정 보 보 호 학 회 지
제27권 제6호, 2017. 12

해사클라우드의 Identity 관리 기술 동향

이 동 혁*, 박 남 제*,**

요 약

현재 해양 환경의 안전을 위해 국제해양기구(IMO) 및 해양수산부에서 e-Navigation이 추진되고 있다. 해사클라우드는 e-Navigation의 핵심 통신 기반 기술에 해당하며, 성공적인 e-Navigation의 도입을 위한 필수적인 기술이다. 안전한 해사클라우드 환경을 위해서는 보안에 대한 고려가 필수적이며, Identity 관리 기술은 해사클라우드에서의 인증 및 권한 확인을 수행하는데 있어 주요 기술로서 작용하게 될 것이다. 따라서 본 고에서는 해사클라우드에서의 Identity 관리 기술 및 주요 현황을 살펴본다.

Ⅰ. 서 론

최근 선박간 및 선박과 육지간 원활한 해사 통신이 가능한 기술인 해사클라우드가 제안된 바 있다. 이는 e-Navigation 프로젝트의 핵심 통신 인프라 역할을 담당하며, 원활한 통신을 기반으로 안전한 해사 환경을 위해 필요한 핵심 기술이다.

현재 다수의 해양사고는 인적과실이 원인인 것으로 알려져 있으며, 이러한 인적과실이 전 세계 해양사고의 82%에 달하는 것으로 추산되고 있다. 따라서 국제해사기구인 IMO에서는 이와 같은 해양사고를 줄이기 위하여 2020년까지 시행을 목표로 선박운항기술에 ICT기술을 융합한 e-Navigation 기술의 도입을 결정하였다. 국내에서도 해양수산부에서 2020년까지 1,300여억원의 투자로 한국형 e-Navigation 개발을 추진중에 있으며, 해사클라우드 기술의 국제 표준화에도 노력을 기울이고 있다. 2016년 12월에는 군산항 인근 해역에서 해양수산부가 덴마크 해사청과 함께 해사클라우드의 공동시험을 성공적으로 실시한 바 있어, 국내의 어선, 소형선이 많은 특성을 고려하여 우리나라에 특화된 서비스를 제공하고, 유관 신산업 창출도 가능할 것으로 기대된다.

그러나, 안전한 e-Navigation 환경을 위해서는 핵심 통신 인프라인 해사클라우드의 보안이 필수적으로 요구된다. 여기에는 메시지의 무결성 뿐만 아니라, 통신 과정에서 발생할 수 있는 메시지 변조, 위조, 중간자공격 등 다양한 경우에 대비할 수 있어야 한다. 악의적인 공격자가 해사클라우드 통신 인프라에 무단 침입하여 불법적인 행위를 시도하는 경우, 선박의 안전에 직접적으로 위해를 끼칠 수 있기 때문이다[1,2].

본 고에서는 현재 해사클라우드의 기술동향 가운데, 인증, 권한 부여 등에 필요한 Identity 관리 기술에 대해 분석한다.

Ⅱ. 해사클라우드

본 장에서는 해사클라우드의 등장 배경과, 해사클라우드의 핵심 구성 요소에 대해 살펴본다.

2.1. 해사클라우드의 등장 배경

해사클라우드는 2012년 가을, 덴마크 정부 해사 기구(DMA:Danish Maritime Authority)의 내부 프로젝트로 시작되었다. e-Navigation 프로젝트의 일환으로, 당시 DMA는 e-Navigation 프로젝트 진행의 일환인 EPD(e-Navigation Prototype Display System)에서 해사클라우드의 연구를 진행한 바 있다.

기존에는 선박 측과 해안 측 사이를 통신할 때 여러

이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호: NRF-2016R1D1A3A03918513)
* 제주대학교 일반대학원 컴퓨터교육전공, 제주대학교 초등교육연구소(bonfard@jejunu.ac.kr)
** 제주대학교 교육대학 초등컴퓨터교육전공 (namjepark@jejunu.ac.kr, 교신저자)

제한점이 있었으며, 특히 상이한 종류의 해사 서비스를 제공하려면 여러 제약점이 존재하였다. 여기에서는 주로 다음과 같은 세가지의 문제점이 지적되었다. 첫번째로, 대역폭 부족의 문제이다. 대역폭 부족은 제한된 분량의 데이터만 전송할 수 있다는 문제를 야기한다. 데이터 전송에 있어 종종 어플리케이션의 특정 AIS 메시지와 같은 복잡한 인코딩 스키마가 사용되는 경우가 있으며 이러한 경우 에는 대역폭 부족에 따른 문제가 발생할 수 있다. 두번째로, AIS 통신 시스템의 시뮬레이션을 위해서는 복잡한 개발자 환경이 요구된다는 문제점이 있다. 즉, 개발하는 과정에서 AIS 통신을 구현하기 위한 간단한 시뮬레이션 환경을 제공하는 것이 현실적으로 어렵다는 문제가 있다. 마지막으로, 신호 범위의 제한에 따른 문제점이 존재한다. 통신이 필요한 객체 모두가 무선 신호의 범위에 닿지 않는다면, 신호 범위 밖의 객체는 무선 통신이 어렵게 된다는 문제가 존재한다[3].

따라서, 해사 객체간 원활한 통신을 위해 새로운 인프라 환경이 필요하며, 해사클라우드는 이러한 배경 아래 개발되었다. 현재의 해사클라우드와 관련된 첫 프로토타입은 2012년 겨울에 제작되었으며, 2013년 봄 EPD에 구현된 바 있다. 이것은 단지 기본적인 point-to-point 통신을 특징으로 하고 있으며, 이는 현재 해사클라우드의 구성요소인 MMS(Maritime Message Service) 서비스에 해당하는 부분이라 볼 수 있다. 이후 2013년 여름에 해사에서의 원활한 통신을 위한 구체적인 틀이 제시되었으며, 여기에는 MMS와 같은 메시지 기반 프레임워크 외에도, 서비스 및 ID에 대한 레지스트리를 포함하고 있다. 해사클라우드(Maritime Cloud)라는 명칭이 다양한 기본 서비스를 위한 명칭으로 본격적으로 사용된 것은 이 시점이다. 이후 2014년에는 해사 클라우드 참조 구현의 첫번째 릴리즈가 공개된 바 있다[4].

2.2. 해사클라우드의 제공 서비스

해사클라우드에서는 다음과 같은 세가지 핵심 서비스를 제공한다. 첫번째로, 해사 신원 레지스트리(Maritime Identity Registry)가 있으며, 이는 해사클라우드를 사용하는 사람, 조직, 또는 선박의 신원에 대해 중앙 집중적으로 권한을 가질 수 있게 한다. 두번째로, 해사 서비스 레지스트리(Maritime Service Registry)가 있으며, 이는 해사클라우드와 관련된 전 세계의 서비스 표준 및 프로비저닝 서비스의 중앙 저장소를 의미한다. 마지막으로 해사 메시지 서비스인 MMS(Maritime Message Service)가 있으며, 이는 TCP/IP 상단의 통신 프로토콜로써, 메시지의 신뢰성 있는 전달과 지오캐스팅 서비스를 제공한다. 여기에서, 해사 신원 레지스트리는 해사 환경에서의 인증과 권한 부여에 필요한 핵심 서비스이다[5].

본 고에서는 해사클라우드의 주요 제공 서비스 가운데, 해사 신원 레지스트리의 주요 현황에 대해 살펴보고자 한다.

Ⅲ. 해사클라우드의 Identity 관리

3.1. 개요

해사클라우드에서 신원(Identity) 관리가 의미하는 것은 기술을 사용하여 객체의 신원에 대한 정보를 관리하고, 리소스에 대한 액세스를 제어하는 프로세스를 의미한다. 신원 관리는 사용자 및 그들의 신원, 속성 및 인증 정보 관리와 관련된 비용을 절감하는 것과 동시에, 생산성 및 보안성을 향상시키는 것을 주요 목적으로 한다.

이를 위해 세계적인 규모의 해양 산업 전체에 대해 가장 일반적인 식별 요구 사항을 충족시키는 솔루션을 만드는 것이 필요하나, 모든 솔루션이 소규모 선박에서부터 다국적 기업에 이르는 모든 가능한 사용자 시나리오를 지원해야 하므로, 간단한 부분은 아니다. 이러한 복잡성으로 인하여 향후 몇 년 동안에 걸쳐 여러 마일스톤을 통해 점진적으로 기능이 제공될 예정이다. 여기에는 인증 지원과 같은 기능 뿐 아니라, 해사클라우드가 지원하는 프로젝트의 사용자 요구에 따라 여러 기능 또한 추가될 예정이다.

3.2. Identity 레지스트리의 주요 객체

본 절에서는 해사 신원 레지스트리와 상호 작용하는 다양한 객체에 대해 살펴보고자 한다.

신원 관리 및 보안은 매우 복잡하고 포괄적인 분야이며, 필수적이지 않거나 불필요한 기능은 가능한한 제한할 필요가 있다. 여기서 불필요한 기능이란, 예를 들어, 엑세스 권한이 필요하지 않은 엔티티의 정보 관리가 될

수 있으며, 또한, 보안에 대한 목적을 두지 않고 엔티티에 대한 정보를 유지하고 있는 경우도 들 수 있다.

필수적이지 않은 정보를 제외하는 주요 이유는 신원 정보 레지스트리에서는 등록된 정보를 상세하고 지속적으로 유지하고 있기 때문이다. 예를 들어, 선박에 대한 지리적 위치 뿐만 아니라, 노선이나 화물과 같은 상세정보가 같이 유지 관리되는 경우를 들 수 있다. 따라서, 정보 관리에 대한 범위가 필수적으로 고려될 필요가 있다.

3.2.1. 조직

해사클라우드에서의 조직은 집단적 목표를 가지고 외부 환경과 연결된 기관, 회사, 또는 협회와 같은 단체이다. 예를 들면, IMO, IALA, IHO 같은 국제기구 및, 미국 연안 경비대(US Coastguard), 스웨덴 해사 행정부(Swedish Maritime Administration)와 같은 조직뿐만 아니라 일반 상업 회사까지도 포함될 수 있다.

3.2.2. 선박

선박은 사람이나 물건의 운송에 사용되는 해양에 떠다니는 모든 객체가 될 수 있다. 해사클라우드에 선박을 등록해야 하는 주된 이유는 선박에 디지털 인증서를 발급받을 수 있으므로 선박간 보안 통신이 가능해 지며, 문서에 대한 디지털 서명도 가능하기 때문이다.

선박 인증서에는 이름, MMSI번호, IMO번호, 호출부호 및 가능한 다른 속성이 디지털 인증서의 헤더에 포함된다.

3.2.3. 서비스

여기서 서비스란 디지털 서비스를 의미한다. 예를 들어, 기계 간 통신으로 타 서비스에서 활용 가능한 기상 서비스를 들 수 있다. 사용자 인증이 이루어질 수 있도록, 서비스가 레지스트리에 등록되어야 한다.

3.2.4. 사용자

여기에서 의미하는 사용자란, 서비스를 사용하는 주체, 즉 사람을 의미한다. 일반적으로 사용자는 로그인 시 ID와 패스워드를 사용하게 되므로, 타 객체와는 상호 작용 패턴이 다르다는 점에서 차이가 있다.

3.2.5. 장치

장치는 해사클라우드를 사용하여 인증해야 하지만, 위에 언급된 다른 객체의 범주에 속하지 않는 엔티티를 의미한다. 또한, 여기에서의 장치는 여러 엔티티의 집합이 될 수도 있다. 예를 들어, 등대가 될 수 도 있고, ECDIS, 또는 자체 인증이 필요한 서버일 수도 있다.

3.3. Identity 인증

인증은 시스템에 엑세스하려는 객체의 신원을 시스템이 검증하는 과정을 의미한다. 특히, 엑세스 제어는 일반적으로 리소스에 대한 엑세스를 요청하는 사용자의 ID를 기반으로 이루어지므로, 인증은 효과적인 보안에 있어 필수적인 요소이다. 사람이나 물건의 신분을 밝히는 행위를 말하는 신분증과는 달리, 인증은 제공된 정보를 통해 신원을 실제로 확인하는 과정을 의미한다. 웹 사이트가 제공하는 디지털 인증서로 웹 사이트의 진위 여부를 확인하거나, 신원 확인 문서의 유효성을 확인하는 작업이 포함될 수 있다.

인증의 방법은 일반적으로 알고 있는 것과 같이 사용자가 알고 있는 것, 가지고 있는 것, 사용자의 고유한 특징의 세가지 범위로 가능하다. 현재 해사클라우드에서는 두가지 측면에서 인증이 이루어지며, 일반 사용자에게는 아이디/패스워드 기반의 인증으로 처리되며, 시스템 객체에 있어서는 디지털 인증서의 소유 확인에 대한 인증에 중점을 두고 있다. 본 절에서는 신원 레지스트리에서의 인증 방법에 대해 살펴본다.

3.3.1. Maritime PKI 기반의 M2M 통신

공개키 인프라(PKI)는 디지털 인증서를 작성, 관리, 배포, 사용, 저장 및 해지하고 공개 키 암호화를 관리하는데 필요한 일련의 하드웨어, 소프트웨어, 사람, 정책, 및 절차이다. 이를 통해 조직은 신뢰할 수 있는 네트워킹 환경을 구축하고 유지 및 관리할 수 있다. 보안 M2M 통신을 가능하게 하는 PKI 기반 솔루션을 사용하기 위한 고유한 요구사항은 별도로 존재하지 않는다[6]. 그러나, 가장 일반적으로 사용되는 솔루션 및 소프

트웨어, 모범 사례에 따라 해사클라우드에서는 M2M 통신을 위해서 X.509 표준을 기반으로 한 PKI 사용을 채택하였다.

PKI 아키텍처의 핵심은 디지털 인증서를 발행하는 엔티티인 PKI CA(Certificate Authority)이다. 인증서의 이름이 지정된 주체에 의해 공개 키의 소유권을 인증하는 디지털 인증서로써, 일례로 특정 선박에 발급된 인증서를 소지한 사람이 서명했음을 증명할 수 있는 선박 인증서를 만드는 경우를 들 수 있다.

현재의 해사클라우드 버전에서는 모든 인증서를 발급할 책임이 있는 단일 하위 CA가 있으며, 이 하위 CA는 해사클라우드의 신원 레지스트리에 존재한다. 그러나 이는 향후에 다른 PKI 계층 구조 디자인을 지원할 수 있도록 변경될 수도 있다.

CA의 가장 중요한 기능은 디지털 인증서를 발급하는 것이며, 이는 인증서의 지정된 주체로 공개키의 소유권을 인증한다. 이러한 신뢰 관계 모델에서 CA는 신뢰할 수 있는 제3자로, 인증서의 주체(소유자)와 인증서에 의존하는 당사자가 모두 신뢰할 수 있다.

해사클라우드의 경우, 이러한 인증서는 일반적으로 인터넷을 통한 해상 행위자 간의 안전한 연결을 위해 사용되며, 대상 서버의 경로에 있는 악의적인 사용자가 실제 대상인 것처럼 위장하지 않도록 man-in-the-middle 공격에 대비할 수 있는 인증서가 필요하다. 클라이언트는 보안 연결을 설정하기 전에 CA 인증서를 사용하여 서버 인증서의 CA 서명을 확인한다. 마찬가지로, 서버는 클라이언트의 인증서 연결을 허용하기 전에 클라이언트의 인증서를 검사할 수 있다. 예를 들어, 선박에 대한 새 인증서를 발급하려면 해당 선박을 소유한 조직의 관리자가 Maritime Cloud Portal에 로그인하여 새로운 인증서 발급을 위한 기능을 사용해야 한다. 발급되는 인증서에는 선박 이름, 소유자, MMSI 및 IMO 번호와 같은 기타 속성에 대한 정보가 포함된다. 그러나, 현재의 해사클라우드는 가입 당시 조직이 수락되어 있어야 한다는것 이외에는 이러한 정보의 유효성을 검증하지 않고 있다. 현재까지는 참여 당사자의 수가 상대적으로 적기때문에 큰 문제가 발생할 소지는 적으나, 향후에 더 많은 조직이 추가될 경우에 대비할 필요가 있을 것이다.

3.3.2. 사용자 로그인

3.3.1에서는 M2M에서 사용하는 디지털 인증서에 대해 살펴보았다. 이러한 관점에서, 일반 사용자가 자신을 인증하기 위해서는 디지털 인증서를 사용하는 것은 기술적으로는 문제가 없으나, 실용적으로는 여러 문제가 존재한다. 즉, 기계간 통신 과정에서는 하드웨어의 구성 변경이 거의 존재하지 않으므로 큰 문제가 없으나, 인간인 사용자가 로그인할 경우는 엑세스가 이루어지는 컴퓨터 또는 휴대폰 등에 항상 인증서가 있어야 한다는 문제가 존재한다. 이는 해사클라우드의 활용성을 심각하게 떨어뜨릴 수 있게 되므로, 현재의 해사클라우드에서는 사용자 인증 과정에서는 디지털 인증서를 고려하지 않고 아이디/패스워드 기반의 인증 방식에 중점을 두는 측면이 있다.

한편, 해사클라우드에서는 연합(Federation)이라는 개념이 존재하며, 연합은 사람의 전자 신원 및 속성에 고유한 신원관리 시스템을 연결하는 수단이 된다. 예를 들어, 해운회사가 해사클라우드의 객체로 표시되는 방식으로, LDAP 또는 Active Drectory를 통해 모든 사용자를 해사클라우드에 노출시킬 수 있다. 따라서, 연합을 통해 해사클라우드에서 사용자를 직접 관리해야 하는 번거로움을 피할 수 있다.

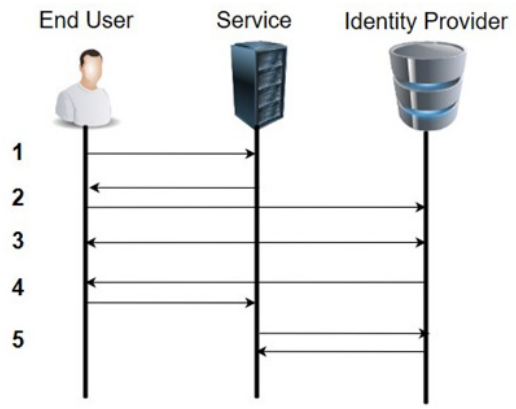
보안 도메인간 인증 및 권한 부여 데이터를 교환하기 위한 몇가지 표준이 존재한다. 특히, 여기에는 OpenID Connect라는 새로운 표준이 있으며, 이는 검증된 OAuth2 표준을 기반으로 구축되었다. 이는 Google 및 Microsoft와 같은 여러 대기업의 지원을 받고 있는 상황이다.

OpenID Connect의 작동 방식은 그림 1과 같다.

OpenID Connect에는 해사클라우드의 사용자 연합에 유용하게 사용할 수 있는 여러 장점이 존재한다. 먼저, 이는 이미 존재하는 공개표준 (OAuth2, JWT)를 기반으로 한다는 것이며, 두번째로, 웹사이트/웹서비스 및 기본 스마트폰 응용 프로그램 모두를 인증하는데 사용될 수 있다는 장점이 있다. 마지막으로, 이미 오픈소스와 상업용으로 많은 구현이 되어있다는 장점이 존재한다.

그림 1에 나타난 OpenID Connect 인증의 세부 설명에 해당하는 부분은 그림 2와 같다.

OpenID Connect는 실제 로그인을 사용자 조직에 위임하게 되므로, 사용자는 사용자가 실제로 누구인지 주



〔그림 1〕 OpenID Connect 인증 흐름[7]

1. 사용자는 웹 기반 서비스(신뢰 당사자)를 열고, “Maritime ID 로그인”을 클릭한다.
2. 사용자는 로그인 정보를 등록한 ID 공급자로 사용자를 리디렉션한다. 여기에는 예를들어, 그가 일하는 조직의 ID 공급자 설정을 들수 있다.
3. 사용자는 회사의 아이디/패스워드를 기반으로 로그인한 후, 정보를 신뢰 당사자에게 다시 전송하는 것에 동의한다.
4. 신원 제공자는 인증 코드를 사용하여 사용자(브라우저)를 신뢰 당사자에게 다시 리디렉션한다.
5. Replying Party는 신원 제공 기관에 인증 코드의 유효성을 검사하도록 요청한다. ID 공급자는 사용자에 대한 정보가 들어있는 JWT 토큰 세트로 응답한다.

〔그림 2〕 OpenID Connect 인증 세부 설명

장할 수 있는지 여부를 확인하는 방법에 대해 자체적인 제어가 가능하다. 즉, 사용자 아이디/패스워드 뿐만 아니라, 2 factor 인증 또는 생체 인식도 사용할 수 있다.

3.4. Identity 권한 부여

신원 관리에서의 또다른 핵심 요소는 특정 신뢰할 수 있는 ID에 부여된 사용 권한 집합을 결정하는 것이다. 실질적으로 시스템이 사용자의 신원을 파악하면, 시스템은 사용자의 권한에 대해 판단이 가능하다. 권한 부여는 사용자 신원만으로도 결정될 수 있지만, 대부분의 경우는 역할, 제목, 플래그 상태 등과 같이 사용자에 대한 추가 속성도 필요한 경우가 많다.

권한 부여는 일반적으로 엑세스 중인 응용 프로그램 또는 서비스에 의해 로컬로 전달되거나, 혹은 응용프로그램 및 서비스의 위치에 관계 없이 인증정책 결정을 중앙집중화하는 두가지의 방법이 있다.

권한은 로컬상의 데이터베이스에 사용자 권한을 저장하는 것으로 엑세스 중인 응용 프로그램에서 수행이 가능하므로, 현재의 해사클라우드에서는 권한 부여에 있어 중앙집중화 방식보다는 로컬상의 사용자 권한 정책 부여 방식을 우선적으로 고려하고 있다.

일반적으로 역할기반 엑세스제어(RBAC) 기술이 많이 사용되며, 역할 권한, 사용자 역할 및 역할 관계와 같은 RBAC의 구성 요소를 사용하면 사용자에 대한 자격 할당을 용이하게 수행할 수 있다. 그러나, 해사클라우드 시스템에 RBAC을 채택할 경우, 몇가지 문제가 발생할 수 있다. 예를 들어, 누가 역할을 정의하고 글로벌 역할을 담당할지에 대한 부분이다. 또한, 특정 서비스 또는 특정 조직에 국한할지에 대한 부분도 문제가 될 수 있다. 예를 들어, 관리자 역할은 특정 조직의 권한과 다른 조직의 권한을 수반할 수 있으며, 이러한 이슈는 현재까지도 논의되고 있는 사항이다.

Ⅳ. 결 론

해사 환경의 안전을 보장하기 위해서는, 현재 IMO 및 해양수산부가 추진중인 e-Navigation의 성공적 안착이 필수적으로 요구되는 상황이다. 특히, 해사클라우드는 e-Navigation의 핵심 통신 인프라가 되는 기반기술이며, 해사 통신 환경이 악의적인 공격에 노출되지 않도록 해사클라우드 보안은 필수로 고려되어야 한다. 본 고에서는 해사클라우드에서의 인증 및 권한 부여에 필요한 Identity 관리 기술에 대해 살펴보았다. 이를 위해 2장에서는 해사클라우드의 등장 배경과 주요 서비스에 대해 살펴보았고, 3장에서는 해사클라우드에서의 Identity 관리 기술에 대해 살펴보았으며, 해당 장에서 구체적인 Identity 레지스트리의 주요 객체와, Identity 인증 방법, Identity 권한에 대한 동향에 대해 살펴보았다. e-Navigation은 2020년 시행을 목표로 국내외로 추진되고 있으며, 해사클라우드는 e-Navigation의 핵심 기술로서 안전한 해사 환경에 큰 역할을 수행할 수 있기를 기대해 본다.

참 고 문 헌

[1] Donghyeok Lee, Namje Park, “A Proposal of SH-Tree Based Data Synchronization Method for Secure Maritime Cloud”, Journal of The Korea Institute of Information Security & Cryptology, 26(4), 2016, Aug.

[2] Gae Il An, Kwangil Lee, Byung Ho Chung, “Analysis of Cyber-Security Threat on Maritime Cloud proposed as Maritime Communication Framework,” In Conference Proceedings of Korea, Information Science Society, pp.892-893, Dec. 2015.

[3] Maritime Cloud Identity Platform, http://developers.maritimecloud.net/identity/index.html

[4] Efficient 2 Project, “http://efficiensea2.org/beta-release-of-the-maritime- cloud-and-balticweb/

[5] https://www.iho.int/mtg_docs/com_wg/ SNPWG/ SNP WG17/SNPWG17-9.3 _An%20overview%20of%20the%20Maritime%20Cloud%20-%20input%20to%20IMO%20e-nav%20CG.PDF

[6] Namje Park, Jungsoo Park, and Hyoungjun Kim, “Inter-Authentication and Session Key Sharing Procedure for Secure M2M/IoT Environment”, International Information Institute(Tokyo) Informa- tion, Vol. 18, No. 1, pp. 261-266, Jan. 2015.

[7] Maritime Cloud Development Forum, “Identity Management and Cyber Security”, IALA, 2016

〈저 자 소 개〉

이 동 혁 (Donghyeok Lee)
정회원

2007년 2월 : 동국대학교 전자상거래기술전공 공학석사
2007년 6월~2008년 5월 : 한국전자통신연구원 정보보호연구단 연구원
2008년 11월~2015년 6월 : KT 플랫폼개발단 과장
2015년 9월~현재 : 제주대학교 컴퓨터교육전공 박사과정
관심분야 : 해사클라우드 보안, IoT 보안, 데이터베이스 보안

박 남 제 (Namje Park)
종신회원

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월~2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월~2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc, WINMEC 연구센터 Staff Researcher
2010년 1월~2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월~현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수
2010년 9월~현재 : 과학기술사회(STS)연구센터장, 정보영재 주임교수, 초등교육연구소장
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등