의료클러스터 기반의 빅 데이터 환경에 대한 IP Spoofing 공격 발생시 상호협력 보안 모델 설계

안 창 호* · 백 현 철** · 서 영 건*** · 정 원 창*** · 박 재 흥*****

요 약

현재 우리사회는 네트워크를 통하여 실시간으로 교류되는 다양한 정보 환경에 노출되어 있다. 특히 정부의 의료정책은 대국민의료서비스 질을 향상시키기 위해 원격진료의 시행을 서두르고 있다. 이러한 원격진료의 시행은 향후 지역에 상관없이 맞춤형 환자 진료를 위한 빅 데이터 기반의 진료 정보 구축도 함께 요구하고 있다. 본 논문은 빅 데이터 기반의 권역별 의료클러스터 구축과 이에 대한 서비스 가용성을 해치는 공격이 발생할 경우 해당 공격을 탐지하고 적절한 대응이 가능한 방어 및 보안 협력모델을 제안하고 있다. 이를 위하여 동일 병원정보시스템으로 전국에 고루 분포된 지방의료원을 권역별 가상 의료클러스터 본부로 하는 네트워크 구성을 제안하였다. 아울러 의료클러스터에 발생할 수 있는 IP Spoofing 공격과 이에 따른 DDoS 공격에 실시간으로 대응 가능한 상호협력 보안 모델을 설계하여 단일 체계, 단일 보안정책이 가지는 한계성도 극복할 수 있도록 하였다.

Designing Mutual Cooperation Security Model for IP Spoofing Attacks about Medical Cluster Basis Big Data Environment

Chang Ho An* · Hyun Chul Baek** · Yeong Geon Seo*** · Won Chang Jeong**** · Jae Heung Park*****

ABSTRACT

Our society is currently exposed to environment of various information that is exchanged real time thro ugh networks. Especially regarding medical policy, the government rushes to practice remote medical treat ment to improve the quality of medical services for citizens. The remote medical practice requires establis hment of medical information based on big data for customized treatment regardless of where patients are. This study suggests establishment of regional medical cluster along with defense and protection cooperatio n models that in case service availability is harmed, and attacks occur, the attacks can be detected, and pr oper measures can be taken. For this, the study suggested forming networks with nationwide local govern ment hospitals as regional virtual medical cluster bases by the same medical information system. The stu dy also designed a mutual cooperation security model that can real time cope with IP Spoofing attack that can occur in the medical cluster and DDoS attacks accordingly, so that the limit that sole system and sole security policy have can be overcome.

Key words : Big Data, Security, Cloud Computing, Encryption, Traceback, Telemedicine, IPSpoofing,DDoS

접수일(2016년 12월 1일), 수정일(1차: 2016년 12월 15일, 게재확정일(2016년 12월 19일)

★ 본 논문은 미래창조과학부 소프트웨어 기반의 첨단과학기술연구망 구축과 서비스 사업에 의하여 연구되었음.

* (사)전국지방의료원연합회 기획운영부
** 경남도립남해대학 스마트융합정보과
*** 경상대학교 컴퓨터과학과
**** 진주보건대학 복지행정계열
***** 경상대학교 컴퓨터과학과(교신저자)

1. 서 론

오늘날 빠르게 발전중인 네트워크 환경은 우리의 생활 패턴에 다양한 변화를 이끌어 내고 있다. 초기의 네트워크 환경은 단순하게 간단한 정보의 송/수신 서비스로부터 시작하여 현재 클라우드 컴퓨팅과 사물인터넷 환경으로 발전하고 있다. 빅데이터 서비스란 방대한 양의 서비스 처리 환경이 일반적으로 클라우드 컴퓨팅 환경을 기반으로 이루어지는 것을 의미한다.

이러한 네트워크 환경의 발전은 우리사회 전반에 걸쳐 많은 영향을 주고 있다. 그 중 원격진료정책은 반드시 진료 의사의 대면 후 진료가 이루어졌던 기존 환경을 넘어서는 정책이라고 할 수 있다.

현재 우리나라의 원격진료 관련 의료법 개정안은 국회와 의료관련단체들의 강력한 반대에 직면해 있다.[1] 그렇지만 2015년 통계청에서 분석한 농림어업 총조사 자료를 보면 차로 30분 이상의 거리에 종합병원이 있는 마을이 전국 3만6792곳 중 59.2%인 2만1789곳으로 나타나고 있다. 이와 함께 10분 거리 미만에 종합병원이 위치한 농어촌 마을은 1574곳(4.3%)에 불과하다고 되어있다. 반면에 10분 이내로 병/의원이나 한의원에 갈 수 있는 마을은 전체 1만 1604곳(31.5%)으로 나타났으며, 10분 거리 내에 보건소나 약국이 있는 마을도 각각 44.6%(1만6411곳), 38.9%(1만4325곳)으로 파악되고 있다.[2] 그러므로 종합병원에 대한 접근성이 부족한 우리나라 진료 환경의 특성상 원격진료 서비스가 반드시 필요하다고 판단하며, 제대로 된 원격진료 시행을 위하여 클라우드 컴퓨팅 환경을 기반으로 하는 의료클러스터의 구축이 요구된다고 할 수 있다.

원격진료의 시행은 환자들이 시간과 공간의 제약으로부터 벗어남을 의미한다고 할 수 있다. 이는 언제든지 자신의 현재 위치에서 필요한 진료를 받을 수 있고 향후 국민건강맞춤형 진료 정책과도 부합된다고 할 수 있다. 그러므로 이러한 의료 환경의 변화에 맞춘 클라우드 컴퓨팅 기반의 원격진료의 시행은 환자들의 진료정보 공유를 통하여 거주지를 벗어나더라도 빠르고 정확한 진단과 중복 진료 문제를 함께 해결할 수 있다.

현재 우리나라의 환자진료정보 공유 정책은 보건복지부의 진료정보교류표준 고시(안)을 통하여 추진하고 있다.[3] 이에 따라 향후 진료정보교류 표준 고시(안)을 기반으로 의료기관들의 진료정보교류 표준안이 마련될 것으로 판단한다. 진료 정보에 대한 빅데이터 구축은 환자들의 개인 정보나 진료 정보를 의료기관에서 상호 공유하는 것이기 때문에 악의적인 목적을 가진 공격자들로부터 집중적인 공격을 받을 수 있다. 아울러 이러한 공격을 사전에 차단하지 못할 경우 환자들의 중요하고 민감한 진료정보가 유출될 수 있다. 그러므로 이에 대한 암호화 정책도 의료정보 국가 표준화 정책에 기반한 공유 자료의 등급 분류를 통하여 세분화 시킬 필요가 있다.

특히 IP Spoofing을 이용한 의료 클러스터에 대한 공격은 그 피해가 엄청날 것으로 예상할 수 있다. 그 이유로 IP Spoofing 공격은 호스트 상호간 신뢰를 기반으로 하는 서비스를 주 공격 대상으로 하고 있기 때문이다. 또한 IP Spoofing 공격은 신뢰 호스트의 IP를 이용하는 것으로 네트워크상에 동일한 IP가 존재할 수 없기 때문에 공격자는 자신이 위장할 IP를 보유한 호스트에 대하여 DoS나 DDoS 공격으로 해당 서버를 무력화시키게 된다. 그 결과 환자들의 중요한 진료 정보는 물론이고 서비스 가용성의 문제도 유발시킬 수 있다.

본 논문은 향후 진료정보 공유를 위한 빅 데이터 구축에 맞춰 전국 지방의료원을 권역별 진료정보 빅데이터 구축 기관으로 가상화시켰다. 그리고 이를 통하여 국민들의 소중한 개인 정보와 진료정보의 안정적인 서비스를 위한 상호협력 보안 모델을 제시하였다.

2. 관련연구

2.1 원격진료의 의미

원격진료의 일반적 정의는 '상호작용이 가능한 정보통신 기술을 이용하여 원거리에서 의료정보와 의료서비스를 전달하는 모든 활동'으로 설명할 수 있다. 이는 환자와 진료를 제공하는 의료기관이 먼 거리에 위치하거나 접근 시간, 또는 기타 다른 문제로 인해 직접 대면 진료가 어려울 때 진료정보나 전문적 조언

을 원격으로 제공하는 시스템을 의미한다. 여기에는 환자 진료 정보뿐만 아니라 의료행정, 의학교육, 자문, 의뢰 등을 모두 포함된다고 할 수 있다. 그러므로 원격진료를 통한 데이터 서비스에는 의학영상, 동영상, 환자기록 등 각종 데이터가 존재 할 수 있다.[4][5][6]

2.2 클라우드 컴퓨팅의 의미

클라우드 컴퓨팅에 대한 정의는 다양한 견해가 있지만, 그 중 공통된 견해로 '네트워크 환경에서 이용자의 요구에 따라 실시간으로 소프트웨어, 플랫폼, 인프라 등 IT 자원을 필요한 만큼 공급받고, 그에 따른 비용을 지불하는 서비스'라는 공통된 시각을 보이고 있다.

본 논문에서는 향후 원격진료 시행과 관련하여 소규모 의료기관들과 중/대규모 의료기관 상호간의 의료 클러스터 구축을 위하여 정보 공유가 가능한 지방 의료원들의 네트워크 환경을 클라우드 컴퓨팅 모델로 가상화시켜 활용하였다.[7]

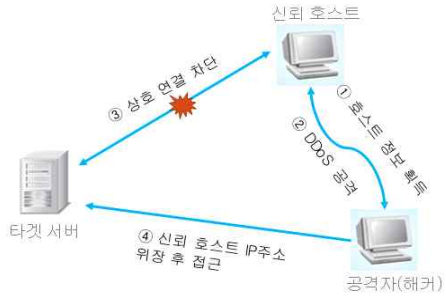
2.3 빅 데이터의 의미

빅 데이터 개념에 대한 일반적 견해는 기존의 분석도구나 시스템 체계에서 처리 가능한 범위를 넘어선 방대하고 다양한 데이터 환경으로 볼 수 있다. 또 다른 측면의 빅 데이터 개념으로는 저렴한 비용으로 가치 추출이 가능하고, 필요 데이터에 대한 빠른 수집과 발굴 및 분석이 가능한 차세대 기술이나 아키텍처라고 할 수 있다.[8][9][10]

본 논문에서는 원격진료 클러스터를 구성하는 의료기관들의 정보를 빅 데이터화 하여 정부의 질병관리와 우리나라 어느 지역에서도 특정 환자의 맞춤형 진료가 가능한 환경으로 구축하였다. 그렇지만 이러한 정보 운영은 클라우드 컴퓨팅 기반의 환경 특성상, 고도의 해킹 기술을 가진 공격자들의 주요 공격 목표가 될 수 있기 때문에 이에 대비한 강화된 보안 정책이 필요한 실정이다.

2.4 IP Spoofing 공격 기법

네트워크 상의 송/수신자 상호 인증 과정에는 연결 과정의 간략화를 위하여 상호 인증 정보로 신뢰하고 있는 IP를 이용하고 있다. IP Spoofing이란 공격자가 자신의 IP를 정상적인 송/수신자가 상호 신뢰하고 있는 IP로 위장하여 불법적인 접근을 시도하는 것을 의미한다. IP Spoofing은 네트워크 연결 과정에 필요한 TCP/IP의 구조적인 문제점을 이용하는 공격으로 해당 패킷이 보유하고 있는 시퀀스 번호, 연결상의 경로 정보, 출발지/목적지 IP 주소 등을 이용하여 불법적인 공격을 시도하는 것을 의미한다. IP Spoofing 공격은 (그림 1)과 같이 타겟으로 하는 서버가 공격자의 시스템을 신뢰하도록 만드는 공격 기법이다. 공격자는 자신이 타겟으로 하는 서버에 대하여 불법적인 접속을 하기 위해 해당 서버가 신뢰하는 임의의 호스트 정보를 획득한다. 그 다음 최종 접속에 앞서 해당 신뢰호스트로 DoS 또는 DDoS 등의 공격을 가하여 자신이 도용할 해당 호스트를 다운시킨다. 이러한 공격 과정을 통하여 타겟 서버와 해당 신뢰 호스트 간의 정상적인 연결 상태가 해제되면, 공격자는 해당 신뢰 호스트의 IP 주소를 자신으로 재설정하고 타겟 서버로 불법적인 접속을 성공시킨다. 이렇게 상호 신뢰하는 IP 주소만 이용하여 불법적인 공격이 가능하기 때문에 원격진료 클러스터 환경의 인증과 보안을 위하여 강화된 인증 과정이 더욱 필요하다.[11][12]



(그림 1) IP Spoofing 공격의 예

2.5 트레이스 백의 의미

네트워크 상의 송신자와 수신자는 일반적으로 다양한 송/수신 과정을 거쳐 최종 목적지까지 연결하게 된다. 이러한 네트워크 과정은 연결에 대한 안정성,

신뢰성 확보를 위하여 해당 경로들의 정확한 분석이 필요하다. 트레이스 백이란 이러한 네트워크 과정의 경로를 분석할 수 있는 프로그램이라고 할 수 있다.

상호 네트워크를 이루고 있는 특정 송신자의 패킷은 최종 수신자까지 도달하기 위해 여러 개의 라우터를 경유하게 된다. 이렇게 경유하는 각 구간의 정보를 획득하여 패킷의 이동 경로를 분석하는 것을 트레이스 백이라고 한다.

본 논문에서는 트레이스 백 정보를 원격진료 클러스터의 접속 과정에 인증 정보로 사용하고 있다.[13]

3. 제안 모델 설계

3.1 제안 모델

본 논문의 환자 맞춤형 진료정보의 빅 데이터 구축과 관련한 권역별 원격진료 의료 클러스터에 참여하는 기관들은 기본적인 의료 정보 교환과 불법적인 공격에 대비하여 다음 정보들을 공유하도록 하였다. 먼저 동일인 여부에 대한 판정을 위하여 주민등록번호와 접근 IP 정보, 트레이스 백 정보를 기본적으로 공유하도록 한다.

주민등록번호의 사용은 동일인의 질병에 대한 검사 결과와 진료 이력 정보를 공유하기 위함이다.

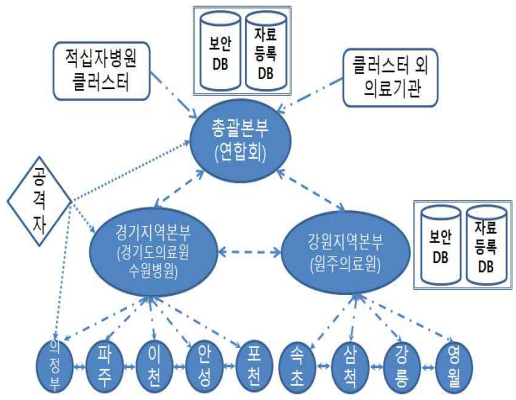
접근 IP와 트레이스 백 정보는 원격진료 의료클러스터 접속에 대한 인증과, 공격 발생 시 해당 정보를 수집하여 상호협력 보안 데이터베이스에 저장한 후 이를 이용하여 정상적인 접근 여부를 판단하도록 한다.

본 논문에서는 이러한 환자들의 개인 정보와 진료정보의 공유 및 서비스를 위하여 빅 데이터 구축과 이를 위한 원격진료 의료클러스터를 구성하였다. 그리고 이와 함께 불법적인 접근과 개인 진료 정보를 조합하는 사례가 발생하면 실시간 대응이 가능한 상호협력 보안 모델을 제시하였다.

아울러 본 논문의 원격진료 의료클러스터 구성에는 경기도와 강원도 지역에서 운영하고 있는 지방의료원과 전국지방의료원연합회를 모델로 하여 다음과 같은 보안 모델을 제안하였다.

원격진료 의료클러스터에 대한 접근 상황은 정상적인 진료정보 서비스를 위한 접근과 IP Spoofing를 이용한 불법적인 접근 상황을 가정하여 다음과 같은 경우를 설정하였다. 첫 번째 원격진료 의료클러스터의 본부격인 전국지방의료원연합회에 대한 직접공격 상황이다. 두 번째는 권역별 의료클러스터 본부에 대한 직접 공격이 있다. 본 논문에서는 경기도의 경우 경기도의료원 수원병원을 본부로 하고, 강원도의 경우 원주의료원을 지정하여 구성하였다. 세 번째는 각 지역 의료원에 대한 직접적인 불법적 접근의 예를 가정할 수 있다.

본 논문에서 제안하는 원격진료 의료클러스터에 대한 네트워크 구조는 향후 원격진료 의료클러스터에 대하여 (그림 1)의 공격자가 IP Spoofing을 이용하여 원격진료 클러스터를 불법적으로 접근할 경우 실시간 능동적인 대응을 할 수 있도록 (그림 2)와 같이 구성하였다. 아울러 원격진료 의료클러스터에 대한 의료기관들의 맞춤형 진료 정보 참조와 공격정보 공유를 위하여 클러스터 총괄 본부와 지역 본부에서 이들 자료를 관리하도록 하였다.



(그림 2) 원격진료 의료클러스터 모형

(그림 2)에서 원격진료 클러스터를 구성하는 의료기관들은 클러스터내 상호정보교환과, 클러스터 외 기관과 상호정보교환이 가능하도록 설계하였으며, 그 과정은 플로우챠트를 통하여 도식화 하였다. 아울러 총괄본부, 지역본부, 개별의료원의 시스템들은 자신을 제외한 다른 원격진료 클러스터 시스템의 상호 트레이스 백 정보와 클러스터 내 자신들의 인식을 위하여 <표 1>과 같이 클러스터 등급코드, 클러스터 위치

코드를 가지도록 하였다.

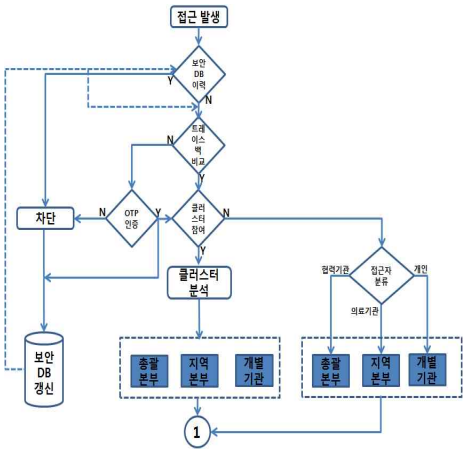
<표 1> 클러스터 구성 등급 자료목록

클러스터 등급코드	등급별 명칭
01	총괄본부
02	지역본부
03	클러스터 내 개별의료기관
77	클러스터 내 환자
88	클러스터 협력기관
99	클러스터 외 의료기관

본 논문에서는 이들 정보를 이용하여 클러스터 외부에서 IP Spoofing 공격이 발생할 경우를 가정하여 적절한 인증과 대응 과정을 수행하도록 하였다. 먼저 원격진료 의료클러스터에 대한 공격이 발생하면 해당 접근 정보를, 대응을 위한 상호협력 보안 데이터베이스로 실시간 참조하여 대응 가능하도록 하였다. 그 다음 정상적인 접근으로 판단하면 이에 대하여 클러스터 내/외 접근여부를 분석한 후 적절한 과정을 거쳐 서비스를 수행하도록 하였다.

3.2 제안 모델 동작과정

본 논문의 원격진료 의료클러스터에 대한 정상적인 접근 과정과 불법적인 접근 가정에 대한 처리 과정은 (그림 3), (그림 4)를 통하여 나타내었다.



(그림 3) IP Spoofing 공격의 예

(그림 3)의 처리 과정은 크게 트레이스 백 정보를 이용한 인증 단계, 원격진료 의료클러스터 참여 여부 분석단계, 요청자료의 서비스를 위한 암호화 단계로 나누어진다.

1. 원격진료 의료클러스터에 대한 특정 IP와 사용자 계정을 이용하여 접근 발생.

1-1. 보안 시스템은 해당 정보를 상호협력 보안 데이터베이스를 참조하여 공격 이력 여부를 검사한다. {현재 상태 트래픽, 공격이력}.

1-1-1. 이상 트래픽을 발생시키거나 공격이력이 존재하면 차단 후 보안 데이터베이스에 해당 정보의 반영 및 갱신.

2. 트레이스 백을 통한 IP Spoofing에 대한 검증을 한다.

2-1. 트레이스 백을 이용한 인증 단계를 정상적으로 수행하면 클러스터 참여 여부를 검사한다.

2-1-1. 인증 과정을 정상적으로 수행하면 클러스터 등급 및 소속 분석 과정을 수행한다.

2-2. 트레이스 백을 이용한 인증 단계의 수행 실패는 다음과 같은 경우가 있다.

2-2-1. 기존의 정상적인 사용자가 상호 협력 보안 데이터베이스에 등록되어 있지 않은 위치에서 접근을 시도한 경우로 OTP를 이용하여 재인증을 받은 후 보안 데이터베이스를 갱신한다.

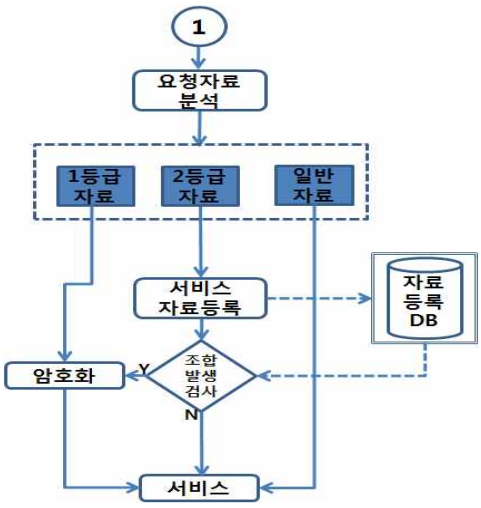
2-2-2. OTP를 이용한 재인증 수행을 하지 못하면 동일한 IP라 하더라도 공격자로 판단한 후 차단작업을 수행하고, 해당 정보를 데이터베이스에 등록한다.

3. 트레이스 백 정보와 OTP를 이용한 인증 단계를 정상적으로 수행하면 원격진료 의료클러스터 참여 여부를 분석한다.

3-1. 접근자가 원격진료 의료클러스터에 존재하는 사용자이면 클러스터 등급과 요청자료에 대하여 자료 조합여부를 분석한다.

3-2. 접근자가 원격진료 의료클러스터에 존재하지 않는 사용자이면 접근자에 대한 분석을 하고 클러스터 내의 적절한 기관과 연결과정을 수행하도록 한다.

(그림 4)는 접근자들에 대한 적절한 인증과 분석 과정을 거친 후 요청 자료의 서비스를 하기 위한 과정을 나타내고 있다.



(그림 4) IP Spoofing 공격의 예

1. 접근자들의 요청자료는 이를 분석한 후 요청 자료의 등급에 따라 서비스를 상이하게 수행하도록 한다.

1-1. 요청자료가 1등급인 경우 해당 자료는 어떠한 경우이든 반드시 암호화를 시켜 서비스 작업을 수행한다.

1-2. 요청자료가 2등급이면 해당 자료는 다음과 같은 처리 과정을 수행한다.

1-2-1. 단일 2등급 자료의 요청시 해당 자료는 바로 서비스를 실시하고, 향후 자료조합의 발생에 대비하여 자료등록 데이터베이스에 기록해 둔다.

1-2-2. 자료등록 데이터베이스 참조 후 자료조합이 발생했을 경우 해당 자료를 암호화하여 서비스 작업을 수행한다.

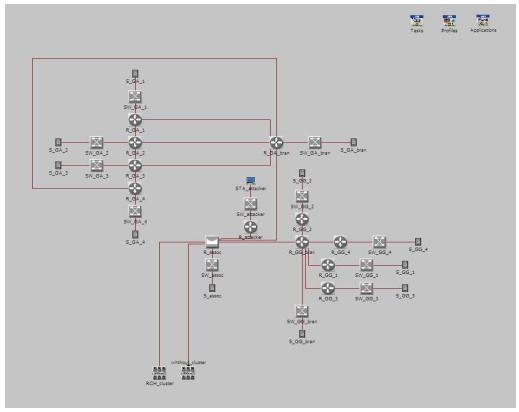
1-3. 기타 일반 자료는 바로 서비스 할 수 있도록 한다.

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 하고 이를 K_E2로 정의하여 사용한다. 본 논문의 암호화 복호화 과정에 필요한 정보는 의료진 요청 자료에 대한 의료진 코드, 특정진료 코드, 상병코드를 동시에 만족해야만 원래의 진료 정보를 알 수 있도록 하였다. 의료진의 대부분은 진료 특성상 특정 상병에 대하여 자신만의 특정 진료코드를 사용하며, 이는 본인만 알고 있는 내용으로 볼 수 있다. 그러므로 본 논문에서는 이를 이용하여 암호화 및 복호화 과정에 이용하도록 한다.[14]

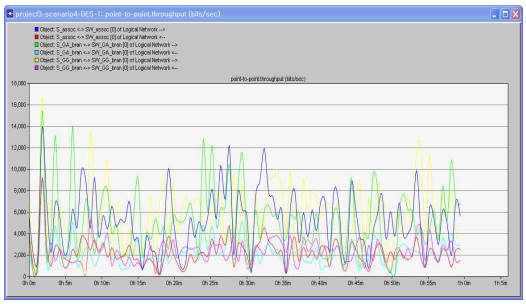
4. 실험 및 평가

4.1 시뮬레이션 환경

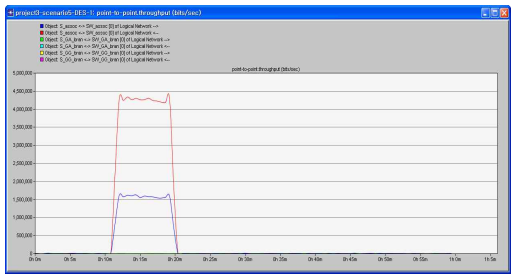
본 논문에서 제안하는 원격진료 의료클러스터를 이용한 진료정보 빅 데이터 구축과 이에 대한 불법적인 정보 수집 및 공격 발생에 대한 방어 시스템의 시뮬레이션 환경은 다음과 같다. 먼저 사용된 응용 소프트웨어는 jdk1. 8.0_45, Eclipse 4.3.2 SR2, 구현언어는 Java를 사용하였다. 시뮬레이션을 위한 운영 체제는 Windows 7 Professional K64비트이고, 시스템 사양은 8GB 메모리를 채택한 Core(TM)i5 2.67GHz System으로 구성하였다. 아울러 전체 네트워크 구성에 대한 시뮬레이션은 OPNET을 이용하여 (그림 5)와 같이 구성한 후 (그림 6)의 정상트래픽과 (그림 7)의 이상 트래픽을 측정하여 보안데이터베이스에 등록해 둔다.



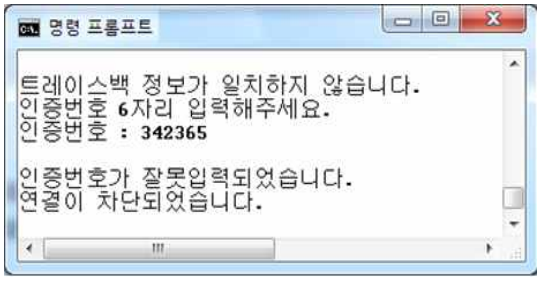
(그림 5) OPNET을 이용한 네트워크 구성도



(그림 6) OPNET을 이용한 총괄본부, 지역본부 상호 정상트래픽 모형

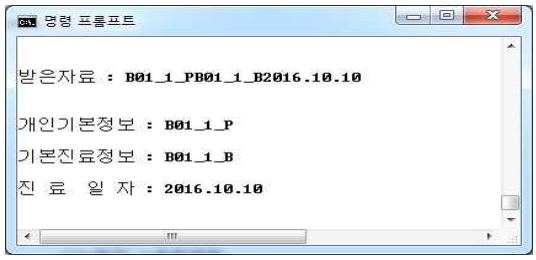


(그림 7) OPNET에서 총괄본부, 지역본부 상호 이상트래픽 모형



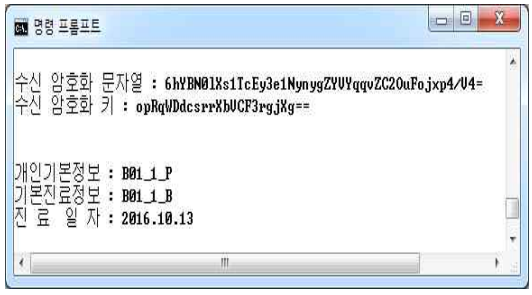
(그림 8) 클라이언트에서 OTP 인증 과정

(그림 8)은 본 논문의 원격진료 의료클러스터에 대한 접근 발생시 그 인증 과정과 불법적인 공격 탐지 과정을 보이는 것이다. 본 논문에서는 구축해 둔 보안 데이터베이스의 트레이스 백 정보와 비교하여 일치하지 않는 경로가 탐지되면 OTP를 이용한 재연결 과정을 수행하도록 한다. 이 때 OTP 인증을 실패하게 되면 연결을 차단한다.



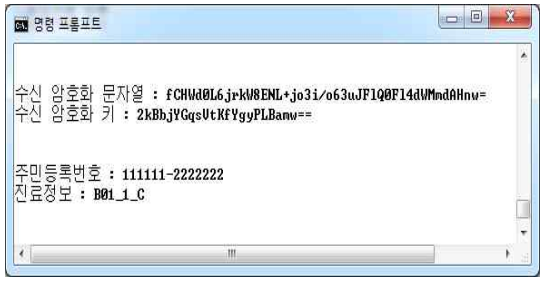
(그림 9) 2등급 서비스 자료의 구조

(그림 9)는 2등급 자료의 서비스 과정을 위한 자료 구조이다. 이 자료는 향후 2등급 자료의 서비스 요청이 발생하면 해당 자료들에 대한 조합 유·무를 검사하기 위하여 자료등록 데이터베이스에 기록해둔다.



(그림 10) 2등급 자료가 조합이 발생한 경우

(그림 10)은 2등급 자료에 대한 서비스 요청이 발생한 후 자료등록 데이터베이스를 통하여 자료 조합을 탐지한 경우이다. 본 논문에서는 이 경우 해당 서비스 자료를 암호화시켜, 자료의 조합으로 야기되는 불법적인 정보 유출에 대비할 수 있도록 하였다.



(그림 11) 1등급 자료 처리 과정

(그림 11)은 민감한 1등급 자료 서비스 요청이 발생할 경우 이에 대한 처리 과정을 보이는 것인데, 본 논문에서는 반드시 암호화 과정을 수행한 후 서비스를 하고 있다.

5. 결 론

본 논문은 향후 원격진료 시행과 우리나라 어떤 지역에서든지 환자 맞춤형 진료를 시행하게 될 것에 대비하여 그 문제점을 분석하고 해결하기 위한 방안을 연구한 것이다. 원격진료의 시행은 진료를 받기 위한 환자들이 시간과 공간의 제약으로부터 벗어남을 의미한다. 이에 따라 환자 맞춤형 진료를 시행하기 위하여 의료기관간 진료정보교류표준을 통한 원격진료 의료클러스터와 이를 이용한 빅 데이터 구축이 선행되어야 한다. 그렇지만 이러한 개인 진료정보의 집단적인 네트워크 구성은 보안에 대한 심각한 우려를 가져 올 수 있다. 본 논문은 이러한 클라우드 기반의 개인 진료정보의 빅 데이터 구축에 따른 원격진료 의료클러스터의 보안 문제를 해결하기 위하여 클러스터를 형성하는 의료기관들 모두 상호협력 보안 정책에 참여시켜 불법적인 공격에 능동적이고 실시간 대응이 가능하도록 하였다. 이는 원격진료 시행시 가장 큰 문제점이라고 할 수 있는 개인의 진료정보를 안정적으로 관리하면서 원격진료 의료클러스터에 참여한 의료기관들의 보안 능력 향상에도 기여할 수 있다고 본다. 향후 연구 과제로는 조속한 입법 과정을 통하여 지역 거점 의료기관이면서, 현재 하드웨어와 소프트웨어 등의 제반 시스템을 거의 동일하게 사용하고, 일반 민간 회원 병원들도 참여하고 있는 전국 지방의료원을 대상으로 조기에 원격진료 의료클러스터를 구성할 필요가 있다고 본다. 이와 함께 그 결과를 인근 보건소와 민간 의료기관으로 점진적으로 확산할 수 있는 정책이 함께 진행되어야 할 것이다. 아울러 이러한 개인 진료정보의 공유로 어느 지역에서도 특정 환자에 대한 맞춤형 진료가 가능한 환경 구축으로 과잉 진료의 감소와 빅 데이터 활용을 통한 국가 질병 관리에 도움이 되는 연구가 함께 진행되어야 할 것이다.

참고문헌

[1] http://www.hankookilbo.com/v/e6104b4b86d4446ba63127649079e13f

[2] http://news.mk.co.kr/newsRead.php?no=845839&year=2016

[3] 의료기관간 진료정보교류표준 고시(안)소개, 보건복지부, 2016. 10.

[4] 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.

[5] J-H. Choi, Analysis of changes in the muscle acti vity and fatigue of the erector spinae using IT co nvergent type medical equipment, Journal of Kno wledge Information Technology and Systems, Vol. 10, No. 6, pp. 665-673, 2015.

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

[7] 전정훈, “클라우드 컴퓨팅 서비스의 취약성과 대응 기술 동향에 관한 연구” 한국융합보안학회, Vol 13, No. 6, pp. 1239~1246, 2013. 4.

[8] 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.

[9] Q. Miao, When intelligence meeting wity bi g data : Review and perceptions of big Data’ S hotspot intelligence tracking, Institute of S cientific & Technical Information of Shangha i,Shanghai 200031, No. 5, Serial No. 187, 2 013.

[10] 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 o f Information Security, Vol. 23, No. 5, pp. 96

9-976, 2013, http://dx.doi.org/10.13089/JKIISC.2013.23.5.96, 2013.

[11] 김명희, 백현철, 홍석원, 박재홍 "빅데이터 환경에서 정부민원서비스센터 어플리케이션 불법 이용에 대한 서비스 자료 암호화 모델", 한국융합보안학회, Vol 15, No. 7, pp. 31~38, 2015. 12.

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

[13] 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.

[14] 허승표, 이대성, 김귀남, "모바일 환경에서 OTP기술과 얼굴인식 기술을 이용한 사용자 인증 개선에 관한 연구", 한국융합보안학회, Vol 11, No. 3, pp. 75~84, 2011. 6.

[著者紹介]

안 창 호 (Chang Ho An)
1990년 2월 학사
2013년 8월 석사
2016년 8월 박사
email : ach7821@hanmail.net

백 현 철 (Hyun Chul Baek)
1988년 2월 학사
1999년 8월 석사
2003년 2월 박사
email :dosi_gas@nate.com

서 영 건 (Yeong Geon Seo)
1987년 2월 학사
1989년 2월 석사
1997년 2월 박사
email : young@gnu.ac.kr

정 원 창 (Won Chang Jeong)
1996년 2월 학사
1999년 8월 석사
2009년 2월 박사
email : jwcblue@hanmail.net

박 재 홍 (Jae Heung Park)
1978년 2월 학사
1980년 9월 석사
1989년 8월 박사
email : pjh@gnu.ac.kr