Cloud Computing의 개인 정보 보안을 위한 취약점 분석*

선재훈** · 김귀남***

요 약

현재 클라우드 컴퓨팅은 연구기관과 학자들에 의해 여러 개념들로 정의되고 있다. 그러나, 최근 IT 분야의 비용과 효율을 더욱 중시하는 비즈니스 트랜드로 인해 클라우드 컴퓨팅은 가상환경 내에서 확장성을 가진 대용량의 자원들을 제공 할 수 있는 컴퓨팅의 한 형태로 정의되고 있다. 또한, 각 기업이 제공하는 클라우드 컴퓨팅 서비스의 다양성으로 인해 보안 문제가 대두되고 있다. 이러한, 다양한 클라우드 컴퓨팅 서비스에 필요한 여러 보안 기술들과 요구사항 및 개인 정보보호를 위한 사항들에 대한 취약점을 분석 하고자 한다.

Cloud Computing in the Vulnerability Analysis for Personal Information Security

Jae Hoon Sun** · Kuinam J. Kim***

ABSTRACT

Cloud computing is defined as numerous concepts by research institutions and scholars. However, due to the present business trend in the IT sector, emphasizing on cost and efficiency, cloud computing has been defined as a form of computing which can provide extendable mass storage components in the virtual environment.

As a result, security issues have been arising due to the variety of cloud computing services provided by the industries.

This paper aims to analyze the weaknesses such as security techniques and inquiries, and personal information protection required for various cloud computing services.

Key words : Cloud Computing, Security, Authentication, DRDos, Man-In-The-Middle

---

접수일 : 2010년 11월 17일; 채택일 : 2010년 12월 17일

* 본 과제는 경기도 기술개발사업의 사업비지원(과제번호A10101110)에 의해 수행되었습니다.

** 경기산업기술보안협의회

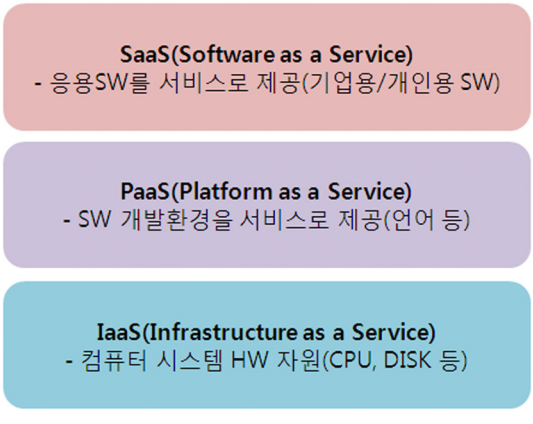
*** 교신저자, 경기대학교 산업보안학과

1. 서 론

최근 IT 분야에서 비용과 효율을 더욱 중시하는 비즈니스 트랜드에 부응하고 있는 클라우드 컴퓨팅은 관계기관, 학자들에 의해 여러 가지 개념으로 정의되어 왔으나, 확장 가능한 대용량의 자원들을 가상의 환경에서 제공할 수 있는 컴퓨팅의 한 형태로 정의 되고 있다[1].

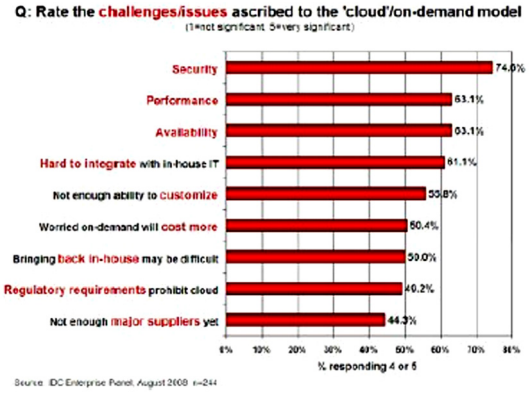
아마존(Amazon)의 AWS(Amazon Web Service), EC2(Elastic Compute Cloud), S3(Simple Storage Service)나 구글(Google)의 Apps 등에 이어서, 최근에는 Microsoft, IBM, HP, Oracle 등의 IT 관련 글로벌 기업들이 참여하고 있다[2].

또한 클라우드 컴퓨팅 서비스를 위해 Software as a Service(SaaS), Platform as a Service(PaaS), Infrastructureas a Service(IaaS) 등 다양한 형태의 클라우드 컴퓨팅 서비스 모델 및 제품들이 앞다투어 출시되고 있다[3].



(그림 1) 클라우드 컴퓨팅 서비스 계층 모델

그러나, 기존의 컴퓨팅 환경이 클라우드 컴퓨팅 환경으로 발 빠르게 진화 되어가며 발생 되는 많은 이슈들이 있으며, 그 중 가장 대표적인 것이 보안(security)문제로 각 기업들의 CEO 및 IT 관계자들 역시 우선적 고려사항으로 생각하고 있다[4].



(그림 2) 클라우드 서비스를 위한 해결과제

클라우드 컴퓨팅 서비스는 데이터를 보호하기 위해 별도의 자원을 할당하고 관리하는 형태를 가지는데 기업 또는 개인이 직접적으로 데이터를 별도 관리 하는 것보다 보안성이 높아지는 것이 일반적이다.

그러나, 기업이나 개인의 민감한 데이터에 대한 직접적인 제어권한을 포기해야 하고 사고발생시 피해의 파급효과가 크기 때문에 기업(기술, 고객정보) 기밀 관리나 개인의 프라이버시 측면에서 많은 문제점들이 존재한다.

2. 클라우드 컴퓨팅 보안 요소기술

위에서 언급된 일련의 사고사례들과 잠재적인 위협의 방지를 위해 클라우드 컴퓨팅 환경에서 아래와 같은 기술적 요구사항들이 만족되어야 한다. 이 사항들은 기존의 IT 환경에서 요구 되었던 내용을 포함하게 되지만, 클라우드 컴퓨팅이 가상화, 분산화, 강화된 인증 등의 특징적인 기술들을 다수 사용하게 되므로 클라우드 컴퓨팅 환경에 맞는 요구사항들을 수용 할 수 있어야 한다[5].

2.1 기밀성과 데이터 암호화

개인과 기업의 데이터에 대한 기밀성(privacy)

보호를 위해서는 암호화(encryption) 기술이 적용되어야 한다. 특히 클라우드 컴퓨팅에서는 서비스의 특성상, 대용량 데이터의 암호화시 전체 시스템의 가용성 감소를 예상해야 하며, 가용성 유지를 고려한 적합한 암호가 이용되어야 하는데, 예를 들어 DES나 AES와 같은 블록 암호 알고리즘을 대신하여 스트림 암호를 사용하는 방안 등을 선택할 수 있다.

또한, 암호화 등 보안 기능이 적용시 컴퓨팅 자원 및 부대비용의 발생과 보안 사고시 예상되는 피해 규모를 예측과 자원 배분이 필요하다

2.2 인증과 제어

클라우드 환경에서는 다수 사용자의 데이터가 운용되므로 인증관련 기술들과 권한 관리 기술의 사용이 필수적인 사항이다.

많은 사이트 및 서비스를 단일 서버로 인증하는 Single-Sign On(SSO) 형태의 인증 기술, XML 기반으로 사용 권한을 제어하기 위한 프레임워크기술 등이 연구되고 있다.

전통적으로 사용자 인증에 쓰이던 전자서명 기술도 활용될 수 있겠지만, AWS의 전자서명에서 취약점이 발견된 사례를 통해, 특히 웹 기반 인터페이스를 사용하는 클라우드 환경에서는 인증 프로토콜에 대한 보안성 검증이 필수적이라 하겠다.

또한, 클라우드 컴퓨팅에서는 코드가 원격으로 실행되는 경우인 원격 인증과 가상 머신(VM) 상에서 프로그램의 실행 영역 및 메모리 보호(memory protection)를 위한 sandboxing 등 관련 연구가 진행되고 있다.

2.3 데이터의 무결성

클라우드 컴퓨팅 서비스의 특성상 외부와 사용자간 데이터의 송수신 및 메시지 교환이 빈번하므로 무결성 검증을 위한 오류 검사가 필수적이라 하겠다. 2008년 7월의 AWS S3 서비스 중단 사례는 서버 간에 교환되는 메시지에 대한 무결성 검사 루틴이 없었던 데서 기인하였다[3].

더욱 최근에 무결성 검증에 많이 사용되었던 MD5와 SHA의 취약점이 발견되면서 보다 강화된 보안성을 요구 받게 되었으며, 미국 NIST에서는 SHA-3의 공모 및 개발이 진행되고 있다[6].

2.4 가용성 및 복구

서비스의 중단이나 데이터의 손실을 막기 위해서는 사고시 서비스를 지속할 수 있는 고장 감내성(fault tolerance) 및 데이터 복구(recovery) 기법에 대한 연구가 매우 중요하다. 클라우드 서비스 중단 및 데이터의 연구적 손실이 발생한 사례들은 이러한 메커니즘들이 제대로 동작하지 않을 때 생길 수 있는 문제들을 보여준 예라 할 수 있겠다.

2.5 네크워크 보안 및 웹 보안

클라우드 컴퓨팅은 기본적으로 네트워크를 기반으로 하고 있기 때문에 기존의 네트워크 보안을 위해 적용되던 IDS, IPS, 방화벽, IPsec 및 VPN등의 보안기술을 효율적으로 적용해야 한다.

클라우드 컴퓨팅 서비스가 웹 인터페이스상에서 사용자의 요청에 따라 자원을 할당하는 방식으로 Dos, DDos, DRDos 공격으로부터 자유로울 수 없는 환경으로 IPV6에 대한 연구 및 https에 대한 연구 등도 진행되고 있다[7].

3. Cloud Computing 보안사고 사례

이러한 각종 보안 요소 기술들의 수용을 권장받고 있으며, 적용하고 있는 클라우드 컴퓨팅 서비스들은 지속적인 개발과 연구에도 불구하고, 아래의 <표 1>의 각종 사고 사례와 같이 이론이나, 기술적 문제와 더불어 심각한 피해로 확산 가능한 사고들이 발생하여 왔으며, 각종 사고 사례들을 통

하여 재발 방지를 위한 대책마련이 시급한 실정이다[8].

〈표 1〉 클라우드 컴퓨팅 서비스 보안 사고 사례

일 시	내 용
2008년 2월	아마존사 AWS S3 서비스 중단 사고
2008년 7월	아마존사 AWS S3 서비스 중단 사고
2008년	Cabonite 사의 백업저장소 손상-데이터 영구 손실
2008년 9월	구글사 Docs 의 데이터 유출 사고

4. Cloud Computing 환경에서의 개인정보보호 취약점 분석

클라우드 컴퓨팅 환경의 다양한 서비스의 구현은 데이터 보호와 자원의 관리, 가용성 확보, 개인정보보호 등 다양하고 복잡한 보안문제를 내포하고 있으며, 특히 개인 인증에 대해서는 높은 보안성의 보장을 요구 받고 있다.

클라우드 컴퓨팅 환경에서의 사용자 인증은 외부 네트워크로부터의 인증을 포함하며 기존의 패스워드 사용으로 인한 여러 가지 취약점들로 인해 이중 인증방식의 사용을 요구받고 있으며, 사용자 개입이 제한 또는 요구되지 않는 이동통신장치를 통한 클라우드 컴퓨팅 환경 접근시 인증에 대한 보안성 검증을 요구받고 있다[7].

본 연구에서는 클라우드 컴퓨팅 환경에서의 다양한 보안 요구사항중 개인인증 방법의 보안상 취약점에 대해 연구하고자 한다.

4.1 클라우드 컴퓨팅 서비스과 인증

기존의 컴퓨팅 환경에서의 인증방식과 유사하게 클라우드 컴퓨팅 서비스를 이용하는 사용자는 새로운 클라우드 컴퓨팅 서비스를 이용하기 위해서는 서비스 제공자가 요구하는 인증과정을 거쳐야 한다.

개인 인증과정은 일반적으로 개인의 이름, 주민등록번호, 전화번호, 이메일, 집주소 등 민감한 정보를 서비스 제공자에게 제공하고, 서비스 제공자는 개인 인증에 필요한 식별자와 인증방법을 제공한다.

서비스 제공자로부터 부여받은 식별자와 인증방법을 통한 인증방식이 임의의 공격에 의해 보안성이 침해되었을 경우, 개인의 정보뿐만이 아니라 해당 서비스 자체가 공격자의 보안위협에 노출되며, 더 나아가 서비스 및 개인정보등과 연관된 단체와 개인들의 정보까지 노출되는 심각한 보안사고가 발생하게 된다. 그러므로, 관리 용이성, 자원 분산성의 장점을 가진 다양한 클라우드 컴퓨팅 서비스의 특성에 맞는 개인 인증 기법 적용이 필요하다.

또한, 서비스제공자는 개인의 정보를 적절히 제어할 수 있는 인증방법을 제공해야하며, 개인 또한 충분한 보안성이 제공된 인증방법을 사용하여야 하겠다. 앞으로의 클라우드 컴퓨팅 서비스가 네트워크 및 단말에 독립적인 웹기반 플랫폼으로 발전이 예산되므로 분산된 클라우드 컴퓨팅 서비스간의 운용성 또한 고려해야 할 사항이다.

4.2 안전한 클라우드 컴퓨팅 개인 인증

온라인상에서 벌어지는 공격행위의 대다수는 부당하게 금전적 이익을 취할 목적으로 발생하는 사고이며, 각종 보안사고의 증가에 따라 보다 안전한 개인인증 방법들의 적용이 제안되고 있다.

아래의 <표 2>에서와 같이 클라이언트의 IP를 검증하는 방법, 전용 단말기에 저장된 키와 인증서를 이용하는 스마트카드 인증, 직접통화 인증방식의 Out-of-band 인증 등 더 나은 보안인증 대책들이 제시되고 있다[9].

〈표 2〉 최근 강화된 개인 정보보호 기법

보안기법	이용 보안 기술 메커니즘
IP-위치 정보 식별	사용자에게 현재 할당된 IP가 있는 지리적 위치 적절성 평가방법
전용단말기 인증	전용 잔말기에 키와 인증서 저장
Out-of-Band	전화응답, e-mail, 메시지를 이용하여 OTP와 정보전달
PKI 인증 기법	개인키와 인증서를 이용하여 보안

4.3 클라우드 컴퓨팅의 개인 정보보호 취약점

〈표 3〉 보안 인증기법의 취약점 분석

보안기법	보안 취약점
IP-위치 정보 식별	사설IP 대역 사용시 보안 위험발생, IP의 세션 탈취 문제 발생
PKI 인증 기법	단말의 공개키와 사설키의 노출 및 키 보관장소 문제 취약
Out-of-Band	공격자에 의해 침해된 통신 경로 등 사용시 보안상 위험
OTP 인증	OTP 유출 및 거래중의 공격시 보안상 위험

강화된 인증방법을 사용하여 개인 정보보호를 지원하더라도 이중인증(2-factor)방식 또는, 2가지 이상의 보안 방법을 병행 운용하는 것이 권장되고 있다. 본 절에서는 대표적인 소프트웨어 중심의 client SW의 사용/비사용 PKI와 하드웨어 중심의 단말기를 사용/비사용 OTP 인증 방식들을 비교 분석하고자 한다.

<표 3>에서 보면, IP-위치 정보 식별을 통한 보안기법은 사용되는 단말 네트워크에서 사설 IP 대역이 적용될 경우에 대표 공인 IP로부터 복수의 단말 IP를 서버가 구분하지 못하여 보안상 위험이 발생할 수 있으며, 또한 IP에 대한 session Hijacking 문제 또한 발생한다.

Client SW를 사용하는 PKI 인증방식의 경우 Private key와 Public key가 노출되어 트로이 목마 공격 등에 위협을 받을 수 있으므로 키 보관 서버 및 장소의 보안이 무엇보다 중요하며, 개인키의 암복호화시 사용되는 CPU와 메모리를 통한 키 노출도 주의하여야 보안성이 유지 될 수 있다. 다음으로 Client SW를 사용하지 않는 토큰기반 PKI 인증 방식의 경우 개인키, 인증서 노출 및 메모리 해킹 등에 비교적 안전한 것으로 알려져 있다.

Out-of-Band 기법의 경우, e-mail, SMS 를 이용하여 OTP와 거래정보를 전달하고 최종 사용자의 직접 통신을 통하여 인증하며, 기존의 통신방법을 사용이 용이한 반면, 통신방법에 따른 비용의 격차와 침해된 경로를 사용하게 될 경우 보안상 심각한 위험에 노출 될 수 있다.

OTP 인증의 경우, 하드웨어 단말기를 사용하지 않는 OTP 복사본을 이미지나 전자문서 형태로 파일 시스템, 메일, 웹하드 등에 보관 중에 유출되는 사회공학적 공격, 키 로깅, 도청 등의 공격 등으로 인해 OTP의 유출 및 거래 중 공격을 주의하여야 한다. 하드웨어 단말기를 사용하는 OTP 인증의 경우정보저장장소가 별도의 독립 단말이며, 동기화된 패스워드의 유지 시간이 짧은 OTP 보안 특성이 있다. 현재 이러한 보안특성으로 인해 대부분의 온라인 금융 서비스 제공업체들이 다양한 방법으로 도입하여 보안에 응용하고 있다, 하지만 단말기를 사용하는 방식 또한 MITM(Man-In-The-Middle) 공격이 증가로 운용상 주의 및 강화된 기술 적용이 필요하다[10].

4. 결 론

클라우드 컴퓨팅에서 개인 정보보호를 위한인증기법은 가상화와 확장성을 기반으로 개인정보의 유출의 난이도를 결정하는 가장 중요한 요소로서, 가상화에 따른 책임부담문제, 확장성에 따른 국가적, 지역적 규제 문제 등은 사용자의 의사결정과는 관계없이 개인정보가 유출될 수 있음을 의미하며,

개인정보보호 강화를 위해 하나의 특정한 보안 인증 방식만으로는 개인인증의 보안성, 접근 편의성, 상호 운용성 등의 사항을 모두 만족 할 수는 없다 적절한 인증방법 도입 비용과 서비스 특성 등에 따라 적절한 인증방식의 혼용이 클라우드 컴퓨팅 환경에서의 개인인증 보안성을 강화할 수 있는 최선의 방법이다.

향후, IPV6 도입 등의 새로운 IT 환경에서의 클라우드 컴퓨팅 서비스 보안에 미치는 영향에 대해 연구 하고자 한다.

참 고 문 헌

[1] Gartner says cloud computing will be as influential as e-business, 2008. http://www.gartner.com/it/page.jsp?id = 707508.

[2] Asia Pacific End-user Cloud Computing Survey, IDC, 2009.

[3] 정제호, 클라우드 컴퓨팅의 현재와 미래 그리고 시장 전략, 한국소프트웨어진흥원, 2008.

[4] Gartner, Assessing the Security Risks of Cloud Computing, 2008. 6, http://www.gartner.com/DisplayDocument?id=685308.

[5] 임철수, “클라우드 컴퓨팅 보안 기술”, 정보보호학회지, 2009.

[6] NIST, Cryptographic hash algorithm competition, http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.

[7] jaehoon. sun, A Study on the Enhanced Security Technique of BGP for DRDoS Attack, ICISA2010, 2010.

[8] Amazon Web Service : Overview of Security Process, Amazon, 2008.

[9] 김현승, 박춘식, “클라우드 컴퓨팅과 개인 인증 서비스”, 정보보호학회지, 2010.

[10] Malware, Man-in-the-Middile and Other Online Mischief, Entrust, 2009.

선 재 훈

2000년 경기대학교 토목공학과 (공학사)
2005년 경기대학교 정보보호학과 (공학석사)
2009년 경기대학교 정보보호학과 (이학박사)
2010년 현재 경기산업기술보안협의회 이사

김 귀 남

미국 캔자스대학(학사)
미국 콜로라도주립대학(석사)
미국 콜로라도주립대학(박사)
현재 경기대학교 산업보안학과 교수