AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Computer Engineering and Systems

A Secure Architecture for Vehicular Cloud Computing

A Thesis submitted in partial fulfillment of the requirements of the degree of Doctor of Philosophy in Electrical Engineering
(Computer Engineering and Systems)

by

Marvy Badr Monir Mansour

Master of Science in Electrical Engineering
(Computer Engineering and Systems)
Faculty of Engineering, Arab Academy for Science,
Technology and Maritime Transport, 2013

Supervised By

Prof. Hoda Korashy Mohamed
Professor at Computer Engineering and Systems, Ain Shams University

Prof. Sherif Ali Mohamed Hammad
Professor at Computer Engineering and Systems, Ain Shams University

Dr. Cherif Ramzi Salama
Lecturer at Computer Engineering and Systems, Ain Shams University

Cairo – (2018)

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Computer and Systems

A Secure Architecture for Vehicular Cloud Computing

by

Marvy Badr Monir Mansour

Master of Science in Electrical Engineering

(Computer Engineering and Systems)

Faculty of Engineering, Arab Academy for Science,
Technology and Maritime Transport, 2013

Examiners' Committee

Name and Affiliation	**Signature**
Prof. Ahmed Fahmy Amin Mahrous Computer and Systems , Arab Academy for Science, Technology and Maritime Transport	……………………
Prof. Mohamed Watheq Ali El-Kharashi Computer and Systems , Ain Shams University	……………………
Prof. Hoda Korashy Mohamed Computer and Systems , Ain Shams University	……………………
Prof. Sherif Ali Mohamed Hammad Computer and Systems , Ain Shams University	……………………

Date: 14 July 2018

Statement

This thesis is submitted as a partial fulfillment of Doctor of Philosophy in Electrical Engineering, Faculty of Engineering, Ain Shams University.

The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Marvy Badr Monir Mansour

Signature

……………………………………………...

Date: 14 July 2018

Researcher Data

Name	: Marvy Badr Monir Mansour
Date of birth	: 7th of February 1985
Place of birth	: Cairo, Egypt
Last academic degree	: Master of Science
Field of specialization	: Electrical Engineering
University issued the degree	: Arab Academy for Science, Technology and Maritime Transport
Date of issued degree	: 2013
Current job	: Assistant Lecturer

Thesis Summary

Vehicular Ad-hoc Networks (VANETs) are a kind of networks that have two main types of communication V2V and V2I, which are vehicle–to–vehicle and vehicle–to–infrastructure respectively. VANET is one of the promising areas for the creation of Intelligent Transportation System (ITS) to provide both safety and comfort for vehicle drivers. Recently, various technologies have evolved for VANETs to accommodate a wide range of driver needs. One of these technologies is known as Vehicular Cloud Computing (VCC), which is designed to enable drivers to access a wide variety of Cloud services while driving. VCC is an emerging technology that vehicle drivers use for different applications, such as Location-Based Service (LBS) applications that require from the vehicles to send frequent location updates to LBS Providers for real-time services.

Thus, the specific nature of VCC brings up the need to address necessary security and privacy issues for VCC to be integrated into the social life. Moreover, VCC imposes some security and privacy challenges for drivers, such as: sender location privacy and identity anonymity. Also, some VCC attacks emerge while using Location-Based Services (LBSs) offered by semi-trusted LBS Providers, such as: location tracking and user identification of drivers that breach users' privacy. At the time when this thesis was written, the applications both safety-related and convenience-related were either under development or in initial stages since VANET system and VCC as a whole are yet to be implemented. Therefore, this thesis is dedicated to provide a secure architecture for a user that mitigates the existing VCC attacks while using LBS applications located in a Cloud.

In this thesis, we propose a secure and privacy-preserving robust system for Vehicular Cloud Computing environment in order to solve the previous problems. Our proposed system offers a wide variety of state-of-the-art security services needed by drivers when using LBS applications, while avoiding any conflicts between user requirements of security and privacy. Our system consists of four main phases: Vehicle Bootstrapping Phase, Vehicle and LBS Provider Certificate Provisioning Phase, Vehicle and LBS Provider Certificate Revocation Phase, and finally the LBS Request in Vehicular Cloud Computing Phase. In our system, we use a novel idea that allows a Road-Side Unit (RSU) to form cluster containing all vehicles within its coverage range, and to act as the Cluster Head of cluster formed. Also, we introduce to use RSU Clouds and Roadside Unit-to-Roadside Unit (R2R) communication in the RSU Cloud, which are needed for LBS applications to guarantee service delivery for vehicles. Also, we include in our protocol a novel Reward System that is used to reward or penalize vehicles while using LBS applications, and to determine Trust Level of an LBS Provider. In addition, our system includes a novel Certificate Revocation mechanism for both vehicles and LBS Providers, where unconditional anonymity is preserved for reporter.

Finally, we present a detailed security and privacy analysis for our proposed system, and show that it is capable of maintaining the security and privacy of drivers while offering a strong protection against a wide range of VCC attacks. Also, we show that our proposed system provides protection against both internal and external system attacks. In addition, we provide some calculations that show that our system provides low storage, communication and computation overhead as compared to other existing approaches. Furthermore, we demonstrate the applicability of our system of providing security and privacy to vehicles in real-life scenarios while thwarting well-known VCC attacks, and so breaking the zero-sum game between providing the needed Quality-of-Service (QoS) and preserving the driver’s security and privacy.

Keywords: Certificate Provisioning in VANET, Certificate Revocation in VANET, LBS Request in Vehicular Cloud Computing, Location Privacy, Security and Privacy in VANET, Security and Privacy Techniques in Vehicular Cloud Computing, Vehicle Tracking.

Acknowledgement

First of all, I thank **GOD** for helping me throughout this thesis.

It is my pleasure to thank my great supervisors who made this dissertation possible. First, I am deeply grateful for **Prof. Hoda Korashy**, whose direct supervision, precious advices and encouragement has got this work started and accomplished in its full potential. Also, I own my great gratitude to **Prof. Sherif Hammad**, whose valuable suggestions, guidance and support throughout this work have brought this thesis to a high standard. In addition, I am very thankful to **Dr. Cherif Salama** for his thoughtful ideas and insightful comments during this thesis that have helped in achieving this work. It is worth to acknowledge that working with my supervisors was a pleasure where I have benefited from their great experience.

Besides that, I am very grateful to my **parents** for their continuous encouragement and support. They gave me precious suggestions for my life and study, and taught me to achieve excellence throughout my study.

July 2018

Table of Contents

List of Figures