진료 클러스터의 보안 문제를 해결하기 위하여 클러스터를 형성하는 의료기관들을 모두 보안 정책에 참여시켜 불법적인 공격에 상호협력하에 능동적이고 실시간 대응이 가능하도록 하였다. 이는 원격진료 시행시 가장 큰 문제점이라고 할 수 있는 개인의 진료정보를 안정적으로 관리하면서 원격진료 클러스터에 참여한 의료기관들의 경쟁력도 제고시킬 수 있기 때문이다. 향후 연구 과제로는 지역 거점 의료기관으로 그 역할을 하고 있는 지방의료원들을 대상으로 먼저 원격진료 클러스터를 구성하고 이를 민간 의료기관으로 확산할 수 있는 정책이 함께 필요할 것으로 본다. 그리고 이러한 의료정보에 대한 의료기관들의 공유를 통하여 어느 지역에서도 특정 환자에 대한 맞춤형 진료가 가능하도록 하여 과잉 진료 현상을 줄일 수 있도록 해야 할 것이다. 또한 환자 개개인의 진료 정보 보호 및 서비스 가용성을 위하여 터널링 기법에 대한 연구도 함께 진행되어야 할 것이다.

References

[1] O. Chen, and O-N. Deng, *Cloud computing and its key techniques,* Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China, Vol. 29, No. 9, pp. 2562-2567, 2009.

[2] J-J. Hoon, *A study on the vulnerability and corresponding technique trends of the cloud computing service*, Journal of Information Security, Vol 13, No. 6, pp. 1239-1246, Apr. 2013.

[3] C-C. Park, G-H. Park, S-H. Kim, and S-H. Koh, *The proposal of evaluation measure from hospital information system : The case study of C national university hospital in Korea*, Journal of The Korea Knowledge Information Technology Systems, Vol. 2, No. 2, pp. 69-77, 2007.

[4] J-H. Choi, *Analysis of changes in the muscle activity and fatigue of the erector spinae using IT convergent type medical equipment*, Journal of Knowledge Information Technology and Systems, Vol. 10, No. 6, pp. 665-673, 2015.

[5] S-K. Park, *A study on the regional differences of telemedicine and digital divide*, Journal of the Korean Geographical Society, Vol. 50, No. 3, pp. 325-338, 2015.

[6] J-K. Park, *A study on measures to active cultural contents service in big data age*, Vol. 20, No. 1, pp. 324-334, Mar. 2014.

[7] Q. Miao, *When intelligence meeting wity big data：Review and perceptions of big Data'S hotspot intelligence tracking,* Institute of Scientific & Technical Information of Shanghai,Shanghai 200031, No. 5, Serial No. 187, 2013.

[8] S-Y. Kim, J-I. Lim, and K-h. Lee, *A study*

on the security policy improvement using the big data, Korea University, Graduate School of Information Security, Vol. 23, No. 5, pp. 969-976, 2013, http://dx.doi.org/10.13089/JKIISC.2013.23.5.96, 2013.

[9] D. Pansa, and T. Chomsiri, *Architecture and protocols for secure LAN by using a software-level certificate and cancellation of ARP protocol*, Third 2008 International Conference on Convergence and Hybrid Information Technology, pp. 21-26, 2008.

[10] S. Bellovin, M. Leech, and T. Taylor, *ICMP Traceback message*, IETF, draft-ietfitrace-04, Feb. 2003.

[11] Y-Y. Mu, H-C. Baek, J-Y. Choi, W-C. Jeong, and S-B. Kim, *A proposal of a defense model for the abnormal data collection using trace back information in big data environments*, Journal of Knowledge Information Technology and Systems, Vol. 10, No. 2. pp. 753-162, 2015.

[12] S-Y. Park, *A study on the regional differences of telemedicine and digital divide, Journal of the Korean Geographical Society*, Vol. 50, No 3, pp. 325-338, 2015.

[13] Y. Liu, S.-B. Kim, J-H. Park, and J-M. Bae, *An encrypted response model using application access failure information for the attack of IP spoofing in a cloud computing environmen*, Journal of Knowledge Information Technology and Systems, Vol. 10, No. 6, pp. 643-651, 2015.

[14] R-W. Huang, X-L. Gui, S. Yu, and W. Zhuang, *Privacy-preserving computable encryption scheme of cloud computing*, Chinese Journal of Computers, Vol. 34, No. 12, pp. 2391-2402, 2011.

[15] J-K. Heo, *Web application authentication system using encipherment and PKI*, Journal of Information and Security, Vol. 8, No. 1, pp. 1 -7, 2008.

클라우드 기반의 전국 지방의료원 원격진료 클러스터 구축에 대비한 보안 모델 설계

안창호[1], 백현철[2], 박재홍[1], 김상복[1,]

[1]*경상대학교 컴퓨터과학과*

[2]*경남도립남해대학 스마트융합정보과*

요 약

오늘날 정부의 의료정책은 다가올 유비쿼터스 기반의 진료환경 구축을 위하여 원격진료시스템 도입을 계획하고 있다. 원격진료시스템은 의료기관을 이용하는 환자 입장에서 시간과 공간에 대한 제약으로부터 벗어나게 됨을 의미한다. 그렇지만 이러한 정책은 의약분업을 실시했을 때와 같이 개별 의료기관들의 강력한 반발을 불러일으키고 있다. 특히 반발의 원인 중 각 개인의 진료 정보에 대한 보안 대책 미비는 원격진료시스템 시행과 관련하여 각 의료기관들을 설득하는데 있어 그 문제점을 더하고 있는 실정이다. 본 논문은 향후 원격진료 시행과 관련하여 개별의료기관들이 생존을 위한 클라우드 기반의 다각적인 네트워크 구성에 대비한 것이다. 아울러 이렇게 개별 의료기관들이 구성하게 될 원격진료 클러스터 환경을 전국 지방의료원 중에서 경기도 지역 의료원을 모델로 하여 가상적으로 구성하였다. 그러나 개인의 중요 정보들이 클러스터에 집중화되기 때문에 불법적인 개인정보 수집을 위한 공격 또한 급격하게 증가할 수 있다. 그러므로 본 논문에서는 미래의 우리 사회에 등장하게 될 유비쿼터스 진료환경에 대비하여, 불법적인 정보 수집 공격이 발생하면 원격진료 클러스터를 구성하고 있는 시스템 상호간 침해 정보의 공유와 암호화 기법을 이용하여 서비스 가용성과 능동적인 방어 협력모델을 설계하였다.

Chang Ho An received the Master of Public Health degree in the Department of Health Information Management from Yonsei University in 2013. His current research interests include Design security model for building telemedicine Cluster of cloud-based. He is employed at The Korea Association of Regional Public Hospitals, 1997. Curenty serving head of the Ministry of planning and Managerment.

E-mail address: ach7821@hanmail.net

Hyun Chul Baek received the Ph.D. degree in the Department of Computer Science from Gyeongsang National University in 2003. He was a chairman in the Committee of Computer System technology at The Korea Association of Regional Public Hospital in 2007. He has been a professor in the Department of smart convergence Information, Gyeongnam Provincial Namhae College since 2013. His current research interests include network, network security, encryption, bigdata security, cloud computing. He is a member of the KKITS.

E-mail address: dosi_gas@lycos.co.kr

Jae Heung Park received the Ph.D. degree in the Department of Computer Engineering from Chungang University in 1989. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1983. He has been a researcher in the Software Engineering Research Institute at The Gyeongsang National University since 1984. His current research interests in clude computer network and security, S/W Reliability. He is a member of the KKITS.

E-mail address: pjh@gnu.ac.kr

Sang Bok Kim received the Ph.D. degree in the Departme nt of Electronics Engineering from Chung-ang University in 1989. He was a director in the Department of Education Information Computer Center at The Gyeongsang National University from 2007 to 2010. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1984. He has been a researcher in the Computer Data Communication Research Institute at The Gyeongsang National University since 1984. His current research interests include com -puter network and security, computer system architecture. He is a member of the KKITS.

E-mail address: sbkim@gnu.kr