클라우드 컴퓨팅 서비스 도입에 따른 데이터보안에 관한 연구

경지훈[*] · 정성재[**] · 배유미[***] · 박정수[****] · 성경[*****]

[*](주)시큐브, [**](주)스컴씨엔에스, [***]한남대학교 컴퓨터공학과, [****]매크로임팩트(주),

[*****]목원대학교 컴퓨터교육과

A Study on the Data Security for Cloud Computing Infrastructure Development

ji-hun Kyung[*] · Sung-Jae Jung[**] · Yu-Mi Bae[***] · Jeong-Su Park[****] · Kyung Sung[******]

[*]Secuve, Inc., [**]Sky Computing C&S, Inc., [***]Hannam University, [****]Macroimpact, Inc., [******]Mokwon University

E-mail : sia2001@secuve.com, posein@naver.com, yumidw@hanmail.net, jparks7@naver.com, skyys04@mokwon.ac.kr

요 약

클라우드 컴퓨팅(Cloud Computing)이 주목받고 활성화되면서 각 기업들 및 공공기관 등에서 급속도로 확산 및 도입되어지고 있다. 이러한 영향으로 인해 클라우드 컴퓨팅 기술을 이용한 정보시스템 자원의 활용과 통합은 크게 각광 받고 있으며 이에 따른 데이터 보안 또한 이슈화되고 있다.

본 논문에서는 클라우드 컴퓨팅 시스템 도입으로 인한 정보시스템의 자원 즉 데이터보안에 관한 측면을 조명하여 클라우드 컴퓨팅 인프라 구축을 위한 기반 지식을 제공하고자 한다.

ABSTRACT

Cloud Computing is attracting attention are activated and rapidly spread to companies and public institutions, etc. have been introduced are getting. Spotlighted these effects due to the utilization and integration of information system using cloud computing technology resources, and the resulting data security issue has been.

In this paper, the side lights on due to the introduction of a cloud computing system, the resources of information systems, data security, and knowledge to provide the foundation for cloud computing infrastructure.

키워드

클라우드(Cloud), 데이터보안(Data Security), 자원(Resource), 정보보안(Information security)

Ⅰ. 서 론

클라우드 컴퓨팅(Cloud Computing)이 주목받고 활성화되면서 각 기업들 및 공공기관등에서 급속도로 확산 및 도입되어지고 있다. 이러한 영향으로 인해 클라우드 컴퓨팅 기술을 이용한 정보시스템 자원의 활용과 통합은 크게 각광받고있으며 이에 따른 데이터 보안 또한 이슈화되고있다.

클라우드 서비스에 대해 IT업체, 포털, PC제조

사 등의 IT관련 사업자뿐 아니라, 세계 각국 또한 국가경쟁력을 크게 좌우하는 산업으로 인식하기 시작하였으며 미국, 유럽 등이 중심이 되어 국가 활성화 전략을 발표한 것도 이 때문이다. 우리나라도 정부차원에서 2014년 클라우드 선진국 도약을 위한 '클라우드 컴퓨팅 활성화 종합계획'을 발표하였다. 기술과 서비스 활성화 측면에서는 선진국에 비해 다소 뒤처지지만, 세계 최고수준의 국내 IT 인프라를 활용한 클라우드 서비스가 상상 이상의 발전과 성과를 이룰 것으로 기대하고 있다.[1]

본 논문에서는 클라우드 컴퓨팅(Cloud Computing) 서비스 도입에 따른 각각의 보안위협요소와 데이터보안에 관한측면을 조명해보고 이에따른 데이터 보안과 관련된 기반지식을 제공하고자 한다.

II. 클라우드 서비스 특징 및 모델

클라우드 서비스는 인터넷 기반의 자원 소프트웨어 및 정보 인프라를 제공한다. 이는, 1960년대 미국의 존 맥카시가 "컴퓨팅 환경은 전기, 수도 등 공공 서비스를 사용 하는 것과도 같을 것"이라는 개념을 제시한 것에 기인하고 있다. 클라우드 서비스는 인터넷을 통한 요청형 제공방식(On-demand)의 서비스다. 클라우드 서비스의 제공자는 다량의 컴퓨터 자원을 분배·가상화하여 각 이용자에게 제공한다. 또한 이용자는 클라우드 서비스를 통해 자신의 컴퓨터에 직접적인 프로그램 설치 없이도 원하는 자원을 필요로 할때, 필요한 만큼, 즉각적으로 인터넷을 통해 서비스 받을 수 있다.

컴퓨팅 환경의 변화를 살펴보자. 초기의 컴퓨팅 환경은 개인PC를 사용하여 직접 연산 및 처리를 수행하는 형태라 할 수 있다. 이후 인터넷의 도입 확산으로 데이터 연산과 처리의 일부가 다양한 인터넷 서비스로 대체되었다. 네트워크의 발전으로 이루어진 클라우드 컴퓨팅 환경에서는 이용자가 직접 컴퓨팅 자원을 구매하지 않아도 원격으로 클라우드 서버에서 컴퓨팅 자원 및 소프트웨어를 전부 임대하여 사용할 수 있다. 이것은 데이터의 위치 및 컴퓨팅의 주체, 데이터의 소유 및 관리, 제공서비스 면에서 기존의 컴퓨팅 환경과 구분되는 특성을 가진다.

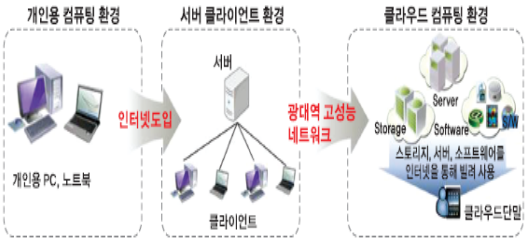

그림 1. 컴퓨팅 환경의 변화

그림 1에서도 알 수 있듯이 클라우드 서비스 이전에는 사용자가 직접 자신의 소프트웨어 및 데이터를 직접 소유 관리를 해온 반면 클라우드 컴퓨팅으로 발전해가면서 사용자의 데이터를 클라우드 서비스 사업자의 서버에 저장(외부)하는 형태로 발전되어지고 있다. 이는 자원 활용의 효율성 증대 및 사용자별 자원 할당 간편화를 위하여 모든 자원을 소프트웨어 기반으로 가상화하여 제공하는 특성을 가지며 모든 연산 및 데이터 처리가 클라우드 서버에서 이루어지므로 사용자가 소유한 정보의 관리를 서비스 제공자에게 위탁한다는 의미이기도하다. 또한 사용자별로 할당된 자원은 논리적으로는 독립적이지만 물리적으로는 동일한 자원을 공유하는 특징을 가진다.

클라우드 서비스는 제공하는 자원의 레벨에 따라 IaaS, PaaS, SaaS의 세 가지 모델로 분류한다.

·IaaS(Infrastructure as a Service) : 사용자에게 서버, 스토리지 등의 하드웨어 자원만을 임대 제공하는 서비스

·PaaS(Platform as a Service) : 사용자에게 소프트웨어 개발에 필요한 플랫폼을 임대 제공하는 서비스

·SaaS(Software as a Service) : 사용자가 원하는 소프트웨어를 임대 제공하는 서비스.

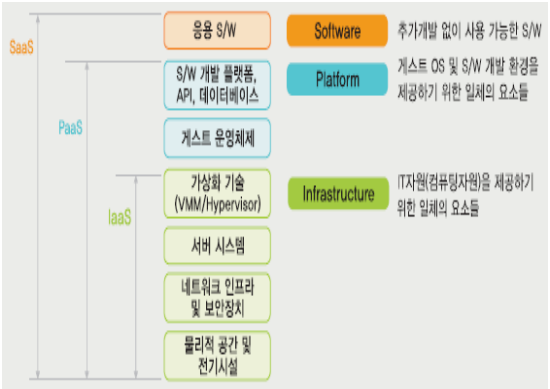

그림 2. 클라우드 서비스별 자원제공 범위

Ⅲ. 클라우드 서비스 보안이슈 및 위협

클라우드 서비스를 이용함에 있어 보안적인 측면에서 우려되는 문제점들은 보안 및 데이터 유출, 서비스 안정성과 가용성, 기존 애플리케이션 서비스와의 연동 이슈, 서비스 제공업체의 안정성, 법규제(컴플라이언스), 서비스 비용 등을 들 수 있다. 이런 문제점들 중에서도 클라우드 서비스 핵심 보안 위협요소로는 아래와 같다.

· 가상화 취약점
(악성코드 및 서비스 가용성 침해)
· 정보위탁
(소유/관리 분리)에 따른 정보유출 위협
· 자원 공유 및 집중화에 따른 서비스 장애
· 단말 다양성에 따른 정보 유출
· 분산 처리에 따른 보안적용의 어려움
· 법규 및 규제의 문제

위와 같은 보안 위협요소들로 인하여 클라우드 서비스 상에는 정보 유출, 서비스 장애등 다양한 보안 위협이 발생 할 수 있다. 이러한 위협 요소들 중에서도 개인사용자의 데이터보안과 기업사용자 관점에서의 데이터 보안이 이슈로 떠오르고 있다. 개인 사용자는 이메일, 블로그, 동호회, 사진 및 파일 저장과 공유 서비스를 주로 이용하며, 무료로 제공하는 서비스를 선호하는 특성을 갖는다. 주로 웹기반 서비스들로 이루어지며 개인 사용자 관점에서 우려하는 보안 문제는 다음과 같다.

· 개인정보 노출
· 개인에 대한 감시(사생활 감시)
· 개인 데이터에 대한 상업적 목적의 가공
· 개인 프라이버시 침해

기업 사용자 관점에서는 자신이 소유하던 IT 자산을 클라우드 형태로 제공받기를 원하지만, 자신의 데이터가 타인과 공유되기를 원하지 않는다. 기업 사용자는 안정성을 제공하면 비용을 지불할 의사가 있으며, 때에 따라서는 local cloud와 같이 자신이 직접 운영하기도 한다. 기업 사용자 입장에서 우려하는 보안 문제는 다음과 같다.

· 서비스 중단 및 서비스 장애
· 기업 정보 훼손 및 기업정보 유출
· 고객 정보 유출
· 법/규제 준수

이와 같이 개인 사용자와 기업 사용자는 클라우드 컴퓨팅에 대한 보안 요구사항이 다르다. 개인 사용자는 익명성 보장과 개인정보의 안정성에 중점을 두는 반면에, 기업사용자는 컴플라이언스에 중점을 두는 경향이 있다.[2]

위와 같은 위협사항 및 문제점들을 살펴보았을 때 클라우드 서비스이전과 이후에 정보보안적인 측면에서 해결해야할 문제점들은 가상화 취약점 상속, 정보위탁에 따른 정보유출, 자원 공유 및 집중화에 따른 서비스장애, 사용단말의 다양화에 따른 정보유출, 분산처리에 따른 보안적용의 어려움, 법규 및 규제의 문제 등을 나열할 수 있다.[3]

표 1. 클라우드 서비스 보안 위협

보안위협	위협내용
가상화 취약점 상속	·악성코드 감염 및 확산위협
정보위탁 및 사용 단말에 따른 정보 유출	·내부자에 의한 정보유출 ·단말기 분실등에 의한 정보유출
자원 공유 및 집중화에 따른 서비스 장애	·시스템 장애 시 모든 고객의 서비스 중단 ·중앙시스템 노출시 DDoS등의 공격대상이 되기쉬움
분산 처리에 따른 보안적용의 어려움	·자원공유와 가상머신 동적 재배치로 인증/접근제어 복잡도 상승 ·분산 컴퓨팅 시스템에 일괄적인 인증/접근제어 적용의 어려움
법규 및 규제의 문제	·정보유출시 책임소재 불문명 ·자원공유에 따라 감사증적이 어려움

Ⅳ. 클라우드 서비스 정보보호 고려사항

클라우드 서비스의 정보보호 고려사항으로는 서비스 제공자 입장에서와 서비스 이용자입장 에서의 고려사항으로 나눌 수 있다. 먼저 서비스 제공자 즉, 관리적 측면에서의 정보보호 고려사항을 알아보며 관련사항으로는 아래와 같다.

정보보호정책 및 약관수립, 정보보호 조직구성 및 보안인력확보, 자산분류 및 통제기법 확립, 비상 대응체계 구축 및 서비스 연속성 확보, 관련 법률 및 제도의 준수 등을 들 수 있다. 이와 더불어 기술적인 측면에서의 고려사항은 네트워크 보안, 시스템 및 가상화 보안, 데이터 센터 구축, 이용자 데이터 저장 및 관리, 사용자 인증 및 접근제어 강화 등을 들 수 있다. 또한 아래와 같은 국내 법규를 준수하여 클라우드 서비스에 안정적인 서비스를 도모하여야 한다.[4]

구분	법률	대상	관련 규정
서비스 안전성	정보통신기반보호법	전체	- 전자적 침해의 법적 정의 - 주요 정보통신 기반시설 보호대책의 수립과 이행 여부의 확인 - 주요정보통신기반시설의 지정 - 취약점의 분석 및 평가 - 주요정보통신기반시설 보호 및 침해사고 대응
	정보통신망이용촉진및 정보보호등에관한법률	민간	- 침해사고 법적정의 - 표준에 적합한 제품의 표준화 및 인증 - 정보통신망의 안정성 확보 - 정보보호 안전 진단, 정보보호관리체계 인정 - 정보통신망 침해행위 등의 금지
개인정보 및 정보보호	개인정보보호법	전체	- 모든 기관, 조직, 단체 등이 보유한 개인정보의 보호를 규정
	통신비밀보호법	전체	- 통신비밀의 보장
	정보통신망이용촉진및 정보보호등에관한법률	민간	- 개인정보의 보호조치방안 및 파기 등의 손해배상 - 주요정보의 국외유출 제한 - 국외에선 개인정보의 보호
	공공기관의개인 정보보호등에관한법률	공공	- 공공기관이 보유한 개인정보의 보호를 규정
	신용정보이용및보호등에 관한법률	금융	- 신용정보의 오남용으로부터 개인의 사생활보호

그림 3. 클라우드 서비스 제공자 관련 국내 법규

클라우드 서비스 이용자 입장에서의 고려사항으로는 기업 이용자와 개인 이용자로 나눌 수 있다. 먼저 기업 이용자의 정보보호 고려사항으로는 전직원의 참여 및 동의하에 클라우드 서비스를 도입하여야 하며 서비스담당자 및 전담부서 채택하고 보안요구수준을 정의하여야 한다. 또한 안전한 클라우드 서비스 이용을 위하여 직원ID 인증 및 다양한 보안정책적용을 실시하여야하며 데이터 암호화 습관과 패스워드 주기적 변경, 그리고 데이터 손실에 대비한 정기적인 백업등을 고려사항으로 볼수 있다.[5]

개인이용자 입장에서의 고려사항으로는 클라우드에 접속하는 단말기를 안전하게 관리하며 중요정보는 암호화하여 저장, 안전한 패스워드를 설정하며 주기적으로 변경, 저작권에 위배되는 자료는 이용하지 않으며 서비스 장애에 대비하여 개인데이터를 암호화 및 정기적인 백업을 한다. 또한 다른 클라우드 서비스로 변경할시 중요정보는 완전히 삭제하고 삭제여부도 확인하여야한다.

Ⅴ. 결 론

본 논문에서는 클라우드 컴퓨팅과 클라우드 서비스기술이 보편화됨에 따라 사용자의 데이터보안 그리고 각각의 기업과 공공기관의 데이터보안적인 측면을 고려하여 제공자 측면과 사용자 측면을 조명하였다. 이와 더불어 클라우드 서비스의 안정적인 제공과 이용을 위하여 정보보안준수사항이행은 물론이거니와 개인정보보호 의식수준이 동반 상승되어야 향후에도 정보보안측면에서의 데이터 유출사고나 개인정보유출사고, 서비스장애 등을 사전에 예방할 수 있으이라 판단된다. 또한 최근 각광을 받고 있는 클라우드 컴퓨팅 환경을 위한 인프라 구축에도 밑거름이 될 수 있으리라 여겨진다.

참고문헌

[1] KISA 안내·해설 제2011-8호“클라우드 서비스 정보보호 안내서” pp. 6-19, 2011년 10월.

[2] 은성경, 조남수, 김영호, 최대선, “클라우드 컴퓨팅 보안 기술”, 전자통신동향분석 제24권, 제4호, pp. 3-4, ETRI, 2009년 8월.

[3] Jon Brodkin, “Seven cloud-computing security risks”, pp. 1-2, Gartner, 2008년 7월.

[4] 이강찬, 이승윤, “클라우드 컴퓨팅 표준화 동향 및 전략”, 전자통신통향분석, 제25권, 제1호, pp. 90-99, 2010년 2월.

[5] 이향진, “안전한 클라우드 서비스 제공이용을 위한 보안 고려사항”, 한국인터넷진흥원(KISA), 제7권, 제4호, pp. 21, 2012년 4월.