카 쉐어링 환경에서 클라우드 서비스 브로커 기반 안전한 통합 인증기법 설계

박상현*, 정하규*, 김형주**, 김은환***, 전문석*
*숭실대학교 컴퓨터학과
**KT R&D Center
**숭실대학교 평생교육원
e-mail:shyeon15@ssu.ac.kr

Design of Secure Authentication Scheme based on Cloud Service Broker in Car-sharing Environment

Sanghyeon Park*, Hague Chung*, Hyungjoo Kim**, Eun-Hwan Kim***, Moon-Seog Jun*
*Dept. of Computer Science & Engineering, Soongsil University
**KT R&D Center
***Department of Computer Engineering, Soongsil University Life-Long Education

요 약

카 쉐어링 서비스는 경제위기 이후 실용적 소비패턴 의식의 확산과 환경의식의 고취, 스마트폰 확산을 통한 서비스 이용 편의성이 증가됨으로 인해 새로운 대중교통으로 자리매김을 하고 있다. 시장이 발전하고 많은 사람들이 이용하면서 다양한 카 쉐어링 업체들이 생겨나고 있다. 또한 각 업체들에서 사용하는 인증방식은 단순 ID/PW 로그인 방식이기 때문에 보안에 취약하다. 본 논문에서 제안하는 모델은 차량의 데이터가 등록되어 있는 다양한 업체들의 클라우드를 클라우드 서비스 브로커를 통해 사용자들에게 편리성을 제공하고 바이오정보를 이용하여 더욱 강력한 인증을 통해 안전한 서비스를 제공하고자 한다. 본 논문에서 제안한 모델을 통해 안전한 토인과 사용자의 편의성이 증대되기를 기대한다.

1. 서론

카 쉐어링 서비스는 자동차와 IT 산업간 컨버전스 서비스이다[1]. 자동차에 무선통신, 결제 서비스 등을 결합함으로써 365일 24시간 무인서비스가 가능해짐으로 인해 카 쉐어링 서비스가 본격화 되었다. 카 쉐어링 서비스는 각 업체들의 클라우드로부터 회원들이 자동차가 필요할 때마다 시간별로 예약을 통해 차량을 공동으로 이용할 수 있는 초 단기 차량렌트 사업이다. 카 쉐어링 서비스는 친환경 소비심리, 실용적 소비패턴 의식의 확산, 비용절감, 스마트폰 확산을 통한 서비스 이용의 편리함 등의 이유로 시장이 빠르게 커지고 있고 북미와 유럽을 중심으로 빠르게 성장중이다[2]. 카 쉐어링 서비스가 성장함에 따라 다양한 카 쉐어링 업체들이 생겨나고 있지만 각 업체들은 자신들만의 고유한 차량을 제공하기 때문에 사용자들은 다양한 업체에 가입을 해야한다. 또한 각 업체들은 사용자의 인증을 단순한 ID,PW 방식만 이용하기 때문에 다양한 곳에서 많은 위협을 받게 된다. 본 논문에서는 이러한 문제점을 해결하기 위하여 클라우드 서비스 브로커를 이용한 통합 인증을 통해 다양한 업체를 한번의 인증을 통하여 사용할 수 있고, 또한 보안성 향상을 위해 사용자 고유의 바이오정보와 ID,PW 방식을 이용한 인증을 제안한다.

본 논문은 2장에서 클라우드 서비스 브로커, 바이오 인증에 대해 설명하고 3장에서 제안하는 통합 인증모델에 대해 기술한다. 4장에서 결론을 맺는다.

2. 관련연구

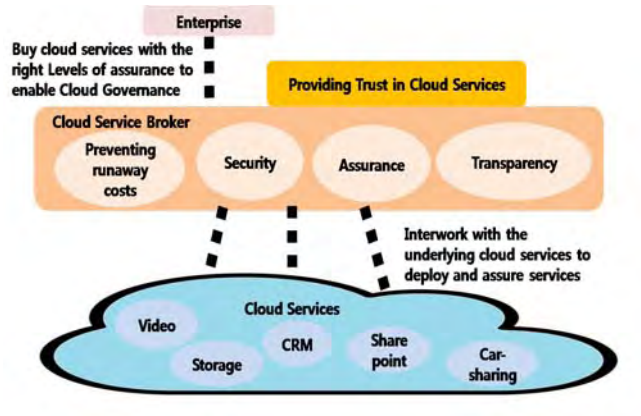
2.1 클라우드 서비스 브로커

클라우드 브로커 환경은 그림1과 같이 클라우드에서 제공하는 서비스들과 클라우드 서비스 프로커, Enterprise로 구성되어 있다[3]. 클라우드 브로커는 사용자와 서비스 제공자 사이에서 서비스를 중재하고, 클라우드 사용자에게 서비스 제공자의 서비스를 기반으로 서비스를 제공해주고, 사용자의 요구사항에 맞춰 최적의 클라우드 서비스를 제안, 선정하고, 다양한 클라우드 서비스의 활용, 성능 관리 및 서비스 제공을 담당한다.

3. 제안

제안하는 카 쉐어링 환경에서 브로커를 이용한 간편한 인증 기법은 사전에 각 서비스 프로바이더와 브로커, 유저와 서비스 프로바이더 간에 상호 등록이 되어있고 브로커와 서비스프로바이더는 비밀키를 나눠가지고 차량과 서비스 프로바이더간에는 안전한 채널이라고 가정한다. 또한 바이오정보는 사전에 CA에 등록 되어있고 바이오 정보는

세션키를 만드는데 이용되기 때문에 브로커나 여타 서비스 프로바이더 측에서 알 수 없다.

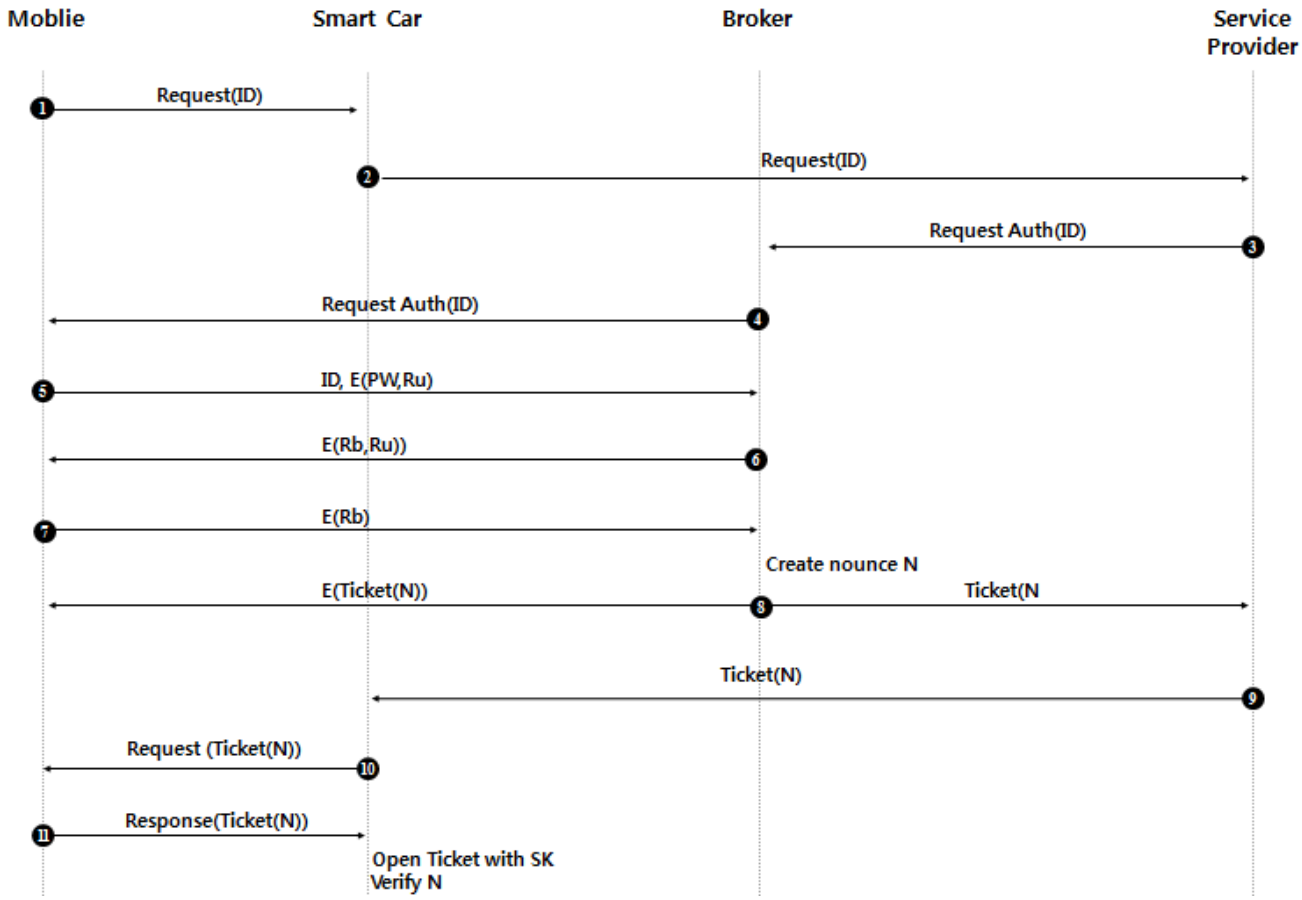


(그림 1) 클라우드 브로커 모델

게 된다. 각각 사전에 등록이 되있고 제 3의 인증기관으로부터 받은 정보를 가지고 세션키를 만들었기 때문에 상호인증이 완료될 수 있다. 그 이후 브로커에서 또 다른 랜덤값 N을 생성하여 Ticket에 넣어 보낸다. 서비스 프로바이더를 통해 티켓은 차량에 전달되고 차량에서 사용자의 티켓의 유효성을 확인 후 차량을 이용한다.

4. 결론

카 쉐어링에서의 인증은 권한이 없는 사용자에 의해 정당한 사용자가 금전적 피해를 볼 수 있을 뿐 아니라 운전능력이 없는 사용자의 운전으로 인해 불특정 다수에게 피해가 갈 수 있기 때문에 안전한 인증이 필요하다. 사용자들의 편리함을 위해 한 업체의 차량뿐 아니라 다른 업체의 차량도 이용하기 위해 브로커 기반 서비스를 제공하고자한다.



(그림 2) 제안 프로토콜

그림 2는 사용자가 모바일 디바이스를 이용해 SP에서 제공하는 차량을 이용하기 위해 인증하는 프로토콜이다. 1번부터 7번까지는 사용자의 인증 과정이다. 사용자는 인증요청을 받은 후 사전에 등록한 바이오정보를 이용 키를 생성 브로커도 같은 방식으로 키를 생성, 이후 유저와 브로커는 챌린지 리스폰스 방식을 통해 유저인증을 완료하

참고문헌

[1] Boyacı, Burak, Konstantinos G. Zografos, and Nikolas Geroliminis. An optimization framework for the 2 development of efficient one-way car-sharing systems. European Journal of Operational Research 240.3 3 (2015) 718-733.

[2] Shaheen, Susan A., and Nelson D. Chan. "Evolution

of E-Mobility in Carsharing Business Models." Electric 5 Vehicle Business Models. Springer International Publishing, 2015. 169-178.
[3] Huang, He Yuan, et al. "Identity federation broker for service cloud." 2010 International Conference on Service Sciences. IEEE, 2010.