클라우드 및 분산 컴퓨팅 환경에서의 보안 이슈

박상배*

I. 서론

최근 들어 대용량 분산 컴퓨팅 시스템인 계산 그리드 시스템이 대규모 계산을 필요로 하는 고에너지 물리, 바이오 분야 등에 널리 채택되고 있다. 그리드 시스템은 클라이언트-서버 환경과는 다른 형태로 가장 큰 차이점은 사용자와 기반 컴퓨팅 자원의 크기가 매우 방대하다는 것을 꼽을 수 있다. 그리드 시스템은 전세계에 거쳐 널리 분포된 많은 사이트들의 컴퓨팅 자원을 공유하는 것이다. 이제 여러 실생활에서도 접할 수 있는 클라우드 컴퓨팅은 컴퓨팅 자원을 원하는 장소에서 원하는 양만큼 사용할 수 있는 유틸리티 컴퓨팅의 실현으로 여겨지고 있으며, 이를 통해 컴퓨팅 인프라 도입, 운영, 관리 비용의 절감과 책임에서 벗어나 핵심적인 부분에 집중할 수 있을 것을 기대하고 있다. 다음 그림은 NIST에서 정의한 클라우드 컴퓨팅 모델이다.

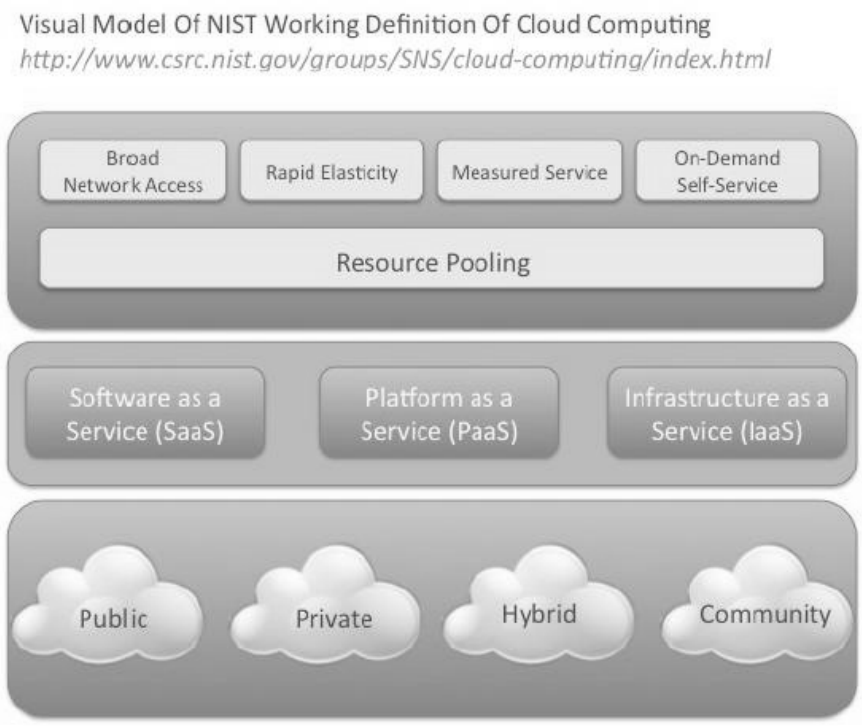

Figure 1 - NIST Visual Model of Cloud Computing Definition

(그림 1) NIST의 클라우드 컴퓨팅 정의

한편 정보의 저장과 정보 시스템의 운영이 아웃소싱되는 상황에서 적절한 정보보호 이루어지지 않거나 정보의 유출과 정보시스템에 대한 직접적인 제어권을 보장과 같은 새로운 보안관련 의문도 생겨나고 있다.

* 박상배, 한국과학기술정보연구원 책임연구원, plucky@kisti.re.kr

본 논문에서는 컴퓨팅 환경의 변화에 따른 새로운 보안 이슈들을 소개하고 그에 대한 대응방안에 대하여 알아본다. 2장에서는 클라우드 및 분산 컴퓨팅 환경에서의 보안 이슈들에 대해 알아보고, 3장에서는 그에 대비하기 위한 방안과 접근 방식에 대하여 소개한다.

Ⅱ. 클라우드 및 분산 컴퓨팅 한경의 보안 위협

분산 컴퓨팅 환경 중 널리 사용되고 있는 그리드 기반의 컴퓨팅 모델은 그리드 컴퓨팅이 기반하고 있는 GSI (Grid Security Infrastructure)를 보안의 근간으로 삼고 있다. GSI는 프록시라는 사용자 위임 인증서를 이용하여 작업을 관리하도록 하고 있으며, 사용자의 인증과 접근통제는 전적으로 시스템 중심으로 설계되어 있다. GSI는 분산 시스템의 가용성을 목표로 설계되었기 때문에 다음과 같은 한계를 갖는다.

- GSI는 해커 또는 악의적인 내부자와 같은 능동적인 악의적 존재를 고려하지 않고 있다.
- GSI는 암호화에 대해 명확히 정의하고 있지 않다.
- 따라서, 사용자는 시스템을 전적으로 신뢰하여야 한다.

하지만 그리드 시스템의 큰 특징은 전세계의 다양한 컴퓨팅 자원들이 연합한 멀티-트러스트 도메인들로 이루어져 있고, 각 도메인의 보안 정도는 매우 다양한 수준으로 구성되어 있다. 또한 그리드 시스템의 저장요소(Storage Element, SE)는 다음과 같은 특징을 갖고 있다.

- SE의 데이터는 가용성을 위해 다른 SE로 자동복제된다.
- SE의 데이터는 거의 업데이트 되지 않는다. 한번 쓰고 여러번 읽는 식으로 동작한다.

따라서 실험에 사용되는 데이터를 SE에 저장하고, 각 계산자원에서 그 데이터를 다운로드하여 계산을 수행하는 전형적인 계산 모델은 SE 관리자에게 모든 데이터를 노출할 수 있고, 계산을 수행하는 계산 노드의 관리자 역시 모든 데이터에 접근할 수 있다는 단점이 있다.

2010년 Cloud Security Alliance(CSA)는 다음과 같이 7개의 클라우드 컴퓨팅의 위협요소에 대해 발표하였다. (http://www.cloudsecurityalliance.org/topthreats/csathreats.v.1.0.pdf) 이 위협요소들은 위협의 경중에 의해 나열된 것은 아니며, 사용자가 처한 상황에 따라 다른 우선순위로 적용될 수 있을 것이다.

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insider
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

이러한 위협 요소에 대한 CSA의 가이드 라인은 다음과 같이 구성되어 있다.

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

위의 13개 영역은 크게 클라우드에 대한 정의와 기본 특성들과 모델들을 살펴보는 Domain 1의 아키텍처 영역과 클라우드의 운영과 사용에 따른 정책적인 요소들을 다루는 Domain 2 - 6을 포함하는 클라우드의 운용적인 영역, 보다 기술적인 요소들을 다루는 Domain 7 - 13의 클라우드 운영적인 영역으로 구분할 수 있다.

Ⅲ. 대책 및 접근방안

클라우드 및 분산 컴퓨팅은 기존의 위협 요소 이외에도 클라우드 컴퓨팅 고유의 정보보호 위협들이 존재하고, 시스템의 운용과 관리에도 많은 정보보호 이슈들이 존재한다. 클라우드 컴퓨팅에서의 정보보호는 단순히 제공하는 기능에 추가되는 요소로서가 아닌 클라우드 컴퓨팅을 제공하기 위한 필수요소이다. 또한 정보보호는 사용자의 중요 데이터를 지키기 위한 것이 아닌 내가 운영하는 자원이 악의적인 사용자들에 의해 악용되는 것을 방지해야 하기도 한다. 최근의 DDOS 같은 형태의 공격의 기지화가 될 경우, 시스템 활용성이 떨어질 뿐만 아니라 운영하고 있는 기관의 평판에도 크게 악영향을 끼친다.

사이언스 클라우드는 일반적인 클라우드 컴퓨팅과 비교하여 단순한 웹 호스팅이나 범국민적인 서비스를 제공하지는 않는다. 사이언스 클라우드는 대용량 데이터의 분석에 포커스를 맞추고 있으며 가상화를 이용하여 동적인 할당이 가능한 데이터 팜의 형태가 될 것으로 예상하고 있다. 계산과학분야의 데이터 처리는 대부분 개인이 생성, 활용하지 않고 커뮤니티 단위로 이루어지고 있으며, 이에 따른 데이터 공유에 대한 대책이 수립되어야 한다. 이 장에서는 현재까지 파악된 사이언스 클라우드에 대한 정보보호 이슈들을 나열하고, 그에 대해 정보보호 체계 구축에 대하여 논해 본다.

빠른 서비스 제공과 안전성 제공을 목표로 사이언스 클라우드의 정보보호 체계 구축을 위해 다음과 같이 실용성을 강조하여 접근한다.

- SLA 또는 정보보호 정책을 통한 관리적 접근
- 기반 SW의 취약성 보강
- Application 수준의 접근부터 시작하여, System Software 수준으로 확대

- 외부 기관과의 협력 확대

우선 SLA 또는 정보보호 정책을 통한 관리적 접근 방법은 현재 사이언스 클라우드가 태동 단계임을 감안하여 제한된 사용자들에게 엄격한 SLA와 사용지침을 제시하여 최소의 사용자들에게 빠른 서비스를 제공하기 위함이다. 자원의 신청에서 할당, 환경 구성, 자원의 활용, 사용 후 반납에 이르는 전 주기에 대한 구체적인 지침이 제시되어야 하고, 본격적인 기술적인 보호대책 개발해야 한다. 이러한 관리적 접근은 기술적 대책이 강구된 뒤에 폐기되는 것이 아니라 지속적으로 유지, 발전시켜 물리적, 기술적, 관리적 보호대책이 유기적으로 작동하도록 추진해야 한다. 또한 상용 소프트웨어의 라이센스 문제와 같은 정책적인 이슈들도 고려되어야 한다.

기반 SW의 취약성 보강은 가상화를 지원하는 Xen 등의 하이퍼바이저와 가상 머신들을 이용하여 클러스터를 관리하는 Eucalyptus, OpenNebula와 같은 Software를 중심으로 사이언스 클라우드를 구축하고, 소프트웨어에서 제공하지 않는 세부 기능들을 중심으로 보강해 나가야 한다.

정보보호 기능의 구현은 어플리케이션 수준의 접근 방법을 우선으로 하여, 사용자들에게 많은 기능들을 제공하고 점차적으로 시스템 소프트웨어 수준으로 접근하도록 한다. 어플리케이션 수준의 구현은 그 구현 난이도가 시스템 소프트웨어보다 쉽고, End to End 보안 개념을 적용하기도 가장 용이하다. 예를 들어, 세션 등을 쉽게 유지할 수 없는 무선 디바이스의 경우, 어플리케이션의 구현을 통해 네트워크 관리 등의 문제를 쉽게 해결할 수 있다. 하지만, 구현의 중복성과 정보보호 정책의 강제를 위해 장기적으로는 시스템 소프트웨어로의 접근은 필수적이다.

외부 기관과의 확대는 기존의 정보보호 시스템을 연구, 개발하는 업계 들이나 가상화, 네트워크 등을 연구하는 대학과의 협조를 통해 보다 연구 개발의 시너지를 얻기 위함이다. 이와 같이 가장 빠르게 서비스 제공이 가능하도록 하면서, 장기적인 기술 확보를 목표로 접근하도록 한다.

Ⅳ. 결론

클라우드 컴퓨팅은 사용자의 요구에 맞추어 유연하고 동적으로 자원을 제공하여 주는 유틸리티 컴퓨팅의 구현을 제안하고 있다. 컴퓨팅 자원의 구축, 운영에 대한 부담을 줄이고, 자신의 비즈니스 핵심 기술에 집중할 수 있다는 장점으로 많은 기대를 받고 있지만, 정보 및 정보 시스템이 외부 조직에 의해 관리, 운영된다는 점에서 정보보호에 대한 요구는 더욱 증가하고 있다. 특히 사용자의 데이터에 대한 엄격한 접근통제를 구현하여 시스템 운영주체조차 사용자의 데이터를 임의로 접근할 수 없도록 해야 한다.

반면, 그리드 컴퓨팅, 클라우드, 유틸리티 컴퓨팅과 같이 방대한 인프라를 활용하는 경우, 침입 또는 악의적인 사용자에 의해 자원이 악용될 여지가 높아지고 있으며, 그러한 침해사고가 발생할 경우 서비스 제공기관의 평판까지 영향을 받을 수 있으므로 자원의 악용을 방지하기 위한 모니터링과 감사 기능의 개발이 필요하다.

이와 같이 프라이버시에 대한 요구와 사용자의 사용형태에 대한 모니터링이 동시에 요구되고 있으며 이러한 상충되는 요구사항들을 만족하기 위해 효과적인 감사 시스템을 구현하여 사용자와 제공자 간의 분쟁 해결이나 범죄 행위에 대한 증거로 활용할 수 있어야 한다.

참고문헌

NIST, NIST Homepage, http://www.nist.gov/.

CSA, CSA Homepage, http://www.cloudsecurityalliance.org.

Globus, Globus Project, GSI, http://www.globus.org/security/.

I. Foster, C. Kesselman, G. Tsudik, S. Tuecke (1988), "A Security Architecture for Computational Grids", Proc. of the 5th ACM Conference on Computer and Communications Security, 1988, pp. 83-92.