한국사물인터넷학회논문지 Vol. 2, No. 2, pp. 15-20, 2016 http://dx.doi.org/10.20465/KIOTS.2016.2.2.015

Powershell을 이용한 안전한 XMPP 프로토콜 기반의 의료기기 IoT환경 구축 제안

박연진, 이근호
백석대학교 정보통신학부, 백석대학교 정보통신학부

Construction of IoT Environment for XMPP Protocol Based Medical Devices Using Powershell

Yeon-Jin Park, Kuen-Ho Lee
Division of Information Communication, Baekseok University

요 약 MicroSoft에서 2015년 8월부터 배포하기 시작한 윈도우10 IoT버전은 익숙한 Window를 IoT 시장에 끌어내어 소비자의 흥미를 끄는 데에 성공했고, IoT에서 웹서버등을 더 손쉽게 구축 할 수 있도록 도왔다. 최근 의료계에서는 과잉진료문제가 대두되고 있다. IoT 서버와 의료장비간의 통신 수립은 사용자에게 의료결과를 전송하고 병원간 커뮤니케이션을 원활히 하여 과잉진료문제를 크게 줄일 수 있을 것이다. 자원이 한정되어있는 IoT 서버에서는 트래픽을 유발하지 않으면서 사용이 수월한 경량화 프로토콜들이 많이 사용된다. 이러한 상황에서 한정적 자원에 무리를 주지 않고 사용 할 수 있는 SSDP(Simple Service Discovery Protocol), 보안성이 높은 XMPP(Extensible Messaging and Presence Protocol) 프로토콜을 사용해 의료기기가 손쉽게 사용자에게 유비쿼터스 환경을 제공할 수 있는 IoT 네트워크를 제안하고자 한다.

주제어 : XMPP, SSDP, Window 10 IoT, Powershell

Abstract MicroSoft Windows 10 IoT version, released in August 2015, successfully drew consumer interest by introducing the familiar Windows into the IoT market, and enabled an easier system construction of IoT web servers. Meanwhile, overdiagnosis has recently emerged as a controversy in medical society. Establishment of communication between IoT servers and medical devices will send treatment results to users and activate communication between hospitals, greatly reducing this problem. The IoT server, with its limited resources, utilizes lightweight protocols that do not generate traffic and are easy to use. This paper proposes IoT networks which will enable medical devices to easily provide ubiquitous environments to their users, through utilization of the lightweight Simple Service Discovery Protocol (SSDP) and the secure Extensible Messaging and Presence Protocol (XMPP).

Key Words : XMPP, SSDP, Window 10 IoT, Powershell

1. 서론

최근 사회 환경 변화가 속히 이루어지고 있는 가운데, 국민의 지 능력 생활수이 향상됨에 따라 건강한 삶과 생활을 해 언제 어디서나 제공 받을 수 있는 U헬스어 서비스에 한 요구가 증하고 있다[1,2,3]. 또한, 의료 과잉 문제

교신저자 : 이근호(root1004@bu.ac.kr)
접수일자 2016년 6월 6일

가 점점 대두되고 있다. 요양기관이 요양급여 기준을 위반하여 치료한 행위에 대해 국민건강보험법이 제 52조 제1항에 따라 과잉진료로 보고 그로부터 얻은 이익을 부당이익으로 평가 한 후, 환수 처분이 적법하다고 한 대법원판결[4] 처럼 요양기관에 대한 의료 과잉문제 뿐만 아니라, 기본적인 진료행위별 수가제를 체택하는것에 대한 의문점을 제기[5]하는등의 기본법제적 조취 및 사용된 의학정보의 재활용에 대한 필요성도 꾸준히 논의되고 있다. XMPP는 IoT기기의 통신 연결에서 실시간 통신을 하기 위해 사용되는 대표적인 프로토콜중 하나이다. 자체적으로 보안 설정이 가능하며, 실시간으로 통신할 수 있다. XML기반의 메세징 프로토콜인 Jabber로 로 누구나 간단하게 메신저 서버와 클라이언트를 만들 수 있다. SSDP(Simple Service Discovery Protocol)는 네트워크 서비스나 정보를 찾기 위해서 사용하는 네트워크 프로토콜이다. SSDP를 이용하면, DNS 나 DHCP 같은 네트워크 서버 혹은 정적인 호스트 설정 없이 네트워크 서비스나 정보등의 일을 손 쉽게 찾을 수 있어, 의료 IoT 환경처럼 손쉽게 자신의 의료정보를 확인 할 수 있도록 사용자가 가지고있는 스마트 기기등과 연동하여 정보를 넘겨주어야 하는 상황에서 유연하게 씌일수있다. IoT 유비쿼터스 의료서비스의 통신을 XMPP와 SSDP를 사용하여 구축한다면 통신이 안전히 이루어질 수 있을 것이다. 특히 국내에서는 의료정보 유출 법제화가 2006년부터 이루어져 그 역사가 짧은만큼 더더욱 유출에 신경을 써야 할 것이다[6]. Powershell은 Window의 서버버전인 2008, 2013등의 버전에서 많이 쓰이는 강력한 스크립팅 도구이며, 서버 셋팅 및 윈도우의 세션 패킷등의 분석에 사용된다. Window 10 IoT Edition에서 Powershell을 이용하여, XMPP 와 SSDP를 사용한 안전한 통신을 손쉽게 구축할 수 있다. 본 논문에서는 PowerShell을 이용하여 IoT 의료 정보 통신을 안전하게 구축하는 방식에 대하여 논하고자 한다.

2. 구성기술

2.1 XMPP 프로토콜

XMPP의 중요아키텍쳐는 클라이언트 -서버모델로 구성되어있다[7]. XMPP는 IoT기기의 통신 연결에서 실시간 통신을 하기 위해 사용되는 대표 세가지(XMPP, CoAP, MQTT) 프로토콜중 하나이다. UDP통신을 하는 CoAP 프로토콜등과는 달리 자체적으로 보안 설정이 가능하며, 실시간으로 통신할 수 있다. XMPP는 인터넷 상의 두 지점 간에 확장 가능한 메시지와 상태정보를 실시간으로 통신하기 위한 XML 기반 의 오픈소스 기술이다. 1999년 Jabber 오픈소스 커뮤니티에 의해 개발되었고, 2000년~2004년에 걸쳐 IETF에 의해 표준화되었다. XMPP Standard Foundation(XSF)의 표준화 작업에 의해 지속으로 확장되고 있으며, XMPP Extension Protocols(XEP)로 별도 확장 스펙을 관리하고 있다.[8] Google Talk, Line, Kakao등이 XMPP 방식의 통신을 사용하지만, 표준 XMPP 프로토콜이 아닌, 보안성을 조금 더 강화한 자체 개발 프로토콜로 사용하고 있다.

2.2 Jabber 메세징 시스템

Jabber메시징 시스템은 실시간 메세징을 위한 XML 기반의 데이터 모델과 프로토콜에 대한 구현이다.[9]Jabber 시스템은 오픈소스 프로젝트이다. Jabber는 인터넷 상의 두 요소들 간에 메시지나 프레센스(presence), 또 다른 구조의 정보를 실시간으로 교환할 수 있도록 한다. Jabber는 XML로 표현된다. 서버와 클라이언트간의 XML 문서형식으로 통신을 하는데, 이 통신을 하는 것이 자원을 소모하여 IoT 통신에 적합하지 않는다고 판단하였지만, 점점 IoT기기들의 퍼포먼스가 좋아지고있는 상황에서 보안성을 인정받아 다시금 등장하였다. 간단한 구조로 정의되어 있어 응용이 용이하고 다양한 플랫폼에서 사용이 가능하다.[10] Jabber 내에서 유저를 식별하는 ID를 JID(Jabber Identifiers)라고 부르는데, @와같은 어노테이션을 사용하여, 각각을 식별하는 식별자의 기능을 하고 있어 사용자가 편리하게 유저를 검색하고, 유저와의 통신을 할 수 있도록 만든다. UTF-8로 인코딩되어있어 한글 지원도 가능하다. Jabber 내부에서 통신하는 문서들은 XML문서로 사용가능하며, 이를 스탠자(Stanza)라고 표현한다. 스탠자에는 3가지 속성이 존재한다. 메시지를 전송할 때 사용하는 Massage(<message></message>)와 현재 접속하는지 접속하지않는지 확인하며, 사용자가 로그아웃 된 경우 type에 available을 추가하여 사용할 수 있는 프레젠스 (<presense></presense>)[11], 친구요청등의 유저간 통신인 IQ(Info/Query)가 있다.

2.3 SSDP 프로토콜

SSDP(Simple Service Discovery Protocol)는 UPnP(Universal Plug and Play) 프로토콜에서 근거리 혹은 인터넷에 연결된 디바이스를 찾는 데 사용되는 프로토콜이다[12]. UPnP(Universial Plug and Play)가 공표한 프로토콜중 하나이며, 대한민국은 오픈 SSDP를 전세계에서 3위로 사용할 정도로 큰 가용성이 있는 프로토콜이다. 1900대 포트를 사용하며, UDP 기반의 HTTP위에서 작동한다. SSDP는 유니캐스트와 멀티캐스트를 이용하며 기본적으로 UDP 239.255.255.250 멀티캐스트 주소를 이용한다.

HTTP 와 완전히 똑같은것은 아니며, 그 형태는 크게 비슷하다. 큰 차이점은 TCP 를 이용하는 것이 아니라 UDP 를 사용하는 것이다

2.3 Powershell

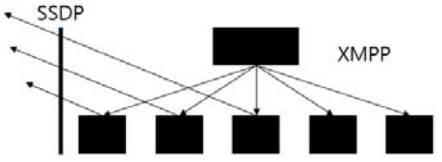
PowerShell은 리눅스의 bash나 C, Corn쉘처럼 윈도우에서 동작하는 스크립트 언어윈도우에서 주로 사용하는 스크립트언어이다. 리눅스의 수 많은 쉘처럼 Window의 파워쉘도 많은 유용한 기능을 가지고 있다. 파워쉘의 가장 특별한 기능중 하나는 다른 쉘들과는 달리 .Net Framework가 기반이 되어 쉽게 인터넷 환경을 사용 할 수 있다는 것이다. 따라서 그 강력한 기능은 윈도우 서버를 관리하는데도 주로 사용되고 있다. 두 세줄만으로도 서버에서 자료를 가져 오는데 무리가 없는 강력한 도구이다. 파워셸에서 관리 업무는 'cmdlets'(커맨드릿)에 의해 실행된다. comlet은 특정 작업을 구현하는데 특화된 닷넷 프레임워크를 사용하는 것이 특징이다. Powershell을 이용하여 윈도우 관리도구(WMI)와 컴포넌트 오브젝트 모델 (Component Object Model, COM)에 대한 접근이 수월해져, 관리가 쉽다.

2.4 argsXMPP

argXMPP는 Powershell의 .Net Framework 환경에서 사용하는 라이브러리중 하나이며 현존하는 가장 강력한 카피레프트 허가인 GPL(General Public License)의 인증을 받았다. argXMPP는 강력하고 손쉬운 파워쉘의 정책처럼 몇줄 사용하지않고도 간단하게 XMPP 프로토콜을 사용한 Jabber 메신저등을 구축 할 수 있다. 파워쉘에서 사용하는 argXMPP cmdlet의 종류는 로그인을 했을 경우에, 사용자와 통신을 시작하고자하는 New-Client, 나를 친구추가 한 사람에게 내가 친구 추가 요청을 보내는 Add-Contact , 프레젠스를 확인 한 후에, 현재 온라인 상태로 표시되어있는 사용자에게 메시지를 보낼 수 있도록 요청하는 Get-Contact와 , 메시지를 보낼 수 있도록 만들어주는 Send-Message 명령어가 있다. 또, Receive-Message는 이름처럼 받은 메시지를 읽을 수 있도록 해주는데 -ALL과 -LOOP 의 Filter를 붙일 수 있다. 이 때 붙인 ALL의 Filter는 받은지 오래 된 메시지들에게도 읽음 표시를 발송하게 해주고, LOOP Filter는 새로운 메시지가 올 때 까지 기다리는 필터이다. Connect-Chat는 파워쉘을 이용하여 채팅방을 시작 할 수 있도록 해주는 Filter이다. Disconnect-Chat를 이용하여 채팅방을 닫을 수 있으며, Start-Chat를 이용하여 채팅방에 접속 할 수 도 있다. 또한 파워쉘을 사용하면 메시지 서버 내에서 -LOOP > log.txt 등의 명령어를 이용하여 현재 상황이나 메시지의 상태등을 텍스트 형식의 로그 파일로 보내거나 재 구축 할 수 있다.

3. 구축방안제안

구축방식은 두가지 프로토콜을 사용하는 외부적단과, 내부단을 분리, 구축한다. 외부적단은 프로토콜이 외부에 사용하는 스마트 기기 및 노트북에 연결하여 사용 할 수 있도록 SSDP 프로토콜을 이용하여 기기를 찾고 노드로 연결하는 기능을 하며, 내부적 단은 XMPP 프로토콜을 사용하여 메신저가 연결된 노드형태를 가진다.

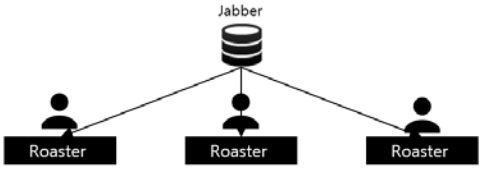


[Fig. 1] 제안한 의료기기 IoT환경의 구축 예상도

구축 예시는 다음과 같다. Jabber의 특성인 누구나 자신의 서버를 설치 할 수 있다는 점을 이용하여 A 병원에서 agsXMPP의 스크립트를 이용하여 B 서버를 만든다. B서버는 의료기기에서 촬영한 파일들을 환자들에게 전송하는 역할을 한다. 촬영하자마자 바로 보내는 형식이 아닌, 촬영한 자료를 환자별로 분류 한다음에 보내는 역할을 분류한다. 환자들이 사용 할 수 있는 IoT 기기들의

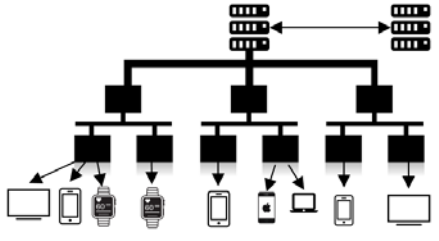
종류가 많기 때문에, 검색 프로토콜로 SSDP를 사용하였다. SSDP는 근거리에있는 디바이스에 접속할 수 있도록 만들어진 프로토콜이므로, 공유기를 통해 서버에서 얻어올 수도 있도록 서버 설정을 한다. 또한, 보안성을 강조하기위해, 속도가 느리고 전송자원이 많지만 보안성이 보장되는 XMPP 프로토콜을 이용하였다. XMPP 프로토콜은 사용자에게 메시지를 전송하며, 만일 사용자가 부재중시에 사용자와 서버간의 프레젠스를 주시하며 사용자가 로그인 하는지 확인하다. 사용자가 로그인 할 경우 로스터 (Roaster) 상대가 보낸 메시지를 전송한다.

Jabber 내부에서는 신뢰된 사용자로 인증된 Roaster (대화상대 목록)끼리만 통신을 할 수 있기 때문에, 신뢰된 사용자로서 병원과 환자간의 1:1 통신만을 허용한다면, 병원에서 환자에게 보내는 메시지 및 파일들을 안전하게 수신받을 수 있다. 사용자의 Roaster에서 또 자신의 기기를 연결하는 방식으로 연결하기 때문에 노드와 노드사이가 분할 되어있어 연결이 하이재킹(Hijacking) 당하더라도, 노드사이의 정보를 유출 하기 어렵다.



[Fig. 2] Jabber와 Roster간의 관계도

일단 메신저 서버를 구축해 두면, 다른병원과의 연결도 손쉽게 할 수 있다. Jabber 서버는 같은 프로토콜(XMPP)을 사용하는 다른 Jabber 오픈 서버에 손쉽게 접속 할 수 있다는 점을 이용하여, 다른 병원과의 관계도 손쉽게 할 수 있다. 물론, 환자의 정보가 기밀인 만큼, 서버간의 접속은 병원간의 서로 확인된 암호 및, 세션을 통해서 서로를 인증 한 후에 의료정보를 연동하여 사용 할 수 있도록 해야 한다.



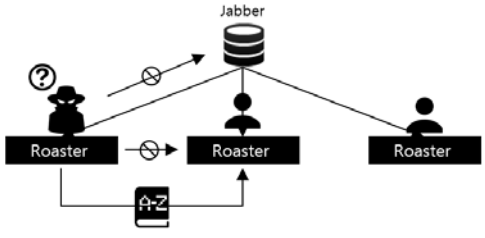
[Fig. 3] 타 병원과 접속할 경우에 보여지는 의료 정보의 흐름

이렇게 Jabber단에서 서로 접속을 할 경우에는 XMPP 프로토콜을 사용하는 Roaster 안쪽단에서 처리를 하기 때문에 의료정보를 유출 할 위험성이 적으며, 세션이 탈취되더라도 Roaster 내부의 세션만 탈취가 되며, Roaster 외부의 세션은 XMPP프로토콜과 Jabber 내부의 보안정책에 따라 탈취 되지 않는다.

4. 안전성 검증 시나리오

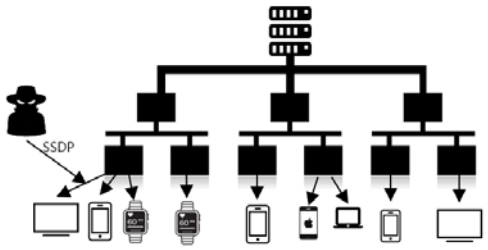
B서버 내부는 보안성이 높은 XMPP 프로토콜로 이루어져있지만, B서버를 지켜보는 해커 K는 B서버와 A병원사이에 오가는 패킷을 스니핑 하다가, Powershell을 이용해 RST 패킷을 보내, 세션을 가로챈다. 세션을 가로채어 Jabber내부로 접속하면, 섭스크립션이나 프로파일 보기 기능을 사용할 수 있지만, Roster 내부의 상대에게만 정보를 보여주는 Jabber의 특성상, 타인의 의료정보를 검색하기가 어렵다. 또한, 접속한 세션의 상태를 확인할 수 있는 프레전스(Presence)를 이용하여, 접속기록이 병원에 남기 때문에, 병원에서 인가되지 않은 사용자에 대한 정보를 확인 할 수있다.

Jabber의 특징인 DNS상태로 볼 수 있는 ID 상태를 이용하여, 다른 사용자의 아이디를 유추 할 수 있지만, 이는 시간이 오래 걸리는 사전공격 (dictionary attack)으로 시도하므로, 특수문자를 섞어 아이디를 어렵게 만든다면 사전공격으로부터의 공격을 방지 할 수 있다.



[Fig. 4] XMPP 프로토콜에 대하여 침입자가 할 수 있는 공격

IoT 통신망의 내부는 XMPP로 구축하였지만 통신망의 외부에서 SSDP 프로토콜을 이용하여, IoT 기기를 검색하고 프로토콜을 연결하는 과정에서도 스니핑 및 세션 하이재킹이 일어날 수 있다. 또한, SSDP 프로토콜은 DDos 공격에 노출되기 쉬워 SSDP프로토콜을 사용하는 병원의 직접적인 서버가 공격에 노출될 위험이 있다.



[Fig. 5] SSDP 프로토콜에 대한 침입자의 공격

하지만, 병원의 공유기 및, 서버자체에서 Pushback등의 기술을 사용하여 원치 않는 패킷들 을 업스트림 라우터들에서 협력을 통해 차단할 수 있다. 만약 SSDP 프로토콜의 취약점을 이용하여 XMPP 프로토콜이 적용된 내부 시스템으로 들어오더라 하더라도 이전의 공격시나리오처럼 대응을 할 수 있을 것이다.

또, Window 운영체제의 특성을 이용하여 Powershell을 사용한 대응 방안도 구축 할 수 있다. Window IoT에서도 기본적인 Window OS처럼 작업관리자를 사용할 수 있다. 이러한 작업관리자에서 SSDP 프로토콜을 사용하는 네트워크 장치 및 서비스를 검색하고 로컬 컴퓨터에서 SSDP 장치 및 서비스를 알리는 관리자인 SSDRPRSV를 손쉽게 프로세스 종료 후 재시작을 하거나, 의심가는 파일이 있다면 Powershell의 프로세스 확인 명령을 내리는 스크립트 파일을 이용하여, 파일을 검사한다.

5. 결론

과잉진료에 관한 불만의 소리는 점점 커져가고 있다. 과잉진료에 대한 법적인 제제는 2006년도부터 점점 강화되고 있지만, 매번 다른 병원을 갈 때마다 검진을 새로 받고, 그 검진의 값을 치르는 것은 병원끼리의 협약 없이는 쉽사리 해결 할 수 없는 문제이다. 병원끼리의 협약을 법으로 규제한다 하더라도 환자 사생활 침해등의 이유로 환자의 차트를 공유하지 않는 일이 일어날 것이다. 또한 법제적으로 강제적으로 규제하는 것 만으로는 이를 해결할 수 있는 없다. IoT (Internet of Things) 환경에서 애플리케이션은 네트워크에 연결된 여러 디바이스들을 이용하여 사용자에게 유용한 정보와 편의를 제공할 수 있다[13]. 이러한 IoT 환경에서 의료문제를 다루는 IoT기기 통신 서버를 구축하는 것이 중요한 문제로 다가올 수 있다. 의료정보 공유 서버의 구축에서는 무엇보다 보안성이 중요하다. 의료정보를 필수적으로 기입해야하는 판례가 있는만큼[14] 의사는 의료정보를 꼼꼼히 적어야 할 필요가 있다. 환자가 어떠한 약을 복용하고 있는지, 어떠한 기질을 보이는지를 상세하게 적어놓은 처방전이 유출된다면 이는 환자의 프라이버시를 지키지 않는 문제가 되며 , 업무상 취득한 비밀의 누설금지 규정을 위반하는 등의 큰 문제가 된다[15]. 때문에, 보안적인 IoT 서버의 구축이 절실한 상황이다. 이러한 상황에서 본 논문에서 제의한 IoT 환경에서 XMPP 프로토콜과 Jabber 메신저를 이용한 안전한 의료기기 IoT 환경 구축은 큰 도움이 될 것이다.

ACKNOWLEDGMENTS

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2013R1A1A1A05012348)

REFERENCES

[1] Schrenker R. A., “Software enginnering forfuture healthcare and clinical systems,” Computervol. Vol, 39, No, -, pp. 26-32, 2006

[2] Eun Jeong Choi, Hee Joung Hwang ,“Multiple User and Service Management Architecture for Medical Gateway”, Korean Society For Internet Information Vol.19, No.-, pp. 315-319, 2009

[3] Eun Jeong Choi, Si Yun Song, Sei Seung Park, Design of N-Screen Broadcast Server for Medical Information System, Korean Society For Internet Information, No. 12, Vol.1, pp. ,131-132, 2011

[4] 대법원 2008.7.10., 2008두3975

[5] Sun Jeong Won, ″ Redemption of unjust enrichment and compensation of damages in tort due to excessive medical treatments and excessive outpatient prescription ″ ,Korea Administrative Law Theory Practice Association Administrative Law Journal, Vol. 29, April, 2011

[6] Young-Ju Jeun. “The Medical Information Protection and major Issues”, No. 17, Vol. 12, pp. 251-258, 2012

[7] Sung-Chan Choi, Jaeho Kim, Jaeseok Yun, Il-Yeop Ahn, “A Tutorial for Energyefficient Communication for

XMPP-based Internet of Things". SmartCR, No. 3, Vol, 6, pp. 471-479, 2013

[8] Do-Kil Pyoun, Liu Hao, Hoe-Kyung Jung, "Android mobile phone information push system based on the XMPP protocol". The Korea Institute of Information and Communication Engineering, No. 17, Vol. 3, pp. 561-566. 2013

[9] Lee Geun Ung, An Geon Tae, Hwang Ui Yun, Kim Jin Hong , Lee Myeong Jun, "Information Processing Application : Extending Jabber Messaging System for Effective Collaboration", The KIPS Transactions : Part D, Vol. 10, No. 7, pp. 1161-1170, 2003

[10] Taeho Kim, Sejong Kim, Moonyoung Chung, Moonkun Lee, "Design and Implementation of XMPP based Collaboration Messenger System for Mobile Officeworking Environment", Korean Society For Internet Information, No. 3, Vol. 2, pp. 641-646, 2006

[11] Hong-Chang Lee, Tae-Ho Lee, Seong-Hune Kim, Myungjoon Lee, "A Jabber Messenger Client for the CoSlide Collaborative System", KOREA INFORMATION SCIENCE SOCIETY, Vol 34, No. 2, pp. 360-365, 2007 [12] Dae Young Kim, Hyun Jung La, Soo Dong Kim, "A Framework for Effectively Managing Heterogeneity of IoT Devices", KOREA INFORMATION SCIENCE SOCIETY, Vol.41 No.5, pp. 353-366, 2014

[13] Jang Seok Cheon, "Problem in the Civil Law and the Protection of Medical Information", Korean Law Association, Vol. 28, No. 11, pp. 159-180, 2007

[14] 대법원 1998. 1. 23. 선고 97도2124 판결.

[15] Choi, Hyunsang, Park, Hyundo, Lee, Heejo. "A Study on Amplification DRDoS Attacks and Defenses", Korea Institute of Electronic Communication Science, Vol. 8, No. 5, pp. 429-437, 2015

박 연 진(Yeon-Jin Park) [학생회원]

▪ 2015년 3월~현재 : 백석대학교 정보통신학부 학생

<관심분야>
개인정보보호, 융합 보안

이 근 호(Keun-Ho Lee) [정회원]

▪ 2006년 8월 : 고려대학교 컴퓨터 학과 (이학박사)
▪ 2010년 3월~현재 : 백석대학교 정보통신학부 부교수

<관심분야>
이동통신 보안, 융합 보안, 개인정보보호