情 報 保 護 學 會 誌
第22卷 第8號, 2012. 12

IaaS 서비스의 정보보호 기술 분석 및 기업의 특성을 고려한 기술 적용방법 연구

강 진 희*, 김 지 연**, 박 춘 식***, 김 형 종***

요 약

인프라스트럭처 상용 클라우드 서비스(IaaS)의 이용 시 클라우드 기반의 네트워크에 어떤 정보보호기술을 적용할지에 대한 고려를 하는 것은 기존의 네트워크에 정보보호기술을 적용하는 것과 차이가 있다. 그 차이점은 클라우드 서비스 사업자가 서비스 형태로 제공하는 정보보호 기술들을 선택하여 적용할 수 밖에 없다는 것이다. 본 연구는 사업자가 제공하는 정보보호 서비스들이 어떠한 것이 있는지를 분석 종합하고, 기술의 특성을 고려해 재분류하고, 기업별로 제공되는 정보보호기술의 적용에 드는 비용을 함께 조사하여 각 사업자들의 정보보호기술의 과금 형태를 분석하였다. 또한, 이러한 분석을 기반으로 게임, 의료 및 소셜 커뮤니티 사이트 등의 기업 유형별 필요 기술을 선택하는 시나리오 분석을 시도 하였다. 본 연구의 기여점은 클라우드 환경에서의 정보보호 기술의 분석을 통해 해당 기술을 적용하고자 하는 사람들이 어떻게 기술을 선택 및 적용 할지에 대한 실질적인 방법을 제시한 것에 있다.

Ⅰ. 서 론

최근 클라우드 컴퓨팅 시장이 성장하면서 클라우드 서비스를 도입하는 개인 및 기업 사용자가 증가하고 있다. 그러나 클라우드 컴퓨팅 기술의 발전 및 서비스 다양화를 위한 노력에 비해 클라우드 서비스 보안 문제에 대한 서비스 제공자 및 이용자의 관심은 미비한 실정이다. 현재 클라우드 서비스 이용자들은 원하는 클라우드 서비스를 선택하고 그에 따른 비용을 지불하지만, 보안 기술의 경우에는 서비스 제공자가 모든 이용자에게 일괄적으로 제공하는 보안 기술만을 이용하거나, 일부 기업 사용자의 경우에는 필요한 기술을 추가 비용을 지불하여 선택적으로 이용하고 있다. 그러나 이러한 경우, 이용자는 서비스 제공자가 보유하고 있는 보안 기술 내에서만 보안 기술을 적용할 수 있다는 한계가 존재하기 때문에 높은 강도의 보안 기술을 필요로 하는 이용자들의 요구를 만족하기 어렵다. 따라서 본 논문에서는 클라우드 서비스 이용자가 클라우드 서비스 뿐 아니라, 보안 기술도 요구에 따라 이용할 수 있도록 클라우드 서비스 유형별로 필요한 보안 기술을 도출하고 적용 방법을 제시하고자 한다. 2장에서는 국내외 클라우드 서비스 제공자들이 현재 보유하고 있는 보안 기술 현황을 분석하고, 3장에서는 각 보안 기술을 클라우드 서비스 유형 및 비용 관점에서 분석한다. 또한, 4장에서는 클라우드 서비스 이용자 유형별로 어떤 보안 기술을 적용할 수 있을 지는 시나리오 기반으로 제시하고, 5장에서 결론을 맺는다.

Ⅱ. 국내외 클라우드 컴퓨팅 보안 서비스

2.1. 국외 클라우드 서비스 보안 기술 현황

2.1.1 아마존

대표적인 국외 클라우드 서비스는 아마존 웹 서비스로서 Amazon Elastic Compute Cloud (Amazon EC2),

* 서울여자대학교 정보보호학과 학사과정(gang7304@naver.com)
** 서울여자대학교 일반대학원 컴퓨터학과 석박사통합과정, 서울여자대학교 클라우드 컴퓨팅 연구센터(jykim07@swu.ac.kr)
*** 서울여자대학교 정보보호학과 조교수, 서울여자대학교 클라우드 컴퓨팅 연구센터(csp@swu.ac.kr, hkim@swu.ac.kr)

Amazon Relational Database Service (Amazon RDS), Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC) 등 다양한 서비스를 제공하고 있다.

사용자의 요청 량에 따라 컴퓨팅 자원을 제공하는 아마존의 가장 대표적인 클라우드 서비스로서 사용자 계정 생성 시, 다중 요소에 대한 인증을 수행하는 Multi-Factor Authentication (MFA) 방식을 채택하고 있다. 또한, 하이퍼바이저 (hypervisor) 수준에서의 방화벽 뿐 아니라 보안 그룹 (Security Group)을 운영하고, 기본적으로 모니터링 서비스를 제공하고 있다. 다음은 Amazon EC2에서 제공되는 보안 기술에 대한 설명이다.

① MFA

액세스 권한이 계정에 부여되기까지 확인하는 요소가 두 가지이기 때문에 Multi-Factor Authentication이라고 한다. 관리자가 관리 호스트로 접근할시 제공되는 서비스로 이 기능을 활성화하면 표준 사용자 이름 및 암호 자격 증명과 함께 6자리로 된 일회용 코드를 제공해야 액세스 권한이 부여된다. 즉, 사용자는 AWS 이메일 ID와 암호(첫 번째 “요소”: 사용자가 아는 사항) 그리고 사용자의 인증 장치에서 얻은 정확한 코드(두 번째 “요소”: 사용자가 갖고 있는 사항), 이 두 가지를 모두 제공해야 한다.

② 하이퍼바이저 수준 방화벽

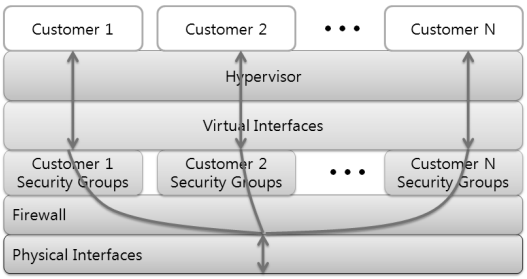
동일한 물리적 인터페이스에서 여러 각각의 인스턴스는 하이퍼바이저에서 서로 분리되어 작동한다. 모든 패킷들은 이 하이퍼바이저를 통과해야 하므로 하이퍼바이저 수준 방화벽은 같은 호스트 상에 있는 이웃 인스턴스들이 해당 인스턴스에 더 이상 접근하지 못하게 한다.

③ 보안 그룹

일종의 사용자 맞춤 방화벽으로써 물리적 인터페이스와 인스턴스의 가상화 인터페이스 사이에서 동작하면서 인스턴스를 생성할 때마다 하나 이상의 보안그룹을 할당하여 해당 VM으로 분리한다.

④ 모니터링

아마존에서는 Amazon CloudWatch를 사용해 Amazon EC2 인스턴스, Amazon EBS 볼륨, Elastic Load Balancer 및 Amazon RDS의 DB 인스턴스를 비롯하여 실시간으로 AWS 리소스를 모니터링 할 수 있다. Amazon CloudWatch는 AWS 클라우드 리소스와 AWS에서 실행되는 애플리케이션을 모니터링 한다. 이 서비스는 리소스 사용률, 작동 성능, 전반적인 수요 패턴을 파악할 수 있는 기능을 제공하며, 이를 위해 CPU 사용률, 디스크 읽기 및 쓰기, 네트워크 트래픽과 같은 메트릭을 모니터링 한다. 통계를 작성하고, 그래프를 보고, 메트릭 데이터에 대한 경보를 설정할 수 있다.



〔그림 1〕 보안 그룹

Amazon RDS는 클라우드 상에서 관계형 데이터베이스를 쉽게 설치, 운영 및 확장할 수 있는 웹 서비스로서 데이터베이스에 접근제어 규칙을 적용한 DB 보안 그룹 및 DB 인증서와 같은 보안 서비스를 제공하고 있다. 또한, 개인 계정에서 여러 사용자를 생성하고 이들의 권한을 관리할 수 있도록 Identity and Access Management (IAM) 기반의 접근제어를 수행하며, 스냅샷 기반의 백업을 통해 문제 발생 시, 원활하게 복구할 수 있도록 한다. 다음은 Amazon RDS에서 제공되는 보안 기술에 대한 설명이다.

⑤ DB 보안 그룹

컴퓨팅 보안 서비스인 보안 그룹과 같이 데이터베이스에 접근 제어 룰을 적용하여 그룹으로 묶어 관리 할 수 있다. 각 데이터베이스 보안 그룹은 해당 데이터베이스 서버 포트에 대한 액세스만 허용하므로 DB 인스턴스를 분리할 수 있다.

⑥ DB 인증서

향상된 보안을 위해 자신의 DB 인스턴스 연결을 암

호화할 수 있도록 각각의 DB 인스턴스에 대한 SSL 인증서를 생성한다.

⑦ IAM

본인의 계정에서 여러 사용자를 생성하고, 각 사용자의 권한을 관리할 수 있다. 여기서 사용자란 리소스에 액세스하는 데 사용하는 고유한 보안 자격을 증명해주는 ID이다. 결국 IAM을 이용하면 암호나 액세스키를 공유할 필요가 없어져 상황에 따라 각 사용자의 액세스를 쉽게 활성화하거나 비활성화 할 수 있다.

⑧ 스냅샷 기반의 백업

원본 데이터베이스의 삭제 여부와 상관없이 보존되며 스냅샷을 뜬 시점의 상태 그대로 데이터베이스를 새로 생성할 수 있다. 또한 현재 서버의 상태를 저장해두고, 사용자가 원할 때 즉시 저장해둔 상태로 복구할 수 있는 이미지를 저장할 수 있다.

Amazon S3는 인터넷 스토리지 서비스로서 사용자들은 물리적인 위치에 관계없이 데이터를 자유롭게 저장하고 이용할 수 있다. Amazon S3 서비스에서는 Amazon RDS와 마찬가지로 IAM을 사용하거나, 목록을 작성하여 각각의 개체들을 관리하는 Access Control List (ACL)를 통해 자원에 대한 접근을 제어한다. 또한, 쿼리 문자열로 인증을 수행하고, 데이터 암호화를 통해 보안을 강화하였다. 다음은 Amazon S3에서 제공하는 보안 기술에 대한 설명이다.

⑨ ACL

액세스 제어 목록을 작성하여 각각의 개체들을 관리하는 기능이다. 액세스 제어 목록을 사용해 개별 개체에 대한 특정 권한을 선택적으로 추가하거나 권한을 부여할 수 있다. 이때, 권한이 인증된 사용자는 인증이 되더라도 액세스 제어목록에 읽기 권한이 부여된 경우에만 개체를 읽을 수 있다.

⑩ 쿼리 문자열 인증

인증을 요구하는 자원에 HTTP 또는 브라우저 접근 시 유용하다. 쿼리 문자열로 인한 서명은 요청을 보호한다. 또한 미리 정의된 만료 기간 동안 유효한 URL을 통해 Amazon S3 객체를 공유할 수 있다.

⑪ 버킷 정책

단일 버킷 내에 있는 일부 또는 모든 객체에서 권한을 추가하거나 거부하는 데 사용한다.

⑫ 암호화

기업에서 암호화키를 관리하거나 사용자가 직접 암호화키를 관리할 수 있다. 대부분 기업에서 암호화키를 관리할 경우 AES-256 암호화 방식을 사용하는데 AES-256은 고급 암호화 표준으로써 256비트의 키 사이즈를 가지는 강력한 블록암호 중 하나이다. 반면 사용자가 직접 암호화키를 관리 할 경우는 스토리지에 업로드하기 전에 데이터를 암호화할 때 사용되며, 스토리지에 업로드 할 때 데이터를 자동으로 암호화할 수 있도록 기업에서 제공하는 자바 SDK를 사용한다.

Amazon VPC는 사용자의 독립적인 자원 사용을 보장할 수 있도록 클라우드 데이터센터 내에 사설 클라우드 환경을 제공하는 서비스이다. 이 서비스에서는 고객이 IP 주소 범위, 서브넷 생성, 경로 테이블과 네트워크 게이트웨이의 구성을 선택할 수 있기 때문에 가상 네트워킹 환경에 대한 자유로운 구성 및 제어가 가능하다. 또한, 보안 그룹 및 네트워크 접근 제어 목록을 포함하고 있는 다중 보안 계층을 활용하여 각 서브넷에서 인스턴스에 대한 접근을 제어하도록 지원한다. 위에서 살펴본 다양한 아마존 웹 서비스들의 보안 기술을 정리하면 [표 1]과 같다.

〔표 1〕 아마존 웹 서비스 종류 별 보안 기술

서비스	보안 기술
Amazon EC2	• Multi-Factor Authentication • 하이퍼바이저 수준의 방화벽 • 보안 그룹 • 모니터링
Amazon RDS	• DB 보안 그룹 • DB 인증서 • Identity and Access Management (IAM) • 스냅샷 기반 백업 • 모니터링
Amazon S3	• Identity and Access Management (IAM) • 접근 제어 리스트 • 버킷 정책 • 쿼리 문자열 인증 • 암호화
Amazon VPC	• 가상 네트워크 구성 • 다중 보안 계층

2.2. 국내 클라우드 서비스 보안 기술 현황

대표적인 국내 클라우드 서비스로는 KT ucloud biz, LG U+ Cloud N, T cloud biz가 있으며, 각 회사 별로 서비스의 규모를 점점 확대하고 있다.

2.2.1 KT ucloud biz

KT ucloud biz는 대표적인 서비스로 ucloud server, ucloud DB, ucloud storage, ucloud VPC를 제공한다.

ucloud server는 KT 클라우드 플랫폼 기반에서 CPU, 메모리, 디스크, 네트워크 등의 컴퓨팅 자원을 클라우드 서비스로 제공하며, 사용자는 웹 인터페이스를 통하여 필요한 컴퓨팅 자원을 구성할 수 있다. ucloud server는 아마존의 보안기술처럼 하이퍼바이저 수준의 방화벽과 보안 그룹을 사용하고 있으며, fail 2 ban이라는 인증 도구를 통해 접속을 차단한다. 부가서비스로는 웹 방화벽을 통해 감시한다. 다음은 ucloud server에서 제공하는 fail 2 ban과 웹 방화벽에 대한 설명이다.

① fail 2 ban

파이썬(2.4 버전 이상)으로 만들어진 특정 서비스로 로그인을 몇 회 이상 실패할 경우, 로그파일을 읽어서 일정기간 동안 접속을 차단하는 툴로 ssh, ftp 등에 무작위로 로그인하는 Brute force attack에 대응하기 위한 모듈이다. iptables, tcpwrapper 등의 접근 제어 프로그램에 해당 host를 등록하여 특정 host의 접속을 차단하는 기능을 가지고 있으며 ssh, apache, ftp 등을 이용한 접속 방어에 사용된다.

② 웹 방화벽

지능형 웹 애플리케이션 방화벽으로서 웹 서버 앞 단에 위치하여 외부로부터 들어오는 HTTP/HTTPS 프로토콜 트래픽을 감시한다. 이때 웹 애플리케이션에 대한 악의적인 공격이 탐지되면 해당 공격이 웹 서버에 도달하기 전에 차단하는 역할을 수행한다. 웹 방화벽은 포지티브(Positive) 보안모듈의 URI 접근 제어와, 네거티브(Negative) 보안모듈의 룰 탐지, White/Black list of IP 주소 관리기능인 IP 필터링/IP Block의 웹 클라이언트 접근 제어의 3중 방어 구조를 기반으로 확실하고 안정적인 웹 공격의 탐지와 차단을 제공한다.

ucloud DB는 사용자가 하드웨어, 소프트웨어, DB 관리자에 대한 초기 투자 없이 데이터베이스를 구축할 수 있는 서비스이다. 스냅샷 기반의 백업을 수행할 수 있고, 데이터 암호화 및 관제 서비스를 제공한다. 또한 아마존에서 제공하는 서비스와 유사한 DB 보안 그룹, DB 인증서, DB 접근 제어 리스트와 같은 보안서비스를 제공할 예정이다. 다음은 ucloud DB에서 제공하는 모니터링에 대한 설명이다. 나머지 보안 기술은 아마존과 같다.

③ 모니터링

사용 중인 클라우드 환경 내 자원현황 및 사용량 등에 대한 정보를 제공해 주고, 임계치 설정에 따른 각종 이벤트 및 알람을 제공해 줌으로써 안정적인 시스템 운용을 위한 환경을 제공하는 서비스이다. 모니터링 서버는 기본 SSH Private 22번으로 원격 접속이 필요하며 이에 대한 포트 포워딩 규칙은 고객이 직접 설정하여 접근한다.

ucloud storage는 대용량 데이터 파일 및 미디어 콘텐츠를 저장할 수 있는 클라우드 스토리지 서비스이다. ucloud storage는 파일 시스템이 아닌 오브젝트 스토리지로써, 간편한 Restful API나 툴로서 접근하며 실시간 데이터보다는 장기간 보관하는 데이터 저장에 더욱 적합하다. 데이터는 포탈, API 및 스토리지 툴에 의해 업로드/다운로드가 가능하며 물리적으로 독립된 스토리지에 동일한 데이터를 여러 번 복제하는 다중복제기술을 사용하여 기본적으로 3개의 복사본을 제공하고 데이터의 안정성을 보장한다.

ucloud VPC는 KT 클라우드 데이터 센터 내에 독립된 사설 클라우드 환경을 제공하며 VPC를 통해 기존의 사설 환경과 같은 커스토마이징(customizing) 및 개별적인 네트워크 프로비저닝(provisioning)이 가능하다. 이 서비스는 특정 고객을 위한 전용 하드웨어를 제공하여 독립적인 자원 사용을 보장하고, 클라우드 환경 내 고성능 물리서버를 제공하여, 대규모 시스템을 클라우드 환경에 수용한다. 또한 클라우드 환경 외부에 위치한 고객사 사이트와 고객의 클라우드 환경을 사설망으로 연결하여, 고객의 데이터 센터 유연성 확장 및 하이브리드 클라우드 환경으로 만드는 Site to Site VPN 서비스를 제공하고, 고객 요청 시 전용회선을 통한 고객사 사

〔표 2〕 KT ucloud biz 서비스 종류 별 보안 기술

서비스	보안 기술
ucloud server	• 하이퍼바이저 단 방화벽 • 보안 그룹 • fail 2 ban • 웹 방화벽 • 모니터링
ucloud DB	• 스냅샷 기반의 백업 • 모니터링 • DB 보안 그룹 (예정) • DB 인증서(예정) • DB ACL (예정)
ucloud storage	• 다중 복제 기술
ucloud VPC	• public / private VLAN • 외부 네트워크 • VLAN간의 라우팅 및 방화벽 설정 기능

이트 연결 지원한다. 뿐만 아니라 Public/Private VLAN을 통해 복수의 VLAN을 구성하고, 이를 가상머신 그룹 (예 : Web-Tier, App-Tier, DB-Tier) 별로 할당하고, 외부 네트워크 또는 VLAN 간의 라우팅 및 방화벽 설정 기능을 제공하여 보안을 강화 하였다.

위에서 살펴본 다양한 KT ucloud biz 서비스들의 보안 기술을 정리하면 [표 2]와 같다.

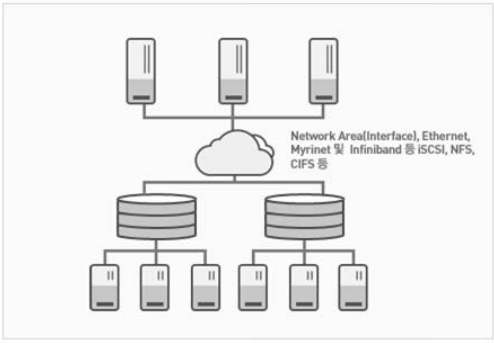
2.2.2 LG U+ Cloud N

또 다른 국내 클라우드 서비스인 LG U+ Cloud N는 컴퓨팅 서비스, 스토리지 서비스, 네트워크 서비스로 구성되어있는데, 각 서비스에서 제공하는 보안 기능이 다음과 같다.

컴퓨팅 서비스에서는 주요 컴퓨팅 자원인 CPU, 메모리, 하드디스크, 운영체제 등을 실시간으로 제공하며, 서버 운영 및 관리에 필수적인 다양한 서비스들을 제공한다. 공개키 기반구조의 PKI 암호화, API 토큰 인증 기술을 통해 보안을 강화하고 있으며, 개별 서버 보안 및 다수의 서버를 관리할 경우 각 서버마다 보안 규칙을 설정하여 관리할 수 있게 하는 네트워크 필터 기능 및 등록된 네트워크 필터를 각 VM에 적용하는 보안 그룹을 구성한다. 또한, 하이퍼바이저 단의 방화벽을 무상으로 제공하고 있으며 컴퓨팅 자원에 대한 실시간 모니터링을 수행한다. 또한 대용량 데이터 등을 저장하는 공간으로서 인터넷 및 엔터프라이즈 응용 프로그램에 최적화된 서비스를 제공한다. 뿐만 아니라 컴퓨팅 서비스에서 스냅샷 기반 백업을 제공한다. 스냅샷 기반 백업에는 현재 서버의 상태를 저장해두고, 사용자가 원할 때 즉시 저장해둔 상태로 복구할 수 있는 이미지를 저장해주는 풀 스냅샷(Full Snapshot)기능과 풀 스냅샷 기능에 번들링(Bundling)기능을 추가한 스냅샷 이미지를 이용하여 동일한 다수 서버를 생성할 수 있는 이미지를 저장해주는 기능이 있다. 이때, OS가 설치된 영역만 스냅샷 생성 가능하며 윈도우는 C드라이브, 리눅스는 disk0에 생성된다.

LG U+ cloud N의 스토리지 서비스는 Enterprise 스토리지 서비스와 웹 스토리지 서비스를 제공한다.

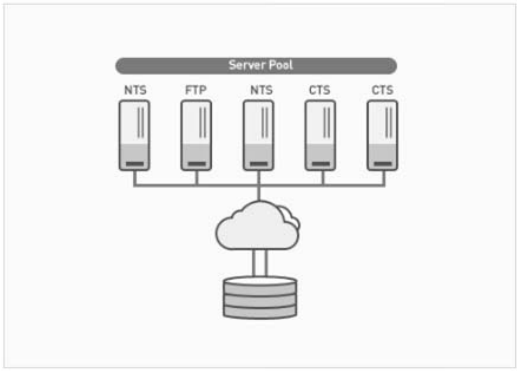
Enterprise 스토리지 서비스는 블록 단위 스토리지를 제공하고, 별도의 재해 복구 솔루션 없이 원거리 스토리지에 대한 미러링이 가능한 서비스로서 VPN/전용회선과 같은 고비용의 전송 매체를 사용하지 않아도 스토리지 자체에서 전송되는 데이터의 안전성 및 위변조 방지를 위해 30여 가지의 암호화 기술 및 해시(hash) 알고리즘 적용하고 있다.



〔그림 2〕 Enterprise Storage Service

웹 스토리지 서비스는 파일 및 디렉토리 등의 오브젝트 기반 스토리지로서 Service Level Agreement (SLA)에 따라 다중 복제 기능을 통한 데이터 안전성을 보장한다. LG U+ cloud N에서 제공하는 다중 복제 기능은 사용자가 2중, 3중 복제중 하나를 택하여 데이터를 안전하게 저장할 수 있다.

네트워크 보안 서비스에서는 네 가지의 보안 서비스를 제공하고 있다. 먼저, 서비스 요청이나 처리가 특정 서버로 집중되어 유발될 수 있는 서버의 성능 저하 방지를 위하여 다수의 서버로 서비스 요청을 분산시키는

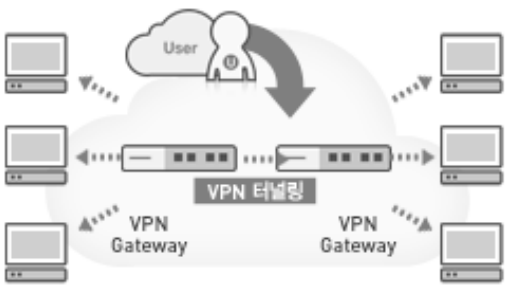


〔그림 3〕 Web Storage Service

L4/L7 서비스가 있으며, VPN 서비스를 이용하여 전용 네트워크를 구성할 수 있다. 또한, 클라우드 환경에서 공인 IP 주소를 특정 서버에 할당하는 것이 아니라 특정 사용자에게 할당하여 서버의 유무 또는 상태와 상관없이 사용자가 지정한 서버에 지정 IP 주소가 할당 될 수 있도록 하는 Elastic IP 서비스 및 가상의 네트워크 인터페이스 카드를 구성할 수 있는 Virtual NIC 서비스가 존재한다.

L4/L7은 서버의 상태 변화 시 알람 기능을 제공할 수 있을 뿐 아니라, 사용자 정의에 의해 서버의 상태를 감시할 수 있는 모니터링 기능이 있다. VPN은 클라우드 데이터센터 내에 수용된 고객의 VPN 장비 및 서버를 VLAN을 통해 독립된 네트워크로 구성할 수 있으며, Virtual NIC는 고객의 VPN, 웹 방화벽 및 IPS/IDS 등의 보안 장비와 전용 네트워크를 구성하고, 서버와의 연동을 지원한다.

위에서 살펴본 다양한 LG U+ cloud N 서비스들의 보안 기술을 정리하면 [표 3]과 같다.



〔그림 4〕 U+ cloud N의 VPN서비스

〔표 3〕 LG U+ cloud N 서비스 종류 별 보안 기술

서비스	보안 기술
컴퓨팅 서비스	• PKI 암호화 • API 토큰 인증 • 네트워크 필터 • 보안 그룹 • 하이퍼바이저 단 방화벽 • 모니터링 • 스냅샷 기반의 백업 서비스
DB 서비스	-
스토리지 서비스	• 암호화 • 다중 복제 기술
네트워크 서비스	• 모니터링 • VLAN 기반 독립 네트워크 • 웹 방화벽 • IPS/IDS 등 보안 장비 • 전용 네트워크 구성

2.2.3 T cloud biz

T cloud biz는 클라우드 서버, 클라우드 스토리지 서비스를 제공한다. 클라우드 서버는 가상화 솔루션과 자체 개발된 솔루션을 통해 안정적인 서버 인프라를 제공한다. 서버의 3대 구성요소인 중앙 처리 장치(CPU), 메모리(Memory), 하드 디스크(HDD)를 가상화하여 제공함으로써 전통적인 형태의 IT 인프라가 제공할 수 없었던 많은 장점을 제공한다.

클라우드 서버 서비스에서 보안 기술은 모니터링과 클라우드 서버의 하드디스크와 메모리 등이 바이러스에 의해 감염되었는지 여부를 진단하고 치료하는 백신 서비스, 하이퍼바이저 기반의 방화벽으로 접속하는 IP대역에 대한 제어가 가능한 VM방화벽 서비스를 제공한다. 또한 네트워크를 이루는 기본 구성 요소인 방화벽, 스위치, L4(로드밸런스) 등을 가상화하여 독립적으로 제공하는 가상 보안 네트워크 서비스, 클라우드 상에서 이용 중인 VM에 대한 외부 공격 및 VM간 악성 트래픽을 탐지 및 대응하는 IDS 서비스 등을 제공한다. 다음은 T cloud biz에서 제공하는 보안 기술들에 대한 설명이다.

① 모니터링

웹사이트에서 서버를 관리하고 서버의 상태를 모니터링 할 수 있다. 보다 체계적인 관리를 원하는 고객을

위해 전용 클라이언트를 통한 상태 관리도 가능하다.

② 백신 서비스

백신 서비스는 서버 운영체제와 함께 제공되어 클라우드 서버의 디스크와 메모리에 대한 실시간 바이러스 진단 기능을 제공하고. 바이러스 탐지 시 해당 파일을 삭제, 격리하거나 시스템을 치료해주는 역할을 수행한다. 바이러스뿐만 아니라 악의적인 광고, 트래픽 점유를 하는 스파이웨어, 혹은 관리자 권한을 획득하여 시스템 파괴를 위한 백도어(Backdoor)를 만드는 루트킷(Rootkit)과 같은 다양한 형태의 서버 위협 진단이 가능하여 하나의 솔루션으로 여러 가지 공격을 효과적으로 대응할 수 있다.

윈도우 기반의 클라우드 서버에서 동작하는 백신 서비스는 윈도우 개발사인 마이크로소프트가 직접 만든 Forefront Endpoint Protection 솔루션을 이용하기 때문에 서버에 가장 최적화된 기능을 제공하며 서버 운영체제의 성능에 적은 영향을 주면서 효과적으로 바이러스를 진담, 탐지할 수 있는 기능을 제공한다.

③ VM 방화벽

VM 방화벽은 하이퍼바이저 커널(Kernel)에서 동작하면서 개별 VM별로 전용 방화벽의 형태로 구동되어 논리적인 서버들 간의 해킹 시도를 원천적으로 차단할 수 있는 기능을 제공하는 서비스이다.

클라우드 인프라 정책에 의해 다른 고객사의 클라우드 서버와 같은 하드웨어에서 클라우드 서버가 구동 되더라도 내부, 외부 네트워크에 대하여 완벽한 격리와 네트워크 차단 기능을 제공하여 내부 트래픽을 효과적으로 제어할 수 있다.또한 대량의 클라우드 서버 사용 시에도 클라우드가 동작하는 물리적인 하드웨어의 위치에 구애받지 않고 그룹 단위의 방화벽 정책 설정이나 개별 가상 네트워크 인터페이스(vNIC, Virtual Network Interface Card) 단위로 룰 적용이 가능해 다양한 사용자 환경에 유연하게 대응할 수 있다.

④ 가상 보안 네트워크

가상 보안 네트워크 서비스는 네트워크를 이루는 기본 구성 요소인 방화벽, 스위치, L4(로드밸런스) 등을 가상화하여 독립적으로 제공하는 서비스로서 서비스에 맞는 별도 설정 및 정책 적용을 할 수 있다.

⑤ IDS 서비스

하이퍼바이저 기반 방화벽을 통해 마치 물리적인 서버와 네트워크 방화벽을 이용하는 것처럼 높은 보안 효과를 누리실 수 있고, VM방화벽을 통해 제공되는 트래픽 모니터링 정보는 사전 정의된 침입탐지 정책 및 현행 화된 공격 패턴, 시그니쳐 업데이트를 통해 외부 공격을 선제적으로 차단하고 적절히 대응할 수 있도록 돕는다.

⑥ 스냅샷 기반의 백업 서비스

풀 백업(Full Backup)과 차등 백업(Differential Backup)을 함께 제공해 1주일 이내의 시점으로 언제든지 클라우드 서버를 복구할 수 있으며, 스토리지 to 스토리지 형태의 백업 서비스를 제공하여 고객의 가상머신, 추가 디스크가 위치하는 스토리지와 별도로 고성능 백업 전용 스토리지를 통해 백업 서비스를 제공한다. Easy 스토리지 서비스는 자체 개발한 분산 파일 시스템 기반인 고속의 대용량 스토리지 서비스이다. Easy 스토리지로 업로드 된 데이터는 3개로 복제되어 3개의 다른 물리적 스토리지 서버에 저장된다. 따라서 데이터 손실 가능성이 극히 낮아 저렴한 비용으로 높은 안정성을 누릴 수 있다

위에서 살펴본 다양한 T cloud biz 서비스들의 보안 기술을 정리하면 [표 4]와 같다.

〔표 4〕 T cloud biz 서비스 종류 별 보안 기술

서비스	보안 기술
컴퓨팅 서비스	• 모니터링 서비스 • 백신 서비스 • VM 방화벽 서비스 • IDS 서비스 • 스냅샷 기반의 백업 서비스
DB 서비스	-
스토리지 서비스	• 다중 복제 기술
네트워크 서비스	• 가상 보안 네트워크

Ⅲ. 국내외 클라우드 서비스 보안 기술 분석

3.1 클라우드 서비스 유형별 보안 기술 분류 및 보안 강도 분석

2장에서 본 결과, 국내외 클라우드 서비스 보안 기술

〔표 5〕 국내외 클라우드 서비스 유형별 보안 기술 분류

유형	KT ucloud biz	LG U+ cloud N	T cloud biz	아마존
컴퓨팅 서비스	• 하이퍼바이저 단 방화벽 • 보안 그룹 • fail 2 ban • 웹방화벽 • 모니터링	• PKI 암호화 • API 토큰 인증 • 네트워크 필터 • 보안 그룹 • 하이퍼바이저 단 방화벽 • 모니터링 • 스냅샷 기반의 백업 서비스	• 모니터링 서비스 • 백신 서비스 • VM 방화벽 서비스 • IDS 서비스 • 스냅샷 기반의 백업 서비스	• 다중 요소 인증 • 하이퍼바이저 단 방화벽 • 보안 그룹 • 모니터링 •
스토리지 서비스	• 다중 복제 기술	• 암호화 • 다중 복제 기술	• 다중 복제 기술	• IAM • 접근 제어 리스트 • 버킷 정책 • 쿼리 문자열 인증 • 암호화
네트워크 서비스	• public / private VLAN • 외부 네트워크 • VLAN간의 라우팅 및 방화벽 설정 기능	• 모니터링 • VLAN 기반 독립 네트워크 • 웹방화벽 • IPS/IDS 등 보안 장비 • 전용 네트워크 구성	• 가상 보안 네트워크	• 가상 네트워크 구성 • 다중 보안 계층
DB 서비스	• 스냅샷 기반의 백업 • 모니터링 • DB 보안 그룹 (예정) • DB 인증서(예정) • DB ACL (예정)	-	-	• DB 보안 그룹 • DB 인증서 • IAM • 스냅샷 기반 백업 • 모니터링

현황을 토대로 분석해보면 현재 클라우드 서비스는 크게 컴퓨팅, 스토리지, DB, 네트워크 유형별로 서비스를 제공하고 있다. 따라서 사용자가 선택한 클라우드 서비스 유형별로 제공하는 보안 기술을 도출하기 위해서는 1절의 현황을 4가지 유형으로 나누어서 정리할 필요가 있다. 이것은 또한 유형별 일반화된 보안기술을 도출하는 데에 필요한 작업이다. 유형을 네 가지로 나누어 기업별 보안 기술을 유형에 맞게 분류해보면 [표 5]와 같다.

[표 5]을 살펴보면 서비스 유형별로 서로 유사한 보안 기술을 제공하는 것을 알 수 있다. 이는 사용자가 선택한 서비스 유형을 제외한 나머지 서비스는 제공이 되지 않고 나머지 서비스의 보안 기술 역시 사용할 수 없기 때문에 보안 기술이 유사하며 중복될 수 있다. 사용자가 한 유형을 선택했다고 가정한다면 그 유형에서 제공하는 보안기술만 사용할 수 있기 때문에 그 유형에는 인증 및 접근제어 등 여러 보안기술이 필요하다. 이때, 사용자들은 각 기업에서 제공하는 보안 기술들 중 유형별로 여러 기술을 선택해야 각 유형에서 보안 강도를 높일 수 있다.

3.2 기업별 클라우드 서비스 보안 기술 비용 분석

클라우드 서비스를 도입할 때 투자에 대비하여 효과가 있어야 한다. 따라서 유형별로 클라우드 서비스에 대한 보안 기술의 비용을 고려하고, 비용별로 나누어 분석할 필요가 있다. 국내외 클라우드 서비스 보안 기술 요금을 분석해보면 [표 6]과 같다.

[표 6]을 살펴보면 보안기술을 무료, 유료 로 과금 형태를 나누고, 유료인 경우 각 기업에서 제공하는 요금이 같은 보안 기술이어도 조금씩 다른 것을 알 수 있다.

아마존이 제공하는 MFA 서비스는 가상MFA서비스와 하드웨어MFA서비스를 제공한다. 가상 MFA서비스는 6자리 인증 코드를 생성할 수 있는 TOTP 호환 소프트웨어 애플리케이션에 만들어진 장치를 제공하여 단일 디바이스에서 여러 토큰을 지원한다. 반면 하드웨어 MFA서비스는 타사 공급자 Gemalto가 제공하는 침입 탐지 가능 하드웨어 전자 키 장치를 제공함으로서 다양한 금융 서비스 및 엔터프라이즈 IT 조직에서 사용하는 동일 유형의 디바이스이다. 가상MFA서비스는 아마존에서 무료로 제공하고 있고, 하드웨어MFA서비스는 타 공급자에 의해 제공되는 서비스로서 유료로 제공되고

〔표 6〕 국내외 클라우드 서비스 보안 기술 요금 분석

과금 형태	보안 서비스				
	보안 기술		요금		
무료	MFA	가상 MFA	기본으로 제공		
		하드웨어 MFA(유료)	12.99 USD ≒ 약 14680원		
	fail 2 ban		기본으로 제공		
	DB 인증서		기본으로 제공		
	쿼리 문자열 인증		기본으로 제공		
	API 토큰 인증		기본으로 제공		
	PKI 암호화		기본으로 제공		
	하이퍼바이저 수준 방화벽		기본으로 제공		
	네트워크 필터		기본으로 제공		
	보안 그룹		기본으로 제공		
	Identity and Access Management (IAM)		기본으로 제공		
	DB 보안 그룹		기본으로 제공		
	Access Control List (ACL)		기본으로 제공		
	버킷 정책		기본으로 제공		
	데이터 암호화	기업 암호화 키	기본으로 제공		
		고객 암호화 키	사용자의 선택		
	모니터링		(DB 서비스)기본으로 제공		
	웹방화벽		기본으로 제공		
	IPS/IDS 보안 장비		기본으로 제공		
유료	웹방화벽		KT cloud biz	Single : 25만원 ~ 60만원 /월	
				Dual : 100만원 ~ 145만원 /월	
	VM방화벽(*IP대역까지 필터링)		T cloud biz	월 5만원/VM당	
	모니터링		Amazon EC2	매달 총 3.50 USD(약 3860원)	
			KT ucloud biz	1,2 vCore	VM당 4천원/월
				4 vCore 이상	무료
	다중 복제 기술	2중화	LG U+ cloud N	사용요금의 2배	
			T cloud biz	기본요금 5000원에 1GB당 사용량 구간에 따라 70원~100원추가된다.	
		3중화	KT ucloud biz	기본으로 3중화 제공(무료)	
			LG U+ cloud N	사용요금의 3배	
			T cloud biz	기본요금 5000원에 1GB당 사용량 구간에 따라 90원~120원추가된다.	
		4중화	LG U+ cloud N	희망시 별도 협의 후 지원 가능	
	스냅샷 기반 백업		아마존	DB 인스턴스가 종료된 후 백업 스토리지 추가시 월별 GB당 0.125USD ≒ 138원	
			LG U+ cloud N	1회 시 월정액 3000원 서버 이미지 생성시 서버마다 1회 당 1000원	
			T cloud biz	월 2000원이며 10G 당 요금이며 디스크 용량만큼 과금	
	Virtual Private Cloud (VPC)		아마존	VPN 연결 시간당 0.05USD	
			KT ucloud biz	1/2 Rack	1580만원
				1 Rack	2430만원
	Virtual Private Network (VPN)		KT ucloud biz	Site to Site VPN (1Gbps Shared) : 15만원/월	
			LG U+ cloud N	스위치 포트 수량 2개 2만원/월	
	IPS/IDS 서비스		T cloud biz	월 5만원/VM당	
	가상 보안 네트워크		T cloud biz	협정가	
	백신 프로그램		T cloud biz	월 천원/VM당	

있다.

데이터 암호화 기술은 기업에서 암호화키를 관리하거나 사용자가 직접 암호화키를 관리할 수 있기 때문에 사용자는 두 방법 중 하나를 택하여 암호화 할 수 있다.

KT ucloud biz에서 제공하는 웹 방화벽은 Single 상품과 Dual 상품이 있다. Single 상품은 단일 웹 서버 머신 1대만을 보호할 사용되고, Dual 상품은 2대 이상의 웹 서버를 로드밸런싱 하여 사용한다. Dual 상품은 Single 상품보다 1대 이상의 웹 서버를 보호하는 만큼 가격이 조금 더 높다.

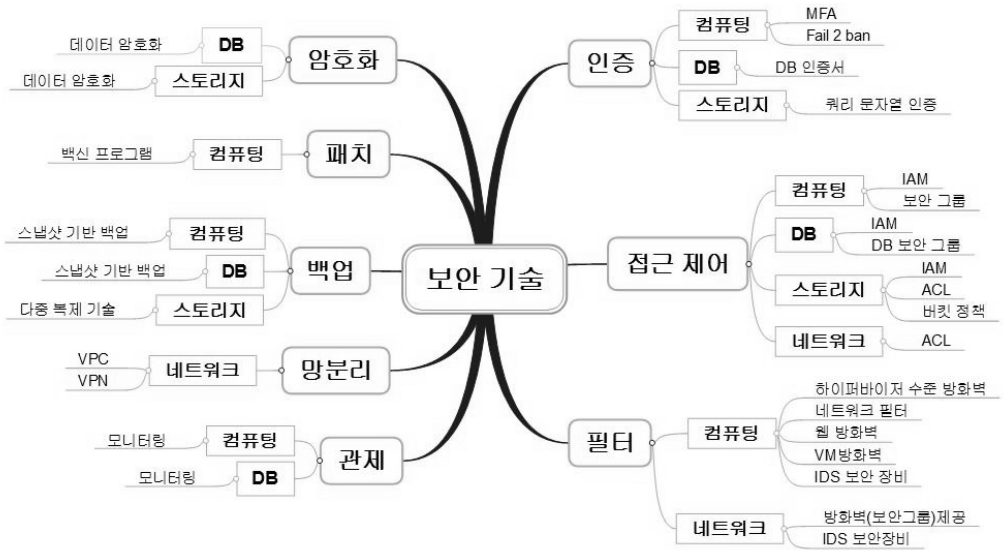
KT ucloud biz와 LG U+ cloud N, T cloud biz에서 제공하는 다중복제기술은 서로 요금이 다르다. KT ucloud biz는 기본으로 3중화를 제공하고, LG U+ cloud N는 2중 복제, 3중 복제, 4중 복제 이상을 사용자가 선택하여 비용을 지불할 수 있도록 제공하고 있다. T cloud biz는 표준 3중 복제로 제공되며 사용 빈도와 중요도가 조금 낮은 데이터를 저장하려는 고객의 요청을 반영하여 보다 저렴한 2중 복제 선택의 옵션을 제공하고 있다. 월 기본료는 5000원이며 스토리지 사용량과 트래픽 사용료로 나누어 과금 된다.

VPC는 아마존과 KT ucloud biz에서 제공하며 요금 측정 기준이 다르다. 아마존은 VPC 서비스 자체는 무료로 제공하나 VPN 게이트웨이를 사용하여 VPC에 대한 하드웨어 VPN 연결을 생성하는 경우 VPN 연결을 프로비저닝하고 VPN 연결 시간당 요금이 청구된다. 반면 KT에서는 특정 고객을 위한 전용 하드웨어를 제공하여 독립적인 자원의 사용을 보장하는데 이것을 1Rack, 1/2Rack 기준으로 제공한다. VPN는 KT ucloud biz와 LG U+ cloud N에서 제공하는데, LG는 스위치 in/out 2 포트와 고객이 소유한 VPN장비를 수용하는 공간을 구성하고 스위치 2개에 대한 요금만 월정액으로 제시한다.

사용자는 보안 기술의 요금으로 보안강도를 예측할 수 있고, 보안기술을 적용하고자 하는 서비스에 맞게 보안 서비스를 선택하여 비용 대비 효과를 기대할 수 있다.

IV. 클라우드 보안 기술 도출 및 클라이언트 유형별 적용 방안

3장에서 살펴본 클라우드 서비스 보안 기술을 분석하면 클라이언트가 적용할 수 있는 보안 기술을 크게 인증, 필터, 접근제어, 암호화, 관제, 백업, 망분리, 패치 기술로 분류할 수 있다. 따라서 각 유형의 보안 기술이 필요한 클라이언트들은 사용하는 클라우드 서비스 유형별로 세부 보안 기술을 선택할 수 있다. [그림 5]은 보안 기술 유형별로 클라이언트에게 제공될 수 있는 세부 기술을 명시한 것이다. 이때 [표 7]는 클라우드 서비스 이용자 유형별로 적용 가능한 보안 기술을 간략히 정리



〔그림 5〕 클라우드 보안 기술 분류

〔표 7〕 클라우드 서비스 이용자 유형별 적용 가능한 보안 기술

분야		게임 회사 및 신문사	병원	소셜 커뮤니티 회사	클라우드 기반 네트워크 운영 기업
클라우드 서비스 유형		컴퓨팅	DB	스토리지	네트워크
적용 가능한 보안기술	인증	MFA Fail 2 ban	DB 인증서	쿼리 문자열 인증	-
	접근 제어	IAM 보안 그룹	IAM DB 보안 그룹	IAM 접근 제어 리스트 버킷 정책	접근 제어 리스트
	필터	하이퍼바이저 수준 방화벽 웹방화벽 VM방화벽 네트워크 필터	-	-	방화벽 제공 IDS 보안 장비
	암호화	-	데이터 암호화	데이터 암호화	-
	백업	-	스냅샷 기반 백업	다중 복제 기술	-
	패치	보안 프로그램	-	-	-
	망분리	-	-	-	VPC VPN
	관제	모니터링	모니터링	-	-

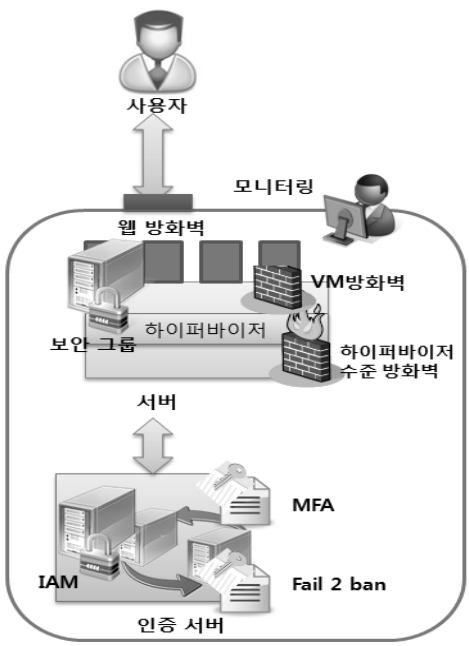
한 것이다. [표 7]과 같이 유형별 보안 기술을 클라우드 서비스 이용자에 적용하여 시나리오 기반으로 설명할 수 있는데 각 분야별로 적용해보면 다음과 같다.

4.1 게임 회사 및 신문사

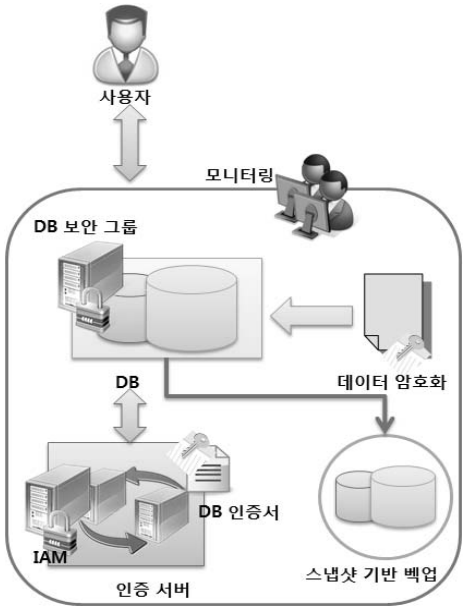
게임 회사 및 신문사와 같이 동시에 많은 사용자들을 수용할 수 있는 대용량 서버가 필요한 클라이언트의 경우, 클라우드 서비스로서 컴퓨팅 자원을 제공받을 수 있다. 게임 회사는 순간 접속자가 증가 할 수 있고, 신문사의 경우 그날 이슈가 되는 기사에 많은 사람들이 접근하기 때문에 컴퓨팅 서비스 중 하나인 서버 서비스를 제공 받을 수 있다. 두 분야의 회사 모두 회원가입에 따른 개인 정보 유출에 대한 대응으로 인증 기술이 필요하고, 회원의 등급별 서비스를 제공하기 위해 접근 제어 기술을 사용할 수 있다. 또한 외부의 악의적인 공격의 서버 유입을 차단하기 위한 필터 기술과, 악성코드에 의한 회원 정보 유출 및 서비스 변경 방지를 위한 패치 기술로 보안 프로그램을 사용할 수 있다.

4.2 병원

병원에서는 환자의 진료 기록을 저장 및 관리와 검색을 하기 위해 클라우드 DB 서비스를 이용할 수 있다. 병원에서는 환자 개인의 정보 유출을 막기 위해 DB 인증서와 같은 기술을 이용한 인증을 수행할 수 있고, 환자 의료기록에 대한 수정 및 읽기 권한을 부여하기 위



〔그림 6〕 컴퓨팅 서비스 원리

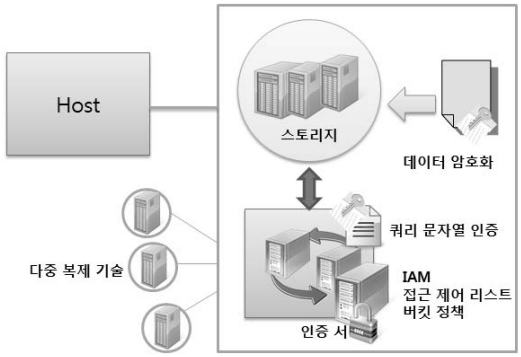


〔그림 7〕 DB 서비스 원리

해 접근 제어 기술을 사용할 수 있다. 또한 환자에 대한 정보 보호, 클라이언트가 서버에서 데이터를 열람할 때 스니핑에 의한 데이터 유출 및 변조 방지를 위해 암호화 기술을 적용할 수 있고, 병원 관계자의 실수나 컴퓨터상의 오류, 바이러스 감염 등의 문제로 데이터가 손실, 혹은 삭제되는 것에 대비하기 위해 백업이 필요하다. 이때, DB 추가 용량 등 중요한 필드가 변경되거나 DB의 자원 상태가 초과 되었을 때 알람 해주는 모니터링 기능을 사용할 수 있다.

4.3 소셜 커뮤니티 회사

클라우드 스토리지 서비스는 동영상 및 이미지 등 많은 데이터들을 고속으로 전송해야하는 소셜 커뮤니티 분야의 회사에서 사용할 수 있다. 소셜 커뮤니티 분야의 회사도 마찬가지로 회원가입에 따른 개인정보 유출에 대한 대응을 위해 인증 기술이 필요하고, 스토리지에 업로드되고 저장된 데이터에 사용자별 읽기 및 쓰기 권한을 부여하기 위해 접근 제어 리스트 기술을 사용할 수 있다. 또한 이미지 및 동영상 등 전송되는 데이터 유출 및 변조를 방지하기 위해 암호화 기술을 적용할 수 있고, 업로드하거나 전송 받은 데이터가 사용자 실수나 컴퓨터상의 오류, 바이러스 감염 등의 문제로 손실 되는

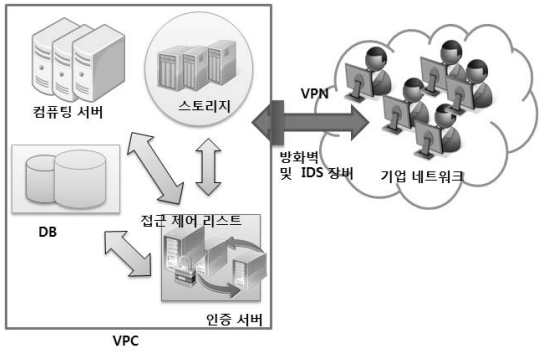


〔그림 8〕 스토리지 서비스 동작 원리

것에 대비하여 백업이 필요하다.

4.4 클라우드 기반 네트워크 운영 기업

자체 네트워크를 구축하고자하는 기업에서는 클라우드 네트워크 서비스를 사용할 수 있으며, 다른 분야의 기업과 마찬가지로 관리자 외 사용자의 접근을 제어하여 내부 공격을 막기 위해 접근 제어 기술이 필요하다. 또한 외부 네트워크로부터 악의적인 공격 및 접근을 막기 위해 필터 기술을 사용할 수 있다. 클라우드 네트워크 서비스는 기본적으로 컴퓨팅, DB, 스토리지 클라우드 서비스 유형이 제공하는 보안 기술을 모두 포함할 수 있지만, 자원을 독립적으로 사용하여 보다 안전하고 망을 운영하기 위해서는 VPC, VPN과 같은 망분리 기술을 적용할 수 있을 것이다.



〔그림 9〕 네트워크 서비스 원리

V. 결론

본 논문은 국내외 클라우드 서비스에서 제공하고 있

는 보안 서비스 현황 조사를 통해 클라우드 서비스 유형별로 클라이언트가 적용할 수 있는 세부 보안 기술을 도출하고, 클라이언트 유형별로 보안 기술을 적용하기 위한 방법을 시나리오 기반으로 제시하였다.

현재 국내외 클라우드 서비스 현황 분석 결과, 클라우드 서비스의 유형은 크게 컴퓨팅, DB, 스토리지, 네트워크 서비스로 분류할 수 있고, 클라이언트는 이용하고 있는 클라우드 자원의 가치를 고려하여 원하는 보안 강도 및 비용 내에서 세부 보안 기술들을 적용할 수 있다. 클라이언트는 보안 강도를 높이기 위해서 여러 세부 보안 기술을 도입할 수 있지만, 여러 보안 기술을 적용하기 위해서는 그 만큼의 보안 서비스 비용을 지불해야 하기 때문에 투자 대비 효과를 생각해보아야 한다. 즉, 보안 기술 도입에 소요되는 비용이 보안 피해발생 시, 어느 정도의 이익을 줄 것인지를 판단하여 보안 서비스를 이용해야 할 것이다.

본 연구에서 도출한 클라우드 서비스 유형별 보안 기술은 클라우드 서비스 제공자가 제공해야할 보안 기술들을 제시하고, 클라이언트 서비스 도입 시 발생할 수 있는 보안 문제 및 대응 방안을 제시할 수 있다는 점에서 의의가 있다. 그러나 클라이언트가 실제로 보안 서비스를 도입하기 위해서는 비용을 고려하여 필요한 보안 기술들을 선택할 수 있어야 하기 때문에 향후연구로서 클라이언트가 도입할 수 있는 보안 서비스를 비용 및 보안 기술 유형을 기준으로 선택할 수 있는 체크리스트를 개발할 예정이다.

참고문헌

[1] http://aws.amazon.com/ko/, 아마존 웹 서비스 보안

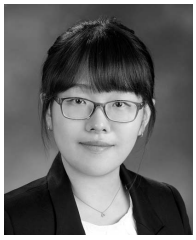
[2] “Amazon Web Services: Overview of Security Processes”, May 2011

[3] http://www.cloudn.co.kr/front/app/index, LG U+ 클라우드 보안 서비스

[4] http://home.ucloud.olleh.com/main.kt, KT ucloud 보안 서비스

[5] https://www.tcloudbiz.com/usr/main/main/main.do, T cloud biz 보안 서비스

〈著者紹介〉



강 진 희 (Jin Hee Kang)
정회원

2009년 3월~현재: 서울여자대학교 정보보호학과 재학
<관심분야> 클라우드 컴퓨팅보안

김 지 연 (Ji Yeon Kim)
정회원

2007년 2월: 서울여자대학교 정보보호공학과 공학사
2007년 3월~현재: 서울여자대학교 일반대학원 컴퓨터학과 석박사 통합과정
<관심분야> 클라우드 컴퓨팅보안, VoIP 보안, 정보보호, 모델링 시뮬레이션 방법론

박 춘 식 (Choon Sik Park)
종신회원

1995년: 일본동경공업대 공학박사
1982년-1999년: 한국전자통신연구원 책임연구원
2000년-2008년: 국가보안기술연구소 책임연구원
2009년 3월~현재: 서울여자대학교 정보보호학과 교수
<관심분야> 개인정보보호기술, 클라우드컴퓨팅보안, 사이버보안

김 형 종 (Hyung Jong Kim)
종신회원

1996년 2월: 성균관대학교 정보공학과 공학사
1998년 2월: 성균관대학교 정보공학과 공학석사
2001년 2월: 성균관대학교 전기전자 및 컴퓨터공학과 공학박사
2001년~2007년: 한국정보보호진흥원 수석연구원
2004년~2006년: 미국 카네기멜론 대학 CyLab Visiting Scholar
2007년 3월~현재: 서울여자대학교 정보보호학과 조교수
<관심분야> 클라우드 컴퓨팅 보안, VoIP 보안, 개인정보보호, 모델링 시뮬레이션 방법론