한국산학기술학회논문지
Vol. 12, No. 3 pp. 1408-1416, 2011

클라우드 컴퓨팅에서의 보안 고려사항에 관한 연구

박춘식[1*]
[1]서울여자대학교 정보보호학과

Study on Security Considerations in the Cloud Computing

Choon-Sik Park[1*]
[1]**Department of Information Security, Seoul Women's University**

요 약 클라우드 컴퓨팅은 컴퓨팅 리소스의 경비 절감과 효율은 물론 서비스의 확장 및 향상을 제공한다. 그러나 클라우드 서비스 사용자(기업 등)들은 클라우드 컴퓨팅 특성에 의한 여러 가지 위험들에 대해서 많은 염려를 갖고 있다. 본 논문에서는 클라우드 컴퓨팅 환경으로 인한, 시큐리티를 포함한 여러 가지 주요 이슈들을 검토하여 보고자 한다. 또한 시큐리티에 관한 문제들을 보다 구체적으로 분석하고 클라우드 컴퓨팅에 관한 위협들을 식별하여 시큐리티 위험을 줄일 수 있는 대략적인 대응책들을 제안하였다.

Abstract Cloud computing provides not only cost savings and efficiencies for computing resources, but the ability to expend and enhance services. However, cloud service users(enterprisers) are very concerned about the risks created by the characteristics of cloud computing. In this paper, we discuss major concerns about cloud computing environments including concerns regarding security. We also analyze the security concerns specifically, identify threats to cloud computing, and propose general countermeasures to reduce the security risks.

Key Words : Cloud Computing, Risks, Threats, Security Risks, Countermeasures

1. 서론

최근 컴퓨팅 환경은 메인 프레임 시대, 클라이언트 서버 시대, 웹 컴퓨팅 시대를 이어 클라우드 컴퓨팅 시대로 급속하게 변천하고 있다. 어플리케이션과 데이터가 메인 프레임에 집중되고 더미 단말에 의한 사용자 입력으로 그리고 Time Sharing System으로 대표되는 메인프레임 컴퓨팅 시대, 개인 PC의 발달로 집중에서 분산으로 패러다임이 변화된 클라이언트 서버 시대, 컴퓨터 가격의 저렴화와 네트워크 속도의 향상으로 그리고 웹 브라우저 활용으로 웹 컴퓨팅 시대를 맞이하였다. 어플리케이션과 데이터를 서버 측에서 집중 관리하고 가상화 기술을 이용해서 서버 관리 부담을 덜어주고 사용자는 확장성이 뛰어난 IT 리소스를 인터넷을 통해서 사용한 만큼의 비용 부담으로 서비스로 제공받을 수 있는 클라우드 컴퓨팅으로 급격하게 변화되고 있다. 또한, 클라우드 컴퓨팅은 분산컴퓨팅, 그리드 컴퓨팅, 유틸리티 컴퓨팅, 서버 기반 컴퓨팅, SaaS(Software as a Service) 등의 개념과는 큰 차이 없는 컴퓨팅 환경으로 새로운 기술보다는 새로운 컴퓨터 비즈니스 출현이라고 보는 면이 많다.

클라우드 컴퓨팅을 이루는 대표적인 기술은 가상화 기술과 대용량 분산처리기술로 클라우드 컴퓨팅의 핵심을 이루고 있다. 가상화 기술은 한 대의 서버로 마치 여러 대의 서버를 이용하고 있는 것처럼 작동시킬 수 가 있으므로 많은 사용자의 요구에 한 대의 서버로 대응할 수 있도록 할 수 있다. 따라서 서버의 이용 효율을 높일 수 있고 저렴한 요금으로 서비스를 제공할 수 있게 된다. 물론 동일한 능력의 처리를 적은 대수의 서버로 가능하므로 지금까지의 전력이나 냉각 비용의 절감 및 서버 설치 공간 등의 축소로 인한 경제적인 면에서의 이점도 있다[1].

본 논문은 2011학년도 서울여자대학교 교내학술특별연구비의 지원을 받았음..
*교신저자 : 박춘식(csp@swu.ac.kr)
접수일 11년 02월 18일 수정일 11년 03월 05일 게재확정일 11년 03월 10일

클라우드 컴퓨팅 환경이 되면 클라우드 컴퓨팅의 사용자인 개인 사용자나 기업 사용자가 피해를 보게 되는 것은 무엇이며 사용자 보호를 위한 것은 무엇을 검토해야 할까. 한편, 클라우드 컴퓨팅 산업 활성화를 위해서는 무엇이 장애가 되며 또한 활성화를 위해서는 무엇을 해야 할 까. 벌써 클라우드 컴퓨팅 활성화 만큼이나 정보 보안 분야의 관심도 높다[2-5]. 이에 본 논문에서는 클라우드 컴퓨팅과 관련된 주요 이슈들은 무엇이 있는 지 그리고 특히 클라우드 컴퓨팅과 관련된 보안 이슈는 무엇이 있는 지 제안하고자 한다. 그리고 클라우드 컴퓨팅과 관련된 보안 이슈와 함께 검토해야 할 보안 요구 및 검토 사항들에 대해서 제안하고자 한다.

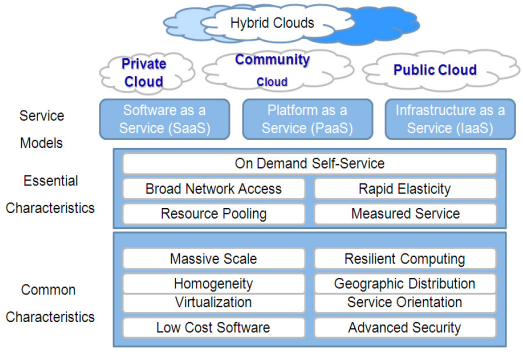
2. 클라우드 컴퓨팅

NIST(National Institute of Standard Technology)에 의한 클라우드 컴퓨팅 정의[6]는 “클라우드 컴퓨팅은 최소한의 관리 노력과 서비스 제공자와의 연동으로 빠르게 제공되고 보급될 수 있는 컴퓨팅 리소스(네트워크, 서버, 스토리지, 애플리케이션 그리고 서비스)의 저장고에 가용, 편리, 온 디멘드 네트워크 접근이 가능한 모델”이다.

다른 편의적인 정의로는, 클라우드 컴퓨팅 서비스는 인터넷 등의 브로드밴드 회선을 경유해서 데이터 센터에 축적되어 있는 컴퓨터 리소스를 서비스하는 것으로 원격지로부터 이용자에게 제공되는 것으로 확장성(Scalability), 가용성(Availability), 민첩성(Agility), 가시성(Visibility), 경제성(Economy) 등의 특징이 있다. 확장성은 이용자측이 필요한 만큼의 컴퓨터 리소스를 이용하도록 하며 업무량에 따라 컴퓨터 리소스를 유연(Flexibility)하게 증감시키는 기능을 말하며, 가용성은 클라우드 서비스 제공자 측의 입장에서 특정 서버 또는 서버 군이 문제가 발생하더라도 다른 서버들이 처리할 수 있도록 하여 서비스를 중단 없이 지속하게 할 수 있는 기능을 의미한다. 민첩성은 서비스 이용자가 컴퓨터 리소스를 이용하고자 할 경우 구매, 설치 등과 같은 별 다른 시간 소요 없이 즉시 이용할 수 있는 기능이며 가시성은 클라우드 서비스 리소스에 대한 측정 관리가 가능하며 컴퓨터 리소스의 초기 투자비용이 소요되지 않고 Pay-to-Use에 따른 경제성이 있다.

한편, 클라우드 컴퓨팅은 웹 2.0과 같은 인터넷 기술을 활용하여 SaaS, PaaS (Platform as a Service), IaaS(Infrastructure as a Service)의 3가지 가상화된 대표적인 서비스를 제공하고 있다 그림 1. SaaS 서비스는 어플리케이션 소프트웨어의 기능을 인터넷에서 제공하는 것이며, PaaS 서비스는 어플리케이션이 동작하는 플랫폼이나 개발 환경이나 도구들을 인터넷의 웹 환경에서 제공하는 서비스 그리고 IaaS 서비스는 서버의 컴퓨팅 능력이나 스토리지 등의 하드웨어를 인터넷을 통하여 제공하는 서비스를 각각 의미한다.

클라우드 컴퓨팅의 구성 모델 정의[6]에 의하면 4개의 구성 모델로 이루어지며, 4개의 구성 모델은 Private cloud, Community cloud, Public cloud, Hybrid cloud로 정의되고 있다. Private cloud는 클라우드 인프라가 조직만을 위해 운용되는 것이다. 조직이나 제 3자에 의해 관리될 수 있으며 구내에 위치할 수 있다. Community cloud는 클라우드 인프라는 여러 조직들에 의해 분산되며 클라우드 인프라는 분산된 관계 사항들을 정리한 특정 커뮤니티를 지원한다. Public cloud는 클라우드 인프라가 일반적인 공공 또는 대기업에게 가용될 수 있으며 클라우드 서비스 제공 조직에 의해 소유된다. Hybrid cloud는 클라우드 인프라가 데이터와 어플리케이션 이동을 가능하게 하는 표준 기술에 의해 하나로 묶거나 대표 사용자로 하기 위해 2개 이상의 클라우드를 합친 것을 의미하고 있다.



[그림 1] NIST의 클라우드 서비스 모델

3. 클라우드 컴퓨팅 주요 고려사항

2장에서 설명한 바와 같이 클라우드 컴퓨팅 서비스는 여러 가지 많은 장점이 있다. 그러나 클라우드 컴퓨팅을 둘러 싼 여러 가지 장애 또는 해결해야 할 과제들도 많이 산적해 있다. 본 장에서는 클라우드 컴퓨팅과 관련한 여러 가지 주요 이슈들을 살펴보고자 한다.

2008년 6월 가트너가 분석 제시한 보고서[7]에 의하면 클라우드 컴퓨팅과 관련하여 사용자에 대한 정보 수집 관리, 규정 준수, 데이터의 물리적 위치, 사용자 데이터 구분, 복구, 조사 지원, 장시간동안의 생존성 확보 등의

7가지 시큐리티 문제들을 맨 처음 거론하였다. 또한, 2008년 미국 CIO Research 리포트에서도 클라우드 컴퓨팅을 둘러 싼 문제점으로 시큐리티, 기존 시스템과의 융합(Integration), 데이터에 대한 제어권 상실, 가용성(Availability), 성능(Performance), IT 거버넌스, 규정 및 컴플라이언스 등의 순서로 지적되고 있다. 2008년 8월 세계적인 조사 기관인 IDC 보고서에 의해서도 클라우드 컴퓨팅에서의 주요 이슈들로 시큐리티, 성능, 가용성, 기존 시스템과의 융합 등이 거론되고 있다[8].

2009년 2월에 발표된 University of California at Berkeley 기술보고서[9]에 소개된 클라우드 컴퓨팅의 발전이나 클라우드 컴퓨팅 도입 시 예상되는 대표적인 10가지 장애물들과 이러한 10가지 장애물들을 극복할 10가지 Opportunity(기회 그리고 해결방안)들이 수록되어 있다.

국내에서도 안정성, 시큐리티, 표준화 부재로 인한 클라우드로의 전환 어려움, 기존 레거시 인프라로부터의 전환에 따른 기회비용 및 정확한 투자대비효과 계산의 어려움과 법제도 부재, 사용자 보호 대책 부재, 기업정보 및 개인정보보호 미흡 등을 클라우드 컴퓨터 활성화의 장애요소로 언급하고 있다[10].

이러한 각종 자료들과 보고서들[4,5,7-10]이 지적하는 클라우드 컴퓨팅과 관련된 주요 이슈들을 크게 분류하며 다음과 같이 정리할 수 있다.

- 시스템 안정화
- 클라우드 데이터 센터(서버) 위치
- 시큐리티/프라이버시
- 상호운용성(표준)
- 컴플라이언스 등

3.1 클라우드 시스템 안정화(Availability)

클라우드 서비스를 도입하는 데 주저하는 이유로 가장 많이 언급되는 이유 중의 하나로 클라우드 서비스의 안정화가 거론되고 있다. 이는 클라우드 서비스를 이용하는 이용자의 업무나 데이터 등이 클라우드에 전적으로 의존하는 형태로, 제3의 업체를 전적으로 신뢰해야 하기 때문이다. 즉 클라우드 서비스를 이용하는 고객의 입장에서 보면 언제 클라우드 서비스가 중단되거나 사용될 수 없을 지 불안함을 갖게 될 것이며 이는 서비스 도입의 중대한 고민을 갖게 되는 이유가 된다.

특히, 클라우드 서비스 제공업체의 폐업이나 클라우드 서비스 제공업체의 M/A 등에 의해 클라우드 서비스가 중단될 경우에는 클라우드 서비스를 이용하는 고객 입장에서는 저장된 데이터나 자료 등에 대한 계속 사용 여부가 중요한 문제가 될 것이다. 또한 클라우드 서비스를 이용하여 또 다른 고객들에게 서비스를 제공하는 경우, 신뢰도 및 책임 문제까지 복잡하게 될 수가 있다.

위키피디아[11]에 의하면 2010년 현재까지 일시적 서비스 중단 및 폐업한 클라우드 서비스 기업과 관련 내용들이 소개되고 있다. 표 1에서는 클라우드 서비스 대표 기업들의 서비스 중단 사례에 대한 내용을 나타내고 있다.

[표 1] 클라우드 서비스 중단 사례

서비스명	회사	서비스 분류	발생 시기 : 정지 시간
Gmail (GoogleApps)	구글	SaaS (메일 서비스)	‘08.6:12시간 ‘08.8:15시간 ‘09.9: 6시간
Force.com (SalesforceCRM)	세일즈포스	PaaS (SaaS)	‘05.12: 5시간 ‘08.2: 7시간 ‘10.1: 1시간
ES2/S3	아마존	PaaS /IaaS	‘08.2: 3시간 ‘08.4: 수시간
BPOS(전자메일, 웹 회의, Sharepoint등)	MS	SaaS	‘10.8: 2시간 ‘10.9: 특정 ‘10.9: 고객

클라우드 서비스 안정화를 위해서는 서비스 이용자의 데이터를 저장 보관하여 비상 시 활용할 수 있는 임치(Escrow) 제도가 필요하며 클라우드 데이터 센터의 백업이나 업무 연속을 통하여 안정된 서비스를 제공할 수 있도록 하여야 한다. 또 다른 방법으로 안정된 서비스와 과금과의 관계 설정을 통하여 보다 높은 품질의 서비스에는 상응하는 요금을 지급하는 서비스 요금 체계를 갖추고 이를 서비스 제공자와 이용자 간에 계약에 의해서 그리고 정량화하여 서비스 품질에 대한 만족을 제공할 수 있는 표준 SLA(Service Level Agreement) 제도를 활용하는 것도 대안이 될 수 있을 것으로 판단된다.

특히, 임치 제도는 클라우드 서비스 제공자의 파산, 폐업, 물리적 파손 등에 대비한 사용자의 저장 데이터를 안전하게 보호하여 클라우드 서비스 제공자의 안전성 및 신뢰성을 제고할 수 있으며 사용자의 보호 및 클라우드 서비스 안정화에 기여할 수 있을 것으로 판단된다.

3.2 클라우드 데이터 센터(서버) 위치

클라우드 서비스는 비교적 클라우드 데이터 센터를 대용량으로 건설하여 IaaS 등의 서비스를 제공하고 있다. 특히 구글 등과 같은 클라우드 서비스 선도 기업들은 거대한 클라우드 센터를 전 세계에 걸쳐서 건설하고 있다. 이는 서버 대수에 의한 규모 경제로 클라우드 서비스의

저렴화를 통하여 시장에서의 경쟁력을 확보하고자 하는 전략에 해당된다. 자국 외에 클라우드 센터(서버)가 존재하는 경우에는 국내 정보의 국외 유출 문제, 국외 센터의 외국 정부(수사기관 등)의 정보 제공 여부, 재판 관할권(어느 나라/어느 주), 개인정보보호법/데이터보호법 /감사 등 적용 여부 등이 심각한 문제로 대두될 가능성이 높다. 실제로 스위스에서는 구글 앱스를 이용하여 스위스 은행 고객의 데이터를 클라우드 서비스로 이용하고자 하였으나 구글의 클라우드 센터가 스위스 외부에 존재하여 서비스 제공이 어려웠지만 구글이 스위스 내에 클라우드 센터 즉 해당 서버를 설치하는 것으로 정리된바 있다. 또한 아마존이 EU에 클라우드 서비스를 전개하는 과정에서 EU내의개인정보는EU 밖으로 전송 곤란한 EU 규정에 의해 EU내에 데이터 센터를 별도로 설치하여 서비스를 제공하게 되었다.

대책으로는 사용자가 국내/국외 서버 위치를 선택할 수 있는 선택권을 제공하는 방안, 사용자가 요구 시 클라우드 서비스 제공자는 서버 위치 정보를 제공하거나 외국 정부(수사기관) 요청에 대한 클라우드 서비스 제공자가 고객의 정보를 제공한 경우에는, 사후라도 그 결과를 사용자에게 통보하도록 하는 방안 들이 고려될 수 있다.

3.3 클라우드 서비스와 보안

클라우드 서비스 도입에 가장 문제가 되는 것으로 시큐리티 문제를 가장 많이 언급하고 있다. 이는 클라우드 서비스가 가지는 특성이 서비스를 제공받기 위해서는 전적으로 제3의 업체를 신뢰해야 하기 때문이다. 기존의 자사 기업 내에서 관리하던 보안 개념과 외부 업체에 데이터나 업무 자료를 보관 의존하여 관리하는 보안 개념은 전적으로 다를 수 밖에 없다.

또한 클라우드 데이터 센터에는 많은 기업이나 개인 등의 고객 정보가 저장 보관되고 있어 해커(테러)의 공격 목표가 될 가능성이 증대되며, 클라우드 센터 내부자에 의한 중요 데이터의 유출 위협도 상존할 것으로 예상된다. 클라우드 실행 환경이나 특성상 분리가 취약한, 즉 복수 이용자가 동일 자원을 사용할 수 밖에 없는 환경에서 그리고 방대한 처리 전송 및 저장 데이터 등의 관점에서 클라우드 서비스는 많은 시큐리티 문제점을 내포하고 있다.

클라우드 컴퓨팅 보안에 관해서는 15개의 도메인별 시큐리티를 설명하고 있는 CSA(Cloud Security Alliance) 보고서[4]와 기술적, 법적, 정책적 권고들을 다루고 있는 유럽연합의 사이버보안기관인 ENISA(the European Network and Information Security Agency) 보고서[5]가 있다. 본 논문에서 제안하고자 하는 클라우드 서비스의 보안 위협과 대책에 대해서는 4장과 5장에 설명하였다.

3.4 Inter-Cloud 상호운용성

클라우드 컴퓨팅 서비스에서의 또 다른 중요 이슈로 클라우드와 클라우드간 그리고 클라우드와 이용자와의 상호 운용 환경에 대한 문제가 있다. cloud - cloud 상호 운용과 user(Enterprise)- cloud 운용 문제로 상호간의 파일 포맷, API, 데이터 포맷 등의 표준이 되어 있지 않아, 즉 Data Lock-in 문제가 발생하여 특정 클라우드 서비스 제공자에서 다른 클라우드 서비스 제공자로의 이전이나 이관이 자유롭지 못하며 클라우드 서비스 제공자 간의 이전도 자유롭지 못한 문제가 발생하게 된다.

이는 클라우드 서비스 제공자 전환을 어렵게 하며, 종료 또는 제공자 파산 시 데이터 및 서비스 전환 또한 어려워 결국에는 특정 클라우드 서비스 제공자에게 종속될 수가 있다. 이러한 문제는 기업 고객 입장에서 보면 업무 연속성(BCP) 에 심각한 문제를 야기할 수 있게 된다.

예상 대책으로 데이터 파일 포맷, API 포맷 등의 Interoperability를 보장하거나 SLA에 의한 서비스 보장, 그리고 클라우드 서비스 표준(상호운용성, 보안 표준 등)을 제정하는 방안이 있다.

3.5 컴플라이언스 등

클라우드 컴퓨팅 서비스와 관련된 기타 이슈로 거버넌스와 컴플라이언스 문제를 고려할 수 있다. 거버넌스 문제는 사용자가 제어권을 서비스 제공자에게 일임하거나 클라우드 서비스 제공자가 데이터 위치 정보를 제공하지 않거나, 외부 침투 테스트 불허 등으로 인한 거버넌스 결여를 말한다. 컴플라이언스 문제는 사용자에 의한 감사(audit)를 서비스 제공자가 수용하지 않거나 규정 준수 증거를 제시하지 못하는 것이 이슈가 될 수 있다.

이외에도 소프트웨어 라이선스 문제, 지적재산권/저작권 문제, e-discovery 등(데이터 복구, 보관, 폐기, 재활용 오남용 등), 기존 어플리케이션과의 병행 사용 여부, 과금 방식 등이 주요 이슈가 될 것으로 판단된다.

4. 클라우드 컴퓨팅의 보안 위협

본장에서는 3장에서 살펴 본 클라우드 컴퓨팅의 주요 이슈 가운데에서 보안에 관련된 부분으로, 클라우드 컴퓨팅 환경이 갖게 되는 보안 위협 요소를 제안하고자 한다.

클라우드 컴퓨팅의 보안 위협으로는 공격이 예상되는 요소와 기존의 일반적인 보안 위협외의 클라우드 컴퓨팅

특성으로 인한 보안 위협으로 크게 나누어 생각해 볼 수 있다. 클라우드 컴퓨팅에서 공격이 예상되는 보안 위협의 주요 요소로는 클라우드 사용자, 클라우드 서비스 제공자 그리고 클라우드 사용자와 클라우드 서비스 제공자 사이와 클라우드 서비스 제공자간의 네트워크가 공격 대상이 될 수 있다.

다음으로 클라우드 컴퓨팅 특성 또는 환경으로 새롭게 예상되는 보안 위협을 생각해 볼 수 있다. 클라우드 컴퓨팅의 특성 중의 하나인 Multi-Tenant 환경으로 인하여 클라우드 데이터 센터에는 복수의 클라우드 서비스 이용자와 다양한 형태의 중요도를 갖는 이용자의 데이터가 공존하고 있다. 이러한 형태의 클라우드 환경은 다양한 형태의 취약성과 복합적인 형태의 위협 패턴이 예상된다.

가상화 기술의 취약점에 의한 공격 등 클라우드 컴퓨팅 환경에 예상되는 보안 위협들은 다음과 같다.

4.1 클라우드 컴퓨팅에 대한 외부 공격

클라우드 컴퓨팅 환경의 특성상 이용자의 데이터 등이 클라우드 데이터 센터 한 곳에 집중되어 관리되고 있기 때문에, 이러한 클라우드 컴퓨팅 환경이 해커 등의 공격 대상이 될 가능성이 높다. 클라우드 서비스 센터 한 곳으로의 데이터 집중은 보호해야할 범위를 줄여주는 면이 있지만 공격이 성공할 경우의 피해 정도는 심각해질 수 있다. 클라우드 데이터 센터에 대한 분산서비스거부공격, 불법 접근, 정당한 클라우드 사용자를 위장한 공격 등이 예상된다.

4.2 가상화 기술 취약성에 의한 공격

클라우드 컴퓨팅에서의 핵심 기술은 가상화, 대용량분산처리, 운용 및 정보보호기술이다. 이중에서 가상화 기술은 현재 많은 취약점들이 발표되고 있으며 이들 취약점을 이용한 공격도 소개되고 있다. 향후 클라우드 컴퓨팅이 활성화되면 가상화 기술의 취약점을 이용한 공격은 크게 늘어날 것으로 예상된다.

가상화 기술 취약성에 의한 이러한 공격은, 클라우드 이용자가 공격자가 되어 동일 클라우드 컴퓨팅 환경 내의 다른 클라우드 이용자가 공격을 받게 되는 사태가 예상된다. 클라우드 컴퓨팅 환경에서는 인접한 환경에 다른 이용자가 있는 것이 일반적이므로 이용자는 인접한 환경에 있는 공격자로부터 클라우드 컴퓨팅 환경을 통해서 공격받게 되고 그 결과 중요한 정보를 잃어버릴 가능성이 있다. 이외에도 클라우드 컴퓨팅 센터 내부의 각종 리소스에 대한 다양한 취약점과 공격 루트를 이용한 공격이 예상된다.

4.3 클라우드 환경을 이용한 공격

요금이 저렴하고 쉽게 이용할 수 있는 클라우드 컴퓨팅 특성을 이용하여 현재까지 공격에 소요되는 대규모 예산으로 인하여 시도해보지 못했던 공격들이 시도될 가능성이 있다. 즉, 클라우드 컴퓨팅 환경을 공격의 도구로써 악용할 가능성이 있다. 클라우드의 막대한 리소스(컴퓨팅 및 스토리지 등)를 이용해서, 제3자에 대해서 DDoS 등의 사이버 공격 등을 시도할 수 있다. 또한 정당한 클라우드 이용자의 환경에 해커 등이 악성코드 등의 주입을 통해서 클라우드 외의 시스템 등에 공격하는 시나리오도 예상될 수 있다. 클라우드 컴퓨팅 이용만으로도 이러한 공격이 쉽게 그리고 저렴하게 이루어질 수 있게 된다.

또한 클라우드 컴퓨팅의 리소스를 이용하여 패스워드 크래킹이나 암호 키 해독 등을 쉽게 수행할 가능성이 있다. 이는 저렴하고 효율적으로 막대한 클라우드 컴퓨팅 리소스(컴퓨팅 파워, 스토리지 등)를 쉽게 이용할 수 있는 점과 클라우드 서비스 제공자가 서비스 이용자의 부정한 행위를 식별할 수 없는 문제점에 기인한 것으로 향후에도 다양한 공격들이 예상된다.

4.4 클라우드 내부 공격 등에 의한 위협

클라우드 컴퓨팅 센터에는 다양한 레벨의 이용자 데이터와 각종 서비스가 운용되고 있다. 이러한 클라우드 컴퓨팅 환경으로 인하여 기존 IDC나 서버 관리센터보다도 더욱 더 내부자에 의한 정보 유출 등이 발생할 가능성이 높다. 특히, 중요 데이터 및 개인정보 유출이 예상되며 데이터 센터 등에서의 정전이나 소프트웨어나 하드웨어의 불일치에 의한 서비스가 정지하여 클라우드 이용자가 서비스를 이용할 수 없게 되는 경우도 예상된다.

4.5 네트워크에 대한 위협

클라우드 서비스 이용자와 클라우드 서비스 제공자간의 네트워크 그리고 클라우드 서비스 제공자와 클라우드 서비스 제공자간의 네트워크에 대한 보안 위협으로는 전송되는 각종 데이터의 도청, 변경 그리고 파괴 등이 예상된다. 물론 이러한 위협은 일반적인 위협이지만 클라우드 컴퓨팅 환경과 관련하여 외부 네트워크를 통해서 클라우드 서비스 등을 이용하거나 데이터를 전송하는 측면에서 훨씬 더 공격을 받을 위협에 많이 노출되어 있다.

또한 네트워크를 통한 불법 접근이 빈번하게 발생할 것으로 예상되며 권한 밖의 접근이나 이용자를 위장한 공격도 예상된다.

4.6 컴플라이언스 등 위협

클라우드 컴퓨팅 환경의 대표적인 특성 중의 하나인 Multi-Tenant 환경으로 인하여 클라우드 컴퓨팅 센터 서버에는 다양한 이용자의 서비스와 데이터가 저장 운용되고 있다. 특정 이용자의 보안 감사가 진행될 경우 동일 클라우드 컴퓨팅 환경에 있는 다른 이용자의 데이터 등에 관한 정보가 새어나갈 수 있는 위협이 있다. 이는 동일 클라우드 컴퓨팅 환경 내에 있는 특정 이용자만의 데이터만을 제공할 수 없기 때문에 발생하는 것으로 향후 클라우드 컴퓨팅의 커다란 위협이 될 수 있다.

특히 어떠한 보안 규정이나 보안 관리 체계를 통하여 보안을 준수하고 있는 지를 외부에서는 파악하기가 어려운 점 등은 물리적 관리적 측면에서의 보안 위협이 예상되는 부분이다.

5. 클라우드 컴퓨팅 보안 대책

5.1 클라우드 컴퓨팅 분야별 보안 대책

본 절에서는 클라우드 컴퓨팅 환경에서의 서비스 이용자, 클라우드 컴퓨팅 서비스 제공자의 분야별 보안 대책 중 기본적으로 고려되어야 할 보안 대책을 제안하고자 한다.

5.1.1. 클라우드 서비스 이용자 보안 대책

먼저 클라우드 서비스 이용자는 이용자 자신의 비즈니스 프로세스 가운데 무엇을 어느 정도까지 클라우드 서비스로 이용할 지를 이용자가 판단해야 한다. 이때, 이용자 자신의 비즈니스 업무의 표준화와 자동화를 이루는 것이 선결되어야 하며 클라우드 서비스 이용 업무와 기존 업무와의 병행 사용에 대한 검토가 선행되어야 한다.

다음으로 이용자 자신의 업무 프로세서나 데이터의 중요성을 평가하여 클라우드 서비스 제공자가 공개하는 정보보호 대책, 안정성, 서비스 레벨, 감사 및 정보 공개 여부, 피해 복구 계획 등의 항목을 참조하여 클라우드 서비스 제공자를 선정하는 것이 바람직하다. 물론 표준 SLA를 참조하여 이용자 자신에 맞는 형태의 SLA를 만들어 서비스 계약하는 것이 필요하다.

클라우드 서비스 이용자의 보호 대책으로 클라우드 서비스 제공자는 이용자에 대한 인증 서비스를 제공해야 하며, 누가 어떠한 서비스, 어떠한 레벨의 권한을 갖고 있는 지, provisioning을 어떻게 하는 지에 대한 관리가 필요하다. 서비스 이용자는 자신의 접근 권한에 대한 보안을 유지하는 것이 중요하다.

또한 클라우드 서비스 제공자에게 보내어지거나 수신되는 모든 데이터가 도청이나 누설 등으로부터 안전하게 보호될 수 있도록 암호 등에 의한 네트워크 보안 대책이 이루어져야 한다.

5.1.2. 클라우드 서비스 제공자 보안 대책

클라우드 서비스를 이용하고자 하는 이용자 입장에서 자신의 데이터 등을 제3자인 서비스 제공자에게 위탁한다는 사실 그 자체가 불안할 수 밖에 없다. 클라우드 서비스 제공자의 경쟁력 강화 차원은 물론이고 기본적으로 클라우드 서비스 활성화를 위해서도 반드시 보안 대책이 마련되어야 한다. 물론 클라우드 서비스 제공자는 제공자의 정보보안정책, SLA, 신뢰성 있는 기관으로부터의 정보보호관리 공인 등 서비스 이용자가 서비스 제공자의 보안 대책을 판단하는 데 도움이 되는 정보를 제공하여야 한다.

제공되어야 할 정보보안 대책으로, 클라우드 데이터 센터는 해커 등의 공격으로부터 노출되어 있으므로, 클라우드 서비스 제공자는 사고나 공격에 대한 예방, 감시 및 사후복구를 위한 CERT와 같은 조직을 만들어 운영하여야 하며 실시간으로 서비스 이용자에게 관련 정보를 제공하도록 하여야 한다.

부정한 사용자의 접근을 방지하거나 사용자 내부의 권한 외의 접근을 방지하기 위한 강력한 접근 방지 및 인증 방식을 제공하여야 하며 정당한 사용자의 클라우드 데이터 센터 접근 후 내부의 다른 이용자의 데이터 등에 접근할 수 없도록 강력한 격리 기능도 제공되어야 한다.

클라우드 서비스 제공자가 관리하고 있는 클라우드 데이터 센터 내의 모든 데이터는 개인정보 및 기업의 비밀정보 등으로 다양한 중요도의 데이터 및 서비스가 관리 운용되고 있으므로 강력한 암호 기술에 의한 보안 대책이 마련되어야 한다.

또한 DDoS와 같은 해킹 공격이나 재난 등에 의한 시스템 및 서비스 중단 사태를 방지하기 위한 업무 연속 계획 및 백업을 통한 복구 계획이 확보되어 있어야 한다. 물리적으로도 내부 유출 범행이나 외부로 부터의 침입 방지를 위한 CCTV, 출입보안 등의 보안 대책이 마련되어야 한다.

5.2 클라우드 서비스의 기술적 보안

본 절에서는 클라우드 컴퓨팅의 기술적 보안 대책 관점에서 특히 기본적으로 필요로 하는 클라우드 컴퓨팅의 핵심 보안 기술들을 제시하고자 한다. 현재 가장 필요로 하는 분야는 가상화 컴퓨팅 환경에 대한 취약점으로 인

한 위협이 발생할 것으로 예상되어 이에 대한 secure virtual technology가 시급한 것으로 판단된다. 클라우드 컴퓨팅 서비스 제공자 입장에서는 부당한 사용과 과금에 대한 보호 대책이 가장 시급할 것으로 예상되므로 IAM(Identity and Access Management)에 대한 효율성과 안전성이 보장되는 기술이 필요할 것이다. 한편 사용자 입장에서는 기업이나 개인의 데이터를 제3자에게 의뢰해야 하는 입장이므로 데이터의 안전한 보관을 위한 기술인 안전도가 높은 암호 기술이 핵심이 될 것이며 또한 개인 정보의 저장 장소에 대한 불명확화로 인한 그리고 클라우드 서비스 제공자에 의한 남용이나 유출로 인한 보호 대책 수단인 암호 기술 또는 프라이버시 보호 기술이 필요할 것으로 판단된다.

대용량 데이터 암호에 따른 고속 처리와 효율적인 키 관리 기술, 빈번한 사용자 접근에 대한 인증 기술, 클라우드 컴퓨팅 환경에서는 보다 더 강력할 것으로 예상되는 DDoS 공격에 대한 대응 기술도 주요한 기술이 될 것이다. 인증기술로는 SSO(Single Sign On), SAML(Security Assertion Markup Language), Kerberos 등이 예상되며 강력한 로그 감시 및 관리 기능, Secure VM, Secure Hypervisor, Secure Hadoop, Secure NAC(Network Access Control) 기술 등이 필요할 것으로 예상된다.

-안전한 가상화 기술(Secure VM)

가상화 기술이 클라우드 컴퓨팅에서는 아주 중요한 역할을 한다. 가상화 환경에서는 가상으로 OS를 동작시키는 기술(게스트 OS)과 그것을 관리하는 호스트 OS가 존재한다. 이러한 가상화 환경에 있어서, 게스트 OS로부터 호스트 OS상의 권한을 취득하는 등의 공격이 가능하게 되면, 다른 게스트 OS의 정보를 훔치거나 변경하는 등의 가상화 기술의 취약점으로 인한 사태가 발생할 수 있다. 가상화 기술에 대한 취약성이 이미 많이 보고되고 있으며 이를 이용한 공격도 보고되고 있다.

따라서 클라우드 서비스에서 새롭게 고려해야 하는 보안 기술로써 가상화 기술에 의한 취약성을 배제하거나 회피하는 등의 효율적이고 안전한 기술이 요구된다.

-저장 데이터 보호 기술

클라우드 서비스에서 가장 중요한 기술 중의 하나로 클라우드 데이터 센터(서버)에 저장되어 있는 데이터가 변경, 유출, 소실, 누설, 소거 등에 의한 위협으로부터 보호하는 암호 기술이다.

외부로부터 요구되는 서비스에 효율적으로 대처하기 위해서는 단순한 암호 기술이 아니라 강력한 암호 기능과 연산 속도가 고속으로 가능한 그리고 접근 제어와 익명성이 제공될 수 있는 암호 기술이 필요하다.

또한 고속이며 안전한 데이터베이스 암호 기술은 물론이고 암호에 따른 키 관리 기술도 클라우드 서비스에 적합한 새로운 기술이 고려되어야 한다. 현재 검토되고 있는 기술로는 속성기반암호(Attribute Based Encryption) 등이 제안되고 있다.

-안전한 Auditing 기술

클라우드 컴퓨팅 환경의 대표적인 것 중의 하나가 Multi Tenant 환경으로 복수의 사용자가 동일 서버의 스토리지 등의 환경을 공유하여 사용하고 있다. 이러한 클라우드 환경에서 클라이언트로부터의 처리가 안전하게 그리고 정확하게 실행되고 있는 지를 확인하기 위해서는 컴플라이언스 차원에서 감사(Auditing)가 클라우드 컴퓨팅 서비스 제공자에게 요구되어 질 수 있다. 이때, 외부기관으로부터의 보안 감사가 진행될 때 해당 사용자의 데이터 등에 대한 감사만 이루어지고 다른 사용자의 데이터에 대한 접근은 통제 하에 이루어질 수 있도록 해야 한다.

이를 효율적으로 제공할 수 있는 기술들이 현재 부족한 실정이므로 암호 기술이나 접근 제어 기술 또는 threshold encryption 기술 등을 이용한 안전한 Auditing 기술이 이루어져야 한다.

-로그 관리 기술

클라우드 서비스나 클라우드 데이터 센터(서버)에 대한 해커 등에 의한 부정 접근이나 내부자에 의한 정보 유출 등의 사고 경위 파악이나 역추적 등을 위한 로그 기록 보존 및 관리가 필요하다. 또한 서비스 이용자와 제공자 사이의 분쟁 발생이나 컴플라이언스에 따른 대책으로 로그 정보 등의 전자적 기록 보존이 일반적으로 요구되고 있다.

특히, 클라우드 컴퓨팅 환경에서의 로그 기록 관리는 클라우드 서비스 제공자가 서비스 이용자의 데이터, 특히 개인정보나 기업비밀정보 등을 볼 수 있으며 그 범위 또한 방대하며 해킹 등에 의한 불법 접근에 대한 정보 또한 광대하여 클라우드 컴퓨팅 환경에 적합한 클라우드 포렌식 기술이나 클라우드 컴퓨팅 로그 관리 기술이 별도로 필요하며 마련되어야 한다.

-강력한 인증 기술

클라우드 서비스 제공자 입장에서는 부당한 사용 방지와 올바른 과금 관리를 위하여 사용자에 대한 정당성 여부를 즉 권한을 가지고 있는 지를 확인하는 것이 중요하다. 또한, 사용자들이 서비스 마다 ID나 패스워드를 만들

지 않아도 상호운용성이나 사용자 편리성을 고려하여 하나의 ID로 서비스가 제공되는 환경이 필요하며 이를 위한 ID 관리가 클라우드 환경에서는 필요하다.

클라우드 서비스 제공자 입장에서의 강력한 인증 및 효율적인 ID 관리 기술로 IAM에 대한 효율성과 안전성이 보장되는 기술이 필요하다. 구체적인 인증 기술로는 SAML, XACML(eXtensible Access Control Markup Language), Open Authentication, Kerberos, Federated Identity(SSO)등이 필요하며 보다 적합한 기술들이 개발되어야 할 것이다.

또한 클라우드 서비스 제공자 관점에서는 서비스 이용자의 PC 등의 기기 인증 기능도 이루어져야 하며 서비스 이용자 관점에서 서비스 제공자의 기기 인증을 위해서 안전한 웹 사이트 이용 등의 기기 인증이 이루어져야 한다. 추가적으로 통합 인증 게이트웨이를 구축하여 다양한 클라우드 서비스 전개 형태에 적합하며 효율적인 인증 시스템이 제공되어야 한다.

5.3 관리적 보안 대책

클라우드 서비스 보안 대책에서도 기술적 보안 대책으로 해결하기 어려운 여러 가지 보안상의 문제점들을 관리적 보안 대책으로 마련해야 하는 경우가 많다. 관리적 보안 대책으로 고려할 수 있는 것들로 클라우드의 정보보호관리체계 및 개인정보보호관리체계 인증, 클라우드 상호 운용 표준, 클라우드 데이터의 임치, 이용자 서버 선택, 서버 접근 정보 공개 등이 있다.

클라우드 컴퓨터의 ISMS(Information Security Management System)와 PIMS(Personal Information Management System) 제도는 관리적 보안 대책의 대표적인 것으로 클라우드 서비스 제공자 등 클라우드 서비스 전반적인 보안 수준을 높일 수 있는 것으로 기존의 ISMS 및 PIMS 제도가 클라우드 서비스에도 반드시 적용 운용되어야 한다.

클라우드 서비스 제공자의 데이터, 파일, API 포맷 등이 특정 서비스 제공자에게 종속되어 다른 클라우드 서비스 제공자로의 이동 시나 다른 클라우드와의 상호 운용 시 data lock-in 문제점이 발생하게 된다. 이러한 문제점의 관리적 보안 대책으로 API나 데이터 포맷의 공통화, 표준화를 통한 클라우드 상호 운용 표준의 환경 구축이 필요하다.

클라우드 서비스의 업무 연속성 확보나 사고 복구 계획에 대한 관리적 대책으로 백업 시스템의 구축이 구축되어야 하며 백업 시스템의 복구 계획 및 성능에 대한 확보가 이루어져야 한다. 복구 및 업무 연속성 확보 차원에서 클라우드 임치 방안과 같은 관리적 보안 대책 또한 제공되어야 한다.

클라우드 서비스 이용자의 서버 선택에 대한 것은 서비스 이용자의 사용 서버가 어디에 있는 어떠한 것인지에 정보를 제공하거나 또는 이용자로 하여금 사용 서버를 선택하게 하는 등의 관리적 보안 대책이 필요하다. 또한 서버에 대한 수사기관 등의 합법적인 접근에 대해서도 해당 이용자에 대해 그러한 접근 정보를 제공해주는 것도 관리적 보안 대책 차원에서 필요한 것으로 판단된다.

6. 결론

본 논문에서는 클라우드 컴퓨팅 환경으로 인한, 시큐리티를 포함한 여러 가지 주요 이슈들을 검토하여 보고자 한다. 또한 시큐리티에 관한 문제들을 보다 구체적으로 분석하고 클라우드 컴퓨팅에 관한 위협들을 식별하여 시큐리티 위험을 줄일 수 있는 대략적인 대응책들을 제안하였다.

클라우드 컴퓨팅에서의 보안은 클라우드 컴퓨팅 산업 활성화 측면에서 아주 중요한 요소가 될 것으로 예상된다. 따라서 클라우드 컴퓨팅 서비스의 전개 및 활성화에 따라 보안상의 많은 문제가 발생할 것으로 예상되므로 향후에는 클라우드 컴퓨팅 환경에 보안 기술이 적용된 신뢰할 수 있는 클라우드 컴퓨팅이 보편화될 것이다. 클라우드 컴퓨팅 서비스에 따른 구체적인 취약점과 공격에 대한 대책 연구를 계속할 예정이다.

참고문헌

[1] 민옥기, 김학영 ,남궁한, “클라우드 컴퓨팅 기술 동향”, 전자통신동향분석, 제24권, 제4호, 8월, 2009년.

[2] 방송통신위원회, 행정안전부, 지식경제부, 범정부 클라우드 컴퓨팅 활성화 종합 계획, 12월, 2009년.

[3] 박춘식, 김형종, 김명주, “클라우드컴퓨팅 보안 동향”, 정보통신산업진흥원 주간기술동향, 제1432호, pp.26-35, 2월, 2010년.

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V.2.1, Dec. 2009.

[5] ENISA, “Cloud computing Risk Assessment: Benefits, risks and recommendations for information security”, http://www.enisa.europa.eu/, 11. 2009.

[6] P. Mell and T. Grance, "The NIST Definition of Cloud Computing(Draft)", SP 800-145, 1월, 2011년.

[7] J.Heiser and M. Nicolett, Assessing the Security Risks of Cloud Computing, Gartner, 6월, 2008.
[8] IDC, "클라우드 컴퓨팅 활성화에 따른 이슈", IDC Enterprise Pannel, 8월, 2008.
[9] Michael Armbrust, etc, Above the Clouds: A Berkeley View of Cloud Computing, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html, 2월, 2009년.
[10] 한국정보사회진흥원, “2009년 주요 IT 전략기술에 따른 보안 이슈 및 해결 방안”, IT Issues Weekly 제197호, 1월, 2009년.
[11] http://wiki.cloudcommunity.org/wiki/CloudComputing:Incidents_Database.

박 춘 식(Choon-Sik Park) **[정회원]**

- 1995년 3월 : 일본동경공업대학교 전기전자공학과 (공학박사)
- 1982년 12월 ~ 1999년 12월 : 한국전자통신연구원 책임연구원
- 2000년 1월 ~ 2008년 12월 : 국가보안기술연구소 책임연구원
- 2009년 3월 ~ 현재 : 서울여자대학교 클라우드컴퓨팅연구센터 정보보호학과 교수

<관심분야>
개인정보보호, 클라우드컴퓨팅보안