클라우드 컴퓨팅 환경을 위한 침입탐지시스템 특징 분석

양환석* · 이병천* · 유승재**

요 약

IT와 네트워크 기술의 발전으로 새롭게 소개된 클라우드 컴퓨팅은 개인의 인터넷 환경뿐만 아니라 기업들의 서비스 환경에도 많은 변화를 가져다주었다. 특히 저렴한 비용으로 IT 자원을 빌려 쓸 수 있고, 인프라를 구축할 필요가 없으며, 가상화를 이용한 다양한 컴퓨팅 환경을 제공받을 수 있는 것은 클라우드 컴퓨팅 환경이 인기를 얻을 수밖에 없는 이유이기도 하다. 이러한 클라우드 컴퓨팅에서는 다양한 접속 방법과 서비스 제공 범위가 넓어지고 있는 것과 비례하여 공격 위협의 범위 또한 넓어지고 있다. 따라서 악의적인 의도를 갖는 다양한 공격으로부터 자원을 보호해 줄 수 있는 침입탐지시스템이 반드시 필요하다. 본 논문에서는 자원의 공유와 가상화가 갖는 특성으로 인해 침입이 발생하였을 때 다른 컴퓨팅 환경에 비해 그 피해가 매우 큰 클라우드 컴퓨팅 환경에서 침입탐지시스템이 가져야할 특징에 대하여 분석하였다.

Study on Intrusion Detection System under Cloud Computing Environment

Yang Hwan Seok* · Lee Byoung Cheon* · Yoo Seung Jea**

ABSTRACT

Clouding computing which is developing newly as IT and network technology develops become changed to internet and service environment of company. Especially, it can lend IT resource at low costs and no need to build up infra. Clouding computing environment become popular more and more because various computing environment using virtualization is provided. The attack threat range also becomes wider in proportion to broaden various connection ways and service supply range at these clouding computing. Therefore, intrusion detection system which can protect resource from various attack having malignant attempts is necessary. In this study, we analyzed about characteristic of intrusion detection system at cloud computing environment having big damage than other computing environment when intrusion happen by sharing of resource and virtualization.

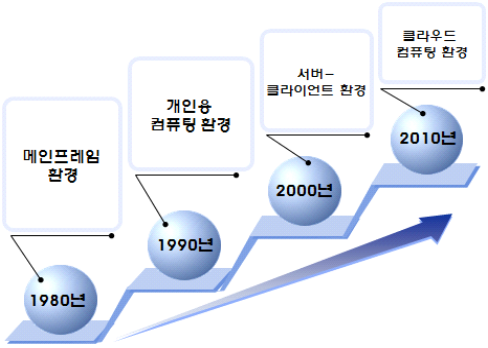
Key words : Cloud Computing, IDS, Virtualization

접수일(2012년 5월 24일), 수정일(1차: 2012년 6월 13일), 게재확정일(2012년 6월 21일)

* 중부대학교 정보보호학과
** 중부대학교 정보보호학과(교신저자)

1. 서 론

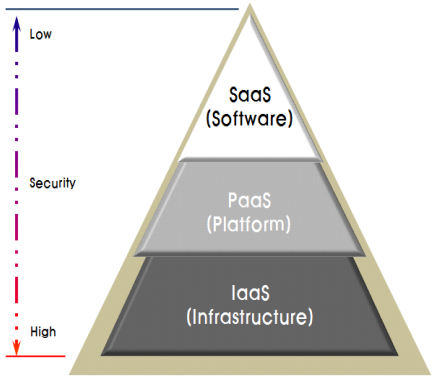
최근 들어 IT 산업의 가장 커다란 이슈 중의 하나가 클라우드 컴퓨팅이다. 인터넷을 통해 고객들의 요구는 맞게 저장장치, 소프트웨어, 서버 등의 자원을 제공해주고, 사용한 만큼의 비용을 지불하는 것이다[1][2]. 이렇게 적은 비용으로 IT 자원을 활용할 수 있게 됨으로써 개인뿐만 아니라 기업의 컴퓨팅 환경도 점차 변화하고 있는 실정이다[3]. IT 환경의 진화하는 과정을 (그림 1)에서 보여주고 있다.



(그림 1) IT 환경의 진화 과정

클라우드 컴퓨팅은 기존의 인터넷 서비스인 웹하드나 ASP(Application Service Provider)등과 비슷해 보이지만 가상화 서버를 기반으로 새로운 기능을 제공하고 이용자 스스로가 자신의 환경을 간단하게 구성할 수 있는 차이점을 가지고 있다[4]. IT 자원을 서비스 형태로 제공을 하는 클라우드 서비스는 제공되는 자원의 수준에 따라서 다음과 같이 분류할 수 있다.

IaaS는 가상화 기술을 이용하여 CPU나 스토리지를 제공하는 서비스로서 네이버의 N드라이브나 애플의 아이클라우드가 여기에 해당된다. PaaS는 이용자들이 직접 소프트웨어를 개발할 수 있도록 컴파일 언어, 제작 툴, 데이터베이스, 웹 프로그램 등을 제공해주는 서비스로서 구글의 AppEngine, Map 서비스 등이 있다. SaaS는 최상위 계층의 모델로 어디서든 사용가능한 소프트웨어를 제공해주는 서비스로 구글의 Docs가 있다. (그림 2)는 클라우드 컴퓨팅 서비스 모델을 보여주고 있다.



(그림 2) 클라우드 컴퓨팅 서비스 모델

클라우드 서비스 특징인 자원의 효율성 증대 및 공유, 가상화, 단말기의 다양성 등은 여러 공격들의 대상이 된다. 그리고 다양한 정보 및 데이터 전달 채널의 다중화는 서비스 제공 범위를 넓혀주는 반면 개인 사용자, 기업 및 기관들의 정보 유출, 탈취 그리고 취약한 서비스 제공자를 통한 공격 위협 범위는 더욱 넓어지는 위험성을 내포하고 있다[5]. 따라서 클라우드 컴퓨팅 환경을 고려한 침입탐지 프레임워크가 필요한 실정이다. 본 논문에서는 클라우드 컴퓨팅 환경이 안고 있는 보안 요소 및 문제점을 살펴보고 클라우드 컴퓨팅 환경에 맞는 침입탐지시스템이 갖추어야 할 특징을 분석하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 클라우드 컴퓨팅에서의 보안 기술에 대하여 살펴보고 3장에서는 클라우드 컴퓨팅에서의 침입탐지시스템의 특징을 분석한다. 마지막으로 4장에서 결론을 맺는다.

2. 클라우드 컴퓨팅의 종류

클라우드 컴퓨팅의 종류는 크게 세 가지로 분류하는데 여기에는 공공 클라우드, 사설 클라우드 그리고 하이브리드 클라우드가 있다.

공공 클라우드는 서비스 이용 대상에 제한이 없으며, 누구나 다양한 단말기를 가지고 네트워크에 접속하여 서비스를 사용한 만큼의 비용을 지불하는 공중 인프라로서 제공업체의 개발 환경에 종속되는 형태이다. 사설 클라우드는 클라우드 컴퓨팅 환경을 구축하

려는 기관이 모든 것을 구축하여 특정 영역 내에서 배타적으로 이용이 가능한 형태로서 데이터 소유권을 확보하고 프라이버시를 보장받고자 할 때 구축한다. 마지막으로 하이브리드 클라우드는 위에서 언급한 두 가지 형태를 조합한 것으로서 중요하고 보안이 필요한 서비스와 데이터는 사설 클라우드를 이용하고 덜 중요한 정보나 서비스는 공공 클라우드를 이용하는 형태이다. 하이브리드 클라우드는 장애 발생시 대안으로 사용을 하거나 시험운용 형태로 사용하는 방법, 특정 시기에만 사용량이 급증할 때 사용하는 방법을 고려할 수 있다. 다음 <표 1>은 클라우드 컴퓨팅 종류별 장단점을 보여주고 있다.

<표 1> 클라우드 컴퓨팅 종류별 장단점

	장 점	단 점
공공 클라우드	· 자체 기술력 부담이 적음 · 활용도가 우수 · 구축 비용 없음	· 데이터 보안의 문제 · 자체 정책 적용 어려움
사설 클라우드	· 문제 해결 용이 · 보안 및 신뢰성 · 정책 적용 용이	· 낮은 탄력성 · 구축 비용 높음 · 개발 기간 길다

3. 서비스 모델별 보안 기술

클라우드 컴퓨팅의 서비스 모델은 앞 장에서 살펴본 것처럼 크게 세 가지로 분류된다. 본 장에서는 각 서비스 모델에서 필요한 보안 요소에 대하여 기술한다.

3.1 SaaS의 보안 요소

SaaS에서 서비스 이용자의 보안은 서비스 제공자가 전적으로 책임져야 한다. 서비스 제공자는 여러 사용자 각자의 데이터를 다른 사용자들로부터 지킬 수 있는 보안 기능을 제공해주어야 한다. 따라서 SaaS에서 제공되는 소프트웨어가 보안 취약점을 갖지 않도록 하는 것이 가장 큰 도움이 된다. SaaS에서 고려되어야 할 보안 요소들은 다음과 같다. 클라우드 서비스는 인터넷을 기반으로 서비스가 제공되기 때문에 네트워크 구축에 있어 강화된 보안 기술이 적용되어야 할 것이며, 네트워크 오류나 장애에 철저하게 대비해야 한다. 그리고 자원의 활용성을 극대화 시키고 비용을 절약할 수 있는 가상화 기술은 악성코드 확산에 대한 취약점을 갖고 있다. 뿐만 아니라 사용자 데이터 위변조 및 손실 등에 대한 보안을 강화해야 한다. 그리고 클라우드 이용자는 다양한 단말기를 이용하여 서비스에 접속하여 서비스를 제공받는다. 따라서 각 단말 장치가 가지고 있는 보안의 취약점으로 인해 사용자의 인증 과정이 보다 철저하게 이루어져야 하며, 불법적인 접근에 대한 모니터링이 이루어져야 한다. 그리고 여러 사용자들이 공동으로 저장장치를 사용하기 때문에 사용자들의 데이터는 안전하게 백업되어야 하고 암호화가 되어 관리되어야 한다.

3.2 PaaS의 보안 요소

PaaS는 플랫폼과 서비스 두 가지 구성 요소로 이루어져 있다. 따라서 PaaS에서 고려되어야 할 보안 요소는 이 두 가지 구성 요소의 관점에서 바라봐야 할 것이다. 먼저 플랫폼에서 SQL 인젝션, 교차 사이트 스크립팅, 트래픽 암호화 등을 처리하여 애플리케이션 개발 과정에서 적용되도록 해야 한다[6]. 그리고 플랫폼에서는 다른 플랫폼에서 개발된 애플리케이션을 통합할 수 있는 기능과 애플리케이션에 걸리는 부하까지 처리해 줄 수 있는 기능을 갖추어야 한다. 그래서 PaaS에서 중요하게 다루어져야 할 보안 요소는 암호화와 데이터 배분이다. 먼저, PaaS를 이용하여 데이터를 클라우드 서비스 제공자에게 전송하기 전에 암호화를 하도록 하고 있다[7]. 이렇게 암호화를 이용하여 데이터를 보호할 수는 있지만 시스템 성능이 저하된다. 따라서 시스템 성능을 떨어뜨리지 않으면서 안전을 보장할 수 있는 암호화 방법을 고려해야 한다. 그리고 클라우드 서비스 이용이 중단되는 사고가 발생하더라도 서비스를 안정적으로 제공하기 위해서 데이터 배분을 적절하게 관리해야 한다. 이를 위해 지역에 따른 데이터 접근 통제 방법들도 PaaS에서 관심을 가져야할 보안 요소이다.

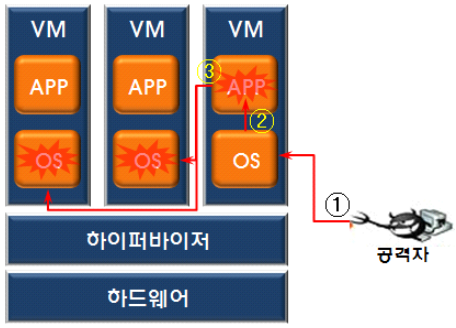
3.3 IaaS의 보안 요소

이 모델에서는 가상머신의 관리와 악의적 의도를 갖는 사용자에 집중해야 한다. 특히 클라우드 컴퓨팅 기술의 핵심 기술인 가상화는 악성코드의 감염확산과 하이퍼바이저에 대한 공격 그리고 물리적인 자원을 재배치하는 과정에서 데이터 손실이 발생하는 등의 취약점을 갖고 있다[8]. 따라서 가상머신을 생성하고 삭제하는 방법을 통제할 수 있는 잘 설계된 보안 프레임워크를 구축해야한다. 그리고 허용되지 않는 사용자가 무단으로 서비스를 이용하지 못하도록 차단해야만 한다. 기업의 일부 직원이 무분별하게 외부의 IaaS를 이용하거나 사설 클라우드를 불법적으로 사용하는 일이 발생할 수도 있다. 따라서 기업의 제공자는 서비스 이용자의 IaaS의 철저한 관리와 감시가 필요하다.

4. 클라우드 컴퓨팅 환경에서의 침입탐지시스템

4.1 공격 위협

클라우드 컴퓨팅에서는 공격 위협의 대상과 범위가 상당히 넓다. 첫 번째로 공격자가 클라우드에서 제공되는 API(Application Programming Interface)의 취약점을 알게 된다면 보안에 심각한 위험 요소가 된다. 이를 이용해서 익명 액세스나 부적절한 인증 및 콘텐츠 전송 등이 이루어질 수 있기 때문이다. 그리고 공격자는 소프트웨어 취약점을 이용하여 사용자의 정보를 빼낼 수도 있고 피싱 공격이나 악성 소프트웨어를 이용한 도청 및 사기 행위를 통해 개인 정보를 훔칠 수 있다. 두 번째는 보안 레벨이 가장 낮은 곳을 공략하여 하이재킹을 시도하기도 한다. 이렇게 다양한 방법으로 침입공격을 시도하여 가상 네트워크에서부터 가상 호스트까지 공격하거나, 가상머신이나 클라우드 인프라에 대한 대규모 공격을 할 수 있게 된다. 가상 호스트를 가진 공격자들은 클라우드 하이퍼바이저나 다른 가상머신을 위협할 수 있다. (그림 3)은 가상화 취약점을 이용하여 공격하는 과정을 보여주고 있다. 그림에서처럼 공격자는 악성코드를 이용하여 OS를 공격한 후 응용 프로그램을 감염시킨다. 감염된 응용 프로그램을 이용하여 다른 가상머신의 운영체제들을 차례로 공격하는 방법으로 모든 가상머신을 공격하게 된다. 세 번째로 악의를 가진 내부자에 의한 정보 유출이다. 내부자에 의한 공격 위협이 그 어떤 공격보다 피해가 크기 때문에 클라우드 제공자는 내부자에 대한 철저한 정보 보안과 관리 감독을 해야 한다.

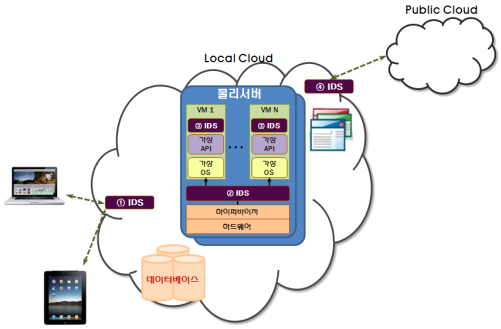


(그림 3) 가상화 취약점을 이용한 공격

4.2 클라우드에서 침입탐지

침입탐지는 컴퓨터 시스템 또는 네트워크에서 발생한 침입을 감시하여 시스템에 정의된 보안 메커니즘을 통과하기 위한 신뢰성, 무결성, 가용성 등에 대한 분석 과정이다. 침입탐지 방법은 정상 행위 프로파일과 비교하여 벗어나는 행위를 탐지해내는 비정상 행위 탐지 방법이 있다. 이 방법에서 행동이 기준에서 벗어났을 때 이벤트를 모으고 측정하기 위한 방법으로 신경망, 통계적 방법, 유전자 알고리즘 등 많은 방법들이 있다. 그리고 침입에 사용되는 패턴과 비교하여 이와 일치하는 패턴을 공격으로 간주하는 오용 탐지 방법이 있다. 클라우드 컴퓨팅 환경에서의 침입탐지시스템은 특정한 공격 유형에 대해서만 탐지가 이루어져서는 안 된다. 클라우드 컴퓨팅 환경에서는 광범위한 위협이 존재하기 때문에 이에 대응할 수 있는 통합 구조가 필요하다. 따라서 클라우드 컴퓨팅에서의 보안 수준을 확대하기 위하여 사용자의 행동을 비교 분석하는 행위 기반 방법과 공격 흔적을 추적하는 지식 기반 방법을 조합한 기능을 제공해야 안정된 침입탐지를 수행할 수 있다. 클라우드 컴퓨팅 환경에서 광범위하게 존재하는 공격에 대응하기 위한 침입탐지 시스템의 위치는 (그림 4)에서 나타낸 곳을 고려할 수

있다.



(그림 4) 침입탐지시스템의 위치

클라우드 서비스 이용자는 다양한 단말기를 이용하여 유무선 네트워크를 통해 서비스를 제공받으려고 한다. 따라서 단말이 갖는 보안의 위협과 공공 Wi-Fi와 같은 접속 환경이 갖는 취약점 때문에 정보 유출의 위협이 따를 수밖에 없다. 따라서 합법적인 사용자라는 인증을 거치는 모든 일련의 과정을 감시하면서 의심스러운 행동의 접근을 통제할 수 있는 침입탐지 기능이 수행되도록 해야 한다. (그림 4)에서 ①의 위치에 침입탐지시스템을 설치하여 이와 같은 기능을 수행하도록 한다. 다음으로 침입탐지시스템 설치가 고려되어야 할 위치는 ②의 하이퍼바이저와 가상머신 사이이다. 이곳에 설치된 침입탐지시스템은 단순히 하이퍼바이저를 감시하는 것뿐만 아니라 가상머신들 사이의 주고받는 모든 트래픽에 대하여 감시 기능을 수행하도록 하여 malware 공격과 같은 가상화로 인한 취약점을 이용한 공격을 탐지할 수 있도록 하고, 하이퍼바이저와 가상머신 사이의 링크를 경유한 공격 또한 탐지할 수 있도록 하는 것이다. 세 번째로 침입탐지시스템의 위치는 가상머신이다. 이 ③의 위치에서 가상머신의 행위를 감시하고 문제를 탐지하는 것이다. 게스트 가상머신은 디버그나 스케줄링을 위해 상속된 가상머신에 의존을 한다. 따라서 상속된 가상머신이 공격자에 의해 감염된 상태라면 게스트 가상머신도 쉽게 공격을 당하게 된다. 따라서 호스트의 잠재적인 침입을 탐지하기 위하여 파일 시스템, 메모리, 네트워크 트래픽 등의 데이터를 수집하고 이를 분석하도록 한다. 여기에는 알려지지 않은 공격을 효과적으로 탐지하기 위해 비정상행위 탐지 기법을 사용하도록 한다. <표 2>는 가상머신에서 감시해야 하는 항목들에 대해 보여주고 있다.

<표 2> 가상머신 감시 항목

항 목	설 명
CPU	호스트 OS와 가상 OS의 CPU 사용량을 측정하여 악성코드의 실행 여부 확인
Memory	프로세스에 의한 메모리 사용량을 감시하여 악성코드 실행 여부 확인
Disk	Disk의 사용량 점검 및 R/W 부하 검사
Port	인가되지 않은 포트의 개방 여부 확인
I/O	호스트 OS와 가상 OS 간의 I/O 검사
Traffic	호스트 머신과 가상 OS의 통신 네트워크 트래픽을 검사

클라우드 컴퓨팅 환경에서는 대용량의 데이터를 많은 서버들에 분산시켜 관리하기 때문에 이용자들에 대한 인증과 접근 제어, 데이터의 암호화 등 여러 가지 관리적인 측면에서 어려움이 뒤따르고 있다. 그리고 데이터가 저장되어 있는 위치가 노출될 경우에는 악의적인 해킹이나 정보 유출 등의 공격이 발생할 수 있기 때문에 이러한 공격을 차단하기 위하여 클라우드간의 정보 교환이 이루어지는 ④의 위치에 설치되어야 한다. 본 논문에서 언급한 위치에 침입탐지시스템을 설치함으로써 외부로 부터의 공격과 내부에서 발생하는 공격에 대비할 수 있고 안전한 서비스를 제공할 수 있게 된다.

5. 결 론

클라우드 컴퓨팅은 인터넷 환경과 비즈니스 환경을 새롭게 바꾸어 나가고 있으며 그 활용 범위 또한 나날이 증가하고 있는 추세이다. 현재 해외 대기업들이 주도적으로 사업을 확장해가고 있으며, 국내에서는 해외의 검증된 솔루션을 기반으로 다양한 시도가 진행중이다. 특히 클라우드 컴퓨팅은 서비스 사용자에게 비용을 절감할 수 있게 하고 제공자는 공유 자원을

이용한 큰 이익을 창출할 수 있어 매력적이다. 하지만 이러한 매력에도 불구하고 클라우드 컴퓨팅의 특징은 다양한 새로운 보안 위협에 놓여있어 클라우드 컴퓨팅 환경에서의 침입탐지시스템을 채택하기 위한 연구가 끊임없이 이루어지고 있다. 본 논문에서는 클라우드 컴퓨팅 환경이 안고 있는 보안 요소와 공격의 위협에 대하여 살펴보았고, 클라우드 컴퓨팅 환경에 맞는 침입탐지시스템의 위치와 특성을 제시하였다. 향후 연구로는 새로운 환경에서의 보안 취약점에 대비한 복합적인 보안 기술에 대한 연구와 함께 공격에 능동적으로 대응할 수 있는 침입탐지 알고리즘에 대해 연구하고자 한다.

참고문헌

[1] P.Jain, D. Rane, and S. Patidar, "A Survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment," IEEE 2011 World Congress on Information and Communication Technologies, pp. 456-461, 2011.

[2] M. Jensen, N. Gruschka, L. L. Iacono, and G. Horst, "On Technical Security Issues in Cloud Computing," IEEE International Conference on Cloud Computing, pp. 109-116, 2009.

[3] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Ensuring Data Storage Security in Cloud Comouting," IT Professional, Vol. 12, pp. 38-43, 2010.

[4] 선재훈, 김귀남, "Cloud Computing의 개인 정보 보안을 위한 취약점 분석," 한국사이버테러대응학회논문지, 제10권, 제4호, pp. 77-82, 2010.

[5] 은성경, 조남수, 김영호, 최대선, "클라우드 컴퓨팅 보안 기술," 한국전자통신연구원, 전자통신동향분석, 제 24권, pp. 81-82, 2009.

[6] Y. Z. Guan, Z. F. Hao, "The MDR Algorithm for Edge Detection on Change-point Theory," IEEE International Symposium on Intelligent Information Technology Application, pp. 558-562, 2009.

[7] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open Source Cloud Computing System," in Proceedings of the 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID '09), pp. 124 - 131, 2009.

[8] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing," 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, 2010.

[저 자 소 개]

양 환 석 (Hwan-seok Yang)

1998년 2월 조선대학교 이학석사
2005년 2월 조선대학교 이학박사
2007년 3월 호원대학교 연구교수
2011년 9월 ~ 현재 중부대학교
정보보호학과 전임강사

email : yanghs@joongbu.ac.kr

이 병 천 (Byoung-cheon Lee)

1986년 서울대학교 물리학과(학사)
1988년 서울대학교 물리학과(석사)
2002년 한국과학기술원 정보보호(박사)
1988년~1993년 (주)엘지전선연구소
1993년~1998년 (주)엘지전자기술원
2003년~2004년 호주 Queensland
Univ. of Technolog
연구교수
2002년~현재 중부대학교
정보보호학과 조교수

email : sultan@joongbu.ac.kr

유 승 재 (Seung-jae Yoo)

1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교
정보보호학과 부교수

email : sjyoo@joongbu.ac.kr