Journal of The Korea Society of Computer and Information
Vol. 20 No. 7, pp. 49-56, July 2015

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.7.049

Cloud System Security Technology Trend

Jeong-Won Yoon *, Beakcheol Jang **

Abstract

In this paper, we introduce recent cloud system security technologies categorizing them according to Reliability, Availability, Serviceability, Integrity, and Security (RASIS), terms that evaluate robustness of the computer system. Then we describe examples of security attacks and corresponding security technologies for each of them. We introduce security technologies based on Software Defined Network (SDN) for Reliability, security technologies based on hypervisor and virtualization for Availability, disaster restoration systems for Serviceability, authorization and access control technologies for Integrity, and encryption algorithms for Security. We believe that this paper provide wise view and necessary information for recent cloud system security technologies.

▸ Keyword : Cloud System, Security, RASIS, Reliability, Availability, Serviceability, Integrity, Security

I. Introduction

클라우드 시스템은 효율적인 IT자원 분배 환경으로 다양한 서비스를 사용자에게 제공한다. 현재 주목받고 있는 차세대 컴퓨팅 환경으로 대용량의 고속 처리와 개인 컴퓨터의 한계에서 벗어나 무한에 가까운 IT자원을 활용한다는 점에서 사용자들에게 각광을 받고 있다. 그리고 어느 곳이라도 네트워크가 연결된다면 항상 접속할 수 있다는 점은 클라우드 시스템의 큰 장점이며, 2012년 IT시장 조사기관인 IHS 아이서플라이에서는 2017년 클라우드 서비스를 이용하는 사용자 수가 13억 명에 이를 것을 예상했다.[1] 즉, 클라우드 시스템은 더 이상 새로운 기술이 아닌 대중적인 시스템으로 자리를 잡아가고 있는 중이다. 하지만 클라우드 시스템은 네트워크를 통하여 구축한 시스템 환경이기 때문에 보안적인 위협에서 벗어날 수 없다. 그리고 기존 네트워크의 보안 위협 예를 들어, 하이재킹을 통한 시스템 내부 침투 또는 분산 서비스 거부와 같은 공격으로부터 완전히 벗어난 것이 아니기 때문에 클라우드 시스템의 보안 기술이 시급하다.[2] 그림 1은 2008년 조사 기관인 IDC에서 클라우드 시스템의 이슈를 분석한 그래프로, 보안에 대한 문제가 가장 중요하다는 것을 알 수 있다. 최근까지도 구글, 아마존, 애플 등과 같은 해외 대형 클라우드 업체도 잇따른 보안사고 사례를 보임에 따라 보안의 취약성을 드러내고 있는 실정이다. 발생한 보안 사고는 2011년 구글에서는 50만 명의 개인정보가 없어진 사태가 일어났으며, 2012년 애플의 아이클라우드에서는 해커에 의해 개인정보가 삭제되었다. 그리고 2013년에는 세계 최고의 보안을 자랑하는 미국 금융권을 무력화 시켰던 오퍼레이션 아바빌(Operation Ababil) 공격과 어도비 사의 3800만명의 데이터 유출 사건 등으로 인해 클라우드 시스템에서의 보안의 중요성이 부각되고 있다. 그리고 클라우드 시스템은 외부에 의한 공격뿐만 아니라 악의적인 내부 사용자에 의한 공격도 방어해야 한다.[4] 2010년 마이크로소프트에서는 악의적인 내부 사용자 또는 관리자에 의해 기업정보가 유출된 사례도 있다. 이처럼 다양한 형태의 공격으로부터

• First Author: Jeong-Won Yoon, Corresponding Author: Beakcheol Jang
*Jeong-Won Yoon(foggyoon@naver.co.kr), Dept. of Media Software, Sangmyung University
**Beakcheol Jang (bjang@smu.ac.kr), Dept. of Media Software, Sangmyung University
• Received: 2015. 02. 26, Revised: 2015. 03. 18, Accepted: 2015. 07. 06.

클라우드 시스템을 보호하기 위해 대형 클라우드 업체와 보안 업체에서는 기존 기술력을 바탕으로 시스템을 보안하는 기술을 개발하고 있는 중이다.

클라우드 시스템의 폭팔적인 보급과 함께, 다양한 위협과 그에 대한 보안 기술들이 개발 되어져 왔다. 이 논문에서 우리는 이러한 위협과 보안 기술들을 컴퓨터 시스템의 견고성을 기술하는 용어인 신뢰성 (Reliability), 가용성 (Availability), 보전성 (Serviceability), 무결성 (Integrity), 기밀성 (Security), RASIS를 기반으로 분류하여 기술한다. 우리는 이 논문이 최근 클라우드 시스템 보안 기술들에 대한 유용한 정보와 현명한 관점을 제시하고 있다고 믿는다.

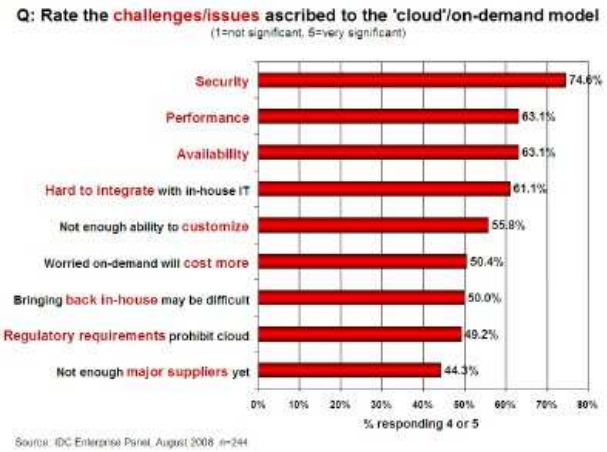

Fig. 1. Cloud system issues[3]

Fig. 2. Cloud Services

II. Related works

1. 클라우드 시스템

클라우드 시스템이란 '인터넷 기술을 활용하여 IT자원을 필요한 만큼 빌려서 사용하고 서비스를 제공하는 시스템'이다. 클라우드 시스템은 서비스 제공 방식과 이용목적에 따라 분류할 수 있다. 서비스 제공 방식은 클라우드 공급자가 사용자에게 지원해주는 방식을 의미한다. 대표적으로 Infrastructure as a Service(IaaS), Platform as a Service(PaaS), Software as a Service(SaaS)가 있다.

그림 2는 클라우드 서비스의 종류들을 시스템 구성도에 따라 사용자와 공급자의 관리 부분으로 나누어 분류하고 있다.[5-8] IaaS는 하위단계인 가상화, 서버, 스토리, 네트워크를 사용자에게 제공하여 상위단계의 부분을 사용자가 직접 구조를 구축하도록 하는 서비스이다. 즉, 서버자원, 스토리지, 네트워크를 가상화 환경으로 만들어 필요에 따라 인프라 자원을 사용할 수 있게 서비스를 제공하는 형태로 PaaS, SaaS의 기반이 되는 기술이다. 현재 제공되고 있는 서비스로는 구글의 컴퓨팅 엔진과 아마존의 S3 및 EC2, 호스트웨이의 FlexCloud 등이 있다.

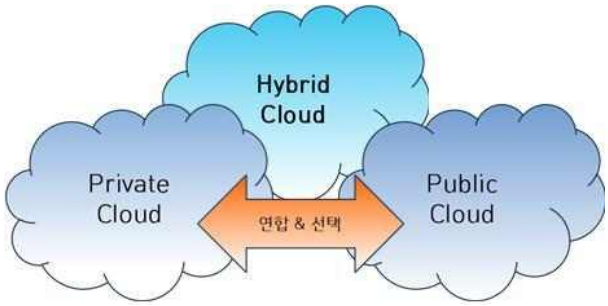

Fig. 3. Cloud systems

PaaS는 플랫폼을 통하여 사용자가 소프트웨어를 개발할 수 있는 토대를 제공하는 서비스이다. 제공하는 개발 요소들로는 컴파일 언어, 웹 프로그램, 제작 툴, 데이터베이스 인터페이스, 과금 모듈, 사용자관리 모듈 등을 모두 포함하며 현재 구글, 네이버 그리고 다음에서 제공하는 Open API들과 마이크로소프트의 Azure 등이 PaaS의 일종이다.

SaaS는 애플리케이션과 같이 단일 플랫폼을 통해 사용자에게 모든 소프트웨어 영역의 서비스를 제공하는 서비스이다. 기존의 애플리케이션 서비스 제공형태인 application serviece provider(ASP)의 발전된 형태이며 세일즈포스의 Customer Relationship Management(CRM)가 대표적이다.

그림 3 클라우드 시스템의 이용목적에 따른 분류를 살펴보면, 시스템의 배치 상태에 따라 형태가 정해지며 사설(Private), 공용(Public), 혼합(Hybrid)으로 분류된다. 혼합 클라우드 시스템은 사설과 공용 클라우드 각각의 특징을 연합과 선택을 통하여 구축한 새로운 형태의 시스템이다.

사설 클라우드 시스템은 기업이 클라우드 시스템을 직접 구축하여 회사 내부의 데이터를 내부 이용자들이 공유하고 운용 및 관리를 하는 서비스이다. 사용자 제어에 대한 권한이 강력하고 안전한 보안 시스템을 구축할 수 있다는 장점이 있지만 유지보수 및 구축비용이 높다는 단점이 있다.

공용 클라우드 시스템은 클라우드 서비스 제공업체가 구축한 시스템을 다수의 사용자가 이용하는 방식으로 IT자원을 외

부 업체에 맡기는 형태이기 때문에 사용한 만큼만 요금을 지불하는 방식이다. 경비절감에 도움이 되지만 개인 및 기업의 기밀 데이터 유출 등의 보안 위험이 존재한다.

혼합 클라우드 시스템은 사설과 공용 클라우드 시스템의 장점만을 결합한 방식으로 개인 및 기업의 중요 데이터들은 사설 클라우드 시스템을 활용하여 보안성과 통제력을 높이고 공용 클라우드 시스템을 통하여 IT자원의 확대와 비용과 효율성을 높이는 시스템이다. 최근 호스트웨이의 FlexLink는 혼합 클라우드 시스템을 활용하여 보안 수준을 높였다.

2. RASIS

RASIS는 처음 IBM 사에서 제창되었으며 컴퓨터 시스템의 견고성을 기술하는 용어이다. 컴퓨터 시스템이 예상되는 기능 및 성능을 안정적으로 발휘할 수 있는지에 대한 여부를 판단하는 평가항목으로 활용된다.

R은 신뢰성(Reliability)으로, '컴퓨터 시스템에서 결함 및 고장, 장애가 발생하지 않으며 시스템에서 제공하는 서비스가 일정하게 유지되는 성질'을 의미한다. 신뢰성 확보를 위해 내구성이나 안정성 그리고 설계 신뢰성 등에 대한 고려가 충분히 이루어져야 한다. 일반적으로 품질보증의 주요항목으로, 신뢰성을 나타내는 척도인 고장률, 수명 등에서 사용된다.

A는 가용성(Availability)으로, '컴퓨터 시스템이 정상적으로 사용 가능한 정도'를 의미한다. 즉, 가동률과 비슷한 의미를 담고 있어서 사용자의 입장에서 컴퓨터 시스템이 어느 정도 사용할 수 있는가를 표시하는 것이다. 가동률은 전체시간 중에서 사용자가 온전히 서비스를 이용하는 작동 시간에 대한 것으로 여기서 사용 불능인 상태는 제외한 나머지 작동시간을 뜻한다.

S는 보전성(Serviceability)로, '컴퓨터 시스템이 고장이 났을 때 신속하게 서비스를 제공할 수 있는 가의 척도'를 의미한다. 컴퓨터 시스템은 고장 또는 장애가 발생했을 때 빠른 대처를 통해 사용자가 서비스 이용에 불편을 느끼는 것을 최소화하는 것이 중요하다. 그리고 시스템을 설계할 때 고장이 발생하더라도 유지 및 관리하기 쉽도록 하는 것이 중요하다.

I는 무결성(Integrity)로, 인터넷 환경이 급속도로 발전해서 추가된 평가항목이다. 시스템 환경에서의 무결성이란, '컴퓨터 시스템 내부의 저장장소의 정확성을 측정하는 척도'이다. 사용자의 데이터가 항상 온전하게 보존되는 것을 뜻하며, 본인 이외의 사용자가 데이터에 접근하지 못하도록 하는 성질을 의미한다.

S는 기밀성(Security)이다. 무결성과 같이 데이터가 중요해짐에 따라 추가된 항목으로 '데이터의 권한을 갖는 자에게 데이터의 원본을 제공하는 것'을 의미한다. 본인 이외의 사용자가 중간에 데이터를 탈취하더라도 데이터의 누설에 대비할 수 있으며, 부정한 침입자가 데이터에 접근하더라도 원본에 접근하지 못하도록 하는 것이다.

위의 5가지 항목인 신뢰성, 가용성, 보전성, 무결성, 기밀성을 통하여 3장에서는 클라우드 시스템 상에서 이루어지는 보안 기술을 분류하고 보안 위협 사례를 통하여 적용되는 기술을 서술하고자 한다.

III. Security tech of cloud system

클라우드 시스템은 인터넷 기반의 기술을 통하여 자원 효율성의 극대화와 사용자 편의성을 만족시키는 등 다양한 이점들을 사용자에게 제공하기 때문에 시스템 활용도가 매우 높다. 하지만 보안적인 측면에서는 매우 취약하기 때문에 본 논문에서는 IBM 사에서 제안한 컴퓨터 시스템이 갖추어야 할 조건인 RASIS에 맞추어 각 요구상황에 대해 위협 사례와 해당 보안기술을 분류 및 기술한다.

1. 신뢰성

클라우드 시스템에서의 신뢰성은 "시스템이 신뢰할 수 있으며 외부로부터의 위협 및 고장 장애가 일으키지 않도록 함"을

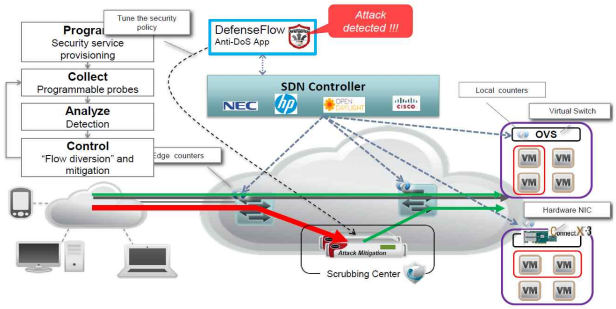

Fig. 4. DefenceFlow of Redware[9]

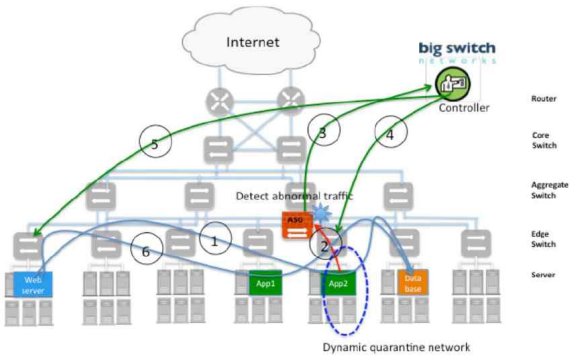

Fig. 5. SDSec of vAmour[10]

뜻한다. 클라우드 시스템은 가상 네트워크를 기반으로 IT자원을 효율적으로 분배하는 시스템이기 때문에 네트워크 자체의 보안이 중요하다. 기존의 네트워크 보안 기술인 SSL과 IPsec 등은 변화해가는 클라우드 시스템에서 보안으로서의 기능을 제대로 수행하지 못하기 때문에 네트워크 통합적인 보안 기술을 필요로 한다.

위협 사례 : 11년 구글에서는 해킹으로 인해 50만명의 메일내용과 주소록이 삭제되었고 11년 일본의 후지쯔 사의 클라우드 서비스는 디도스 공격으로 인해 네트워크 오류가 발생하였다.

보안 기술 : SDN기반의 Redware 사의 DefenceFlow와 vArmour 사의 Software Defined Security(SDSec)

SDN기술이란, 모든 네트워크의 트래픽의 전달을 중앙집권적인 컨트롤러를 통해 제어 및 관리하는 소프트웨어 기술이다. 기존의 하드웨어에 의존하는 네트워크 체계에서 벗어나 소프트웨어를 통해 관리함으로서 보안 기술 및 장비가 하나의 네트워크 자원으로서 사용이 되는 기술을 뜻한다.

그림 4 Redware사의 DefenceFlow는 트래픽 모니터링을 통해 자료를 수집한 후 분석한다. 만약 공격적인 위협이 발견된다면 컨트롤러를 통해 해당하는 트래픽을 Attack Mitigation 장비를 통하여 격리시킨다. 그리고 최근 많이 발생하는 Denial of Service(DoS) 공격에 특화되어 있는 기술이며 다른 공격방식에 대해서도 효과적으로 대응할 수 있다.

그림 5 vArmour사의 SDSec는 클라우드 시스템의 네트워크 보안을 위해 데이터 저장소마다 보안 장비인 Application Security Gateway(ASG)를 배치하였다. 공격 또는 이상 징후

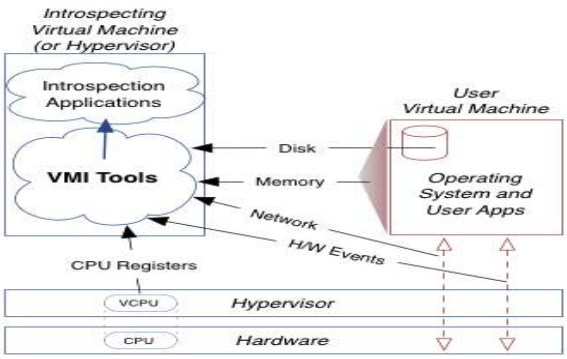

Fig. 6. VMI Architecture[11]

감지 시 해당하는 서버를 격리시킨 후 트래픽의 부하가 걸리는 것을 방지한다. ① 웹 서버가 데이터베이스에 접속하고 ② 응용계층에서 트래픽을 감지하게 된다. ③ 이상 징후가 감지되면 컨트롤러를 통해 ④ 해당 응용계층을 격리시킨 후 ⑤ 서비스 운용을 원활하게 하기 위해 다른 응용계층으로 연결하는 기술이다. 이를 통해 트래픽 초과 및 과부하를 막을 수 있으며, 서비스가 정상적으로 작동하게 한다.

2. 가용성

시스템 가용성이란 "내부의 문제로 인한 장애가 발생을 최소한으로 하는 것"을 의미한다. 클라우드 시스템의 가용성을 높이기 위해서는 시스템 내부의 실시간 모니터링을 통해 수집된 자료를 분석한 후, 장애 및 위협을 미리 예방하는 기술을 필요로 한다. 클라우드 시스템에서의 핵심은 가상화 기술이지만 물리적인 보안 시스템인 방화벽과 침입탐지시스템 그리고 침입방지시스템은 시스템 외부의 영역만을 감시하기 때문에 시스템 내부의 문제에 대한 대비가 부족하다.

위협 사례 : 09년 구글 Gmail에서는 시스템 내부의 문제로 인하여 서비스가 일시중단이 되었고 2012년 FirstServer 에서는 내부 시스템의 업그레이드 중 오류로 인하여 서비스가 중단되는 사태가 발생하였다.

보안 기술 : 하이퍼바이저 기반 보안 기술과 가상화 기반 보안성 향상 기술

하이퍼바이저 기술은 가상화 시스템에서 다수의 운영체제를 모니터링하기 위한 플랫폼이다. 하이퍼바이저 기반 보안 기술로 대표적으로 Virtual Machine Introspection(VMI)[11]와 Agentless Virtual Security Appliance[12]가 있으며 가상화 기반 보안성 향상 기술로는 VMware사의 Overshadow[13]와 삼성전자의 Xen on ARM[14], Zhang의 CloudVisor[16]가 있다.

그림 6 VMI 구성도를 살펴보면, 가상머신과 하이퍼바이저 내부의 시스템을 계속적으로 모니터링을 하여 분석한 후 보안상태 점검 및 공격을 감지한다. VMI Tools을 이용하여 다양한 형태의 자료를 수집하고 Introspection Application을 통하여 해당하는 자료의 분석을 기반으로 보안 상태를 점검할 수 있다.

Agentless Virtual Security Appliance 기술은 독립된 보안 전용 가상머신을 통하여 시스템 내부를 보호한다. 보안용 가상

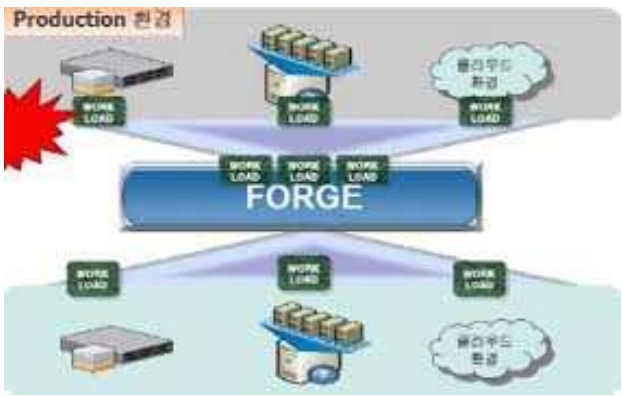

Fig. 7. Forge of Novel[17]

머신이 독립된 형태로 운영되기 때문에 시스템 외부의 공격에 대해서도 효과적으로 보호할 수 있으며 불필요한 IT자원의 소모를 줄일 수 있다.

가상화 보안성 향상 기술인 Overshadow는 multi-shadowing 기법을 통하여 호스트와 게스트의 메모리를 일대다 매핑을 한다. 보안이 요구되는 수행 작업에 대해서 해당하는 메모리에 대해서만 복호화를 하며 그 외 메모리에서는 암호화 과정을 수행한다. 이를 통해 게스트가 호스트의 메모리에 접근하여 해킹하는 행위를 차단할 수 있다.

Xen on ARM은 보안이 필요로 하는 프로그램의 경우에만 보

안용 가상 머신이 사용이 되고, 일반적인 프로그램의 경우에는 범용 가상 머신을 사용한다.[17] 사용자가 직접 보안화를 설정할 수 있는 분리된 형태의 시스템을 구성할 수 있다. 이를 통해 하나의 물리계층에서 다수의 가상머신을 각각 격리시켜 서로 간의 접근을 통제함으로서 안정적인 시스템을 제공하는 기술이다.

Zhang이 제안하는 CloudVisor는 악의적인 관리자에 대한 위협에 대한 문제 해결을 위해 개발된 기술로, 중첩 가상화 기술을 통하여 구현하였다. 데이터와 관리자의 위치를 분리하여 직접적으로 관리자가 데이터에 접근할 수 없도록 만든 것이 특징이다.

3. 보전성

클라우드 시스템에서 보전성은 "시스템 내부 또는 외부에 의해 서비스가 원활하게 작동하지 않을 때 정상적으로 복구되는 시간을 최소화하는 것"을 의미한다. 일반적으로 데이터 센터를 통하여 시스템을 구축하는 클라우드의 경우 지진 또는 낙뢰에 의해 서비스가 중단되는 사태가 빈번하게 일어난다. 예상치 못한 상황으로 인해 서비스 장애를 일으켰을 때 신속하게 대처하는 재난 복구 시스템(DRS)을 필요로 한다.

위협 사례 : 2011년 구글에서는 일본 대지진으로 인해 해저케이블이 손상이 되어 서비스 장애를 일으켰으며, 같은해 아마존에서는 벼락으로 인한 정전사고로 EC2 서비스 장애를 일으켰다.

보안 기술 : Site 기술, 가상화 기반 재난 복구 시스템

재난 복구 시스템의 기술 형태로는 Mirror Site, Hot Site, Warm Site, Cold Site이 있다.[16] 먼저, Mirror Site는 주 데이터 센터와 실시간 연동을 통하여 재난 발생 시 즉시 복구 및

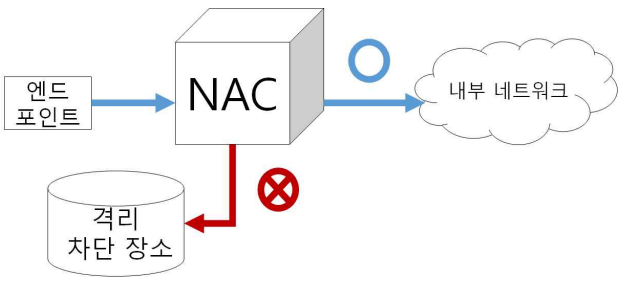

Fig. 8. Network Access Control Architecture

이용이 가능한 기술이다. 실시간 모니터링을 통하여 분석을 하기 때문에 복구시간이 가장 짧지만 IT자원의 소모가 다른 방식들에 비해 가장 높다. Hot Site는 주 데이터 센터와 동일한 시스템을 보유하여 최단시간 내 가동상태를 확보하는 기술이다. 하지만 데이터 센터와 호스트의 접속 자체가 불가능한 경우에는 복구가 불가능하다는 단점이 존재한다. Warm Site는 일부 시스템과 입출력 장치만을 보유하여 장애 발생 시 추가 장비를 도입하는 기술로, 경제적으로 효율적이나 재난 발생 시 신속한 대처가 불가능하다. Cold Site는 재해 발생에 대비하여 주기적으로 주요 데이터를 백업해 보관하여 시스템 운용을 재개할 수 있도록 별도의 물리적인 공간을 이용하여 복구하는 방식이다. 비용이 저렴한 반면에, 시스템 복구 시간이 가장 길고 백업 시점 차에 따른 복구 대책이 없는 것이 단점이다.

클라우드 환경에서 데이터 센터는 물리적 서버와 이기종의 가상서버가 혼재되어 있기 때문에 기존의 재난 복구 시스템으로는 안전하게 관리할 수 없다. 따라서 가상화 시스템을 통해 자동 백업 데이터 관리 및 복구 시스템을 구축하는 것이 필요하다.

가상화 기반 재난 복구 시스템으로는 그림 7 노벨 사의 포지(Forge)가 있다.[18] 포지는 운영 중인 다수의 가상머신의 워크로드를 통하여 데이터를 주기적으로 복제하고 재난 발생 시 최신 데이터로 복원하는 기술이다. 서비스가 장애를 일으켰을 때 데이터의 유실과 손상을 막는 시스템이며, 데이터 파일은 가상화 머신 형태로 변환 및 복제를 하기 때문에 클라우드 폼으로의 전환이 자유롭고 경제적이다. 유사한 기술로는 한국IBM의 Express Server Recovery(ESR)[19]로, 가상화 기반의 자동화된 재해복구 솔루션으로, 포털에서 한 번 클릭을 통한 시스템 명령만으로 빠르게 복구가 실행된다는 것이 가장 큰 특징이다. 또한, 셀프 모니터링 기능을 지원해 실시간으로 복구 진행 상태와 결과를 확인할 수 있다.

4. 무결성

데이터 무결성은 "시스템 상에 저장되어 있는 데이터의 수정 및 접근과 관련된 권한은 사용자 본인에게만 있고 제 3자에 의한 무단 변조 또는 접근을 허가되지 않은 방법으로 접근하는 것을 막는 것"을 의미한다.

무결성 보호 방법으로는 네트워크 관리자만의 서버 접근, 전송 선로 관리, 전기적 충격으로부터의 하드웨어 및 저장 장치의 보호 등을 통해 이루어지며, 사용자 인증 수준 유지, 시스템 관리 절차·유지 보수 지침 문서화, 그리고 장애 및 외부 공격에 대비한 복구 대책의 수립 등 관리 대책이 필요로 한다.

위협 사례 : 08년 아마존 사의 S3 서비스는 무결성 검사 루틴이 존재하지 않아서 서비스 다운 사태가 일어났으며, 12년 애플에서는 데이터 접속 권한이 없는 해커가 다른 사용자의 개인정보를 삭제한 사태가 발생하였다.

보안 기술 : 사용자 인증 및 접근 제어 기술, 무결성 확인 기술

사용자 인증 기술로는 OpenID, OAuth, XAuth가 있다.[20-22] OpenID는 개방형 인증 기술로 웹 서비스마다 ID를 생성하는 것이 아니라 소유하고 있는 사용자의 계정을 다른 웹 서비스에 인증하는 것이다. 하지만 사용자의 권한을 제어하지 못하기 때문에 악용할 수 있는 가능성이 있다.

OAuth는 OpenID의 사용자의 권한을 제어가 불가능한 문제로 등장한 기술이다. 웹 서비스 사용 시 ID와 패스워드가 필요 없으며, 사용자의 권한 제어가 가능하다. 그리고 사용자의 권한이 악용되어도 웹 서비스 자체에서 거부할 수 있도록 설계된 기술이다.

XAuth는 기본적인 인증 방식인 아이디와 패스워드를 통해 구현되어 있으며 OAuth와는 달리 웹서비스에서 사용하는 사용자의 아이디와 패스워드를 전달하기 때문에 인증 방법 및 절차가 간단하다. 그리고 브라우저 없이 인증할 수 있기 때문에 확장성과 유연성이 다른 인증 기술보다 높다는 장점이 있다.

접근 제어 기술로는 Network Access Control(NAC)가 있다.[23] 그림 8에서 NAC는 외부 네트워크 보호 기술들과는 달리 내부를 보호하는데 중점적인 기능을 두고 있다. 네트워크에 접근하는 사용자의 단말기인 엔드포인트를 제어하기 때문에 IP 기준이 아니라 사용자를 기준으로 네트워크를 통제할 수 있다. 이후 정책에 따라 허용된 사용자에게는 접속을 가능하게 되지만 허용되지 않은 사용자의 경우에는 격리 차단 장소로 보내게 된다.

무결성 확인으로 대표적인 기술로는 해시함수를 이용한 Secure Hash Algorithm(SHA)가 있다.[24] SHA는 미국 국가안보국(NSA)에서 처음 설계되었으며 이후 SHA-0, SHA-1 그리고 SHA-2가 개발되었다. 기본적으로 SHA 기술은 보안 프로토콜과 프로그램을 사용하여 보안을 하고 있으며 최근 공모전에서 채택된 SHA-2는 “아주 큰 소수로 된 합성수를 인수분해 하는 것의 어려움”에 기반을 두고 있으며, 이 기술을 토대로 데이터의 해시 값을 통하여 변조되거나 변형되었을 시 다른 값을 송출하여 무결성을 검증한다.

5. 기밀성

클라우드 시스템에서의 기밀성은 “정당한 사용자가 아닌 사용자들은 시스템 상의 데이터 또는 데이터 통신 간 통신 회선을 통해 교환, 전송되는 데이터의 원문을 볼 수 없게 하는 것”이다. 암/복호화 기술을 통하여 송수신 당사자가 아니면 데이터가 유출되더라도 변조되거나 위조되지 못하게 하는 기본적인 보안 기술이다.

위협 사례 : 2009년 마이크로소프트에서 제공하던 스마트폰 서비스 사이드킥에서 대규모 정보 손실로 인해 이용자의 정보가 유출되었고 2010년 BPOS 서비스의 시스템 오류로 인해 클라우드 상의 기업정보가 타인에게 열람되는 사건이 있었다.

보안 기술 : 암호 알고리즘, 암호 키 알고리즘, 암호 응용 기술

암호 알고리즘의 대표적인 기술로는 Advanced Encryption Standard(AES)가 있다. AES는 기존의 Data Encryption Standard(DES)를 대체하기 위해 National Institute of Standards and Technology(NIST)에서 개최한 공모전에서 채택된 기술로 4가지의 암호화 함수와 암호 키를 통하여 암호화를 한다. 하지만 복호화 시에는 같은 암호 키를 사용하지만 4가지 복호화 함수를 통하여 수행한다. 현재까지 대중적으로 사용되고 있는 암호 알고리즘이며, AES-128, AES-256과 같이 비트 수에 따라 다양한 형태로 사용이 가능하다.[25]

기본적으로 암호 알고리즘은 암호 키를 필요로 한다. 암호 키는 암호화 함수의 수행과정 중 핵심적인 역할을 하며 이를 생성하는 대표적인 기술로는 RSA 기술이 있다.[26] RSA는 공개 키 암호화 기술로 전자서명이 가능한 최초의 알고리즘으로 공개 키를 통해 사용자의 개인 키를 식별할 수 없도록 제작되었다. 이를 통해 사용자 개인 키를 활용하여 사용자만이 데이터의 복호화를 가능하게 만드는 암호 키를 생성하는 기술이다.

암호 응용 기술은 Transport Layer Security(TLS)가 있다.[27] 이 기술은 네트워크로 통신하는 과정 중 간섭 또는 위조를 방지하기 위해 설계되었으며, 중간 단계에서 암호화를 하기 때문에 최종 단계까지 통신의 기밀성을 유지시킨다. 클라우드 시스템 환경에서 가장 중요한 데이터 통신의 중요한 보안 역할을 하며, 다양한 암호 프로토콜과 인증 시스템을 통하여 구현되어 있기 때문에 데이터 통신의 중간 위치에서 악의적인 사용자가 중간에 데이터의 원문을 볼 수 없게 한다.

IV. Conclusions

클라우드 시스템은 단순한 파일 저장 시스템에서 원격 데스크탑 형태의 서비스까지 다양한 형태의 서비스를 사용자에게 제공하고 있으며, 많은 분야에서 그 활용성이 폭발적으로 증가하고 있다. 하지만 클라우드 시스템의 모델이 다양해짐에 따라, 새로운 형태의 보안 위협이 계속 발생될 것으로 예상된다. 클라우드 시스템은 보안 문제가 해결되지 않는 한 사용자로부터 안정적인 시스템으로 인정받을 수 없으며, 안정적인 서비스를 제공하기 위해서는 보안 위협에 따른 보안 기술을 마련하는 것이 시급하다. 현존하는 다양한 형태의 보안 기술들을 체계적인 보안항목을 통하여 분류하기 위해, 본 논문에서는 클라우드 시스템의 위협 사례와 보안 기술들을 컴퓨터 시스템의 견고성을 평가하는 용어인 RASIS에 맞추어 기술하였다. RASIS의 각 항목인 신뢰성, 가용성, 보전성, 무결성, 기밀성을 통하여 클라우드 시스템에서 이슈화되고 있는 보안 문제를 구체화하고 사용자가 신뢰할 수 있는 시스템이 된다면, 클라우드 시스템은 차세대 IT 환경을 주도하는 시스템 중 하나가 될 것이라고 믿는다.

REFERENCES

[1] http://www.ciokorea.com/news/13908, 2012.
[2] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0", March, 2010.

[3] IDC Enterprise Panel, n=244, August 2008.
[4] Jinhyung Kim, Dal-Nim Choi, Ji-Yeon Kim, Eun-young Jang, Hyung-Jong Kim, "Study of Trade-off Model Considering Privacy Protection Level and Privacy Violation Level", Journal of Security Engineering, vol. 8(2) April 2011.
[5] Cloud Computing Use Case Discussion Group, "Cloud Computing Use Case White Paper Version 4.0", July, 2010.
[6] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, Vol. 28(3), March, 2012.
[7] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", December, 2009.
[8] W. Jansen, and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", January 2011.
[9] REDWARE, http://www.radware.com/
[10] vAmour, http://www.varmour.com/
[11] Tal Garfinkel, Mendel Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection", 2003.
[12] Ibrahim, A.S, Hamlyn-Harris, J, Grundy, John, Almorsy, M, "CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model", Sept 2011.
[13] X. Chen, T. Garfinkel, E. C. Lewis, P. Subrahmanyam, C. A. Waldspurger, D. Boneh, J. Dwoskin, and D. R. K. Ports, "Overshadow: a virtualization-based approach to retrofitting protection in commodity operating systems", 2008.
[14] S. B. Suh, "Secure architecture and implementation of xen on arm for mobile devices", 4th Xen Summit, 2007.
[15] F. Zhang, J. Chen, H. chen, and B. Zang, "CloudVisor : Retrofitting Protection of Virtual Machines in Multitenant Cloud with Nested Virtualization", 2011.
[16] Seongmong Lee, "Information System Security", Inforever Consulting, 2010.
[17] Dae-Kyun Cho, Seok-Cheon Park, "Development and Implementation of Monitoring System for Management of Virtual Resource Based on Cloud Computing", Journal of The Korea Society of Computer and Information Vol. 18, No. 2, February 2013.
[18] Novel, http://novellkorea.co.kr/bbs/edm_forge
[19] IBM, http://www-935.ibm.com/services/kr/ko/it-services
[20] David Recordon, Drummond Reed, "OpenID 2.0: a platform for user-centric identity management" Proceedings of the second ACM workshop on Digital identity management, Pages 11 - 16, 2006.
[21] Jorge Fontenla Gonzalez, Manuel Caeiro Rodrıguez, Martı´n Llamas Nistal, Luis Anido Rifo'n, "Reverse OAuth: A solution to achieve delegated authorizations in single sign-on e-learning systems", 2010.
[22] Gaoyuan Pan, Yongbin Wang, "Securing RESTful WCF Services with XAuth and Service Authorization Manager - A Practical Way for User Authorization and Server Protection", 2012.
[23] Gabriel Lo'peza,, Oscar Ca'novasb, Antonio F. Go'meza, Jesu's D. Jime'neza, Rafael Marı'na, "A network access control approach based on the AAA architecture and authorization attributes", July 2005.
[24] Markku-Juhani O. Saarinen, "Beyond Modes: Building a Secure Record Protocol from a Cryptographic Sponge Permutation", September 2013.
[25] Jung-Oh Park, Gi-oug, Oh, "A Study on Parallel AES Cipher Algorithm based on MultiProcessor", Journal of The Korea Society of Computer and Information Vol. 17, No. 1, January 2013.
[26] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing", Proc. of the 29th conference on Information communications, pp.525-533, 2010.
[27] E. Rescorla, N. Modadugu, "Datagram Transport Layer Security", April 2006.

Authors

Jeong-Won Yoon is expected to receive the B.S. degree in Media Software from Sangmyung University, Seoul, Korea in 2016.

Mr. Yoon entered the Department of Media Software at Sangmyung University, Seoul, Korea, in 2010. He is interested in computer networks, and cloud system.

Beakcheol Jang received the B.S. degree from Yonsei University in 2001, the M.S. degree from Korea Advanced Institute of Science and Technology in 2002, and the Ph.D. degree from North Carolina State University in 2009, all in Computer Science.

Dr. Jang joined the faculty of the Department of Media Software at Sangmyung University, Seoul, Korea, in 2009. He is currently an assistant professor in the Department of Media Software, Sangmyung University, Seoul, Korea. He is interested in wireless networking with an emphasis on ad hoc networking, wireless local area networks, and mobile network technologies.