클라우드 컴퓨팅 보안 기술

Cloud Computing Security Technology

클라우드 컴퓨팅 특집

은성경 (S.K. Un) 암호기술연구팀 책임연구원
조남수 (N.S. Jho) 암호기술연구팀 선임연구원
김영호 (Y.H. Kim) 지식정보보호연구팀 선임연구원
최대선 (D.S. Choi) 인증기술연구팀 선임연구원

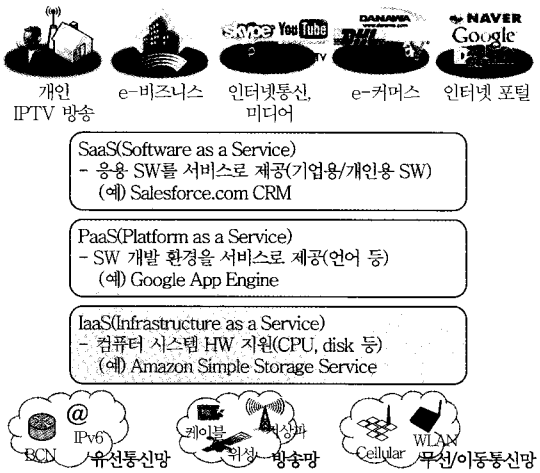
목 차

클라우드 컴퓨팅은 인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅으로 최근 많은 관심을 받고 있다. 클라우드 컴퓨팅이 널리 사용되기 위해서 해결해야 할 첫 번째 문제는 보안인 것으로 조사된 바 있다. 클라우드 컴퓨팅의 보안은 사용자의 영역에 따라 개인 사용자와 기업 사용자 분야로 나눌 수 있으며, 개인 사용자는 익명성에 관심을 두고 있고, 기업 사용자는 컴플라이언스에 관심을 두고 있다. 클라우드 컴퓨팅은 플랫폼, 스토리지, 네트워크, 단말로 구성되어 있고, 각각의 위치에서 필요한 보안기능이 따로 존재한다. 본 고에서는 클라우드 컴퓨팅 보안의 기술들에 대해서 알아보고, 현재 클라우드 컴퓨팅의 대표적인 서비스 중의 하나인 아마존 AWS의 보안 기능에 대하여 살펴보고자 한다.

Ⅰ. 클라우드 컴퓨팅 모델

클라우드 컴퓨팅이란 '인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅'으로 정의할 수 있다[1]. 주요한 특징으로는 IT 자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼의 비용을 지불하는 것을 들 수 있다.

이러한 컴퓨팅을 제공하기 위한 서비스로 그 추상화 정도에 따라 분류해보면 (그림 1)과 같다.

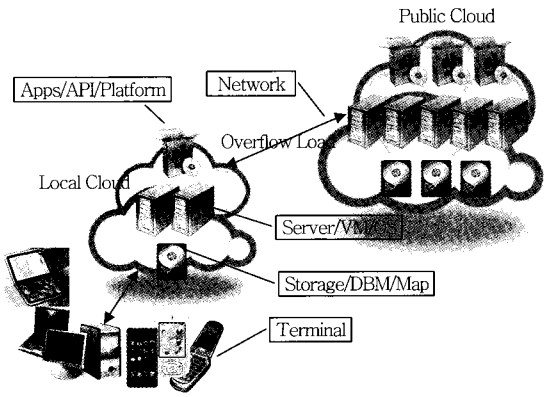


(그림 1) 클라우드 컴퓨팅 서비스 모델

IaaS는 CPU, 디스크 등 컴퓨터 시스템의 하드웨어 자원을 가상화하여 여러 사용자에게 제공하는 것으로 아마존의 Elastic Compute 서비스가 이에 해당한다. PaaS는 하드웨어 자원을 추상화하고 그 위에 소프트웨어 개발과 수행환경을 제공하는 것으로 구글의 App Engine과 아마존의 Simple Storage Service 등이 이에 해당한다. SaaS는 응용 소프트웨어를 서비스 형태로 제공하는 것으로, 대표적인 서비스로는 Salesforce.com과 구글의 Docs 등을 들 수 있다.

이러한 서비스들을 수요자별로 시장을 구분하고 각각의 사례와 주요한 사업자를 <표 1>에서 확인할 수 있다[2].

클라우드 컴퓨팅을 구성하는 요소들은 (그림 2)



(그림 2) 클라우드 컴퓨팅 구성 요소

〈표 1〉 시장별 서비스 유형과 주요 사업자

시장 유형		제공서비스 사례	주요 사업자 서비스
소비자 시장	웹기반 서비스	· 인터넷 기반 서비스 (Blog, Wiki, Social Service)	· 구글 · Mysapce.com
	SW 서비스(SaaS)	· Office 생산성 애플리케이션 · 협업 솔루션 · 기타 클라이언트 애플리케이션	· 구글 Apps for Your Domain · MS Office Live · IBM Bluehouse
IT 구매자 시장 (클라우드 인프라)	애플리케이션 컴포넌트 서비스	· 서비스나 애플리케이션 개발을 위한 API와 웹기반 SW 모듈 (애플리케이션 레이어 수준)	· 아마존 Flexible Payment API · 구글 Calendar API · 세일즈포스닷컴 AppExchange API
	SW 플랫폼 서비스 (PaaS)	· 신규 애플리케이션 개발을 위한 개발 플랫폼 (미들웨어 레이어 수준) - Hosted App Plalform Server, Hosted DB - Housted Data 관리, Massage Queue 등	· 아마존 SimpleDB, Simple Storage Service(S3), Simple Queue Service · 구글 App Engine · MS SQL Server Data Service · 세일즈포스닷컴 Force.com
	가상인프라 서비스	· 가상 서버, 가상 스토리지, 가상 네트워크 · 시스템 관리	· 아마존 Elastic Compute Cloud(EC2)

<자료>: 한국소프트웨어진흥원, 2008.

에서 확인해 볼 수 있다.

단말은 서비스를 요청하거나 그 결과를 보는 장비이며, 여기에는 개인용 컴퓨터를 비롯하여 노트북과 이동형 기기인 휴대전화 등을 들 수 있다. 서버는 실제 작업을 수행하는 장비를 지칭하며 여기에는 서버 컴퓨터를 비롯하여 운영체제 등이 포함된다. 스토리지는 결과를 저장하는 곳으로 디스크 및 데이터베이스 등을 포함한다. 응용프로그램은 서버와 스토리지를 이용하여 원하는 작업을 수행하는 프로그램이다. 단말과 클라우드 그리고 한 클라우드와 다른 클라우드는 네트워크로 연결한다.

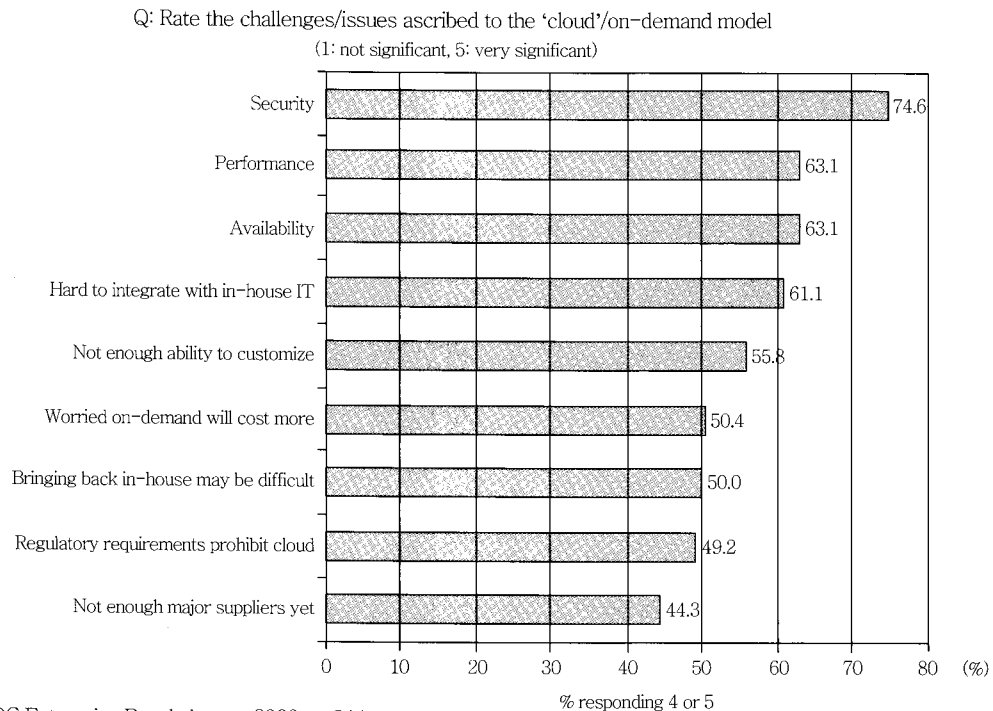
클라우드 컴퓨팅은 이용 목적에 따라서 public cloud와 local cloud로 나눈다. Public cloud는 일반 사용자에게 공개되어 있는 클라우드 컴퓨팅 서비스로 구글과 아마존의 서비스가 이에 해당한다. 이러한 종류의 서비스는 대규모로 이루어지는 특성이 있다. 반대로 local cloud는 기업 내부와 같이 폐쇄된 환경에서 특정사용자만 사용하는 클라우드 서비스를 지칭하며, private cloud 혹은 enterprise cloud라는 이름으로 부르기도 한다. 또, local cloud를 운영하다 서비스가 감당할 수 있는 한계에 다다르면, 넘치는 서비스 요구를 외부의 public cloud 서비스를 이용하여 처리하는 형태를 생각할 수 있는데, 이러한 형태를 hybrid cloud로 부르기도 한다.

Ⅱ. 클라우드 컴퓨팅 보안 이슈

클라우드 컴퓨팅은 IT 자원을 소유하지 않고 일부 또는 모두를 아웃소싱 하는 형태이다. 이런 경우는 필연적으로 보안 문제가 제기될 수 밖에 없는데, (그림 3)은 이를 잘 대변해 준다.

이 그림은 시장 조사 기관인 IDC에서 244명의 IT 관련 임원들에게 IT cloud 서비스에 관하여 그들의 견해와 활용에 대하여 조사한 것 중의 하나로, 보안을 해결해야 할 첫번째 과제로 꼽고 있다.

클라우드 컴퓨팅의 보안 이슈는 두 가지 소비자 영역으로 나누어서 생각해 볼 수 있다. 첫번째는



<자료>: IDC Enterprise Panel, August 2008. n=244

(그림 3) IT Cloud 서비스의 해결 과제

개인 사용자 관점의 보안이다. 개인 사용자는 이메일, 블로그, 동호회, 사진 및 파일 저장과 공유 서비스를 주로 이용하며, 무료로 제공하는 서비스를 선호하는 특성을 갖는다. <표 1>의 웹 기반 서비스들이 주로 이들을 위한 것이다. 개인 사용자 관점에서 우려하는 보안 문제를 열거하면 다음과 같다.

- 개인정보 노출
- 개인에 대한 감시
- 개인 데이터에 대한 상업적 목적의 가공

두번째는 기업 사용자 관점을 들 수 있다. 기업 사용자는 자신이 소유하던 IT 자산을 클라우드 형태로 제공받기를 원하지만, 자신의 데이터가 타인과 공유되기를 원하지 않는다. <표 1>에서 웹 기반 서비스를 제외한 다른 서비스들이 기업 사용자를 위한 것이다. 기업 사용자는 안정성과 안전성을 제공하면 비용을 지불할 의사가 있으며, 때에 따라서는 local cloud와 같이 자신이 직접 운영하기도 한다. 기업 사용자 입장에서 우려하는 보안 문제를 열거하면 다음과 같다.

- 서비스 중단
- 기업 정보 훼손
- 기업 정보 유출
- 고객 정보 유출
- 법/규제 준수
- e-discovery 대응

이와 같이 개인 사용자와 기업 사용자는 클라우드 컴퓨팅에 대한 보안 요구사항이 다르다. 개인 사용자는 익명성 보장에 중점을 두는 반면, 기업 사용자는 컴플라이언스에 중점을 두는 경향이 있다.

기업 사용자의 보안 고려사항은 Cloud Security Alliance에서 가이드로 제시한 것을 참고해 볼 수 있다[3]. Cloud Security Alliance는 클라우드 컴퓨팅의 안전성 증진과 사용자 교육을 목적으로 만든 비영리 기관으로, 다음과 같은 보안 고려사항을 제시하고 있다.

① Governance and Enterprise Risk Management
② Legal
③ Electronic Discovery
④ Compliance and Auit
⑤ Information Lifecycle Management
⑥ Portability and Interoperability
⑦ Traditional Security, Business Continuity and Disaster Recovery
⑧ Data Center Operations
⑨ Incident Response, Notification and Remediation
⑩ Application Security
⑪ Encryption and Key Management
⑫ Identity and Access Management
⑬ Storage
⑭ Virtualization

Ⅲ. 클라우드 컴퓨팅 보안 기술

클라우드 컴퓨팅에서 보안 기술은 아직 확립된 것이 없다. 그러나, 클라우드 컴퓨팅이 완전히 새로운 기술이 아니고 기존 IT 기술의 연장선상에 있는 것으로, 보안도 이와 같은 맥락에서 기존 보안기술들 중 클라우드 컴퓨팅 구성 요소별로 구분하여 적용할 수 있다.

1. 플랫폼

플랫폼에 사용되는 보안기술로는 접근제어와 사용자 인증 기술이 가장 대표적이다. 접근제어는 운영체제상의 한 프로세스가 다른 프로세스의 영역(파일 혹은 메모리)에 접근하는 것을 통제하는 기술로 DAC, MAC, RBAC 등이 대표적이다.

DAC는 사용자가 자신이 소유한 자원에 대한 접근 권한을 임의로 설정하는 것을 말한다. 대표적인 것으로 UNIX의 파일 permission을 들 수가 있다. MAC는 자원에 대한 보안 등급과 영역을 기준으로 수직과 수평적 접근규칙을 시스템 차원에서 설정하여 사용하는 것을 말한다. 주로 군이나 정부기관 등

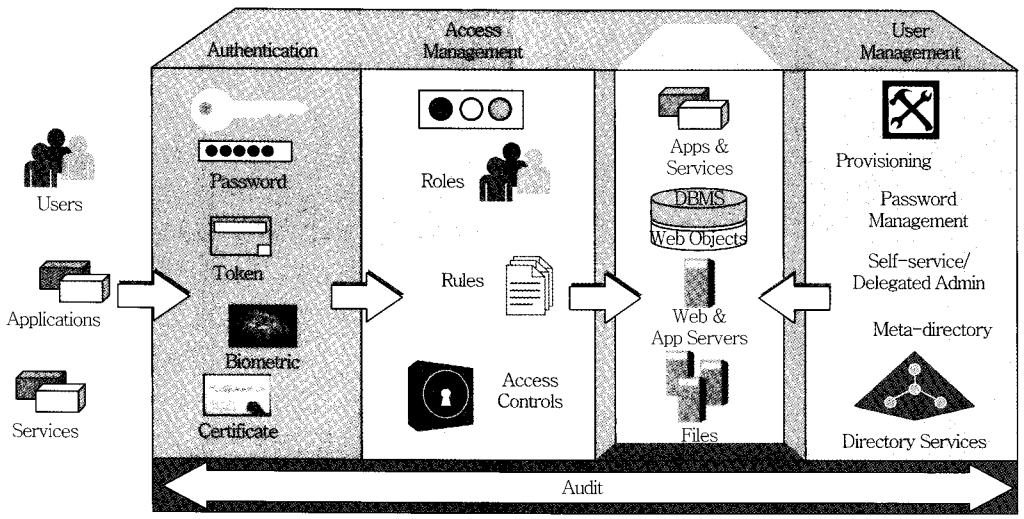
보안 정보를 다루는 기관에서 사용한다. RBAC은 사용자의 조직상에서의 역할을 기반으로 접근권한을 특정사용자가 아닌 해당 역할을 가진 사용자 그룹에게 부여하는 방식이다. 상업적인 조직에 잘 맞아 널리 사용되고 있다.

사용자 인증을 위해 사용되는 기술로 대표적인 것들은 아래와 같다.

- Id, password: 대표적 인증수단으로 암기만으로 사용할 수 있지만, 일정 수준 이상의 복잡성과 주기적 갱신만이 보안성을 담보할 수 있다.
- PKI: 공개키 암호기법을 이용한 인증 수단으로 사전에 공유된 비밀 정보가 없이도 인증서에 기반해서 상대방을 인증할 수 있다.
- Multi-factor 인증: 보안강도를 높이기 위해 몇 가지 인증 수단을 조합해서 사용하는 기법이다. Id, password 이외에 지문, 홍채 등과 같은 생체인식, 인증서, OTP 등이 사용된다.
- SSO: 한 곳에서 인증 후 인증확인 정보의 전달을 통해 다른 곳은 인증 절차 없이 통과하는 것으로 인증확인정보(assertion)의 대표적 표준은 SAML이 있다.
- i-PIN: 현재 한국에서 인터넷 이용시 본인확인을 위해 사용되는 기술로, 직접 본인확인을 수행한 기관에서 확인정보를 발급해주는 방식으로 동작한다.

네트워크 상에서의 사용자 인증은 다음의 4가지 형태로 발전되어 왔다.

- 통합 인증서버: Microsoft .Net Passport(LiveID) 서비스가 대표적으로, 전세계에 하나의 인증서버를 두고 여기에 등록해서 id를 만든 뒤 그 id를 이용해서 passport 서비스에 가맹한 사이트를 모두 이용하는 방식이다.
- ID 연계 기반: ETRI의 EIDMS가 대표적으로, 인증대행 및 사용자 정보를 제공하는 IDP가 있고, IDP와 ID 연계를 통해 인터넷 ID 서비스를 이용하는 가맹 웹사이트인 SP에 SSO를 이용할 수도 있고, IDP나 타 SP에 저장된 사용자 정보를 서로 교환하는 방식이다.
- url 기반: OpenID가 대표적으로 누구나 인증서비스 제공자가 될 수 있고 인증서비스제공자를 찾기 위해 id에 url을 붙여서 id를 만든다. 웹사이트에 방문해서 url이 포함된 id를 입력하면, 웹사이트는 url을 이용, 해당 인증서비스 제공자를 찾아가서 인증확인을 요청한다.
- User-centric: Microsoft Cardspace Client 기반 솔루션은 웹사이트에 등록된 id와 password



<자료>: Burton Group, 2006.

(그림 4) Enterprise IAM 구조

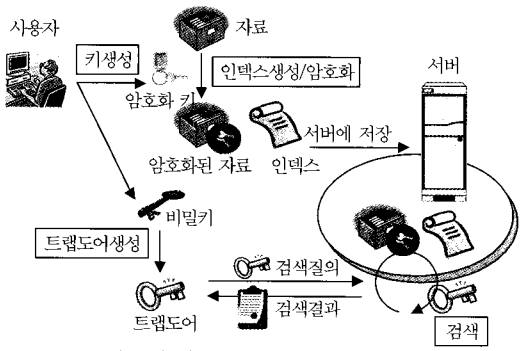
를 클라이언트마다 저장해 두고 로그인시 자동 입력해주는 방식으로 로그인 및 패스워드 관리 문제를 해결하고, 개인정보도 저장해 두었다가 자동 입력한다.

기업 환경의 사용자 인증 및 접근제어는 Enterprise IAM 기술로 패키지화 되어 있다. (그림 4)는 IAM의 구조를 보여준다.

2. 스토리지

스토리지에 대한 대표적인 보안 기술로 '검색 가능 암호시스템'과 'PPDM' 기술을 들 수 있다.

검색 가능 암호 시스템은 기존의 암호 기술과 같이 암호화된 정보에 대한 기밀성을 보장하면서 동시에 특정 키워드를 포함하는 정보를 검색할 수 있도록 고안된 암호 기술이다[4]. 이를 위해서 (그림 5)에서처럼, 검색 가능 암호 시스템에서는 암호화된 데이터 외에 검색에 사용할 인덱스(index)를 추가로 생성하여 저장한다. 사용자가 특정 키워드를 포함하는 자료를 검색하고자 할 때는, 키워드와 비밀키를 사용하여 키워드의 정보를 포함한 트랩도어(trapdoor)를 생성한다. 서버는 사용자가 전해준 트랩도어와 저장된 인덱스를 이용하여 검색을 수행하여 검색의 결과를 사용자에 전달한다. 이 과정에서 인덱스와 트랩도어로부터 저장된 자료 또는 사용자가 검색한 키워드에 대한 정보의 유출을 최소화하는 것이 검색 가능 암호 시스템의 기본 요구조건으로 볼 수 있다. 기본적인 검색 이외에도 범위 검색, 결합 키워드 검색 등의

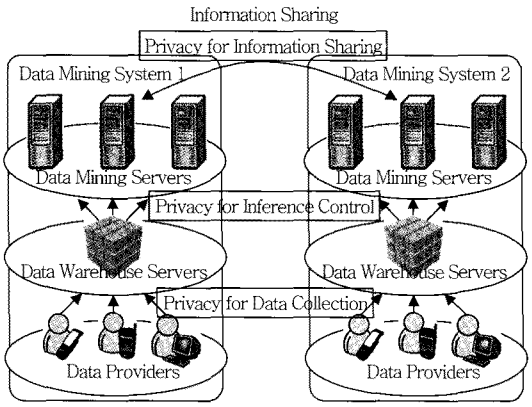


(그림 5) 검색 가능 암호시스템

다양한 검색 기능을 제공하는 검색 가능 암호 시스템도 존재한다.

암호화 단계에서 키를 생성한 사용자만 자료를 암호화할 수 있는 시스템을 대칭키 기반 검색 가능 암호 시스템이라 부르고 공개키 방식의 암호 시스템을 이용하여 사용자 이외의 다른 제공자가 암호문 및 인덱스를 생성할 수 있는 시스템을 공개키 기반 검색 가능 암호 시스템이라 부른다. 공개키 기반 검색 가능 암호 시스템은 공개키 암호 시스템을 바탕으로 설계된 검색 가능 암호 시스템으로 높은 안전성, 특히 증명 가능한 안전성을 제공하며, 공개키 암호 시스템의 특성을 활용하여 다양한 검색 기능을 제공할 수 있다. 하지만, 많은 공개키 기반 연산을 사용하여 효율적이지 못하다. 반면, 대칭키 기반 검색 가능 암호 시스템은 높은 효율성을 지니고 있어 대용량의 자료에 적용하기 용이하다. 이외에도, 암호학에 기반하지 않은 방법을 사용하여 더 낮은 안전성을 제공하는 대신 효율성을 극대화 하고 기존 데이터베이스와의 연계성을 높인 검색 가능 암호 시스템도 제안되고 있다.

데이터 마이닝(data mining)은 많은 양의 데이터에 함축적으로 들어 있는 지식이나 패턴을 찾아내는 기술이다[5]. 데이터 마이닝은 1983년 IBM Almaden 연구소를 중심으로 Quest 데이터 마이닝 프로젝트가 시작된 이후로 활발하게 연구가 진행되고 있다. 데이터를 모으고 이를 여러 가지 방법으로 분석하는 과정에서 프라이버시와 관련된 문제는 자연스럽게 대두된다. 특히, 데이터 마이닝이 전자상거래나 마케팅과 같은 분야에 주로 활용되면서, 개인 프라이버시 침해 이외에도 경쟁 회사들 사이에 이윤 추구를 위해 협력하는 경우 개별 회사가 수집한 정보의 노출이 문제시 되었다. 데이터 소유자의 프라이버시를 침해하지 않으면서 유용한 정보를 추출해 내는 것은 정보를 공유하는 것과 프라이버시를 유지하고자 하는 것의 취사선택(trade-off)에 대한 문제로 볼 수 있으며, 이를 해결하고자 프라이버시 보존형 데이터 마이닝(PPDM)에 대한 연구가 시작되었다. (그림 6)은 PPDM 시스템의 구조를 보여준다.



(그림 6) PPDM 시스템 구조

PPDM 관련 연구는 크게 두 가지로 대별된다. 먼저 우리가 일반적으로 실용적인 프라이버시 보존형 데이터 마이닝이라 일컫는 방법으로, 원래의 데이터에 노이즈를 더해주거나 다른 종류의 랜덤화를 적용시키는 것이다. 이 방법은 실용적으로 다양한 통계적 데이터를 위해서 널리 사용되었으나, 높은 안전성을 요하는 응용에는 적절하지 못하다. 두번째 방법은 데이터 마이닝에 SMC 기술이 적용된 것으로, 이 경우의 모든 개체는 자신의 입력과 계산 결과 이외에는 어떠한 정보도 얻을 수 없다. SMC를 사용한 PPDM은 데이터 변형이 전혀 없는 것으로 가정되기 때문에 데이터 송신 전 단계에서 데이터를 변형시키는 첫번째 방법에서 발생할 수 있는 정확성 문제는 발생하지 않는다. 그러나 SMC 기반 PPDM 기술은 계산 효율성이 매우 낮기 때문에 아직까지 실용적이지 못하다는 한계를 지닌다.

현재 상용 데이터 마이닝 소프트웨어에서 제공되는 알고리듬 중에서 최근 개발된 중요한 기술로는 연관 규칙(association rules), 분류(classification), 순차 패턴(sequential patterns), 군집화(clustering) 등이 있다. 각각에 대해 간략히 살펴보면 다음과 같다.

연관 규칙은 데이터 마이닝을 소개할 때 대표적으로 언급되는 기술로서 여러 데이터 사이의 연관성을 찾아내는 것이다. 일례로 미국의 대형 편의점에 연관 규칙 기술을 적용한 결과 일회용 기저귀를 사는 사람은 맥주도 같이 산다는 연관 규칙을 발견한 것을 들 수 있다.

분류는 주어진 데이터와 각각의 데이터에 대한 클래스가 주어진 경우, 그것을 이용하여 각각의 클래스를 갖는 데이터들은 어떤 특징이 있는지 분류 모델을 만들고, 새로운 데이터가 있을 때, 그 데이터가 어느 클래스에 속하는지를 예측하는 것을 의미한다.

연관 규칙은 물건을 한 번에 살 때 같이 구매한 것들을 이용해 규칙을 찾는 것인 반면, 순차 패턴 발견은 순서대로 일어난 데이터를 분석해 빈도수가 높은 순차 패턴을 찾아내는 기술을 말한다.

군집화 기술은 주어진 데이터를 몇몇 그룹으로 나누는 것을 말한다. 분류와 다른 점은 각 클래스에 해당되는 정보가 제공되지 않고 단지 데이터들 사이의 유사성만을 바탕으로 여러 그룹으로 나눈다는 점이다.

3. 네트워크

네트워크 보안 기술은 인터넷의 발전과 함께 해왔다. 대표적인 기술로 통신상의 기밀성을 보장하는 SSL과 IPsec 기술, 그리고 네트워크를 통한 공격을 차단하는 application firewall과 DDoS 방지 기술을 들 수 있다.

• SSL

네트워크 계층에서 보안성을 제공해 주는 IPsec이 만들어지기 전에 사용하던 것으로, Internet Protocol 위에서 인증서에 의한 상대방 인증, 기밀성과 무결성을 제공한다. SSL은 표준화되기 이전의 이름으로, 표준화된 명칭은 TLS[6]이다. 오랫동안 사용된 관계로 인터넷 브라우저 등을 비롯하여 널리 채용되고 있다. 웹에 기반한 작업이 많아지면서 전용 하드웨어 가속 장비도 개발되어 사용되고 있다.

• IPsec

네트워크 계층인 Internet Protocol에서 보안성을 제공해 주는 표준화된 기술이다[7]. 상대방 인증, 기밀성, 무결성 등을 제공한다. IPv4에서는 옵션으로, IPv6에서는 필수로 제공하도록 되어 있다.

• Application Firewall

기존 firewall이 IP 주소와 port 번호를 기반으로 통신의 허용과 금지를 설정했으나, 허용된 주소와 port 번호를 통한 공격에는 효과적이지 않아 응용계층의 메시지까지 분석하여 공격을 차단하는 것을 application firewall이라 한다. 웹 서버 보호를 위한 web firewall과 DBMS 보호를 위한 DB firewall이 많이 사용된다.

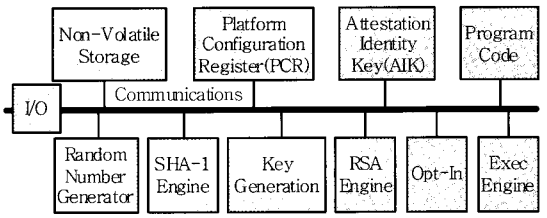
• DDoS 방지

프로토콜 상의 약점이나 구현상의 허점을 이용하여 서버를 서비스 불능상태로 만드는 서비스거부공격(DDoS)에 대한 방어기술이다. Scanning 방지, 흔하지 않은 option 사용, 정상범위를 벗어난 폭주 패킷의 차단 기술이 사용된다. 고속 처리가 필요하여 전용장비로 개발되어 사용되고 있다.

4. 단말

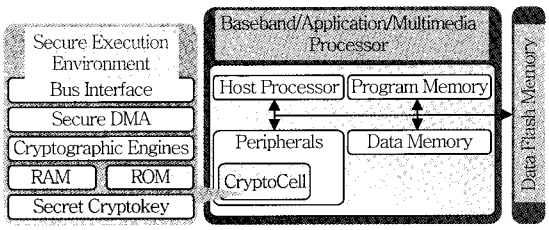
단말 보안 기술들은 대부분 암호학적 이론에 근거한 알고리듬 및 프로토콜 기반으로 동작되기 때문에 단말 인식 및 인증 기법, 암호학적 프리미티브에 대한 안전성 보장 기법 등에 관한 연구 방향으로 꾸준히 진행되고 있다. 이중에서 하드웨어를 이용하여 암호학적 프리미티브를 물리적으로 보호하는 기술들은 현재까지 가장 안전한 기술로 여겨지고 있다. 여기에 해당되는 대표적인 상용 기술로는 TCG의 TPM[8], Discretix의 CryptoCell[9], SafeNet의 SafeXcel IP-Trusted Module[10] 기술 등이 있다.

TPM은 TCG의 신뢰 플랫폼(trusted platform)을 구현하기 위한 핵심 기술로서 디바이스에 대한 식별 및 신용 정보를 별도의 하드웨어 모듈로 관리한다. TPM 내부에는 키 생성, 암호 엔진, 해시 함수, 난수 생성기 등을 포함하고 있으며 물리적인 보호장치를 통해 외부로부터의 조작을 방지한다. 특히 TPM에 저장된 키는 외부로 노출되지 않기 때문에 디바이스 인증 및 디스크 암호화 등의 응용 분야에 사용되고 있다. (그림 7)은 TPM의 구조를 보여준다.



<자료>: TCG Specification Architecture Overview Revision 1.2

(그림 7) TPM Component 구조



<자료>: http://www.discretix.com

(그림 8) CryptoCell의 구조

CryptoCell은 Discretix사의 모바일 단말 보안용 칩셋 기술로서 TCG의 TPM과 유사한 형태의 기능을 제공한다. 특히 CryptoCell은 모바일 단말 환경을 고려해서 성능, 전력 소비, 칩 공간 등의 민감한 조건들을 개선시켰으며 부채널 공격을 방지하기 위한 Attack-Resistant Cryptographic Core 기술도 탑재하고 있다. 대표적인 응용 분야는 Mobile TV, FOTA, VPN 등이 있다. (그림 8)은 CryptoCell의 구조를 보여준다.

SafeXcel IP-Trusted Module은 단말의 안전한 실행 환경(trusted execution environment)을 위한 SafeNet사의 Silicon IP 솔루션으로서 신뢰 모듈(trusted module) 내부에 하드웨어 가속기와 로컬 메모리를 탑재하여 보안 기능 추가로 제기되던 성능상의 문제점을 극복하고 있다. 이 기술은 라이선스를 통해 TI, AMD, ARM 등의 다양한 벤더에서 출시되는 칩에 적용되고 있다.

최근 단말 보안에서는 외부로부터의 공격을 원천적으로 막기 위한 방어 기술뿐만 아니라, 사후 관리(risk management) 차원에서의 단말 보안 기술이 활발히 진행되고 있다. 이중에서 가상화와 재생화를 이용한 보안 기술에 대해서 살펴보면 다음과 같다.

• Virtualization Security

현재 가장 많이 사용되는 단말인 이동 통신 단말에서 가장 큰 위협 중 하나는 서비스 중단 및 불법 사용이다. 우리나라의 경우 폐쇄적인 단말 환경으로 인해 웜이나 바이러스와 같은 악성 코드에 의한 피해 사례가 보고되지는 않았지만, 실제로 유럽에서는 몇몇 바이러스와 그의 변종들이 보고되고 있다. 이와 같은 이동 통신 단말에서 기존의 보안 기술인 방화벽과 백신을 이용하는 것뿐만 아니라 악의적인 공격에 노출되더라도 통신 서비스를 안전하게 유지하기 위한 것은 방어 못지 않게 매우 중요한 문제로 부각되고 있다. 최근 제안된 가상화 기술들은 통신 서비스와 사용자 개인 서비스를 서로 다른 도메인으로 분리시켜 공격에 쉽게 노출되는 사용자 개인 서비스로부터 통신 서비스를 격리하는 역할을 수행한다.

• Renewable Security

최근 IPTV 셋톱박스를 포함하는 많은 단말들이 인터넷 또는 이동통신 망을 이용하여 사업자의 서버와 온라인 상태를 유지할 수 있는 인프라를 구축하고 있다. 과거 콘텐츠 또는 서비스를 일방적으로 제공받는 단방향 통신에서 상호 작용이 가능한 양방향 통신 환경으로의 변화는 단말 보안에 대한 새로운 접근방향을 제시하고 있다. 이러한 양방향 통신을 통해 원격에서 단말에 대한 무결성을 검증하거나 최근 발견된 위협에 대응할 수 있는 보안 업데이트를 수행함으로써 단말의 보안성을 높이는 서비스가 최근 제안되고 있다.

Ⅳ. 클라우드 컴퓨팅 보안 사례

클라우드 컴퓨팅 보안 사례로 AWS의 보안 기능을 알아보면 다음과 같다[11].

• Certifications and Accreditations

법률이나 규정 또는 규격에 부합함을 인정받는 것으로, AWS에서는 미국의 회계관련법인 SOX와 기업 내부 제어에 대한 인증인 SAS70 Type II 그리고 의료관련 법률인 HIPPA 지원을 목표로 하고 있다.

• Physical Security

시설물 보호를 위하여 경비원, CCTV 및 침입감지 시스템을 두고 있으며, 모든 직원은 데이터 센터에 들어갈 때까지 세 번 이상의 two-factor 인증을 거친다.

• Backups

S3와 SimpleDB 그리고 elastic block store의 모든 데이터는 복수 개의 원격지에 중복 저장하고 있으며, 따로 backup을 수행하지는 않는다.

• EC2 Security

EC2 instance로의 접근은 SSH에 의하여 보호하며, 네트워크 접속은 firewall을 이용하여 통제하고 있다. Instance의 생성 및 제거와 firewall 설정 변경 등 주요한 EC2 API 호출은 X.509 인증서나 Amazon Secret Access Key에 의하여 서명된 것만 처리된다. Instance들은 Xen hypervisor를 이용하여 격리하고 있다. EC2의 네트워크 보안 기능으로 syn cookie, connection limiting, bandwidth limitation 등에 의한 DDoS 공격 방지, SSL 사용에 의한 MITM 공격 방지, firewall에 의한 IP spoofing 방지와 port scanning 방지 등이 있다.

• S3 Security

S3의 모든 데이터는 bucket 또는 object별로 access control list에 의하여 접근이 통제된다. 외부로의 데이터 이동 시에는 SSL을 사용하여 데이터를 보호한다. S3에 데이터를 저장할 때 자동으로 암호화해서 저장하지는 않는다. S3에서 데이터를 삭제하면, 해당 영역은 다시 덮어쓸 때까지 write operation으로만 접근 가능하다.

• SimpleDB Security

SimpleDB는 AWS의 계정 ID별로 접근이 통제되는 access control list를 가지고 있다. 외부와의 통신 시에는 SSL을 이용하여 데이터를 보호한다. SimpleDB에 데이터를 저장할 때는 자동으로 암호

화를 수행하지는 않는다. 사용자가 암호화해서 저장할 수는 있지만, 이런 경우 query의 조건으로는 사용할 수 없다. SimpleDB에서 데이터를 삭제하면, 해당 영역은 다시 덮어쓸 때까지 write operation으로만 접근 가능하다.

● 용 어 해 설 ●

클라우드 컴퓨팅: 인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅. 주요한 특징으로는 IT 자원(SW, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼의 비용을 지불하는 것을 들 수 있다.

컴플라이언스: 외부 규제나 표준을 정의하고 지속적인 관찰을 통해 준수여부를 확인하며, 발견된 문제를 개선하고 발전시켜 나가는 활동

약어 정리

API	Application Programming Interface
AWS	Amazon Web Service
CCTV	Closed Circuit Television
CPU	Central Processing Unit
DAC	Discretionary Access Control
DB	Database
DBMS	Database Management System
DDoS	Distributed Denial of Service
EC2	Elastic Compute Cloud 2
EIDMS	ETRI ID Managemant System
FOTA	Firmware Over The Air
HIPPA	Health Insurance Portability and Accountability Act
HW	Hardware
IaaS	Infrastructure as a Service
IAM	Identity & Access Management
IDP	ID Provider
IPsec	Internet Protocol Security
IPTV	Internet Protocol Television
IT	Information Technology
MAC	Mandatory Access Control
MITM	Man In The Middle
OTP	One Time Password
PaaS	Platform as a Service
PKI	Public Key Infrastructure
PPDM	Privacy Preserving Data Mining
RBAC	Role Based Access Control
S3	Simple Storage Service
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAS	Statement on Auditing Standard
SMC	Secure Multi-parity Computation
SOX	Sarbanes Oxley
SP	Service Provider
SSH	Secure Shell
SSL	Secure Socket Layer
SW	Software
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module
VPN	Virtual Private Network

참 고 문 헌

[1] 김명준, "Korea's Cloud Computing Strategy," 2009년도 IT21 글로벌 컨퍼런스, 2009. 5.

[2] 정제호, "클라우드 컴퓨팅의 현재와 미래, 그리고 시장 전략," 한국소프트웨어진흥원, 2008. 10.

[3] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, Apr. 2009.

[4] 검색 가능 암호 시스템 기술 연구, 기술백서, 한국전자통신연구원, 2008.

[5] 프라이버시 보존형 데이터 마이닝 기술 연구, 기술 백서, 한국전자통신연구원, 2008.

[6] T. Dierks, RFC5246 Transport Layer Security(TLS) Protocol Version 1.2, IETF, Aug. 2008.

[7] S. Kent et al., "RFC4301 Security Architecture for the Internet Protocol," IETF, Dec. 2005.

[8] http://www.trustedcomputinggroup.org

[9] http://www.discretix.com

[10] http://www.safenet-inc.com

[11] Amazon Web Services: Overview of Security Processes, Amazon, Sep. 2008.