정 보 보 호 학 회 지
제24권 제2호, 2014. 4

차량 클라우드 컴퓨팅 활용 방안과 보안 요구사항

허 명 학*, 이 경 현**

요 약

차량 클라우드는 차량 네트워크 기술에 클라우드 컴퓨팅을 접목한 IT 융합 기술이다. 차량 클라우드는 인가된 사용자들을 위해서 협력하거나 동적으로 할당 할 수 있는 컴퓨터, 센서, 통신, 물리적 자원들을 통합한 대규모의 자주적인 차량 그룹으로 오늘날 인간의 삶에 많은 기여를 할 수 있을 것으로 예상된다. 본 논문에서는 차량 클라우드 컴퓨팅의 활용 방안을 소개하고, 이에 관련된 보안 위협과 이를 해결하기 위한 보안 요구사항에 대하여 기술한다.

Ⅰ. 서 론

최근 클라우드 컴퓨팅(Cloud Computing)이라는 새로운 IT 패러다임이 부각되면서, 클라우드 컴퓨팅에 기존의 IT 기술을 접목시키려는 움직임이 활발하게 일어나고 있다. 차량 클라우드(Vehicular Cloud)는 차량에 클라우드 컴퓨팅을 접목한 IT 융합 기술로, 이는 VANET(Vehicular Ad Hoc Network)이라는 차량 네트워크를 기반으로 하고 있으며, VANET은 DSRC (Dedicated Short Range Communication)라 불리는 근거리 무선 통신 방식을 이용하여 OBU(On- Board Unit)를 갖춘 차량과 차량 간의 통신(Vehicle-to-Vehicle, V2V) 뿐만 아니라 차량과 도로상에 설치된 RSU (Road-Side Unit)와의 통신(Vehicle-to-Infrastructure, V2I)을 지원한다[1].

차량 클라우드는 인가된 사용자들을 위해서 협력하거나 동적으로 할당 할 수 있는 컴퓨터, 센서, 통신, 물리적 자원들을 통합한 대규모의 자주적인 차량 그룹으로 정의 할 수 있는데[2], 이러한 차량 클라우드는 두 가지 유형으로 나눌 수 있다. 첫 번째 유형은 인터넷과 연계되어 구성되는 차량 클라우드로, 차량 소유주는 노변 인프라와의 통신으로 서비스에 접속 할 수 있다. 두 번째 유형은 자주적인 차량 클라우드로[3], 차량들은 비상시나 다른 애드 혹 이벤트를 위해 그때마다 차량들을 조직화하여 차량 클라우드를 형성할 수 있다.

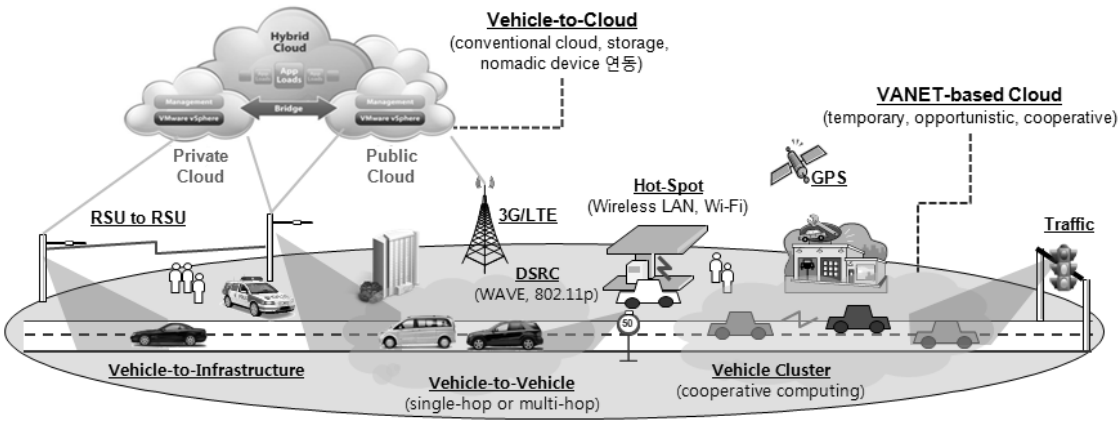
차량 클라우드는 오늘날 인간의 삶에 많은 기여를 할 수 있을 것으로 예상되며, 이러한 차량 클라우드 서비스를 안전하게 제공하기 위해서는 보안문제가 해결되어야 할 필요가 있다. 따라서 본 논문에서는 차량 클라우드의 유형 및 아키텍처, 서비스 모델, 활용 방안에 대하여 소개한 뒤, 이에 관련된 보안 위협과 이를 해결하기 위한 보안 요구사항에 대하여 기술한다.

본 논문의 구성은 다음과 같다. 2장에서는 차량 클라우드 유형 및 아키텍처에 대해서 기술한 뒤, 3장에서는 차량 클라우드의 서비스 모델에 대하여 기술한다. 4장에서는 차량 클라우드의 활용 방안을 소개하고, 5장에서는 차량 클라우드의 보안 위협과 이를 해결하기 위한 보안 요구사항에 대하여 기술한다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 차량 클라우드 유형 및 아키텍처

본 장에서는 차량 클라우드의 유형과 아키텍처에 대해서 기술한다.

이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.
(No. NRF-2013R1A1A4A01009848)
* 부경대학교 대학원 정보보호학협동과정 (mhheo@pknu.ac.kr)
** 부경대학교 IT융합응용공학과 (khrhee@pknu.ac.kr), 교신저자



〔그림 1〕 차량 클라우드 컴퓨팅 환경의 구성 및 유형

2.1 차량 클라우드 유형

차량 클라우드의 유형은 구성 형태에 따라 차량 네트워크를 기반으로 구성되는 VANET-based Cloud와 차량에 탑재된 컴퓨팅 단말이 인터넷과 연계되어 구성되는 Vehicle-to-Cloud 두 가지로 나누어 질 수 있다[2, 3]. 그림 1은 이러한 차량 클라우드 컴퓨팅 환경의 구성 및 유형을 도식화하여 보여주고 있다.

2.1.1 VANET-based Cloud

VANET 기반의 차량 클라우드는 차량들이 보유한 컴퓨터, 스토리지, 센서, 통신, 물리적 자원들을 통합하여 도로상에 가상의 컴퓨팅 플랫폼을 구현하고 인가된 사용자들에게 동적으로 할당하기 위한 차량 협력 모델로, 일시적인 처리나 지역적인 데이터를 매번 인터넷 클라우드로 업로드/다운로드 하는 대신 도로상의 차량 클라우드에서 처리함으로써 지연시간을 줄일 수 있다. 이러한 유형의 차량 클라우드는 도로상에서 혹은 일상생활 환경에서 발생 가능한 문제들을 사전에 감지하고 예방하거나 사후 해결활동을 위한 목적으로 활용될 수 있다.

2.1.2 Vehicle-to-Cloud

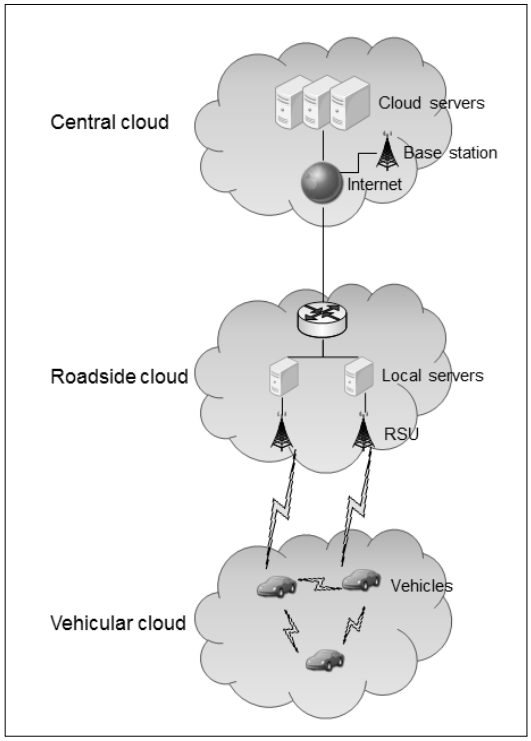
Vehicle-to-Cloud 유형은 고성능의 컴퓨터와 대용량의 스토리지를 갖춘 인터넷상의 상용 클라우드와 연계하여 VANET 기반의 클라우드에서 지역적으로 수집된 데이터의 처리결과를 바탕으로 중앙 클라우드는 전역적인 결과를 도출하고 이러한 데이터를 장기적으로 저장하고 활용하는 것을 주요 목적으로 하는 모델이다. 이러한 유형의 차량 클라우드는 모바일 클라우드의 확대된 개념으로 볼 수 있으며 현재 관련 업계에서는 카 클라우드(Car Cloud)라 부르기도 한다. 인터넷 기반의 클라우드에 차량의 관리와 운행에 필요한 정보뿐만 아니라 멀티미디어 콘텐츠 등을 저장해두고 운전자가 필요 시 자신이 보유한 자동차나 휴대용 스마트 단말기를 통해 다운로드하여 활용하는 서비스 모델을 제시하고 있다.

2.2 차량 클라우드 아키텍처

차량 클라우드 아키텍처는 차량 클라우드, 노변 클라우드, 중앙 클라우드 이렇게 세 가지로 구성할 수 있다[4]. 그림 2는 클라우드 기반의 차량 네트워크 구조를 보여주고 있다.

2.2.1 차량 클라우드

그림 2에서 차량 클라우드는 차량들의 컴퓨팅 자원과 스토리지 자원을 공유하는 목적을 가진 차량들로 구성된 클라우드로, 차량과 차량 간의 통신으로 형성된다. 차량 클라우드는 개인 차량과 비교해서 훨씬 더 많은 자원을 보유하고 있다는 이점이 있으며, 각 차량은 클라우드에 접속해 서비스를 이용할 수 있다.



〔그림 2〕 클라우드 기반의 차량 네트워크 구조

2.2.2 노변 클라우드

인접한 노변 장치들로 구성된 노변 클라우드(Roadside Cloud)는 차량과 노변 장치간의 통신으로 접근할 수 있다. 노변 클라우드는 로컬 서버와 노변 장치 두 부분으로 구성되어 있으며, 로컬 서버는 물리적 자원의 가상화와 클라우드 장소로의 기능을 하고, 노변 장치는 차량이 클라우드에 접속할 수 있도록 무선접속 인터페이스를 제공한다. 노변 클라우드는 통신 범위가 제한되어 있기 때문에 한정된 범위 내에서만 접속이 가능하다.

2.2.3 중앙 클라우드

인터넷을 이용한 전용 서버로 구성된 클라우드로 차량은 차량과 노변 장치간의 통신 또는 무선 통신을 이용해서 중앙 클라우드(Central Cloud)에 접속할 수 있다. 중앙 클라우드는 차량 클라우드, 노변 클라우드와 비교해서 더 많은 자원을 가지고 있으며, 복잡한 계산 및 방대한 데이터 처리를 위해서 사용된다.

Ⅲ. 차량 클라우드 서비스 모델

대부분의 차량은 하루 중 많은 시간을 도로, 차고, 주차장에서 보내는데, 이때 사용되지 않는 컴퓨터 자원과 스토리지 자원이 잘 활용되지 못하고 낭비되고 있다. 차량 클라우드 서비스는 이렇게 낭비되고 있는 자원을 다른 차량에게 클라우드 컴퓨팅 서비스 형태로 제공해 줄 수 있다〔5〕. 그림 3은 차량 클라우드 컴퓨팅의 특징 및 서비스 모델에 대해 보여주고 있으며, 차량 클라우드를 위해 논의되고 있는 서비스 모델은 다음과 같다.

3.1 Network as a Service

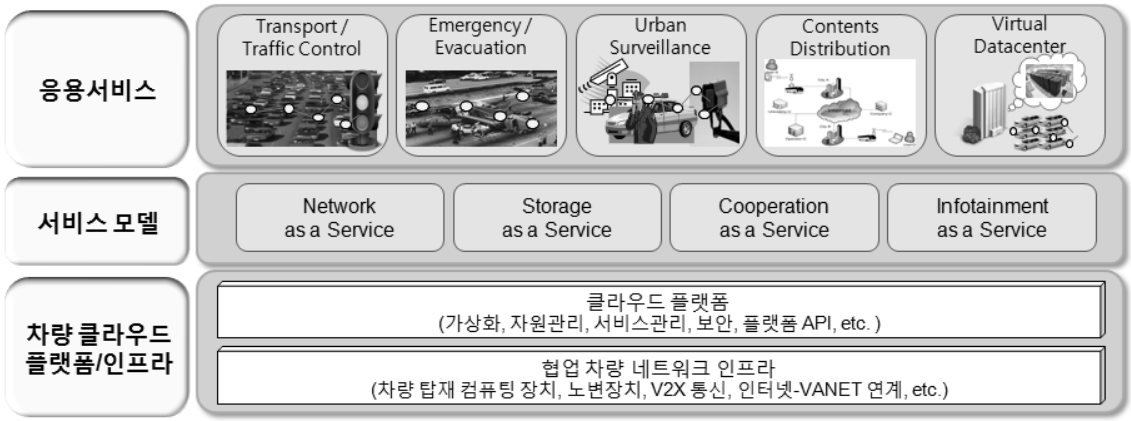
도로 위의 대부분의 차량은 인터넷 접속이 가능하지 않지만, 일부 가능한 차량도 있다. NaaS(Network as a Service)는 인터넷 접속이 가능한 차량이 운행 중에 자신의 유휴 네트워크 자원을 이 네트워크 연결이 필요한 차량에게 할당하여 네트워크 서비스를 제공해 주기 위한 모델이다.

3.2 Storage as a Service

도로 위의 일부 차량은 충분한 스토리지 자원을 가지고 있다. 그 외, 다른 차량은 자신의 응용 소프트웨어를 실행시키기 위한 추가적인 저장 공간이 필요할 수 있다. 이때 충분한 스토리지 자원을 가지고 있는 차량이 자신의 여분의 자원을 이용해 스토리지 서비스를 제공해 줄 수 있는데, 이러한 모델이 STaaS(Storage as a Service)이다.

3.3 Cooperation as a Service

차량 네트워크는 운전자의 안전과 관련된 서비스를 포함하여, 교통 정보, 교통 혼잡과 사고에 대한 경고, 날씨와 도로 상황 알림과 같은 다양한 서비스를 제공한다. 현재, 지능형 교통시스템인 ITS가 이러한 서비스를 제공해 주고 있지만, 비용관련 문제로 인해서 새로운 방안을 제안했다. CaaS(Cooperation as a Service)는 커뮤니티 서비스의 새로운 유형으로, 노변 장치와 같은 최소한의 기반 시설이 갖춰져 있는 경우에는 이를 이용해서 운전자에게 서비스를 제공해주고, 만약 갖춰져 있지 않



〔그림 3〕 차량 클라우드 컴퓨팅의 특징 및 서비스 모델

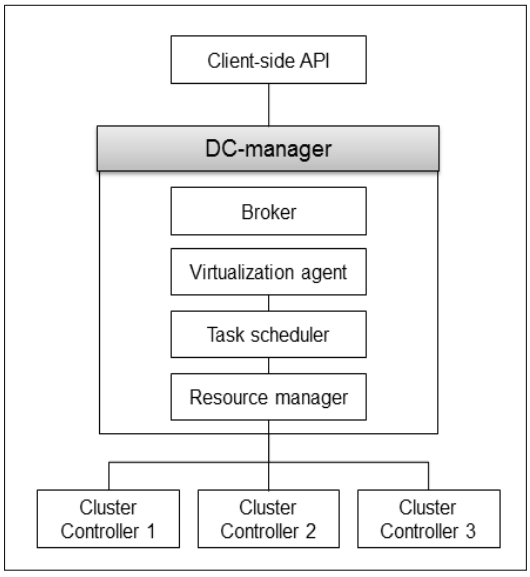
다면, 차량 간의 통신을 이용해서 서비스를 제공해 줄 수 있다.

Ⅳ. 차량 클라우드 활용 방안

본 장에서는 차량 클라우드의 예상 활용 방안에 대해서 소개한다.

4.1 차량 클라우드를 이용한 데이터 센터

오늘날 우리 주변의 차들은 실제로 운행되는 시간보다 주차되어 있는 시간이 더 많다. 이렇게 주차되어 있는 차량들을 활용하여 데이터 센터로 이용할 수 있다. 예를 들면, 공항에서 비행기를 타고 여행을 다니는 동안 그들의 차량은 오랜 기간 동안 공항에 주차되어 있을 것이다. 공항 주차장에 주차되어 있는 차량으로 차량 클라우드를 구축하여 하나의 데이터 센터로 이용할 수 있다. 물론, 공항은 차량 클라우드에 참여하는 차량에 인터넷과 전력을 제공해야하고, 차량 클라우드에 참가 할 의사가 있는 차량에게는 무료 주차와 같은 금전적인 보상을 해줄 필요가 있다. 주차장과 쇼핑몰에 있는 차량도 동일하게 적용될 수 있다[5, 6].



〔그림 4〕 공항 데이터 센터 구조

Arif 등은 공항에 주차되어 있는 차량들을 데이터 센터로 이용하기 위한 데이터 센터 구조를 제안하였다. 그림 4는 Arif 등이 제안한 데이터 센터 구조의 구성 요소로, broker는 클라우드 서비스를 요청하는 잠재적인 고객과 협상하고, 실현 가능한 요청을 수락할 수 있다. virtualization agent는 이용 가능한 클라우드 자원을 구성한다. resource manager는 클라우드 자원을 발견하고, 운영을 담당한다. task manager는 각 클러스터에게 계산 작업을 할당한다[7].

4.2 교통량 관리

4.2.1 교통 신호 관리

대부분의 교통 신호 시스템은 시간 간격이 사전에 정의되어 있는데 이러한 시스템은 두 가지 단점이 있다. 첫째, 적절한 신호 시스템 설계를 위해서 주기적으로 교통량이 수집 되어야 하고, 두 번째로는 이렇게 사전에 시간 간격이 정해져 있는 시스템은 교통사고를 포함한 예상치 못한 교통 환경에 잘 적응할 수 없다. 이 결과로 인해서 교통체증이 발생하고, 도로는 혼잡해진다. 이에 대한 해결 방안으로 차량에 탑재 되어 있는 컴퓨터를 이용해서 현재의 교통 상황을 클라우드 서버에 전송하고, 교통 신호를 상황에 맞게 효율적으로 변경하여 원활한 교통 환경을 조성할 수 있다[5].

4.2.2 특수한 상황에서의 교통량 관리

매년 콘서트, 스포츠 경기 같은 엄청나게 많은 수의 대규모 이벤트가 열린다. 이벤트가 끝나면 사람들은 가능한 빨리 떠나려고 할 것이다. 이때 교통체증이 발생하게 되는데, 평소의 정적인 교통 신호 동기화 시스템은 이 상황을 악화시킨다. 시당국에서는 교통체증을 완화시키기 위해 신호를 재조정할 수 있다. 시당국은 신호를 재조정할 프로그램을 실행시키기 위해서 필요한 컴퓨터 인프라를 가지고 있지 않지만, 차량 클라우드를 통해서 자원을 제공받을 수 있다[5]. 시당국은 이 같은 특수한 경우를 제외하고 대부분의 시간 동안 사용되지 않을 비싼 컴퓨터 시설을 구입할 필요가 없다.

4.3 도시 감시

비디오카메라와 센서 등을 이용한 주변 환경 관찰과 감시는 도심지에서 중요한 역할을 한다. 가로등, 카메라, 센서가 갖춰져 있는 도시 환경과 전원 공급의 제한이 없는 차량의 특징으로 인해서, 차량은 도시를 감시하기에 이상적인 도구이다. 오늘날 대부분의 차량에는 GPS 장치와 카메라가 장착되어 있는데, 이 장치들을 이용하여 도시에서 일어나는 위험한 일들을 방지하거나, 사고가 발생한 뒤, 당시의 증거를 찾는데 이용할 수 있다[8].

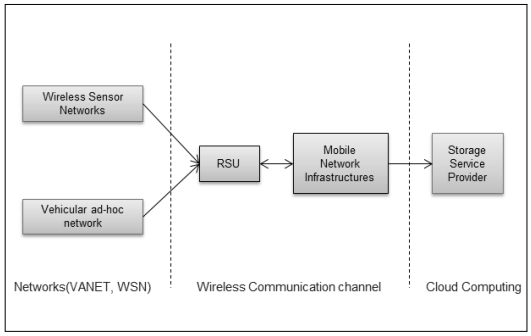
Gerla 등은 클라우드 서버를 이용한 사진 감시 시스템을 제안하였다[9]. 이 감시 시스템에서는 사진을 제공해주는 차량과 서비스를 이용하고는 고객, 두 분류로 나눌 수 있다. 사진을 제공해 주는 차량은 클라우드 서버에 차량과 위치를 등록하고, 일정한 간격으로 현재 위치를 업데이트 한다. 고객은 클라우드 서버에 자신이 원하는 사진의 위치와 그 시간대를 포함한 메시지를 보내서 서비스를 요청하면, 클라우드 서버는 그 조건에 맞는 차량을 검색한다. 그리고 조건과 일치하는 차량을 찾으면 그 차량에서 찍은 사진을 고객에게 전달해 준다.

4.4 재난 상황 관리

허리케인과 같은 자연 재해가 발생했을 때, 사람들은 휘발유, 식수, 의료 물품, 대피처와 같은 이용 가능한 자원을 찾을 것이다. 만약 재해가 발생하면, 응급 상황 관리자와 차량 클라우드를 구축한 차량 간의 통신을 통해서 대피하는 피난민들에게 최신 관련 정보를 제공해 주거나 현재 대피 상황으로 인한 교통 정보를 클라우드 서버로 전달할 수 있다. 이 상황에서는 전력과 네트워크 연결이 가능하다고 가정한다[5].

Ⅴ. 차량 클라우드의 보안 이슈 분석

차량 클라우드는 VANET, MANET(Mobile ad hoc network), WSN(Wireless Sensor Network), 클라우드 컴퓨팅과 같은 다양한 네트워크 기술이 결합된 새로운 기술이다. 무선 또는 유선 네트워크에서 같은 공간에 있는 자원을 공유하는 사용자들의 보안과 프라이버시는 가장 중요한 문제다. 그림 5는 차량 클라우드에서의 데이터 전송흐름을 보여주고 있는데, VANET, WSN을 이용해서 주변 환경으로부터 정보와 이벤트를 수집하고, 이 정보를 무선 통신 채널을 이용해서 클라우드로 전송한다. 이와 같은 흐름으로 데이터 전송이 일어나기 때문에 네트워크 계층, 전송 계층, 클라우드 컴퓨팅 모두 보안이 제공되어야 한다[6].



〔그림 5〕 차량 클라우드에서의 데이터 전송

5.1 차량 클라우드 보안 위협

차량 클라우드는 일반적인 인터넷 클라우드와 다른 특성을 가지고 있기 때문에 보안에 더 취약하다. 표 1은 차량 클라우드의 특징과 이로 인해서 발생하는 보안 관련 문제점을 나타내었다. 차량 클라우드의 보안 위협은 다음과 같이 나눌 수 있다[5].

- 사용자 신분 속이기 : 차량 클라우드는 인가된 사용자에게 서비스를 제공해 줄 수 있는데, 공격자는 자신의 신분을 속여서 차량 클라우드에 접속해 불법적으로 데이터를 획득하거나 불법적인 이점을 얻을 수 있다.
- 데이터 및 메시지 위변조 : 차량 클라우드에서 노드들 간 메시지를 전송할 때, 공격자는 중간에서 메시지 내용을 수정, 위조하고 다른 노드들에게 위변조된 메시지를 전송해서 피해를 줄 수 있다. 그리고 차량 클라우드는 차량의 공유된 자원을 고객에게 제공해 줄 수 있는데, 이때 공격자는 다른 차량의 데이터에 접근해서 내용을 변경할 수 있다.
- 부인 : 공격자는 차량 클라우드에서 노드들 간 전송되는 메시지를 위변조하고 다른 노드들에게 전송해 피해를 줄 수 있다. 나중에 이러한 사실이 드러났을 때, 공격자는 이를 부인 할 수 있다.
- 정보 폭로 : 공격자는 차량 클라우드 서비스를 제공하는 차량에 접속해서 민감한 정보를 노출 시킬 수 있다.

〔표 1〕 차량 클라우드의 특징과 보안 문제점

특징	보안 문제점
높은 이동성	차량은 빠른 속도로 이동하기 때문에 차량과 차량 소유주에 대한 인증에 어려움이 있다.
다수의 네트워크 노드	차량 클라우드는 수많은 차량과 노드들로 이루어져 있기 때문에 네트워크 규모가 크다. 이로 인해서 노드들 간의 신뢰 관계 설립에 어려움이 있다.
위치기반 서비스	대부분의 차량 클라우드 서비스는 위치정보에 의존하기 때문에 차량의 위치정보가 노출될 우려가 있다.
이질성	차량 마다 서로 다른 장치와 서비스를 제공하기 때문에 보안에 관련된 문제가 발생할 수 있다.

5.2 차량 클라우드 보안 요구 사항

차량 클라우드의 보안 위협을 방지하기 위해서는 다음과 같은 보안 요구사항을 만족하여야 한다[3, 10].

- 인증 : 차량 클라우드에서 인증은 사용자 신분과 메시지 무결성을 증명하는 것을 포함한다. 차량은 빠른 속도로 이동한다는 특징이 있으며, 위치가 계속 변하기 때문에 차량과 차량 소유주를 인증하는데 어려움이 있다.
- 프라이버시 보호 : 교통량 관리, 감시 시스템 등 차량 클라우드를 이용한 대부분의 서비스는 차량의 정확한 위치정보에 의존한다. 차량은 자신의 위치정보를 클라우드 서버 또는 차량 클라우드 서비스 고객에게 지속적으로 제공 하는데, 이때 자신의 위치정보가 공개되는 문제가 발생할 수 있다. 그리고 차량과 차량 소유주의 인증을 위해서 자신의 개인정보를 제공해야 하는 경우에도 자신의 개인정보가 공개되는 문제가 발생할 수 있다.
- 무결성 : 차량을 이용한 감시 시스템에서 차량은 장착된 카메라를 통해서 주변 환경을 계속 촬영할 수 있다. 만약 사고가 발생했을 경우에는 이전에 촬영한 자료가 당시의 증거자료로 사용될 수 있는데, 이 증거자료는 변경되지 않아야 하기 때문에 무결성이 보장되어야 한다.

- 데이터 보호 : 차량 클라우드는 차량의 공유된 자원을 제공해 줄 수 있는데, 이때 데이터 보호의 제약사항이 없다면 차량은 다른 차량의 데이터에 접근하거나 내용을 변경하여 저장할 수 있다. 그러므로 민감한 데이터가 인가되지 않은 사용자로부터 보호되기 위해서는 암호화되어야 한다[6]. 그리고 주차되어 있는 차량을 데이터 센터로 이용하는 경우, 고객들은 차량 클라우드로 구축된 데이터 센터에 접속하여 서비스를 제공 받을 수 있다. 서비스를 제공 받고 난 뒤에는 고객의 개인정보 같은 민감한 데이터가 남아 있을 수도 있다. 이 같은 경우, 고객에게 서비스를 제공하고 난 뒤, 남아 있는 모든 데이터를 삭제처리 해야 할 필요가 있다.

Ⅵ. 결 론

본 논문에서는 차량 클라우드의 유형 및 아키텍처, 서비스 모델, 차량 클라우드의 활용 방안에 대해서 소개하였고, 이에 관련된 보안 위협과 보안 요구사항에 대해서 기술하였다. 최근 몇 년간 차량 네트워크 및 차량 통신보안 기술에 대한 연구가 활발히 진행되었으나, 차량 클라우드 컴퓨팅 보안기술에 대한 연구는 미비하다. 그러므로 차량 클라우드 컴퓨팅 환경의 특성 및 서비스를 고려한 특화된 보안기술의 연구가 필요하다. 따라서 향후 도입이 예상되는 차량 클라우드 서비스를 안전하게 사용하기 위해서는 본 논문에서 제안한 보안 요구사항에 대한 연구가 이루어져야 할 것으로 사료된다.

참 고 문 헌

[1] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, 15(1), pp.39-68, 2007.

[2] S. Olariu, M. Eltoweissy, and M. Younis, "Towards autonomous vehicular clouds," ICST Transactions on Mobile Communications and Applications, 11(7-9), 2011.

[3] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security Challenges in Vehicular Cloud Computing," IEEE Transactions on Intelligent Transportations System, 14(1), pp.284-294, 2013.

[4] R. Yu, Y. Zhang, S. Gjessing, W. Xia and K. Yang, "Toward Cloud-Based Vehicular Networks with Efficient Resource Management," Network, IEEE, 27(5), pp.48-55, 2013.

[5] S. Olariu, T. Hristov, and G. Yan, "The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds," Mobile Ad Hoc Networking: Cutting Edge Directions, Second Edition, John Wiley & Sons, Inc., 2013.

[6] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," Journal of Network and Computer Applications, 40, pp.325-344, 2013.

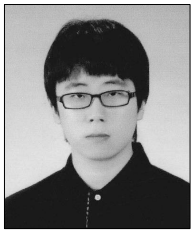
[7] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang and I. Khalil, "Datacenter at the Airport: Reasoning about Time-Dependent Parking Lot Occupancy," IEEE Transactions on Parallel and Distributed Systems, 23(11), pp.2067-2080, 2012.

[8] M. Gerla, "Vehicular Cloud Computing," Ad Hoc Networking Workshop, pp.152-155, 2012.

[9] M. Gerla, J. T. Weng and G. Pau, "Pics-On-Wheels: Photo Surveillance in the Vehicular Cloud," 2013 International Conference on Computing, Networking and Communications, pp.1123-1127, 2013.

[10] G. Yan, D. B. Rawat and B. B. Bista, "Toward secure vehicular Clouds," 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems, pp.370-375, 2012.

〈저 자 소 개〉



허 명 학 (Myeonghak Heo)
학생회원

2013년 8월 : 동명대학교 정보보호학과 졸업
2014년 3월~현재 : 부경대학교 대학원 정보보호학협동과정 석사과정
관심분야 : 클라우드 보안, 애드 혹 네트워크 보안

이 경 현 (Kyung-Hyune Rhee)
종신회원

1982년 2월 : 경북대학교 수학교육과 졸업
1985년 2월 : 한국과학기술원 응용수학과 석사
1992년 2월 : 한국과학기술원 수학과 박사
1993년~현재 : 부경대학교 IT융합응용공학과 교수
관심분야 : 정보보호, 암호론, 암호 프로토콜, 차량통신 보안, 애드 혹 네트워크 보안, 멀티미디어 보안