모바일 클라우드 컴퓨팅을 위한 신뢰 컴퓨팅 연구 및 고찰

박지수, 박종혁†
서울과학기술대학교 컴퓨터공학과
e-mail:{jisoo08,jhpark1}@seoultech.ac.kr

A Study on Trusted Computing for Mobile Cloud Computing

Ji Soo Park, Jong Hyuk Park
Department of Computer Science and Engineering, SeoulTech

요 약

현재 클라우드 컴퓨팅은 컴퓨팅 장비 설치에 대한 비용을 낮추고 관리 및 유지 보수 비용을 감소시키는 강점을 가지고 구글과 아마존 등의 기업을 선두로 하여 각종 서비스와 기술들이 활발히 개발되어 사용되고 있다. 이러한 클라우드 컴퓨팅 서비스는 기존 웹 환경을 이용하고 있기 때문에 기존의 보안 문제를 포함하고 있고 모바일 기기에서 클라우드 컴퓨팅을 이용하면 모바일 기기가 갖는 보안 문제도 갖게 된다. 본 논문에서는 클라우드 컴퓨팅을 이용하는 모바일 단말에서 보안성을 높이기 위한 신뢰 컴퓨팅 방안에 대해 논의한다.

1. 서론

클라우드 컴퓨팅은 기존의 웹 환경을 이용하기 때문에 기존 보안 문제를 내제있고 특히 스마트폰에서 클라우드 컴퓨팅을 이용하게 되면 모바일 단말과 웹의 취약점으로 많은 보안 위협이 존재하게 되며 최근 이를 해결 위한 방안으로 신뢰 컴퓨팅(Trusted Computing)에 대한 연구가 진행되고 있다.

본 논문에서는 신뢰 컴퓨팅의 개념과 클라우드 컴퓨팅을 이용하는 모바일 단말을 위한 신뢰 컴퓨팅 기술에 대해 살펴본다.

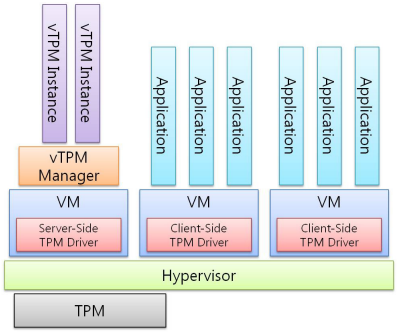
Trusted Platform Module (TPM)은 Mobile phone, Authentication, Infrastructure, PC security, Storage 등의 분야에서 활용되고 있는 오픈 플랫폼에서 신뢰 지표를 측정하는 유일한 표준 물리적인 장치를 말하며 Trusted Computing Group (TCG)에서 원칙 및 개념, 하드웨어 구성 요소 등을 정의하고 있다. TPM은 하드웨어 레벨에서 보안성을 강화하는 것으로 기기 자체의 보안성을 강화하는 특징을 가지고 있다 [1, 2, 3].

● TPM의 구성과 보안요소

TPM의 구성은 입출력을 담당하는 I/O, 명령을 검증 및 실행하는 Execution Engine과 Program Code, 사용되는 키와 상태정보를 저장하는 Non-Volatile Storage, Volatile Storage 그리고 키를 생성하는 RSA Engine, Key Generation 등으로 구성되어 있다 [1, 3].

TPM은 접근제어, 인증, 로깅 및 리포팅 세가지 보안 요소를 제공한다. 접근제어는 암호키와 PCR 및 키 생성과 같은 민감 데이터 및 실행 권한에 따라 접근을 제어하며 인증은 서비스에 접근하고자 하는 서비스 공급자와 같은 원격 개체의 무결성이 충족되는지 확인하기 위해 제공되며 하드웨어와 소프트웨어의 무결성이 검증되어야 한다. 로깅 및 리포팅은 하드웨어나 소프트웨어의 상태를 측정하여 측정 대상에 대한 무결성 정보를 제공한다. 이러한 정보를 관리하기 위해 Root of Trust for Measurement (RTM) 이라고 정의된 모듈이 사용되며 측정된 결과는 PCR이나 TPM 외부에 기록 된다 [1, 2].

● TPM 가상화 모델



(그림 1) TPM 가상화 모델

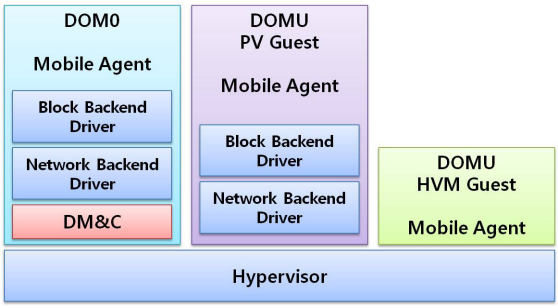
(그림 2)는 클라우드 컴퓨팅의 가상화 상에서 TPM을 적용하기 위한 모델이다. Hypervisor에 의해 Virtual

† 책임 저자 : 박종혁 (서울과학기술대학교 컴퓨터공학과 교수)

Machine(VM)이 생성되며 각각의 VM은 TPM 드라이버를 갖게 된다. Server-Side에서는 vTPM Manager을 통해 생성되는 VM을 관리하게 된다 [1, 2, 4].

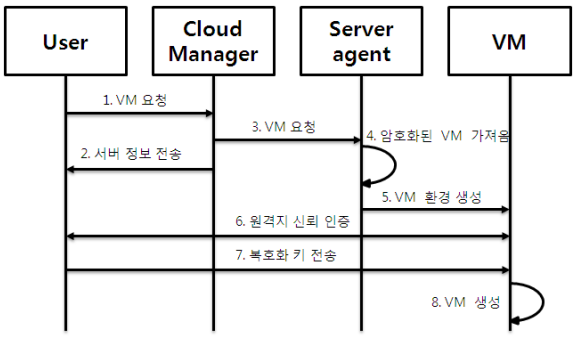
2. 모바일 클라우드 컴퓨팅을 위한 신뢰 컴퓨팅

모바일 클라우드 컴퓨팅에 신뢰 컴퓨팅을 적용하기 위해서는 2장에서 살펴본 TPM의 구성과 TPM의 가상화 모델이 적용되어야 한다. (그림 3)은 이러한 TPM과 가상화 모델을 적용한 모바일 기반의 클라우드 컴퓨팅 신뢰모델이다.



(그림 2) 모바일 클라우드 컴퓨팅 신뢰 모델

VM과 하드웨어 간의 상호작용을 하는 Hypervisor를 기반으로 클라우드 컴퓨팅을 이용하는 모바일 기기, DOM0, DOMU 세가지로 구성된다. 사용자의 모바일 기기는 클라우드 자원을 안전하게 사용하기 위한 보안 통신 제공을 위해 사용되고 DOM0은 가상머신 내에서 드라이버 및 응용 프로그램의 무결성을 검사하고 알려주는 기능을 갖는다. DOM0의 DM&C는 각 도메인의 관리와 제어를 담당한다. DOMU는 VM 인스턴스를 생성 및 관리하며 VM들을 모니터링하여 악의적인 활동을 모니터링하고 사용자에게 알려주게 된다. VM인 DOM0와 DOMU는 네트워크 하드웨어와 통신을 위한 Network-Backend Driver와 저장장치를 읽고 쓰기 위한 Block-Backend Driver를 포함하고 있다 [5].



(그림 3) VM 생성 Sequence Diagram

사용자가 VM을 사용하기 위해서는 (그림 3)과 같이 Cloud Manager를 통해서 Server agent에게 VM 생성 요청을 하게 되고 Sever aget는 암호화된 VM 환경을 생성하게 된다. 사용자의 인증을 위해 2장에서 살펴본 RTM이 사용되며 사용자 인증이 성공한다면 사용자의 키를 VM에서 수신하여 VM을 생성하고 사용하게 된다 [2].

3. 결론 및 고찰

본 논문에서는 신뢰 컴퓨팅의 개념 및 클라우드 컴퓨팅을 이용하는 모바일 단말을 위한 신뢰 컴퓨팅 기술에 대해 살펴보았다. 클라우드 컴퓨팅은 기존 데스크탑 PC 환경에서 벗어나 스마트폰, 태블릿 등 다양한 스마트기기를 단말로 이용할 수 있다. 하지만 모바일 단말이 가지는 성능적, 기능적 특성으로 인해 다양한 보안 위협이 존재하게 된다. 이러한 모바일 단말의 보안 문제를 해결하기 위해서 단말이 가지는 보안성을 강화하기 위하여 신뢰 컴퓨팅이 이용되고 있고 단말의 강화된 보안성을 통해 클라우드 컴퓨팅의 신뢰성과 보안성을 강화하고 있다.

모바일 단말에서의 클라우드 컴퓨팅의 보안성을 더욱 향상시키기 위해서는 모바일 단말이 가지는 성능적인 제약 사항과 이동성과 같은 특징을 반영하여 보다 모바일 단말에 적합한 인증 방안과 프로토콜에 대한 연구가 필요하다.

감사의글

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2011-0024052).

참고문헌

[1] Achemlal, M., Gharout, S., Gaber, C.,, "Trusted Platform Module as an Enabler for Security in Cloud Computing", Network and Information Systems Security (SAR-SSI), 2011 Conference on, IEEE, May 2011.

[2] Rocha, F., Abreu, S., Correia, M., "The Final Frontier: Confidentiality and Privacy in the Cloud", Computer, Vol.44, Iss.9, pp.44-50 Sept. 2011.

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

[4] S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, "vTPM: virtualizing the trusted platform module", in Proceedings of the 15th conference on USENIX Security Symposium, Vol.15, USA: USENIX Association, 2006.

[5] Priyank Singh Hada, Ranjita Singh and Mukul Manmohan,"Security Agents: A Mobile Agent based Trust Model for Cloud Computing", International Journal of Computer Applications Vol.36, No.12, pp.12-15, December 2011.