Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.2, Apr. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.2.319

SW-IaaS 클라우드 서비스 보안 프레임워크에 관한 연구 - SW-IaaS를 중심으로*

최 명 길,[1†‡] 박 춘 식,[2] 정 재 훈[1]
[1]중앙대학교, [2]서울여자대학교

A Study on Service Security Framework for SW-IaaS Cloud*

Myeonggil Choi,[1†‡] Choonsik Park,[2] Jaehun Jeong[1]
[1]Chung-Ang University, [2]Seoul Women's University

요 약

최근 발생한 클라우드 컴퓨팅 관련 보안사고는 한 기업의 보안사고 범위를 넘어 클라우드 컴퓨팅 환경을 사용하는 전체 고객에게 보안사고 범위가 확대되고 있다. 이를 위해 클라우드 데이터센터의 전반적인 통합 보안을 위한 관제기술이 요구된다. 본 연구는 기존 관제기술을 이해하고 클라우드 데이터센터 관제를 위하여 추가 및 통합되는 보안요소를 연구하고자 한다. IaaS 클라우드 환경의 이해를 돕고자 CloudStack으로 IaaS 클라우드 환경을 구축하였다. CloudStack의 구조와 NIST에서 제시한 IaaS 클라우드 모델을 접목하여 본 연구에서 제안한 SW-IaaS 클라우드 구조를 제시하였다. SW-IaaS 클라우드의 구성 요소인 Cloud Manager, Cluster Manager, Computer Manager의 각 계층에서 고려해야할 보안 프레임워크를 도출하고자 한다.

ABSTRACT

Cloud computing-related security incidents have occurred recently are beyond the scope of a enterprise's security incident is expanded to the entire range of customers who use the cloud computing environment. The control technology for the overall integrated security of the cloud data center is required for this purpose. This study research integrated and additional security elements for the cloud data center control to understand the existing control technology. It is a better understanding of the IaaS cloud environment to build the IaaS cloud environment by CloudStack. SW-IaaS cloud structure by combining CloudStack and IaaS cloud model presented by NIST is proposed in this study. This paper derive a security framework to consider in each layer of The SW-IaaS cloud components, which are composed of the Cloud Manager, Cluster Manager, and Computer Manager.

Keywords: Cloud Service, Security Framework, IaaS Cloud

I. 서 론

클라우드 컴퓨팅은 인터넷 기술을 활용하여 다수의 고객들에게 높은 수준의 확장성을 가진 IT 컴퓨팅 자원을 서비스로 제공하는 컴퓨팅 환경이다. 클라우드 컴퓨팅에 대한 관심은 다양한 단말기의 확장과 이에 대한 사용자들의 요구가 반영되어 지속적으로 증가하고 있다[1].

클라우드 컴퓨팅 환경의 도입은 공공기관, 통신사, SI업체, 대형 제조업체들로 확산되고 있다. 그 중심에 IT 자원의 최대한 효율성을 추구하기 위해 클라우드 데이터센터를 구성하게 된다. 클라우드 데이터센터의 경제적인 모델은 클라우드 서비스 제공자들이 인력 자원과 기술 자원을 최대한 활용하여 경쟁력을 얻고 운영 이익을 극대화하는 것이지만 보안을

Received(12. 16. 2015), Modified(01. 26. 2016), Accepted(02. 06. 2016)
* 이 논문은 2014년도 중앙대학교 연구결과물로 제출됨
† 주저자, mgchoi@cau.ac.kr
‡ 교신저자, mgchoi@cau.ac.kr(Corresponding author)

보장하기 위한 가상화 기술(자원의 분류, 분할)등 보안에 대한 새로운 패러다임이 요구된다.

IaaS 서비스는 클라우드 컴퓨팅 서비스 사용자가 임의의 소프트웨어를 설치하고 사용할 수 있도록 컴퓨팅, 스토리지, 네트워크, 데이터베이스 등의 인프라 자원을 요청기반으로 제공하는 서비스 모델이다. SW-IaaS 클라우드 서비스는 SW 기반으로 구축된 IaaS 클라우드 서비스 환경을 말한다.

클라우드 컴퓨팅 기술이 도입되던 시기인 2008년 클라우드 컴퓨팅의 해결과제로 보안, 성능, 가용성 순으로 나타났다. 최근 발생한 클라우드 컴퓨팅 관련 보안사고(서비스 거부, 데이터 손실, 서비스 남용 등)는 한 기업의 보안사고 범위를 넘어 클라우드 컴퓨팅 환경을 사용하는 전체 고객에게 보안사고 범위가 확대되는 것을 볼 수 있다[2],[3]. 이를 위해 클라우드 데이터센터의 전반적인 통합 보안을 위한 관제기술이 요구된다. 본 연구는 기존 관제기술을 이해하고 클라우드 데이터센터 관제를 위하여 추가 및 통합되는 보안요소를 연구하고자 한다.

따라서 본 연구는 IaaS 클라우드 서비스 보안 프레임워크를 제안한다. 본 연구에서 제안하는 IaaS 클라우드(SW-IaaS 클라우드 서비스)는 NIST에서 표준으로 정의한 IaaS 구조[4]와 IaaS 클라우드 서비스 환경을 제공하는 CloudStack 구조를 참고하였다.

II. 클라우드 서비스 위협 식별

클라우드 컴퓨팅은 서비스 기반의 IT자원 제공 방식으로 가상화 기술을 이용한 자원 관리, 자원의 통합적 관리 등의 새로운 기술을 도입하였다. 그러나 클라우드 서비스는 사업자 및 사용자의 보안 가이드라인의 부재로 보안 위협에 노출되어 있다.

CSA(Cloud Security Alliance)에서 발표한 클라우드 컴퓨팅의 위협 도메인 중 SW-IaaS에 대한 위협은 다음과 같다[5],[6],[7],[8].

2.1 클라우드 컴퓨팅의 남용과 비도덕적인 사용

IaaS 사업자들이 제한 없는 자원 제공을 위해 사용자들이 언제나 유요한 카드를 등록하고 즉시 클라우드 서비스를 사용 수 있게 하였기 때문에 PaaS보다 IaaS가 해커들의 타깃이 되고 있다.

2.2 안전하지 않은 인터페이스와 APIs

클라우드 컴퓨팅 사업자는 고객들이 클라우드 서비스들을 관리하고 상호작용하기 위해 소프트웨어 인터페이스나 API들의 셋을 노출 시켰다. 권한 설정, 관리, 결합, 모니터링은 이러한 인터페이스들을 사용하여 수행되는 것들인데, 일반적인 클라우드 서비스의 보안과 가용성은 기본 API들의 보안에 의존적이다. 조직과 제 3자는 이러한 인터페이스들에 따라 설계된다.

2.3 공유 기술 문제

IaaS 사업자는 공유된 인프라로 확장 가능한 서비스를 제공, 종종 CPU 캐시, GPU 등의 인프라 구조를 만드는 기본 컴포넌트들은 다중 채용(multi-tenant) 구조를 위하여 강력한 격리 속성의 제공을 설계하지 않는다. 이 간격을 어드레스 하기위해, 가상 하이퍼바이저는 게스트 OS와 물리적 컴퓨트 자원간의 접근을 조정한다. 하이퍼바이저는 게스트 연산 시스템이 제어의 부적당한 레벨을 획득하는 것과 기본 플랫폼에 영향을 끼칠 수 있다는 결함이 있다.

2.4 데이터 손실이나 유출

모바일 컴퓨팅 환경에서 물리적 장치 손실이 데이터 손실이나 유출 유발 할 수 있다. 기존 내용의 백업 없이 레코드 삭제나 변경, 레코드 연결 해제, 암호화 키 손실은 효과적인 파괴를 야기한다._

III. SW-IaaS 클라우드 서비스 보안 프레임워크

본 연구는 클라우드 데이터센터 환경을 고려한 보안 프레임워크를 제시하는 것으로 IaaS 클라우드 서비스 환경으로 범위를 결정하였다.

IaaS 클라우드 서비스 제공자는 물리적 자원(스토리지, 네트워킹)을 관리 및 제공하여 IaaS 고객에게 클라우드 인프라 및 환경을 호스팅한다. IaaS 클라우드 고객은 SLA에 명시된 서비스 범위 안에서 IT 인프라 환경에서 서비스를 생성 및 실행하고 이후 서비스들에 대하여 관리 및 모니터링을 한다[9]. 아래 Fig. 2.는 IaaS 구성요소인 Application, Middleware, Guest OS, Hypervisor,

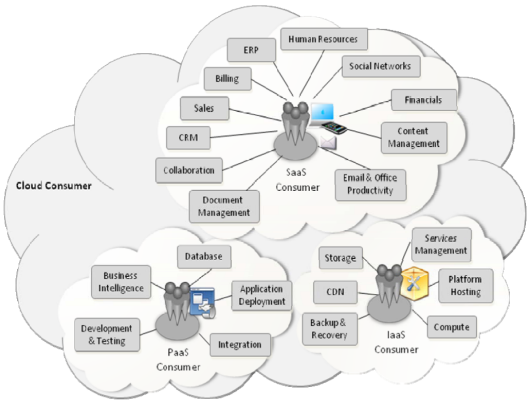

Fig. 1. Example of Available Services to Cloud Customers

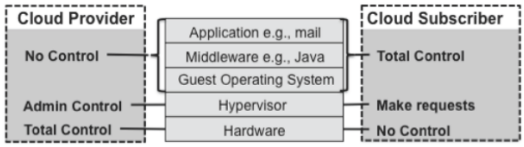

Fig. 2. Cloud Components Stack and Control Range

Hardware에 대하여 클라우드 서비스 제공자와 클라우드 고객 각각 제어 범위가 다름을 보여준다.

클라우드 서비스 제공자는 물리적 하드웨어와 하이퍼바이저 계층의 제어까지 제어 범위에 속한다. 클라우드 서비스 고객은 제공되는 게스트 OS위의 모든 미들웨어 및 어플리케이션을 전반적으로 제어할 수 있다.

NIST에서는 IaaS 클라우드 구조를 Cloud Manager, Cluster Manager, Computer Manager 세 가지로 나눈다. NIST에서 제시한 IaaS 클라우드 구조는 Fig. 3.과 같다.

Cloud Manager는 클라우드 외부와의 접근 포인터 역할을 하는 것으로 고객의 계정 로그인을 통해 클라우드 환경에 있는 데이터 저장소 접근 및 클라우드 리소스 관리를 제공한다. Cluster Manger는 로컬 지역의 네트워크 속도를 높이기 위해 연결되어진 것으로 Computer들을 수집하는 기능을 가진다. 주요 기능은 Cloud Manager로부터 전달된 쿼리와 명령에 대하여 computer들의 만족 여부를 계산 및 판단하여 요청의 일부 또는 전체를 실행할 수 있는 Computer Manager에게 쿼리하여 응답된 정보를 Cloud Manager에게 응답한다. Cluster

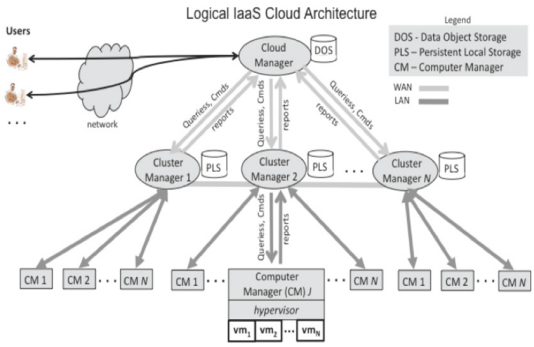

Fig. 3. IaaS Cloud Structure (NIST)

Manager 계층은 Computer Manager의 가상 자원의 보안 및 가상 자원 정보를 모니터링 하는 보안 요소와 Cloud Manager로부터 전달되는 메시지에 대한 보안 요소가 필요하다. Computer Manager는 하이퍼바이저를 통하여 각 computer 시스템을 구성한다. Computer Manager는 Cluster Manager로부터 쿼리를 전달 받으면 VM의 연동(얼마나 VM이 동작하는지, 준비 중인지) 정보를 포함한 상태 정보를 응답한다. 또한 Cluster Manager로부터 명령(VM의 start, stop, suspend)을 전달 받아 VM을 재구성하고 로컬 상에 있는 가상 네트워크 환경을 재설정한다.

위에서 살펴본 NIST 표준 IaaS 클라우드 계층 구조를 기반으로 각 계층에서 요구되는 보안요소를 도출하여 다음 Fig. 4.와 같이 IaaS 클라우드 서비스 보안 프레임워크를 제안한다.

SW-IaaS 클라우드 서비스는 IaaS 클라우드 서비스 환경을 말한다. 이를 위해 테스트 베드로 구축

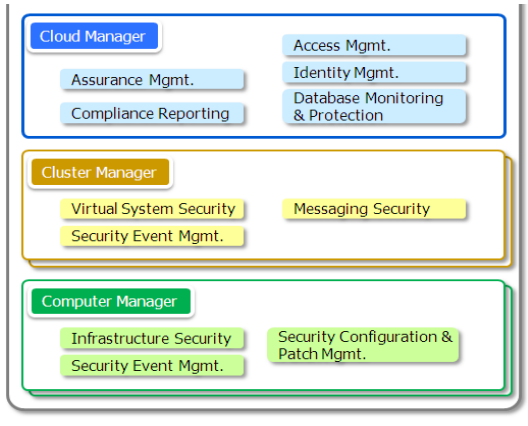

Fig. 4. IaaS Cloud Service Security Framework

된 CloudStack 구조를 참고하여 IaaS 클라우드 서비스 보안 범위를 정리하고 IaaS 클라우드 서비스 환경의 핵심 기술인 가상화 환경 운영의 이해를 돕기 위해 NIST의 IaaS 클라우드 계층 요소(Cloud Manager, Cluster Manager, Computer Manager)를 참고하여 Fig 4. Sw-IaaS 클라우드 서비스 보안 프레임워크를 구성하였다.

Cloud Manager는 클라우드 외부와의 접근 포인터 역할을 하며, 고객이 계정으로 접속하면, 클라우드 환경에 있는 데이터 저장소 접근 및 클라우드 리소스 제공을 관리한다. Cluster Manger는 로컬 지역의 네트워크 속도를 높이고, computer 정보를 수집한다.

Cluster Manager의 주요 기능은 컴퓨터가 Cluster Manger에서 받은 쿼리와 명령을 만족하는지 여부를 계산 및 판단하고, 쿼리를 실행할 수 있는 Computer Manager에게 요청하여 획득한 정보를 Cloud Manager에게 응답한다. Cluster Manager 계층은 Computer Manager의 가상 시스템에 대한 보안, 보안 사건 관리 및 전달 메시지의 보안을 관리한다.

Computer Manager는 하이퍼바이저를 통하여 개별 컴퓨터 시스템을 구성한다. Computer Manager는 Cluster Manager로부터 쿼리를 전달 받으면 가상머신(virtual machine)의 연동(VM이 동작중인 상태인지, 준비 상태인지) 정보를 포함한 상태 정보를 응답한다. Cluster Manager로부터 명령(VM의 start, stop, suspend)을 전달받아 VM을 재구성하고 로컬에 있는 가상 네트워크 환경을 재설정한다.

프레임워크의 모든 Manager는 가상화 환경을 구성 및 운영한다. SW-IaaS 클라우드 서비스 보안 프레임워크는 Cloud Manager 테스트베드 운영을 통해 SW-IaaS 클라우드 구조를 제안한다. Cloud Managr는 서비스 사용자 요청에 의해 Secondary Storage에 있는 템플릿을 이용하여 Zone → Pod → Cluster 순서로 가상화 환경을 구성한다. Cluster Manager는 Primary Storage(PS)와 Host를 추가하여 Dom0 영역에 Secondary VM, ConsoleVM을 생성하고 이후 Guest VM를 생성한다.

SW-IaaS 클라우드 보안 프레임워크에서 요구되는 보안 범위는 SW-IaaS 클라우드 서비스를 운영하는 ① 가상화 환경 운영 보안 영역, 자원 풀을 관리하는 ② 가상화 서버 인프라 보안 영역, 물리적인 인프라 보안을 위한 ③기존 관제기술 영역으로 나눈다.

3.1 Cloud Manager

다음은 각 계층별 보안요소에 대하여 살펴보고자 한다. Cloud Manager 수준에 따른 보안 구성 요소는 다음 Fig. 5.에 제시되어 있다.

cloud manager은 보안 구성 요소로 assurance management가 있다. IaaS 클라우드 서비스를 체결할 때 서비스 고객과 서비스 제공자 간의 서비스 수준 협약서를 합의하여 서비스 품질을 제공한다. SLA(Service Level Agreement)는 전제조건, 위탁범위, 역할과 책임, 서비스레벨 항목, 결과대응 및 운영으로 구성되어 있다. compliance reporting은 보안 규제에 대한 준수 사항을 리포팅하고, 서비스 사용자의 인스턴스 내에서 보안 사고가 발생했을 경우 로그 정보 및 감사 자료에 대한 리포팅 기능을 수행한다. access management는 사용자 유형별 패스워드 관리, 연속적인 로그인 실패 대처방법, 패스워드 자릿수, 사용 가능한 문자의 종류, 유효기간, 이력관리 등 패스워드 정책을 관리한다.

IaaS 클라우드의 경우 사용자가 클라우드 서비스 접근에 다양성이 제공된다. 예를 들어, 그룹 형태의 사용자와 하나의 인스턴스 서비스 접근과 그룹 형태의 사용자와 여러 인스턴스 서비스 접근은 관리적인 측면에서 다르다. 따라서

다음으로 Identity Management 구성요소가 존재한다. 권한 있는 사용자가 클라우드 서비스를 사용하는지에 대한 모니터링 기능, 제3의 인증 시스템 또는 기업을 통한 정상적인 인증절차 및 유기적인 인증 시스템 기능과 같은 보안이 요구된다.

마지막으로 Database Monitoring & Protection 구성요소 이다. Cloud Manager는 서비스 사용자와 제공자 간의 SLA 정보 및 인스턴스 정보에 대한 스토리지를 보유하게 된다. 이에 대

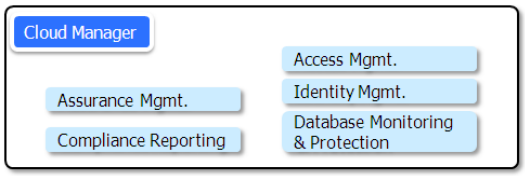

Fig. 5. Security Components of Cloud Manager Layers

한 데이터베이스 모니터링 및 보호 기술이 요구된다.

3.2 Cluster Manager

다음은 각 Cluster Manager의 계층별 보안요소에 대하여 살펴보고자 한다. Cluster Manager 수준에 따른 보안 구성 요소는 다음 Fig. 6.과 같다.

Cluster Manager 수준에 따른 보안 구성 요소로 첫째 Virtual System Security가 있다. Cluster Manager는 Computer Manager를 구성하는 Host와 VM 정보를 가지고 있다. 이들 정보는 서비스 가용성 보장을 위한 주요 정보가 됨으로 이에 대한 보안 기술이 요구된다.

다음으로 Security Event Management 구성요소가 존재한다. Cluster Manager를 구성하는 시스템들의 이벤트 정보를 관리하는 보안 기술이 요구된다.

마지막으로 Cluster Manager 수준에 따른 보안 구성 요소는 Messaging Security가 있다. Cluster Manager는 상위 계층 Cloud Manager와 하위 계층 Computer Manager간의 통신 역할을 담당한다. Cluster Manager의 쿼리 및 명령 정보를 실행하기 위하여 Cluster Manager는 Computer Manager에게 필요한 정보를 요청하고 전달 받아 Cloud Manager에게 전송하게 된다. 이때 메시지 전달 과정에서 악의적인 정보를 전달함으로 부정확한 정보를 전달함으로 IaaS 클라우드 환경에 영향을 줄 수 있다. 따라서 이에 대한 보안 기술이 요구된다.

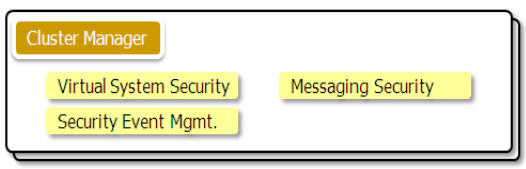

Fig. 6. Security Components of Cluster Manager Layers

3.3 Computer Manager

다음은 각 Computer Manager의 계층별 보안요소에 대하여 살펴보고자 한다. Computer Manager 수준에 따른 보안 구성 요소는 다음 Fig. 7.과 같다.

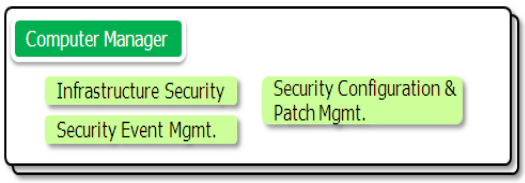

Fig. 7. Security Components of Computer Manager Layers

Computer Manager 수준에 따른 보안 구성 요소로 첫째 Infrastructure Security가 있다. 이는 물리적인 자원의 접근 제어에 대한 보안이 요구된다. 이를 위해 기존 관제기술(Firewall, IDS/IPS)을 활용한 인프라 보안과 End-point 보호를 위한 보안 기술이 요구된다.

다음으로 Security Event Management 구성요소가 존재한다. Host와 VM에서 발생되는 보안 관련 이벤트에 대한 관리 기술이 요구된다.

마지막으로 Computer Manager 수준에 따른 보안 구성 요소는 Security Configuration & Patch Management가 있다. Host 시스템의 하드웨어 및 운영체제에 대한 정기적인 패치 관리 등의 가상화 서버 환경에 대한 보안 기술이 요구된다.

IV. 결 론

클라우드 컴퓨팅 환경은 자원을 탄력적으로 지원하기 위해 가상화 기술을 사용한다. 가상화 기술은 사용자에게 동일한 환경을 제공하고 인프라 환경의 의존도를 탈피, 자원 사용의 최적화를 제공한다.

본 연구는 클라우드 컴퓨팅 환경에서의 보안 사고를 조사하고 클라우드 서비스 보안에 관한 문서를 참고하여 클라우드 컴퓨팅 보안 위협을 도출하였다. 클라우드 환경의 관제 연구를 위해 IaaS 클라우드 환경, 특히 SW-Iaas 클라우드 서비스 환경에 대해 제어 범위를 고려하여 SW-IaaS 클라우드 서비스 보안 프레임워크를 도출하였다. 이에 대한 요약 내용은 다음과 같다.

IaaS 클라우드 환경의 이해를 돕고자 CloudStack으로 IaaS 클라우드 환경을 구축하였다. CloudStack의 구조와 NIST에서 제시한 IaaS 클라우드 모델을 접목하여 본 연구에서 제안한 SW-IaaS 클라우드 구조를 제시하였다.

SW-IaaS 클라우드의 구성 요소인 Cloud

Manager, Cluster Manager, Computer Manager의 각 계층에서 고려해야할 보안 프레임워크를 도출하고 SW-IaaS 클라우드 서비스 기반 관제 연동 모델 제시를 위해 SW-IaaS 클라우드 계층 구조를 객체 모델링하고 SW-IaaS 클라우드 서비스 운영(서비스 시작, 가상 자원 운영, 가용성 보장을 위한 운영, 기존 관제시스템과의 연동)에 대한 매커니즘을 제시하였다. 이는 기존 클라우드 서비스 유즈케이스와 달리 가상화 자원과의 연동을 포함하여 제시하였으므로 클라우드 환경의 보안 위협 범위를 보다 구체적으로 제시하였다.

본 연구는 실무적, 학술적 시사점을 가지고 있다. 실무적으로는 본 연구에서 제시한 IaaS 클라우드 서비스 보안 프레임워크가 클라우드 서비스 공급자에게 서비스 운영에 대한 참고자료로 활용될 수 있다. 향후 연구로 클라우드 환경에서 보안 사고가 발생하였을 때 보안 정책을 결정하기 위한 기준 지표에 대한 연구가 계속되어야 할 것이다. 클라우드 환경 관제기술의 보안요소를 제시하므로 클라우드 컴퓨팅을 활용하는 국가 기반 시설 및 국가 기관에서 적용할 수 있는 클라우드 인프라의 기술적 가이드라인을 제시하는데 활용될 수 있다. 따라서 향후 클라우드 컴퓨팅의 특징 및 보안기술이 반영된 관제시스템은 해당 분야 선진 기술을 일부분 담당할 수 있을 것으로 기대된다.

학술적으로는 본 연구의 SW-IaaS 클라우드 서비스 보안 프레임워크가 클라우드 산업 활성화에 큰 걸림돌이 되는 서비스 보안을 해결할 수 있어서, 클라우드 서비스 보안 연구 분야를 넓혔다. 특히 클라우드 서비스가 개인정보보호, 빅데이터, 기타 서비스 산업 분야에 폭넓게 사용될 수 있는 점을 감안할 때, 해당 분야의 연구들과도 컨버전스 될 수 있을 것으로 기대한다.

References

[1] J. Brodkin, "Gartner: Seven Cloud-Computing Security Risks," Infoworld, 2008.

[2] M. Zareapoor, P. Shamsolmoali and M.A. Alam, "Establishing Safe Cloud: Ensuring Data Security and Performance Evaluation," International Journal of Electronics and Information Engineering, vol. 1, no. 2, pp. 88-99, Dec. 2014.

[3] M. Darwish, A. Ouda and L.F. Capretz, "A Cloud-Based Secure Authentication (CSA) Protocol Suite for Defense Against Denial of Service (DoS) Attacks," Journal of Information Security and Applications, vol. 20, pp. 90-98, Feb. 2015.

[4] G. Brunette and R. Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing," v2.1, Cloud Security Alliance, pp. 1-76, 2009.

[5] D. Hubbard and M. Sutton, "Top Threats to Cloud Computing," v1.0, Cloud Security Alliance, 2010.

[6] European Network and Information Security Agency, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," ENISA, 2009.

[7] D. Catteddu, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," In Web Application Security Springer Berlin Heidelberg, pp. 17, 2010.

[8] L. Badger, T. Grance, R. Patt-Corner and J. Voas, "DRAFT Cloud Computing Synopsis and Recommendations," SP 800-146, NIST, May. 2011.

[9] M. Hogan, F. Liu, A. Sokol and J. Tong, "NIST Cloud Computing Standards Roadmap," NIST Cloud Computing Standards Roadmap Working Group, SP 500-291-v1.0, NIST, Jul. 2011.

〈저자소개〉

최 명 길 (Myeonggil Choi) 종신회원
2004년 9월: 한국과학기술원 박사
1995년 9월~2000년 1월: 국방 과학연구소(ADD) 연구원
2000년 2월~2005년 8월: 한국전자통신연구원 (ETRI) 부설연구소 선임연구원
2005년 9월~2008년 2월: 인제대학교 시스템경영공학과 교수
2008년 3월~현재: 중앙대학교 경영학과 교수
관심분야: 정보보안시스템평가, 정보보호정책 및 관리, 암호정책

박 춘 식 (Choon Sik Park) 종신회원
1995년: 일본동경공업대 공학박사
1982년~1999년: 한국전자통신연구원 책임연구원
2000년~2008년: 국가보안기술연구소 책임연구원
2009년 3월~현재: 서울여자대학교정보보호학과 교수
〈관심분야〉 개인정보보호기술, 클라우드컴퓨팅보안, 사이버보안

정 재 훈 (Jaehun Jeong) 학생회원
2009년 2월: 인제대학교 시스템경영공학과 학사
2011년 2월: 중앙대학교 일반대학원 경영학과 석사
2011년 3월~현재: 중앙대학교 일반대학원 경영학과 박사과정
관심분야: 정보보안 인식, 정보보안정책 준수