차량 클라우드를 위한 서비스 모델과 보안 요구사항 연구

조원준*, 이경현**
*부경대학교 정보보호학과
**부경대학교 IT융합응용공학과
e-mail:{fafata, khrhee}@pknu.ac.kr

A Study on Service Models and Security Requirements for Vehicular Clouds

Won Jun Cho*, Kyung Hyune Rhee**
*Dept of Information Security, Pukyong National University, Korea
**Dept of IT Convergence and Application Engineering, Pukyong National University, Korea

요 약

클라우드 컴퓨팅은 공유된 컴퓨팅 자원을 사용자의 요구에 따라 원하는 만큼 네트워크를 통해 사용하는 IT기술이다. 최근 이러한 클라우드 컴퓨팅의 개념을 차량 Ad-hoc 네트워크에 도입한 차량 클라우드 서비스에 대한 연구가 시도되어지고 있다. 차량 클라우드에서도 기존의 클라우드 서비스나 차량 Ad-hoc 네트워크에서와 같이 서비스 모델에 따른 보안기술이 적용되어야하지만, 차량 클라우드 서비스를 위한 보안기술의 연구는 국내·외적으로 미비한 실정이다. 따라서 본 논문에서는 차량 클라우드에서 가능한 서비스 모델을 제시하고 이에 따른 보안위협 및 안전한 차량 클라우드 서비스를 구축하기 위한 보안 요구사항에 대하여 기술한다.

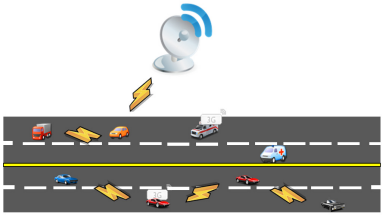
1. 서론

클라우드 컴퓨팅은 사용자에게 계산, 저장 능력, 네트워크와 같은 가상의 하드웨어 자원을 빌려주는 IaaS(Infrastructure as a Service)와 사용자에게 애플리케이션 개발을 위한 OS, 소프트웨어 환경, 프로그래밍 도구 등의 플랫폼을 제공하는 PaaS(Platform as a Service), 그리고 사용자가 자신의 하드웨어에 애플리케이션을 설치하지 않고 클라우드에 접속해 애플리케이션을 사용하는 SaaS(Software as a Service)로 분류할 수 있다. 이러한 클라우드 컴퓨팅은 사용자의 요구에 따라 원하는 만큼 가상의 하드웨어·소프트웨어 자원과 서비스를 제공하고 사용한 만큼 지불하는 서비스 모델이며, 또한 대량의 컴퓨팅 자원을 요구하는 작업을 분산, 병렬 처리 할 수 있는 방법을 제공한다. 이로 인해 사용자는 저렴한 비용으로 필요한 서비스를 이용 할 수 있다. 클라우드 컴퓨팅의 대표적인 서비스로는 아마존의 EC3, S3(IaaS), 구글의 App-engine(PaaS), IBM(SaaS)가 있다[4].

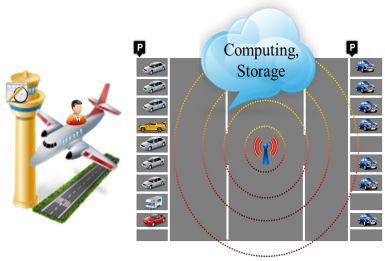
한편 이동통신 기술과 IT융합 기술의 발달로 차량간의 통신은 이동 Ad-hoc 네트워크(MANET, Mobile Ad-hoc Network)의 형태로 이루어지게 되었고 이러한 네트워크를 차량 Ad-hoc 네트워크(VANETs, Vehicle Ad-hoc Networks)라고 한다. 차량 Ad-hoc 네트워크는 크게 차량간(V2V, Vehicle-to-Vehicle) 통신과 차량과 인프라간(V2I, Vehicle-to-Infrastructure) 통신으로 나뉜다. 이러한 차량 Ad-hoc 네트워크는 도로의 상태나 교통상황, 컨텐츠 분배를 통해 운전자의 안전과 편리를 제공하는 것이 목적이며 국내·외적으로 다수의 연구가 진행 되고있다[10].

최근 이들 기술을 결합하여 차량 Ad-hoc 네트워크에서 차량의 유휴 컴퓨팅 자원을 사용할 수 있는 차량 클라우드 서비스가 소개되었다[2]. 차량 클라우드는 한 그룹의 차량에 대해서 컴퓨팅, 센서에 의한 감지, 통신과 같은 물리적인 자원을 공유하여 사용자가 해당 서비스를 필요로 할 때 제공하는 서비스이다. 이러한 차량 클라우드 서비스를 안전하게 제공하기 위해서는 보안 문제가 해결되어야 한다. 하지만 클라우드 컴퓨팅을 위한 보안 기술[3, 4, 9]과 안전한 차량 Ad-hoc 네트워크를 위한 보안 기술[1, 5, 6, 8, 11]은 최근까지 많이 제안되었지만 차량 클라우드를 위한 보안 기술에 대한 연구는 이루어지지 않았다. 따라서 본 논문에서는 차량 클라우드에서 가능한 서비스 모델을 제시하고 이에 따른 보안위협 및 안전한 차량 클라우드 서비스를 구축하기 위한 보안 요구사항에 대하여 기술한다.

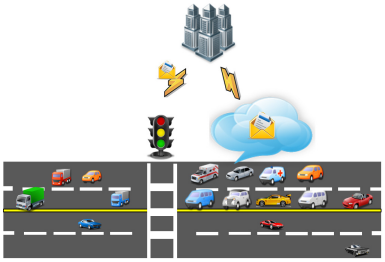
이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2012-0001331)



(그림1) NaaS 모델



(그림2) STaaS 모델



(그림3) CaaS 모델

본 논문의 구성은 다음과 같다. 2장에서는 차량 클라우드에서 가능한 서비스 모델을 제시한다. 3장에서는 차량 클라우드의 보안위협을 정의하고 이에 따른 보안 요구사항을 기술한다. 마지막으로 4장에서 결론을 맺는다.

2. 차량 클라우드 서비스 모델

차량 Ad-hoc 네트워크는 운행중인 차량들에 대해서 차량상태, 교통상황의 메시지 교환에 주 목적을 두고 연구가 진행 되었다. 하지만 차량 클라우드는 차량이 주차되어 있는 경우의 잉여 계산, 저장 능력까지 고려하여 지속적인 네트워크 연결성, 부족한 계산, 저장 능력 등을 보완하기 위해 클라우드 컴퓨팅을 접목한 시스템이다. 이로인해 사용자는 클라우드 컴퓨팅의 장점들인 사용자의 필요에 의해 원하는 만큼의 서비스 제공, 사용자의 초기투자 비용절감, 사용자의 요구에 따른 즉각적인 문제해결 능력들과 각 차량에 장착되어있는 OBU(On-Board Unit)의 계산·저장 능력 공유로 슈퍼컴퓨팅 기능 등을 사용할 수 있다. 한편 일반적인 클라우드 컴퓨팅과는 달리 차량 클라우드에서는 OBU의 컴퓨팅 자원이 서비스를 실행하기에는 부족할 수 있기 때문에 여러대의 OBU가 하나의 가상머신을 구현해야 한다.

차량 클라우드에서 나타나는 서비스 모델은 아래와 같이 3가지 모델로 구별되어질 수 있다.

- NaaS(Network as a Service) : 인터넷 연결이 자유로운 기존의 클라우드 컴퓨팅 환경과 다르게 차량 클라우드에서는 일부분의 차량에서만 인터넷 연결이 가능할 것이다. 이 때 인터넷 연결이 가능한 차량들은 (그림1)과 같이 자신의 네트워크 자원을 다른 차량에게 제공할 수 있다. 차량은 노변장치(RSU, Rodeside Unit)를 통한 인터넷 연결과 인터넷 연결이 가능한 차량들 중 자신에게 적합한 서비스를 선택해 네트워크 서비스를 제공 받을 수 있다.
- STaaS(Storage as a Service) : 대부분의 차량은 실제로 운행되는 시간보다 차고지에 주차 되어있는 시간이 많다. 이 때, 차량에 장착된 OBU의 계산 능력과 저장 능력을 필요한 사용자에게 제공할 수 있다. 이 모델에서 선행되어야 할 조건은 충분한 양의 차량이 인터넷의 연결이 자유로운 장소에 존재하여야 한다. 예를 들어 (그림2)와 같이 공항 주차장의 경우 별도의 네트워크망을 구축한다면 공항이용객의 출발, 복귀 시간을 알 수 있고, 충분한 수의 차량이 주차되어 있으므로 유연한 데이터 클라우드를 구성하여 컴퓨팅 자원이 필요한 사용자에게 서비스 제공을 할 수 있다. 이러한 서비스 모델에서는 차량 소유자의 참여를 위해 무료 주차와 같은 유인방안이 필요할 것이다.
- CaaS(Cooperation as a Service) : 지능형 교통시스템(ITS, Intelligent Transport System)을 위한 기반시설이 갖추어지지 않은 환경에서 차량 한 대의 OBU에서는 연산 할 수 없는 애플리케이션을 많은 차량의 유휴 자원들을 사용하여 차량 클라우드를 형성해 실행 한다면 기반시설에 준하는 서비스를 제공할 수 있다. 현재의 교통 시스템은 해당 기관의 통계적 모델을 사용하여 교통 신호제어와 교통 정보를 제공한다. 이 모델은 갑작스러운 상황 발생 시 빠른 대처가 곤란하다. 예를 들어 (그림3)과 같이 교통사고가 발생하여 교통 체증이 심한 지역에서 다수의 차량이 정체되어 있다면 기존의 교통 흐름 제어 모델에서는 교통 체증 해소를 위해 인력의 투입이 필요하거나, 운전자들에게 교통 정보를 방송으로 알려주어 완화하는 방법을 사용한다. 이 때 차량 클라우드 모델에서는 운전자들이 자신의 차량에 남는 컴퓨팅 자원을 사용하여 클라우드를 형성한 다음 주변의 신호체계 시스템이나 교통 흐름을 관리하는 기관에 컴퓨팅 자원을 빌려 줄 수 있다. 관리기관에서는 형성된 클라우드의 자원을 사용하여 교통흐름을 계산, 예측하여 한층 더 빠르고 유연하게 교통체증을 완화 할 수 있다.

3. 차량 클라우드의 보안 위협 및 보안요구사항

차량 Ad-hoc 네트워크에 클라우드 컴퓨팅을 도입한 차량 클라우드는 많은 비용의 투자없이 고비용의 시설이 필요한 연산들을 가능하게 만들어 주지만 기존의 차량 Ad-hoc 네트워크에서의 보안문제[1, 10]와 클라우드 컴퓨팅에서의 보안문제[3, 4, 9]까지 고려해서 사용해야한다. 차량 클라우드는 클라우드 컴퓨팅을 도입함으로써 기존의 차량 Ad-hoc 네트워크보다 높은 시스템 복잡도와 자원공유시스템 환경을 가지게 되며 이는 동일한 컴퓨팅 자원을 사용하는 가상머신들 간의 정보누출이 가능하게 한다. 또한 모든 차량의 권한이 동일한 클라우드 서비스의 특성으로 인해 서비스 거부 공격에 취약하다. 이러한 위협과 함께 차량 클라우드에서는 메시지의 특수한 성질이 존재하고, 차량간의 통신이 항상 매끄럽게 이루어지지 않는 점, 차량의 고속이동성으로 인한 잦은 구성원 변화와 네트워크 토폴로지의 변화 발생, 그리고 각 차량에 장착된 OBU의 컴퓨팅 능력이 상이한 특징을 가진다. 한편 차량의 고속이동성으로 인해 특정 지역에서 형성되는 클라우드에 대한 공격은 공격자가 공격 목표의 주변에 존재해야 하기 때문에 기존의 클라우드 서비스에 대한 공격에서보다 강한 모습을 보인다.

이러한 보안위협을 방지하기 위해서는 다음과 같은 보안 요구사항을 만족하여야 한다.

- 인증 : 차량 클라우드는 가상화를 통한 가상 머신상에서 형성되기 때문에 데이터의 저장이 다양한 형태와 장소에 저장된다. 차량 클라우드 서비스 제공자는 민감한 데이터에 대한 접근 통제를 하여 적절한 사용자만 해당 데이터에 접근할 수 있도록 해야 하며 이는 사용자 인증을 통해 이루어 질수 있다. 기존의 클라우드 컴퓨팅에서는 고정된 장비와 미리 인증된 사용자에게 서비스를 제공한다. 하지만 차량 Ad-hoc 네트워크에서는 운전자가 요구할 때 즉시 서비스를 제공하여야하는 점과 차량의 고속이동성, 짧은 통신 거리로 인해 인증 메시지의 전달이 실패할 수 있고, 보안 토큰 업데이트가 힘들다는 점이 차량 클라우드에서의 인증을 힘들게 한다.
- 프라이버시 보호 : 차량 클라우드에서의 통신에서는 자신과 메시지의 인증을 위해 상대방에게 자신의 개인정보를 함께 전송하고 사고 정보, 교통상황 등의 메시지에서는 차량의 위치정보 또한 전송하게 된다. 이 때 사용자의 개인정보와 차량의 위치정보는 메시지 발신자의 사생활을 노출 할 수 있으며 이를 방지하기위해 사용자의 프라이버시 보호가 필요하다.
- 가용성 : 차량 클라우드에서는 클라우드 서비스 제공자측의 문제로 인한 서비스 단절과 차량의 이동성으로 인해 발생하는 인터넷 연결의 부재로 인한 서비스 단절 그리고 서비스 거부 공격으로 인한 서비스 단절이 발생할 수 있다. 이러한 단절은 차량의 유휴 컴퓨팅 자원을 공유하여 서비스를 제공하는 차량 클라우드의 가용성에 영향을 준다.
- 무결성 : 차량 클라우드에서 교환하는 메시지에는 안전을 위한 메시지, 사고 시 법적근거로 사용할 수 있는 메시지, 클라우드 서비스의 결제정보 등이 있다. 이러한 메시지가 변조된다면 전송된 메시지의 정보는 더 이상 안전하지 않을 것 이며 법적 근거로서의 효력도 보장할 수 없다.
- 데이터 보호 : 공유된 자원을 사용하는 차량 클라우드에서는 사용자의 데이터에 대한 보호가 필요하다. 사용자의 데이터에 대한 보호는 사용자 인증을 통한 접근통제와 데이터의 암호화로 이루어 질 수 있다.

4. 결론

본 논문에서는 차량 Ad-hoc 네트워크에 클라우드 컴퓨팅을 도입한 차량 클라우드를 소개 하였고 그에 따른 보안 위협과 보안요구사항을 기술하였다. 향후 안전한 차량 클라우드를 사용하기 위해서는 본 논문에서 제시된 보안 요구사항에 적합한 보안 메커니즘에 대한 연구가 필요하다.

참고문헌

[1] A. Aijaz, B. Bochow, F. Doetzer, A. Festag, M. Gerlach, R Kroh, and T .Leinmueller, “Attacks on Inter-vehicle Communication Systems An Analysis”, International Workshop on Intelligent Transportation, pp. 189-194, 2006.

[2] J. Eriksson, H. Balakrishnan, and S. Madden, “Cabernet: Vehicular Content Delivery Using WiFi,” 14th ACM International Conferenceon Mobile Computing and Networking, pp. 199-210, 2008.

[3] M. Jensen, J, Schwenk, N. Gruschka, and L. Lacono, “On Technical Security Issues in Cloud Computing,” IEEE International Conference on Cloud Computing, pp. 109-116, 2009.

[4] W. Jansen and T. Grance, Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144, Information Technology Laboratory, NIST. 2011.

[5] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, “ECPP : Efficient Conditional Privacy Preservation protocol for secure vehicular communications,”IEEE

INFOCOM2008, pp. 1229-1237, 2008.

[6] X. Lin, X. Sun, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, 2007

[7] S. Olariu, T. Hristov, and G. Yan, "The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds," Mobile Ad hoc networking: the cutting edge directions, Wiley, 2012.

[8] Y. Park, C. Sur, C. Jung, and K. H. Rhee, "An efficient anonymous authentication protocol for secure vehicular communications," Journal of Information Science and Engineering, vol. 26, no. 3, pp. 785-800, 2010.

[9] G. Russell, and R. Macfarlane, "Security Issues of a Publicly Accessible Cloud Computing Infrastructure," IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1210-1216, 2012

[10] M. Raya, and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39-68 2007.

[11] C. Sur, Y. Park, K. Sakurai and K. H. Rhee, "Providing Secure Location-Aware Services for Cooperative Vehicular Ad Hoc Networks," Journal of Internet Technology, vol. 13, no.4, pp. 631-644, 2012.

[12] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security Challenges in Vehicular Cloud Computing," IEEE Transactions on Intelligent Transportation Systems, vol. 99, pp. 1-11, 2012.