클라우드 컴퓨팅 보안 프레임워크 연구

박준영*, 나상호*, 허의남*
*경희대학교 컴퓨터공학과
e-mail : { jypark | shna }@icns.khu.ac.kr, johnhuh@khu.ac.kr

A Study on Security Framework for Cloud Computing

Jun-Young Park*, Sang-Ho Na*, Eui-Nam Huh*
*Dept. of Computer Engineering, Kyung Hee University

요 약

클라우드 컴퓨팅 서비스는 새로운 컴퓨팅 기술의 패러다임으로 주목 받으면서 단기간에 많은 발전을 이루고 있다. 하지만 상업적인 목적으로 클라우드 컴퓨팅 서비스 제공을 위한 연구가 비약적으로 이루어지면서 각 서비스 영역에서 필요한 데이터 보호와 개인 정보 보호, 서비스 관리, 보안 정책 등의 선결되어야 하는 보안 기술이 많이 뒤쳐져 있는 실정이다. 그러므로 클라우드 컴퓨팅의 연구현황과 보안위협 분석, 그에 따른 요구사항을 분석하고 이를 바탕으로 클라우드 컴퓨팅 서비스의 참조 모델을 제안한다. 또한 클라우드 컴퓨팅 서비스의 위협분석을 통해 사용자 편의성, 클라우드 간 (Inter Cloud) 확장성, 가상 자원 연동이 가능한 보안 프레임워크를 제안하고자 한다.

1. 서론

클라우드 컴퓨팅 서비스가 주목 받으면서 구글, 아마존, 애플, 마이크로소프트와 같은 국외 IT 대기업이 클라우드 컴퓨팅 서비스를 선보이며 클라우드 컴퓨팅 시대를 열어가고 있다. 국내기업도 클라우드 컴퓨팅 연구를 위한 클라우드 센터건립과 클라우드 컴퓨팅 네트워크 구축 및 개인 사용자 서비스 제공 등 국내에서도 클라우드 컴퓨팅 연구 및 서비스를 준비 중에 있다. 클라우드 컴퓨팅 서비스는 Public Cloud 와 Private Cloud 등 4 가지의 클라우드 컴퓨팅 서비스 타입으로 발전하고 있으며, 최근 Public Cloud 와 Private Cloud 의 서비스 타입을 결합한 Personal Cloud Computing 서비스를 제공과 함께 서비스 확장이 진행 중이다[2].

클라우드 컴퓨팅의 발전하면서 클라우드 컴퓨팅의 신뢰성, 보안성, 법적 문제, 개인정보보호 문제, 표준화 등 제반 문제에 대한 우려의 목소리도 높다[5].

이와 같은 해결되지 않은 보안 문제가 있음에도 불구하고 서비스를 제공중인 몇몇의 기업에도 뚜렷한 보안 정책이나 보안 프레임워크, 정보 유출에 대한 대책이 없어 클라우드 발전에 악영향을 끼칠 우려가 있다.

본 논문에서는 2 장에서 클라우드 연구현황, 클라우드 컴퓨팅 보안 위협과 그에 따른 요구사항 및 대책, 클라우드 컴퓨팅의 참조 모델과 보안 프레임워크에 대해 알아본다. 클라우드 컴퓨팅 서비스 구조와 향상된 보안 프레임워크를 3 장에서 제안하고, 4 장 결론을 통해 본 논문의 요약과 향후 연구 방향을 제시한다.

2. 관련 연구

2.1 클라우드 컴퓨팅 연구현황

국내· 외에서 클라우드 컴퓨팅이 차세대 컴퓨팅으로 주목 받으면서 글로벌 IT 기업들과 연구기관에서 많은 연구와 표준화가 활발히 진행 중이다. 국내외 기관과 기업들이 진행 중인 클라우드 관련 연구는 다음과 같다.

- NIST (National Institute of Standards and Technology)[2]
  클라우드 컴퓨팅에 대한 5 가지 특징, 3 가지 배포 모델, 4 가지의 서비스 타입 정의
- CSA (Cloud Security Alliance)[13]
  클라우드 컴퓨팅 보안을 위해 13 가지의 보안 도메인 정의
- Cloud Computing Use Case Discussion Group[4]
  클라우드 컴퓨팅 서비스에 대한 Taxonomy 와 서비스 사용 시나리오, 보안시나리오 등 클라우드 컴퓨팅 서비스의 정의와 시나리오 제시
- ENSIA (European Network and Information Security Agency)[3]
  사용자의 클라우드 서비스 이용 가이드라인과 보안 위협 경고
- Euro Cloud[6]
  2010 년까지 유럽 25 개국 참여를 목표로 클라우드 컴퓨팅에 대한 회의 개최(2010. 6. 28)
- CompTIA[7], Intel[8]
  클라우드 컴퓨팅 서비스에 대한 Taxonomy 정의
- IBM[9], Red Hat[10]
  IaaS 제공을 목표로 각 Blue Cloud, Delta Cloud 를 구축 사업 진행

2.2 클라우드 컴퓨팅 보안 위협

클라우드 컴퓨팅 환경과 서비스 구조에 대한 연구가 활발히 진행 중인 가운데 클라우드 보안 연구기관인 CSA (Cloud Security Alliance)는 보안 위협[12]을 다음과 같이 7 가지로 나누어 분석하였다.

- 위협 1: 클라우드 컴퓨팅의 오용과 비도덕적인 사용(Abuse and Nefarious Use of Cloud Computing)
- 위협 2: 불안전한 인터페이스와 응용 프로그래밍 인터페이스 (Insecure Interfaces and APIs)
- 위협 3: 악의적인 내부자 (Malicious Insiders)
- 위협 4: 기술 공유 문제 (Shared Technology Issues)
- 위협 5: 데이터 유실 또는 유출 (Data Loss or Leakage)
- 위협 6: 계정 또는 서비스 하이잭킹 (Account or Service Hijacking)
- 위협 7: 알려지지 않은 위협 프로파일 (Unknown Risk Profile)

2.3 클라우드 컴퓨팅의 보안위협에 대한 요구사항과 보안 대책

CSA 에서는 앞서 제시한 보안위협에 대한 정의와 함께 각각의 위협에 대한 보안 요구사항과 대책[12]을 분석하였다. 그 세부 내용은 다음과 같다.

- **플랫폼 접근 제어 (위협 1)**
  엄격한 초기 등록 및 절차 확인, 강화된 신용카드 사기 감시 및 조정, 고객 네트워크 트래픽의 종합적인 자가진단
  - **관련 기술 :** SAML[18], X.509[15]
- **응용 프로그램 (위협 2)**
  클라우드 서비스 제공자 인터페이스의 보안 모델 분석, 강력한 인증과 접근제어의 보장을 통한 암호화 전송, 응용프로그램 인터페이스 간의 종속성 이해
- **리소스 및 서비스 통합 (위협 3)**
  엄격한 공급망 관리와 광범위한 공급업체 평가를 실시, 인적자원 요구사항에 법적 계약사항 적용, 모든 정보보안과 관리 규정에 대한 규정 준수, 보안 위반 통지 프로세스 적용
- **서비스 인프라 관리 (위협 4)**
  설치와 구성에 대한 보안 최고 방법 구현, 비인가된 수정 및 활동에 대한 감시 환경 구축, 강력한 인증과 접근제어를 권장, 취약점 대책을 위한 서비스 수준 관리 시행, 취약점 분석과 감사 구성을 수행
- **사용자 데이터 관리 (위협 5)**
  강력한 API 접근제어 구축, 데이터 전송시 데이터의 암호화와 데이터 무결성 고려, 데이터 구조 설계에서부터 실행까지 데이터 보호를 고려, 강력한 키생성, 저장, 관리 구현과 키 소멸 사례 분석, 데이터 백업과 유지 관리 명세
  - **관련 기술:** KMIP[14]
- **서비스 접근 제어 (위협 6)**
  사용자와 서비스간의 계정 증명서 공유를 금지, 강력한 다중요소 인증기술을 가능한 적용, 직원을 고용하여 허가되지 않은 활동을 감시, 클라우드 제공자 보안 정책과 서비스 수준관리(Service Level Agreement) 를 이해
  - **관련 기술:** SAML, XACML[16], SPML[17], X.509, KMIP
- **리소스 모니터링 및 감사 (위협 7)**
  적용 가능한 로그와 데이터 공개, 인프라 세부 정보를 부분적 또는 전부 공개, 중요 정보에 대한 감시 및 경보

2.4 클라우드 컴퓨팅 참조 모델

국제표준화 기관인 ITU-T (Focus Group, FG) 에서도 클라우드 컴퓨팅 서비스에 대한 표준화가 진행되고 있다. 클라우드 컴퓨팅 서비스를 위한 "*Functional Requirements and Reference Architecture*"[11] 표준화가 아래 제시된 3 가지 도메인을 중심으로 진행 중에 있다. 3 가지 도메인은 클라우드 컴퓨팅 서비스에 대한 FG 의 시각과 그에 필요한 요구사항이 잘 반영되어 있다.

- **End User Request and Access**
  최종 사용자들의 활용 용도에 맞는 서비스 품질과 보안 수준을 관리하며 클라우드 서비스 제공자와의 서비스 연결에 필요한 서비스를 포함
- **Provider Cloud Orchestration**
  기존의 IaaS, PaaS, SaaS 뿐만 아니라 서비스 제공자들간의 서비스 연동을 통한 다양한 서비스 모델 및 유스케이스 (Use-Case)를 제공
- **Virtualized Resource Management**
  IaaS, PaaS, SaaS 와 같이 자원을 가상화하여 서비스 제공에 제한이 없도록 관리와 각 서비스를 사용자 임의로 이용이 가능하도록 제공

End User Request and Access 는 사용자 입장에서 인트라넷과 같은 안전하고 편리한 환경 제공을 위함이며, Provider Cloud Orchestration 을 통해 현재까지 알려진 서비스 모델 그 이상의 서비스 간 연동(Inter Cloud)을 고려하고 있다. 또한 서비스 제공자에 구애받지 않을 수 있는 서비스 간 자원 연동을 위하여 Virtualized Resource Management 를 제시하였다.

2.5 클라우드 보안 프레임워크

클라우드를 위한 보안 기법은 현재 국내외 연구 기관(NIST, CSA, ENSIA 등)을 통해 가이드라인이 제시되고 있다. 최근 연구 발표된 [1]에서 제안된 클라우드 보안 프레임워크는 다음과 같은 요구사항 분석을 토대로 제안되었다.

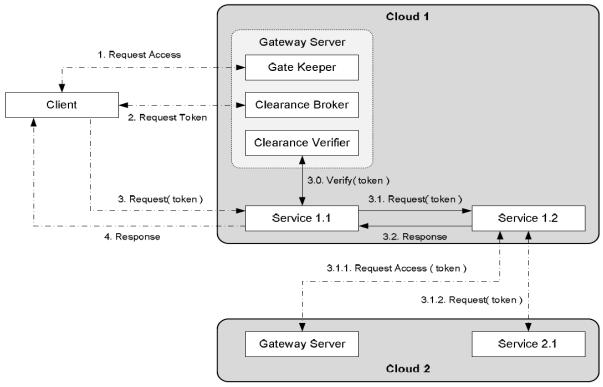
- IaaS 부터 SaaS 까지 모두 서비스형태로 제공
- 사용자는 정해진 모델에서만 제공됨
- 사용자와 서비스에 대한 접근 권한 설정 가능
- 다수 서비스 이용에 Single Sign-On 사용가능
- 서로 다른 클라우드 서버에서도 인증 가능
- 통신간에는 암호화 필요

다음 (그림 1)은 제안된 보안 프레임워크로 크게 3 개의 컴포넌트(Client, Gateway Server, Service)로 구성이 되어있으며, SSAT(Single Sign-on Access Token)를 이용하여 사용자 인증을 한다.

- **Client :** 사용자는 Client 를 통해 클라우드 서버에 접속이 가능
- **Gateway Server :** Gate Keeper, Clearance Broker,

Clearance Verifier 로 구성되어 있으며, 각각 Gateway Server 의 보안, 사용자 인증 절차 제공

- **Service :** 클라우드에서 IaaS 부터 SaaS 까지 모든 클라우드 컴퓨팅 서비스에서 제공하는 서비스



(그림 1) 클라우드 컴퓨팅 보안 프레임워크[1]

(그림 1)의 보안프레임워크는 SSAT 를 이용하여 다른 클라우드 서버에서도 추가 Token 생성없이 기존의 Token 으로 인증을 받는 방법을 사용하므로 같은 클라우드 서비스 제공자에서는 추가 인증이 필요 없으므로 빠른 서비스 이용이 가능하지만 단일 클라우드 서비스 제공자에서만 사용이 가능하여 클라우드 간 (Inter Cloud) 서비스 연동, 확장에 어려움이 있다. FG 에서 언급한 클라우드 컴퓨팅 서비스 구조를 따르면 IaaS, PaaS, SaaS 등의 서비스는 사용자 임의대로 서비스를 선택이 가능하여야 한다. 단일 서비스 제공자가 아닌 각 서비스 유형별로 다양한 서비스 제공자를 선택 가능 하도록 설계하여야 한다.

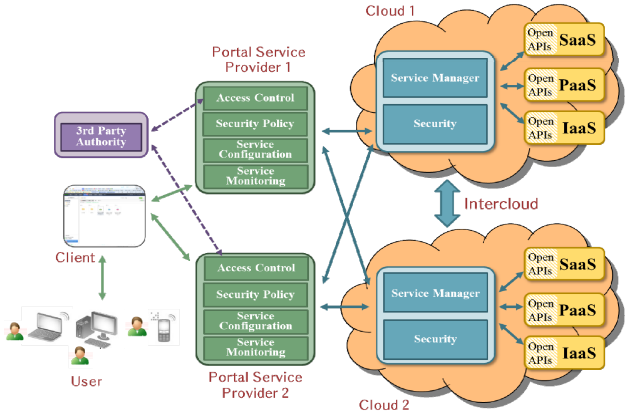
클라우드 보안 프레임워크는 앞서 2.2 에서 제시한 바와 같이 접근 제어뿐만 아니라 내부의 악의적인 공격자 및 다양한 서비스에서의 데이터 유출 및 감사 기능 등 다각도에서 보안이 고려되어야 한다. 그러나, 제안된 보안 프레임워크는 접근제어로 제한되어 있어 추가적인 보안 요소에 대한 고려가 필요하다.

3. 클라우드 컴퓨팅 보안 프레임워크

클라우드 컴퓨팅 보안 프레임워크를 제안하기 위해 본 논문에서는 확장(Inter Cloud) 가능한 클라우드 컴퓨팅의 서비스 모델을 제안한다. 이를 토대로 서비스에 필요한 보안 요구 사항(2.3, 2.4)을 반영하여 보안 프레임워크를 제안하고자 한다.

3.1 클라우드 컴퓨팅 서비스 모델

기존의 클라우드 컴퓨팅 구조는 사용자에게 VPN 을 활용한 Intranet 형 서비스로 일반 클라우드 컴퓨팅 서비스 모델에는 맞지 않다. 제안하는 (그림 2)의 클라우드 컴퓨팅 서비스 모델은 ITU-T Focus Group on Cloud Computing 에서 정의한 참조 모델의 요구사항을 반영하였다.



(그림 2) 클라우드 컴퓨팅 서비스 참조 모델

(그림 2)와 같이 사용자는 Client 를 이용하여 클라우드 컴퓨팅 서비스를 제공받을 수 있는데, 여러 서비스 제공자가 존재할 것이며, 제공자에 따라 서로 다른 서비스 제공과 서비스 정책이 존재할 것이다. 또한 제공자들간의 협력관계가 생성되어 제공자들간의 자원연동이 가능하고 사용자의 안정성과 편의성을 갖춘 컴퓨팅 환경이 제공될 수 있다. 이는 단일 클라우드 서비스 제공자에 종속되지 않고 클라우드 간 (Inter Cloud) 연동 및 확장을 통해 폭넓은 서비스를 제공을 위함이다. 이러한 요구사항들을 충족하기 위해서는 클라우드 컴퓨팅 서비스 제공자와 다양한 서비스를 제공받고 싶은 사용자간에 Portal Service 혹은 Portal Service Provider 가 존재하여 사용자가 원하는 서비스를 구성 및 제공한다. 서드파티(3rd Party) 인증으로 서로 다른 클라우드 서버의 서비스를 제한 없이 제공받을 수 있다.

또한, 클라우드 서버의 Service Manager 는 서버내의 서비스 관리 및 User Profile 에 따른 서비스를 관리한다. 클라우드 내 보안, 서비스 자원 감사 및 사용자 서비스 접근제어는 Security 컴포넌트에서 수행된다.

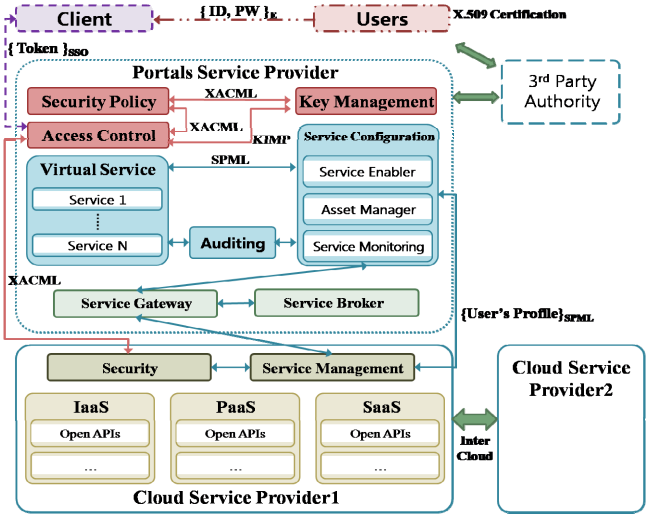
3.2 클라우드 컴퓨팅 보안 프레임워크 제안

본 논문에서 제안하는 보안 프레임워크는 FG 의 표준화 방향인 확장성, 사용자 편의성, 서비스 자원의 연동을 고려하여 설계되었다.

사용자 편의성을 위해 Portals Service Provider 는 3rd Party Authority 와 연동하여 SSAT(Single Sign-On Access Token) 제공한다. 사용자는 Service Provider 에 제한 없이 토큰을 이용하여 서비스를 제공받을 수 있다. 그리고 서로 다른 Cloud Service Provider 에서 각 서비스(IaaS, PaaS, SaaS)를 가져와 Service Configuration 에서 서비스를 결합하여 제공하며 서비스 제공시 서비스의 오류 및 관리를 위해 Service Monitoring 과 Auditing 을 수행한다. Cloud Service Provider 는 각 서비스(IaaS, PaaS, SaaS)에 대한 접근성 및 Cloud 간 연동(InterCloud)을 위하여 OpenAPIs (Iaas, SaaS, PaaS)를 제공하며 서비스의 확장성을 보장 받는다. Portal Service Provider 는 각 자원의 OpenAPIs 를 통해 유저 맞춤 Cloud Service Configuration (Service Configuration 컴포넌

트)를 제공하고, 서비스 관리를 위해 Service Management 와 Security 를 수행한다.

앞에서 언급한 보안 위협과 그에 따른 요구사항 및 대책을 참고로 X.509 Certification, KIMP, XACML, SAML, SPML 의 표준화 된 기술을 (그림 3)과 같이 적용한다. 세부 컴포넌트의 구성과 기능 이후 서브 섹션에서 자세히 다룬다.



(그림 3) 클라우드 컴퓨팅 보안 프레임워크

3.3 컴포넌트 정의 및 기능

3.3.1 Client

사용자는 클라이언트에 ID 와 PW 를 이용하여 접근이 가능하며 클라이언트와 Portals Service Provider 간의 사용자 인증은 {ID, PW}, {X.509 Certification} 등의 Multi-factor 를 이용하여 생성된 Token 으로 서비스 사용 요청을 한다.

3.3.2 Portals Service Provider

Portal Service Provider 는 사용자 인증 및 보안을 위한 Access Control, Security Policy, Key Management 로 구성된다. 각 컴포넌트 간 사용자 인증 정보 및 보안 정책 정보는 XACML, KIMP 를 이용한다.

Service Configuration 컴포넌트는 Service Gateway, Service Broker 간에 SPML 을 이용하여 User's Profile 을 공유하고 맞춤 서비스를 구성 및 제공한다.

Service Gateway 는 Service Configuration 과 Cloud Service Provider 간의 네트워크 자원 할당 및 클라우드 자원의 원활한 연동을 담당한다.

Service Broker 는 User Profile 의 사용자 서비스 정책 정보를 참고하여 사용자 데이터 및 서비스 생명 주기를 관리한다.

3.3.3 Cloud Service Provider

Cloud Service Provider 는 XACML 과 SPML 을 이용하여 Portals Service Provider 간의 User Profile 및 인증 정보를 공유한다. Service Management 컴포넌트는 클라우드 내 자원 및 할당을 수행하며, Security 컴포넌트를 통해 사용자 인증 및 클라우드 내 보안(암호화, 감사) 기능 등을 수행한다.

4. 결 론

클라우드 컴퓨팅 서비스의 상용화를 위해서는 무엇보다도 보안은 필수이다. 하지만 현재 많은 서비스가 제공되고 있지만 클라우드 컴퓨팅의 특징에 맞는 보안 기술과 보안 정책은 아직 미흡한 실정이다.

본 논문에서 클라우드 서비스 제공자 간 자유롭게 자원 및 서비스 연동 모델 제안을 통해 향후 Cloud Service 의 나아갈 방향을 고려하여 확장이 용이한 보안 프레임워크를 제안하였다. 이를 통해 단일 클라우드 서비스 및 서비스 제공자 종속을 해소하고 다양한 사용자 중심의 서비스 제공이 가능하다.

향후 연구에서는 클라우드 컴퓨팅 서비스를 이용하는 사용자의 다양한 환경에 따라 유연성을 지닌 보안 프레임워크에 관한 연구를 수행할 것이다.

Acknowledgment

본 연구는 한국산업기술평가관리원(KEIT)의 연구결과로 수행되었음(No. KI002153)

참고문헌

[1] Michael Brock and Andrzej Goscinski, "Toward a Framework for Cloud Security, Algorithms and Architectures for Parallel Processing"
[2] P.Mell and T.Grance, "The NIST Definition of Cloud Computing"
[3] European Network and Information Security Agency (ENISA) "Cloud Computing Risk Assessment : Benefi ts, risks and recommendations for information security"
[4] Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases White Paper"
[5] 박춘식, 김형종, 김명주, "클라우드 컴퓨팅 보안 동향"
[6] Euro Cloud, "http://www.eurocloud.org"
[7] CompTIA Cloud/SaaS Community, "Cloud Computing: The Call for Standardisation. The Need for Certification"
[8] Intel Information Technology, "Architecting Software as a Service for the Enterprise"
[9] IBM, "http://www-3.ibm.com/press/us/en/pressrelease/2613.wss
[10] Cloud Computing Forum, "RED HAT: UNLOCKING THE VALUE OF THE CLOUD"
[11] ITU-T Focus Group on Cloud Computing. "Draft deliverable on Functional Requirements and Reference Architecture"
[12] Cloud Security Alliance, "Top Threats To Cloud Computing V1.0"
[13] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1"
[14] OASIS, "Key Management Interoperability Protocol (KMIP)"
[15] ITU-T X.509, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks"
[16] OASIS, "eXtensible Access Control Markup Language"
[17] OASIS, "Service Provisioning Markup Language"
[18] OASIS, "SAML V2.0 Executive Overview"