한국시뮬레이션학회 논문지
Vol. 24, No. 3, pp. 77-87 (2015. 9)
http://dx.doi.org/10.9709/JKSS.2015.24.3.077
ISSN 1225-5904

국방 재사용 자원의 클라우드 저장소를 위한 계층형 보호 시스템

박찬종 · 한승철 · 이강선*

A Layered Protection System for a Cloud Storage of Defense M&S Resources

Chanjong Park · Seungchul Han · Kangsun Lee*

ABSTRACT

Defense M&S (Modeling & Simulation) is utilized as a realistic method to analyze MOE (Measure of Effectiveness) of weapon systems by modeling weapons and their operational environment on the computer, and simulating them under various war scenarios. As weapon systems become complex in their structure and dynamics, model engineering are experiencing difficulties to construct simulation models on a computer. A model repository helps model developers to save model development time and cost by systematically storing predefined and already validated models. However, most repositories for Defense M&Shave not been successful partly due to limited accessability, vulnerability to security threats, and low level of dependability. In this paper, we propose W-Cloud (Weapon Cloud), a cloud model repository for reusing predefined weapon models. Clients can access W-Cloud on any platforms and various devices, yet security and confidentiality concerns are guaranteed by employing multi-tier information protection mechanism.

Key words : Simulation-Based Weapons System Analysis, Model Repository, Layered-Protection, Cloud Storage

요 약

국방 M&S(Modeling & Simulation) 분야는 컴퓨터상에 모의 전장 환경 및 무기 모델을 구축하고 다양한 시나리오에 의해 시뮬레이션을 수행하여 무기체계의 효과도를 분석하는 현실적인 수단으로 이용되고 있다. 그러나, 무기체계의 구조 및 행위가 복잡해짐에 따라 이를 시뮬레이션 모델로 만드는 과정이 어려워지고 있다. 모델 재사용 저장소는 시뮬레이션 모델 구축에 필요한 비용을 절감하기 위해 기존에 개발 및 검증된 모델을 저장하고 있다. 그러나 기존의 재사용 저장소들은 특정 플랫폼 및 환경에서만 운용되어 사용자 층에 제한이 있으며, 보안 및 무중단 서비스를 위한 메커니즘이 미흡하여 무기체계 모델과 같은 보안 및 신뢰성이 필요한 모델을 저장하기에는 한계가 있다. 본 논문에서는 무기체계 모델의 재사용을 장려하기 위한 클라우드 저장소인 W-Cloud (Weapon Cloud)를 구축하여 다양한 플랫폼 및 환경에서 활용될 수 있도록 하였다. 또한, 계층형 정보 보호 및 기밀성 보장을 통해 무기 모델의 재사용 과정에서 생길 수 있는 보안상의 문제를 효과적으로 해결할 수 있도록 하였다.

주요어 : 시뮬레이션 기반 무기체계 분석, 모델 저장소, 계층형 보안, 클라우드 저장소

1. 서 론

시뮬레이션 기반 무기체계 분석은 무기체계의 효과도를 분석하기 위해 무기 및 전장 환경 모델을 구성하고 해당 무기 체계가 활용되는 다양한 시나리오를 모의 실험하는 일련의 작업을 포함한다. 이때 무기체계 모델을 컴퓨터상에 구축하는 것은 많은 시간과 비용이 필요하며, 기존에 개발된 모델을 재사용하고자 하는 요구가 있어왔다. 모델 저장소는 개발 및 검증이 완료된 모델들을 체계적으로 저장 및 관리 하여 이들의 재사용을 향상시키는 것을 목표로 하며, 국방 M&S 분야뿐만 아니라 다양한 응용 분야에서 운용되고 있다[1-6]. 그러나 시뮬레이션 기반 무기체계 효과도 분석 시 활용될 수 있는 모델 재사용 저장소

Received: 24 August 2015, **Revised:** 4 September 2015, **Accepted:** 10 September 2014

***Corresponding Author:** Kangsun Lee
E-mail: ksl@mju.ac.kr
교신저자소속(영문으로 기재요망)

구축에 관련된 연구는 매우 제한적으로 이루어지고 있으며, 구축된 저장소들은 대부분 특정 플랫폼 및 환경에서만 운영되어 사용자층에 제한이 있을 수 있다. 또한, 무기체계 효과도 분석을 위한 무기 모델들은 보안이 필요한 중요한 자료들이 존재하므로, 저장소 운용 시스템에 대한 예상치 못한 공격이나 침입행위가 발생하거나 또는 시스템 결함이 발생할 경우에도 무중단 될 수 있도록 의존성(dependability)을 보장해야 한다[5].

최근 연구되고 있는 클라우드 저장소는 인터넷을 활용할 수 있는 환경이라면 어디서든 접근이 가능하다는 특성으로 인하여 폭넓은 사용자층을 제공할 수 있으며, 재사용 저장소 구축 비용이나 유지비용 절감을 가능하게 한다. 클라우드 컴퓨팅 환경은 이러한 장점이 있지만 동시에 개인 PC와는 달리 외부의 접속을 허용해야 하는 태생적 속성 때문에 보안에 취약하다는 문제점이 있다. 본 논문에서는 무기체계 효과도 분석 시 기존 무기 모델의 적극적인 재사용을 장려하기 위해 클라우드 기반 저장소를 구축하고, 저장소에 대한 보안을 강화하기 위해 다음과 같은 계층형 정보 보호 방안을 제시한다.

- 첫째, 무기체계 모델 재사용 저장소에 대한 해커의 침입을 예방하기 위하여 사용자 인증 시스템을 구축하며, 데이터에 대한 접근 권한을 부여하여 인증된 사용자에게도 제한된 접근을 가능하도록 한다.
- 둘째, 해커들의 패턴을 분석한 룰에 의해 작동하는 IDS(Intrusion Prevention System)[8] 프로그램을 사용하여 예방계층에서 방어하지 못한 해커의 침입을 탐지한다.
- 셋째, 상기 두 계층으로 방어하지 못한 공격에도 지속적인 서비스를 제공하기 위하여 데이터들을 백업하고 스냅샷 정보를 유지한다[9-10].
- 넷째, 공개키 암호화 방식과 비밀키 암호화 방식의 조합으로, 데이터에 대한 기밀성(confidentiality을 유지한다[6-7].

본 논문에서는 상기한 정보 보호 방안들을 적용하여 W-Cloud(Weapon Cloud)를 구축하였다. W-Cloud는 무기체계 모델들의 재사용을 지원하기 위해 등록(registration), 검색(search), 업로드(upload) 및 다운로드(download) 서비스를 제공하며, 계층형 정보보호를 적용하여 보안상의 문제점을 해결할 수 있도록 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해 알아보고, 3장에서는 무기체계 시뮬레이션 모델 저장소가 제공해야 하는 보안상의 요구사항을 식별하고 이를 해결할 수 있는 아키텍쳐를 제안한다. 4장에서는 W-Cloud의 구현 내용을 소개하며, 분석 및 실험을 통해 보안 요구 사항 만족 여부를 검증한다. 5장에서는 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

2.1 M&S 자원 저장소

국방 분야의 M&S 활동은 무기 및 환경 모델의 복잡성으로 인해 개발 시간과 노력이 많이 필요하며, 신뢰성과 정확성 또한 타 분야에 비해 더욱 강조된다. 이에 따라 이미 검증된 기존 자원들의 효율적인 저장 및 관리를 지원하는 저장소에 대한 연구가 진행되었다.

컴포넌트 기반 소프트웨어 개발 방법론은 개발된 컴포넌트를 단위로 재사용하여 새롭게 소프트웨어를 만드는 방법으로, 무기체계 분석 시뮬레이션의 경우 해당 무기 전문가들이 컴포넌를 개발하고 다른 소프트웨어 개발에 그 컴포넌트를 재사용함으로써 생산성을 높일 수 있다. 유도무기체계에 대한 컴포넌트들을 개발하여 이들의 조합으로 새로운 모델을 만들기 위한 컴포넌트 관리도구에 대한 연구가 제한적으로 이루어지고 있으나[1-2], 대부분 기존 저장소들은 재사용 가능한 국방 자원들을 개별적으로 저장 및 관리하여 특정 플랫폼 및 실행 환경에 국한된 재사용을 지원한다. 그러나 대규모 무기체계에 대한 효과도 분석의 경우는 다양한 실행환경 및 플랫폼을 사용하는 지리적으로 산재된 모델러 및 분석가의 협동 모델링 과정을 포함하므로, 구축된 저장소를 전사적으로 운영하는데 어려움이 있다.

최근 등장한 클라우드 저장소인 OB-Cloud(Ontology Based Cloud)는 저장된 자원의 전사적인 재사용을 지원할 수 있다[3-4]. OB-Cloud는 국방 M&S의 자원을 저장 및 관리하고, 의미기반 검색을 지원하는 클라우드 저장소로서, 사용자는 클라우드를 통해 어디에서나 접근할 수 있다는 장점을 제공하나 보안에 대한 대비책은 마련되지 못하였다.

2.2절에서는 보안의 강화와 무중단시스템을 구축하고자 본 논문에서 적용한 계층형 정보보호 기술에 대하여 알아보도록 한다.

2.2 계층형 정보보호

무기체계 모델을 재사용 하기 위한 중요한 서비스이효율적으로 이루어지기 위해서는 의존성(dependability)이

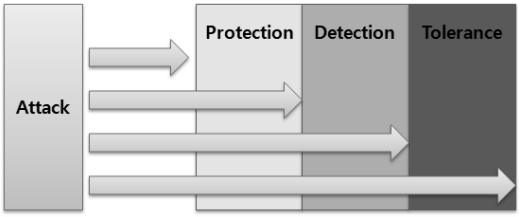

Fig. 1. Layered information protection

만족되어야 한다[11]. 의존성은 사용자가 실제로 시스템을 사용할 수 있는 시간인 가용성, 사용자의 요구에 시스템 기능이 적정하게 수행하는지에 대한 신뢰성, 데이터나 프로그램을 권한이 없는 사용자가 이용할 수 없게 하는 보안성 등을 보장할 때 달성 될 수 있다. 의존성의 특성을 해치는 기본적인 원인은 시스템의 손상인데, 시스템의 결함 또는 해커의 공격이 시스템 손상을 초래하게 된다. 침입 감내는 시스템의 손상에도 지속적인 서비스를 제공하기 위한 일련의 활동으로, 계층형 정보 보호는 침입 감내를 위해 현재 널리 사용되고 있는 개념이다. Fig. 1은 계층형 정보보호의 개념을 보여준다.

계층형 정보보호는 3 계층으로 이루어진다. 첫 번째 계층으로서, 예방계층(Protection Layer)은 해커들의 공격으로부터 침입을 방지하기 위한 계층이다. 두 번째 계층인 탐지계층(Detection Layer)은 예방계층에서 미처 방어하지 못한 공격에 대해 침입을 탐지하기 위한 계층이다. 마지막 계층인 감내계층(Tolerance Layer)은 앞에서 언급한 두 계층으로 방어되지 않는 경우를 대비하여, 지속적인 서비스를 제공하고자 존재한다. 본 논문의 W-Cloud는 계층형 정보보호의 개념을 적용하여 3단계에 걸쳐 저장된 무기체계 모델에 대한 보안을 보장한다.

3. W-Cloud

본 장에서는 먼저 국방 M&S 자원 재사용 저장소에 필요한 보안 요구사항을 명세하고, 이를 실현할 수 있도록 W-Cloud의 아키텍처를 정의한다. 또한, W-Cloud 아키텍처를 이루는 주요 보안 모듈에 대한 설명을 한다.

3.1 W-Cloud 보안 요구사항

클라우드 기반으로 무기 시뮬레이션 모델의 재사용에 필요한 등록, 검색, 다운로드, 업로드 등의 서비스를 제공하는 저장소를 구축할 때 갖추어야 할 보안 요구 사항은 다음과 같이 정의될 수 있다.

- 기밀성(Confidentiality): 시뮬레이션 기반 무기체계 효과도 분석은 무기체계 모델을 자연 환경 및 교전 환경 모델과 컴퓨터상에 그대로 모의함으로써 해당 모델의 전투 효과도를 분석하게 된다. 이때 무기체계 효과도 분석을 보다 현실에 가깝게 도출하기 위해, 무기 체계 시뮬레이션 모델에는 실제 무기가 지니는 속성 및 성능치 (예. 최대 속력, 최대 탐지 거리, 최고 잠항 깊이)를 그대로 활용하게 된다. 또한, 특정 무기의 제어 알고리즘 (예, 미사일 유도 알고리즘, 전투기 회피 알고리즘)을 그대로 메소드로 구현하게 되므로, 해당 정보가 외부에 유출되었을 경우 군사 보안상 많은 위험을 초래할 수 있다. 따라서, 무기체계 시뮬레이션 모델의 내용에 대해 기밀성이 보장되어야 한다.
- 접근제어(Access Control): 국방 자원은 각 자원이 포함하고 있는 정보의 비밀 정도를 고려하여 1등급, 2등급, 3등급 및 대외비 등으로 보안 등급이 부여된다. 또한, 보안 자료를 취급하는 사람에게도 접근 등급이 부여되어 등급별로 열람, 수정 등의 권한이 주어지게 된다. 무기체계 시뮬레이션 모델의 경우 역시, 모델링된 무기체계 시스템 자체의 보안 수준, 또한 해당 모델을 재사용하고자 하는 사용자의 보안 등급을 고려하여 접근 여부를 결정할 수 있어야 하며, 만약 권한이 없는 사용자가 저장소를 접근하거나, 권한이 있는 사용자의 경우도 부여되지 않은 권한으로 재사용 하고자 하는 경우에 대한 제어가 이루어져야 한다.
- 무결성(Integrity): 클라우드 저장소에 저장된 무기체계 시뮬레이션 모델에 대한 재사용 서비스(자원 등록, 재사용 가능 자원 탐색, 자료 업로드 및 다운로드 등)를 다양한 사용자에 제공함에 있어, 사용자가 의도하지 않은 방식으로 데이터를 변경하는 상황을 방지 하여, 저장된 무기체계 시뮬레이션 모델에 대한 무결성을 보장하여야 한다.
- 가용성(Availability): 해커의 공격 혹은 천재지변에 따른 서비스 중단을 최소화하기 위한 부가적인 정책이 필요하다. 즉, 무기체계 시뮬레이션 모델 저장소의 모든 서비스들이 중단 없이 실행되도록 장치를 마련하여 저장소의 가용성을 높여야 한다.

본 논문에서는 클라우드 기반 무기체계 시뮬레이션 모델 저장소를 구현함에 있어 이상과 같은 보안적 요구사항을 고려하였다.

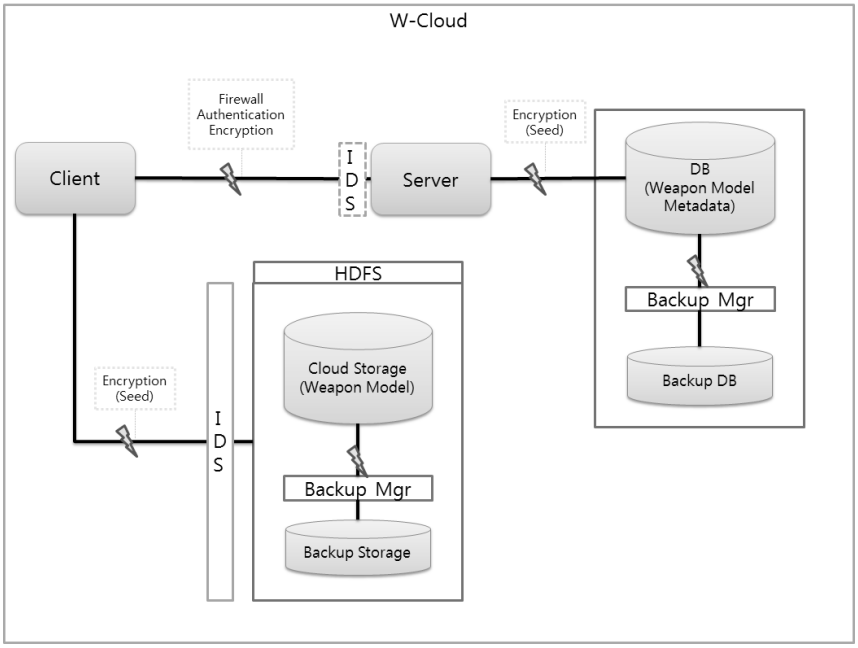

Fig. 2. W-Cloud: Architecture

3.2 W-Cloud 아키텍처

Fig. 2는 상기한 보안 요구사항을 실현하기 위한 W-Cloud의 아키텍처를 보인다. W-Cloud는 Client, Server, HDFS (Hadoop File System)의 3가지 요소로 구성된다.

Server는 HDFS에 저장될 재사용 모델들의 카탈로그를 별도의 DB에 유지하는 역할을 한다. 이 카탈로그에는 재사용 가능 모델을 검색할 때 필요한 메타정보(예. 무기 타입, 주요 속성, 작성 정보, 실제 모델이 저장되어 있는 HDFS상의 디렉토리 및 파일이름 등)가 담겨있기 때문에 다양한 침입으로부터 카탈로그를 보호해야 한다. Server는 이를 위해 사용자 인증을 지원하며, 암호키 제공자로서 중개자적 역할을 수행한다.

사용자는 Client 프로그램을 사용하여 Server로부터 사용자 인증을 받고, 재사용을 위한 서비스를 제공받는다. Client와 Server 사이의 통신인터페이스는 XML로 채택하였으며, XML 정의는 Fig. 3과 같다.

Client 및 Server에게 호출하고자 하는 함수명을 최상위 태그로 정의하였고, 하위 태그로서 전송하고자하는 속성명 및 속성값로 데이터 셋을 정의하도록 하였다. Fig. 3에서 보듯이 로그인의 경우 Server의 Login 함수를 요청을 하고, 파라미터로 Id 및 Password 값을 넘기게 된다.

W-Cloud는 예방계층을 통해 인증된 사용자만 재사용

XML정의
<?xml version='1.0' encoding='UTF-8'?> <FunctionName> <AttributeName>AttributeValue<AttributeName> </FunctionName>
예시
<Login> <Id>pcj</Id> <Password>1234</Password> </Login>

Fig. 3. W-Cloud: Interface

자원을 검색할 수 있도록 한다. 탐지계층은 IDS(Intrusion Detection System)을 활용하여 예방계층에서 방어하지 못한 공격에 대하여 탐지를 수행한다. 마지막으로, 감내계층은 무기 모델 자원을 백업하여 해커들의 공격 등으로 시스템이 파괴되었을 시에도, 백업했던 자원을 복구함으로써 지속적인 서비스가 가능하도록 한다. 이를 위해 Server와 Client 모두 Backup Manager를 운영한다. 또한, 기밀성을 보장 하고자, Client와 Server간의 통신은 공개키 암호화 방식인 SSL(Secure Socket Layer)을 사용하였으며, 국방자원데이터의 보호를 위해 한국인터넷진흥원에서 개발한 블록 암호화기법 SEED[7]를 사용하여 불법적인 사

용자가 비정상적인 루트로 얻어진 정보들을 해독하지 못하게 하였다.

4. W-Cloud 구현

Table 1은 W-Cloud의 구현 환경 및 보안 시스템 개발 환경을 요약한 것이다.

이번 장에서는 W-Cloud를 이용하여 모델을 등록시키고, 재사용 가능한 모델을 검색하여 자신의 작업환경으로 download하는 과정에서 보안적 요구사항을 어떻게 실현하였는가를 3개의 계층별로 보인다.

4.1 침입예방 계층

W-Cloud는 침입예방 계층을 위하여 방화벽과 접근제어를 구현하였다.

먼저, W-Cloud는 재사용 가능한 모델들의 정보를 기록해놓은 네임노드를 리눅스에서 제공하는 ufw를 활용하여 특정 아이피 및 포트만을 허용하는 방화벽을 구축하였다. 다음은 네임노드에서 사용된 방화벽 룰을 보인다.

```
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
9000                       ALLOW       Anywhere
```

Table 1. W-Cloud: Configuration

저장소 구성			
컴퓨터 종류	대수	H/W (CPU / HDD / RAM)	OS
NameNode	1	Quad 2.33GHz / 500G / 4G	Ubuntu 10.04 LTS
Secondary Node	1		
DataNode	3		
Client	1	i5-3320M 2.60GHz / 300G / 8G	Windows7
Server			

보안시스템 개발 환경	
Development Tool	Eclipse Juno
JAVA version	JDK 1.7
Database	HSQL
IDS	Snort 2.9.7.0 Snortrules-snapshot 2956
SSL(TLS)	javax.net.ssl package
SEED	SEED 1.0

네임노드로 접속하기 위하여 사용된 포트는 9000번이며, 네임노드와 데이터노드는 ssh로 통신하므로 22번 포트도 허용하였다.

또한, 사용자 인증 및 데이터에 대한 등급별 열람 등급을 부여함으로서 침입예방 계층을 구축하였다. 인증을 받지 못한 사용자는 W-Cloud 서비스를 이용하지 못하며, 인증을 받더라도 데이터에 대한 열람 등급 및 ReadWrite 권한이 부여됨으로 권한별 데이터 관리가 가능하다. Table 2는 데이터에 대한 열람 등급 과 등급별 암호화 여부이다.

데이터의 열람 등급은 0~3까지이며, 모든 데이터는 SEED 알고리즘을 통하여 암호화 되어 저장하지만, 0 등급인 경우에는 대외비와 같이 기밀 사항 정도는 아니나 일반에 공개되면 곤란할 정도의 보안을 유지할 데이터 및

Table 2. W-Cloud: Access control list

RW / 열람등급	ReadOnly	ReadWrite	군사기밀
0	비암호화	비암호화	대외비 (Restricted Document)
1	암호화	암호화	군사 3급 비밀 (Confidential)
2	암호화	암호화	군사 2급 비밀 (Secret)

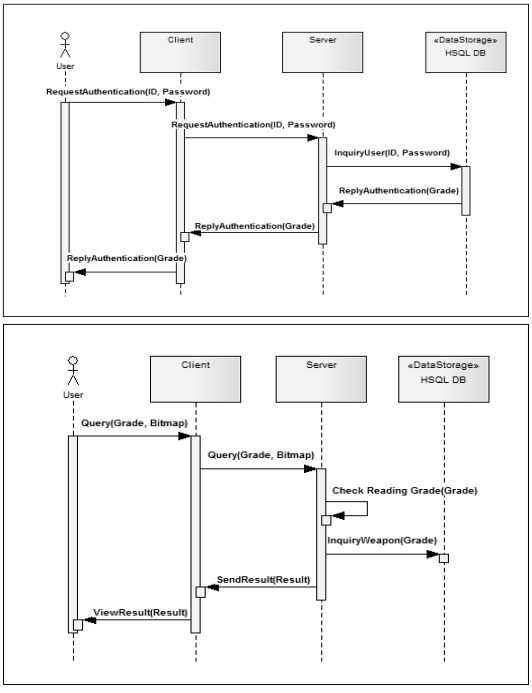

Fig. 4. Secure retrieval in W-Cloud

Table 3. Retrieved models based on access control

미사일 명칭	미사일 열람 등급	검색 결과
FGM-148 재블린	2	O
신궁(KP-SAM)	2	O
미스트랄	3	X
9K38 이글라	3	X
BGM-71 TOW	1	O
9K115-2 메티스-M	0	O
천마(KSAM-1)	3	X
KM-SAM	3	X
MGM-140 ATACMS Block 1	3	X
현무-2	2	O
현무-1	0	O
MGM-140 ATACMS Block 1A	1	O

파일로 취급하고 암호화를 하지 않는다.

Fig. 4는 사용자 등급에 따른 재사용 자원의 검색 과정을 보인다. 사용자는 Client 프로그램을 통하여 Server에 사용자 인증을 요청한다. Server는 사용자 정보 DB를 조회하여 사용자 인증을 거친 후 사용자에게 데이터에 대한 열람 등급을 부여한다. 사용자는 Server에 국방 M&S 자원에 대한 질의를 요청하고, Server는 사용자의 열람 등급과 무기모델의 열람 등급을 비교하여 사용자의 열람 등급에 맞는 데이터를 검색하여 준다. 인증이 완료된 사용자는 Client를 통하여 무기모델에 대한 질의를 요청하게 된다. 사용자 질의를 받은 Server는 무기모델을 조회하기 전에 사용자의 열람등급을 확인하고, 사용자에게 맞는 무기모델 결과 리스트 Client로 보내주면 사용자는 이를 통하여 무기모델 결과를 열람할 수 있다.

예를 들어 미사일 효과도 분석 시뮬레이션을 수행하기 위해 재사용가능한 미사일 모델을 검색한다 하자.

미사일 모델들의 열람 등급이 0~3까지 존재한다고 하였을 때, 열람 등급이 2등급인 사용자는 질의를 통하여 Table 3과 같은 결과를 가져 오게 된다.

사용자는 무기모델의 열람 등급이 2 이하 데이터에 대해서만 결과를 볼 수 있다. W-Cloud에서는 이상과 같은 2 단계에 걸친 인증으로 불법적인 외부의 접근을 최소화하고 정보보호를 강화하였다.

4.2 침입탐지 계층

IP나 Port를 기준으로 비정상 트래픽을 차단하는 것이 방화벽이라면 또 하나의 주목받는 보안 솔루션으로는 침입탐지시스템이라 불리는 IDS(Intrusion Detection System)가 있다. IDS는 포트에 대한 정보뿐만 아니라 패킷의 데이터까지 분석하여 정상적인 트래픽 여부를 결정하여, 로그에 남기도록 할 수 있다. W-Drive에서는 공개 IDS프로그램 Snort[8]를 사용한다. Snort는 해커들의 공격이라 판단되는 패턴을 정의하고, 패턴에 의해 공격을 감지하는 룰 기반 침입탐지 시스템이다. Snort의 시그네쳐는 rules라는 확장자를 가진 파일에 기술되어 있으며, 1행에 1개의 시그네쳐를 정의할 수 있다. Snort 시그네쳐의 구조는 다음과 같다.

Rule header							Rule option
action	protocol	IP address	port	->	IP address	port	(option)
처리방법	프로토콜	송신자		패킷방향	수신자		옵션

시그네쳐는 8개로 분류되며 룰 헤더와 룰 옵션의 2가지 섹션으로 구성된다. 룰 헤더에는 처리방법, 프로토콜, IP주소, 포트 번호 등으로 처리 대상으로서 판단 기준을 기술한다. 룰 옵션에는 alert 메시지나 패킷 내부의 조사 내용을 기술한다. 이를 통해 외부의 공격에 대한 탐지가 가능하다. Fig. 5는 최근에 가장 많이 이슈가 되었던 GNU (Gnu's Not Unix) Bash 취약점 탐지를 위하여 Snort Rule에 등록된 룰의 예시이다. TCP 네트워크 프로토콜로 외부에서 내부로 HTTP 포트로 HTTP Hearder 부분에 (){ 문자열이 있으면 탐지를 하라는 의미이다.

Snort는 공식 홈페이지에서 제공되는 룰 이외에도 보안 전문가가 직접 룰을 정의할 수 있기 때문에 다양한 침입 패턴에 대한 보안으로 쉽게 확장될 수 있다. Table 4는 W-Cloud에서 탐지하는 침입 유형을 정리한 것이다. W-Cloud는 snort 공식 홈페이지에서 제공하는 blacklist.rules 외 67개의 룰을 적용하여 다양한 경로에서부터 오는 침입을 탐지한다.

4.3 침입 감내 계층

앞서 소개한바와 같이 W-Cloud의 데이터 저장소는 사

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"Volex-Possible CVE-2014-6271 bash Vulnerability Requested (header)"; flow:established,to_server; content:"() {"; http_header; threshold:type limit, track by_src, count 1, seconds 120; sid:2014092401;)
```

Fig. 5. Snort rule for GNU bash

Table 4. Intrusion detection rules in W-Cloud (parts)

침입경로	rules
Browser	browser-chrome.rules, browser-firefox.rules, browser-ie.rules
File	file-executable.rules,file-flash.rules file-identify.rules, file-image.rules file-java.rules, file-multimedia.rules file-office.rules, file-other.rules,file-pdf.rules
Malware	malware-cnc.rules, malware-other.rules malware-tools.rules
OS	os-linux.rules, os-mobile.rules os-solaris.rules, os-windows.rules os-other.rules
Protocol	protocol-dns.rules, protocol-finger.rules protocol-ftp.rules,protocol-icmp.rules protocol-imap.rules, protocol-nntp.rules, protocol-pop.rules, protocol-rpc.rules protocol-scada.rules,protocol-services.rules protocol-snmp.rules,protocol-telnet.rules protocol-tftp.rules,protocol-coip.rules
PUA	pua-adware.rules, pua-p2p.rules, pua-other.rules, pua-toolbars.rules
Server	server-apache.rules, server-iis.rules, server-mail.rules, server-mssql.rules, server-oracle.rules, server-samba.rules, server-webapp.rules
Policy	policy-multimedia.rules, policy-other.rules, policy-social.rules, policy-spam.rules

용자 정보 및 무기모델의 간략한 메타데이터를 저장한 Server의 DB가 있으며, 무기모델 코드를 저장하기 위한 파일저장소인 HDFS(Hadoop Distributed File System)로 구성되어 있다. 이러한 데이터 저장소들은 시스템에 결함이 발생하더라도 데이터 백업을 통하여 지속적인 서비스를 제공하여야한다. DB와 파일저장소의 백업 과정은 다음과 같다.

- 서버 DataBase: Server의 DB는 사용자 인증을 위하여 사용자 정보를 저장하고 있으며, 무기모델에 대한 키워드 및 의미기반 검색을 지원하기 위하여 간략한 메타데이터를 저장하고 있다. Server의 DB를 백업하기 위하여 Backup Manager라는 프로그램을 통하여 일정한 시간 간격으로 DB 백업이 가능하다. Fig. 6은 Backup Manager 프로그램의 사용자 인터페이스 화면 및 1시간 간격으로 저장된 백업 내용을 보여준다.
- 모델저장소: W-Cloud의 파일저장소인 HDFS(Hadoop Distributed File System)에서의 침입감내는 데이터의 백업과 네임노드의 스냅샷의 정보를 관리를 통하여 이루어진다. HDFS의 침입감내 계층을 통하여 무정지 시스템을 구축할 수 있다. Fig. 7은 HDFS 데이터복제 과정을 보여준다. HDFS는 네임노드와 세컨드리네임노드 각각 1대, 데이터노드 3대로 총 5대의 PC로 구성된다. 클라이언트가 네임노드에 파일저장을 요청하면 네임노드는 파일패스에 대한 네임스페이스를 구성한다. 데이터노드에는 파일을 저장할 때, 같은 데이터를 백업의 목적으로 중첩하여 저장할 수 있다. W-Cloud는 2개씩 중첩으로 저장하도록 하였

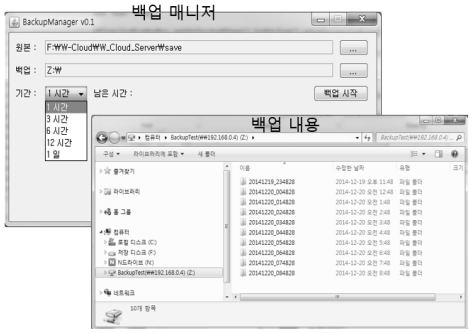

Fig. 6. Intrusion tolerance by backup manager in W-Cloud

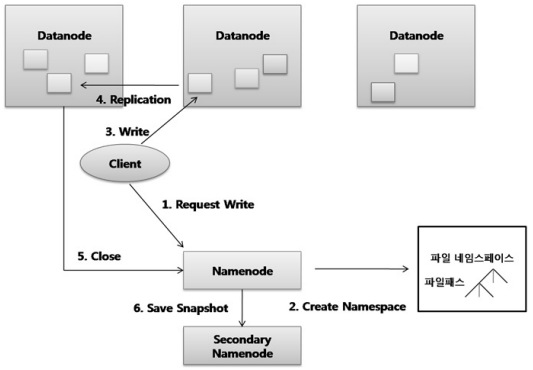

Fig. 7. Intrusion tolerance by HDFS in W-Cloud

으며, 데이터노드의 데이터 중복은 네임노드에서 설정이 가능하다. 저장이 완료되면 세컨드리노드에 네임노드의 스냅샷의 정보를 저장함으로써 모든 데이터에 대한 백업이 이루어진다. 이러한 백업과정을 통하여, 해커의 침입된 공격으로 인하여 시스템에 결함이 발생하더라도 스냅샷의 정보와 백업된 정보를 사용하여 지속적인 서비스 제공이 가능하다.

4.4 기밀성 보장

W-Cloud에서는 2가지 암호화 기법을 사용함으로써, 기밀성을 보장하였다. 이번 장에서는 국방 M&S 자원의 등록, 검색 및 다운로드하는 과정을 통하여 SEED를 사용한 기밀성 보장에 대해 알아보도록 한다.

4.4.1 국방 M&S 자원 등록

W-Cloud에서는 무기를 Server에 등록하기 위해, 무기명, 열람등급, 무기종류 및 특성을 비트로 표현한 비트맵 정보를 함께 등록하게 된다. 비트맵 정보는 이미 무기모델에 대한 정보가 비트로 암호화되어 있음으로 암호화할

원문

```
<?xml version='1.0' encoding='UTF-8'?>
<Dublincore>
 <Title>Mistral</Title>
 <Creator>Chanjong</Creator>
 <Type>Missile</Type>
 <Contributor>SELAB</Contributor>
 <Publisher>SELAB</Publisher>
  :
 <Description>적외선 유도체계를 사용하는 지대공 미사일</Description>
 <Grade>3</Grade>
  :
 <Use>대공</Use>
 <Range>단거리</Range>
 <MultyFidelity>높음</MultyFidelity>
 <Inducement>적외선</Inducement>
 <MaxSpeed>2.60</MaxSpeed>
 <MaxRange>5.30</MaxRange>
  :
```

암호문


```
hueJXhNRf5+eD46KlB5YkHdUO85aryAwXn93+vZr8YJkkIVF6L31Vd4m7CdAQy+I//ZpgO
9IQcGUkSg77bvveZF4AaXcndAJ4cy+ySf0NYm43m0sXTCtw1kYnhoFhLR78M5/V9+KONs
nIVpQiOlCb1pFaKBOpXnaTbSKiSn4cINK5tbiQhLE/ej4mL+A899V/IU90FrY/hUx/AE5Upk
P7G0/vSYOgIk6rSsjVfPm0biQeCmDhLf/uBWAJeIymxHlo7xg5hTIJDNKTBqdaZXFooQZNu
95bastZ04GBcY+vuC+S6aG1cDw798ft79jpcxBFIcpKS+mmWJwpFHVlyXiarpxBSTQ/oZsTx
rfU/dPKx0vuN+xCfwRcWVGJhD6yzpPGyQjakaAIVl0VGBfB7dY91LQb1SEGW91iQRIIqo
H+YnCL7liaa2leZJJzdBxQkEqnLRFDXfxsiUJBOACPuI1OPeOr+HxpykZZzAHYPOFvfgL+5
lLyvknHEvgCiRt9r8hwZGPuZqde9jQbG8iN5nVyBa7D9LTou/DULbogMo+oGZg+JdXkMQ
OW5tADZhKH8xLdNBwerkogs//2VVAnxCCx0fDst4EUgE4QEAIxvqKGOQ79PuvRv06Ji+N
k0dlOiachGd3M5SblCBpIHSdVyqokwix5+tm96xCtawfQhi95TxCGXKTgnSjUjtB6LDxSqGw
jxWkmb+HA7Kn8qf4waNnk/0rO3S9UOBAWGfNu3eMtE9AGSjM1Etd/rDaszSQ26Ewt/bAfF
zFsfvz00krBfpvIFCR+7xMYKUyKnFhpHBJW3c1POjAUmOr61GM9MKJkum7B97O9BAwo
ThGm2Bbjd3P89UFXAU4HlmHR9SaMVW9kexsqlATpHHRXKAIC31VtmiNdLCVQVahQ1
ngUeFYZgA+yX/+tzGyEi13iqmPIU3KefBbo7MZVidbfl0Pmhrjk/UljciO4+9VzeIbfQJE5046w
HitQ+mReCiip8jIZizTp3n5KMur4CQ4aKLng5rONi3o6i1Oz81C/CH1kCGti8CpZDe5YOL2K
Oh2lWPsk2mF27SzIx+/Q1Sku29Bdg8s1YWhqhmXYPcYQa5mFctSZ6XwdwJFBpQqaS7T5s
nfVKZCGKE=
```


Fig. 8. Encryption results of RDF files

필요가 없다. 열람 등급 또한 암호화하지 않고 저장하더라도 무기명과 무기모델이 저장될 파일경로 정보들만 암호화하면 어느 무기모델에 대한 정보인지, 어느 위치에 저장되어 있는지 알 수가 없다. 또한, 열람등급과 비트맵 정보는 검색 수행의 중요한 요소이므로, 비암호화시 검색 시간의 효율을 증대할 수 있다. 따라서 Server는 무기모델의 중요한 정보인 무기모델이 저장될 파일경로 및 무기명만을 SEED 알고리즘을 통하여 암호화하여 무기모델 정보를 DB에 저장한다. 무기모델에 대한 저장이 이후 Server는 Client에 HDFS의 설정 정보 및 저장될 위치에 대한 정보를 알려주면, Client는 컴포넌트 파일, 데이터 파일, XML[13], RDF[14] 파일을 SEED 알고리즘을 통하여 암호화하여 HDFS에 직접 업로드하여 암호화된 상태로 저장한다. Fig. 8은 무기모델의 더블린 코어 정보가 기술된 RDF 파일이 암호화된 모습을 보여준다.

Fig. 8을 통해 알 수 있듯이 해커가 Client에서 HDFS로 업로드되는 파일들을 가로채거나 HDFS에 저장된 파일을 불법적인 방법으로 다운로드 하더라도 데이터에 대한 정상적인 열람이 불가하다.

3.4.2 국방 M&S 검색 및 다운로드

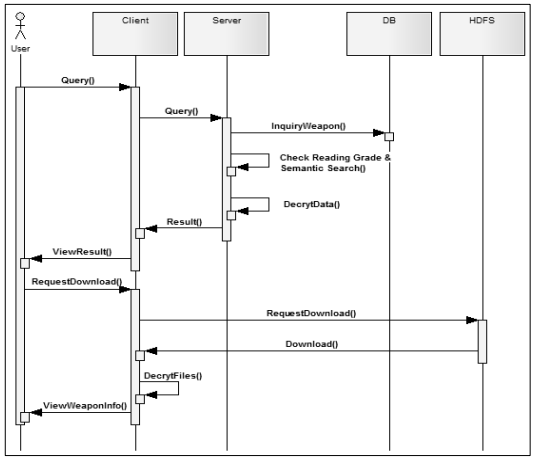

Fig. 9. Retrieval and Download service in W-Cloud

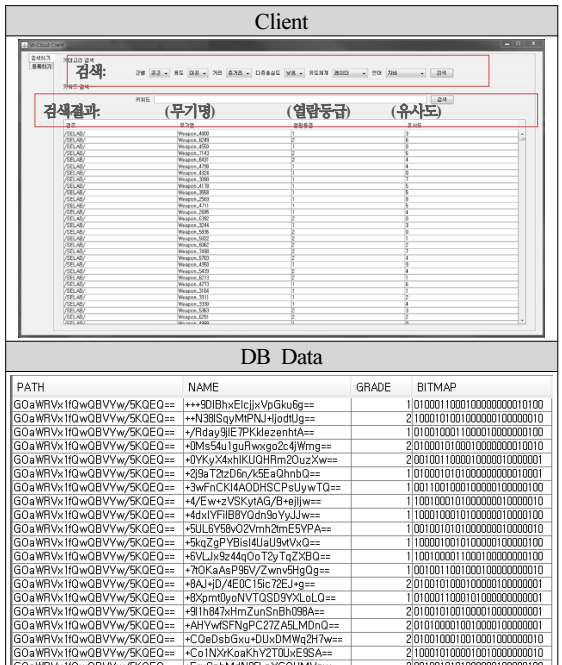

Fig. 10. W-Cloud: Encryption of catalogue

사용자 인증을 거쳐 열람 등급을 부여 받은 사용자는 의미기반 검색을 통해 결과를 보고 컴포넌트 파일, 데이터 파일, RDF 파일 다운로드하고자 Fig. 9와 같은 과정을 수행한다. 사용자는 Client 프로그램을 통하여 질의할 내

용을 비트맵 정보로 변환하여, Server에 검색을 요청한다. Server는 무기모델 DB를 조회하여 사용자의 등급에 적합한 무기모델만을 검색한다. W-Cloud에서는 무기모델의 저장경로 및 무기모델명은 암호화되어 저장되어 있었기 때문에 복호화하여 검색결과와 더불어 HDFS의 설정 정보 및 파일들을 복호화 하는데 필요한 키를 제공하여 준다.

Fig. 10은 W-Cloud Client 프로그램으로 열람등급 2등급 사용자가 보는 결과 화면 및 동일한 질의를 한 실제 DB의 데이터의 내용이다. Fig. 10에서 보인바와 같이 DB에 입력된 데이터는 SEED 알고리즘으로 암호화되어 저장되기 때문에 데이터가 유출되더라도 정상적인 열람이 불가능하다.

질의한 결과를 확인한 사용자는 본인이 원하는 무기모델에 대한 파일들을 HDFS에서 직접 다운로드 할 수 있다. 다운받은 파일들은 암호화되어 저장되어 있음으로 복호화한 후 무기모델에 대한 상세한 정보 열람 및 컴포넌트 재사용을 사용할 수 있다.

5. 평 가

5.1 보안 요구 사항 검토

W-Cloud는 클라우드 저장소를 국방 분야에 적극적으로 활용하기 위해, 계층형 정보보호 개념을 적용하여 기밀성, 무결성, 가용성을 해결하고자 하였다.

- 기밀성: W-Cloud는 기밀성을 보장하기 위해 사용자 인증시스템을 고용하여, 허가된 사용자만 저장소를 접근할 수 있도록 하였다. 또한, 저장된 데이터에 열람등급을 부여하여 합법적 사용자가 합법적 데이터만을 열람 할 수 있도록 하였다. 또한, 암호화 및 키 관리를 통하여 비합법적인 사용자가 데이터를 열람하더라도 내용을 볼 수 없도록 하였다. 따라서 W-Cloud는 기밀성을 충족시켰다고 할 수 있다.
- 가용성: W-Cloud는 가용성을 보장하기 위해 백업시스템을 구축하였다. W-Cloud는 무기체계 시뮬레이션 모델에 대해, 모델 자체 데이터 뿐만 아니라 모델에 정보를 명세한 메타 데이터를 저장한다. W-Cloud는 HDFS(Hadoop Distributed File System)를 통하여 세컨드리노드에서 네임노드의 스냅샷을 저장하도록 하고, 데이터노드에서는 데이터를 중복하도록 하여 데이터의 지속적인 백업 기능을 사용하였다. 또한, Server에서 관리하는 모델 메타 데이터의 DB 또한 자체 마련한 백업 매니저 시스템을 통하여 일정시간마다 백업이 가능하도록 하였다. 그러므로 시스템에 장애가 발생하더라도 복구가 가능하도록 하여 무중단 및 가용성을 충족시켰다.
- W-Cloud는 제한된 수준의 무결성만을 제공한다. W-Cloud의 접근 제어를 통해 저장된 모델 데이터에 대해 쓰기 권한이 있는 합법적인 사용자만 데이터에 대해 수정할 수 있도록 하여 자료에 대한 어느 정도의 무결성 보호만을 제공하고 있을 뿐, 합법적 사용자의 의도적인 변경 또는 삭제, 중복된 모델 데이터의 일부 변경 또는 삭제에 대한 방지책, 컴퓨터 바이러스 등에 의한 손상을 포함한 적극적 무결성 보안 장치를 포함하고 있지 않다.

5.2 보안 정책에 따른 성능 오버헤드 분석

W-Cloud에서는 임의의 무기 모델에 대한 정보를 XML, RDF의 형태로 기술하고 해당 DLL 파일과 같이 등록하게 된다. 이 3가지 파일들은 보안을 위해 SEED 알고리즘에 의해 암호화 되어 저장되며, 추후 사용자의 검색 요청이 있을 때 복호화 된다. 우리는 가장 많은 오버헤드가 예상되는 재사용 가능한 무기 모델 검색시 발생하는 복호화 오버헤드에 대하여 측정하였다. 검색된 무기모델의 개수에 따라 N번의 복호화 오버헤드가 발생한다. 이 오버헤드에 대한 비용을 측정하고자 DB에 500개의 무기모델 정보를 넣고 보안을 적용한 경우와 그렇지 않은 경우를 비교하였다. 검색 시간은 Client에서 검색에 대한 요청을 지시한 시점에서 부터 Client에서 모든 검색 결과를 받은 시간까지의 차를 측정하였다. Table 5는 검색된 무기 모델의 개수를 100개씩 증가시키면서 측정하여 암호화 알고리즘을 적용 하였을 때와 비적용 하였을 때를 비교한 결과 이다.

Table 5에서 볼 수 있듯이 암호화 알고리즘 적용한 것

Table 5. Performance overhead of encryption/decryption in W-Cloud

무기 모델 갯수	암호화 알고리즘 미적용	암호화 알고리즘 적용
	시간차 (s)	시간차 (s)
100	0.047	0.057
200	0.051	0.079
300	0.127	0.073
400	0.073	0.124
500	0.105	0.166

과 미적용한 것의 시간차는 매우 미세하여 성능 저하를 초래 하지 않음을 알 수 있다. 이상의 실험결과를 볼 때 본 논문에서 구현한 W-Cloud는 무기 모델에 대한 높은 수준의 보안을 제공하면서도 성능상의 주목할 만한 오버헤드는 발생하지 않는 것을 알 수 있었다.

6. 결 론

본 논문에서는 무기체계 모델에 대한 재사용을 증대하기 위하여 보안이 강화된 클라우드 저장소인 W-Cloud를 구현하였다. W-Cloud는 무기체계 모델의 검색 및 조회에 요구되는 보안성을 위해 해커의 공격에 대한 예방, 침입에 대한 탐지, 침입된 공격에도 지속적인 서비스가 가능하도록 하였으며, 암호화 기법으로 기밀성을 보장함으로써 유출된 정보를 해커가 알 수 없도록 하였다. 실험을 통해 보안된 자원의 복호화 오버헤드가 심각한 성능상의 문제를 초래하지 않음을 확인하였다. 이에 따라 제안된 W-Cloud 아키텍쳐는 HDFS과 같은 분산 파일 시스템의 보안을 위해 적용될 수 있을 것으로 판단된다. 향후, 다양한 크기의 무기 모델에 대해 검색 뿐 아니라 등록, 다운로드 등의 업무를 수행할 때에도 제안된 보안 메커니즘으로 인한 성능상의 오버헤드가 있는지에 대해 확인하여, 지속적 개선을 수행 할 예정이다.

References

1. 석지범,이재오,이재진,서윤호, “컴포넌트 관리 및 검증도구 설계와 동적 재구성 아키텍쳐 기반 SAM 시뮬레이션 개발”, 한국시뮬레이션학회논문지, 22(2), pp. 1-10, 2013.
2. 한승진,이민규, “해군무기체계 수중교전 모델 라이브러리 개발”, 한국시뮬레이션학회논문지, Vol. 22, No. 4, pp. 1-9, 2013-12.
3. 김태섭, “온톨로지 기반 국방 컴포넌트 클라우드 저장소”, 명지대학교 학위논문, (2012).
4. 김태섭, 박찬종, 김현휘, 이강선, “무기체계 모델 재사용을 위한 온톨로지 기반 클라우드 저장소 서비스 방안연구”, 한국시뮬레이션학회논문지, 21(3), pp. 35-42.
5. 이강택, 이동휘, 김귀남, “침입감내기술 기반의 보안시스템 설계 및 구현”, 정보보증논문지 제5권 제4호(2005).
6. M S.Bhiogade, “Secure Socket Layer”, InSITE - “Where Parallels Intersect” (2002).
7. KISA, “SEED 암호화 알고리즘”, www.kisa.or.kr(1999).
8. Martin Roesch, Snort - Lightweight Intrusion Detection for Networks, Proceedings of LISA '99: 13th Systems Administration Conference (1999).
9. Konstantin Shvachko, Hairong Kuang, Sanjay Radia, Robert Chansler, “The Hadoop Distributed File System”, Mass Storage Systems and Technologies (MSST)(2010).
10. 최중섭, 이경구, 김홍근, “침입감내기술 연구 동향”, 정보보호학회지(2003).
11. Jean-Michel Fray, Yves Deswarte, David Powell, “Intrusion-Tolerance Using Fine-Grain Fragmentation-S-cattering”, IEEE Symposium on Security and Privacy (1986).
12. Jiang Guo and Luqu, “A Survey of Software Reuse Repositories”, IEEE ECBS Proceedings, 92-100 (2000).
13. XML, http://www.w3.org/XML/
14. RDF, http://www.w3.org/RDF/

박 찬 종 (pcj0824@mju.ac.kr)

2011 명지대학교 컴퓨터공학과 학사
현재 IBM GBS

관심분야 : 컴퓨터시뮬레이션, 국방 M&S

한 승 철 (bongbong@mju.ac.kr)

2003 미) 퍼듀대, 컴퓨터공학 석사
2007 미) 플로리다 대학교, 컴퓨터공학 박사
2008～현재 명지대학교 컴퓨터공학과 교수

관심분야 : 컴퓨터 보안

이 강 선 (ksl@mju.ac.kr)

1992 이화여자대학교 전자계산학과 학사
1994 이화여자대학교 전자계산학과 석사
1998 미) 플로리다 대학교, 컴퓨터공학 박사
1999 삼성전자중앙연구소 소프트웨어센터 선임연구원
2000～현재 명지대학교 컴퓨터공학과 교수

관심분야 : 컴퓨터시뮬레이션, 국방 M&S