



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**

<b>Name and Affiliation</b>	<b>Signature</b>
<b>Prof. Ahmed Fahmy Amin Mahrous</b> Computer and Systems , Arab Academy for Science, Technology and Maritime Transport	.....
<b>Prof. Mohamed Watheq Ali El-Kharashi</b> Computer and Systems , Ain Shams University	.....
<b>Prof. Hoda Korashy Mohamed</b> Computer and Systems , Ain Shams University	.....
<b>Prof. Sherif Ali Mohamed Hammad</b> 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	: 7 <sup>th</sup> 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

## Thesis Summary

---

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.

## Thesis Summary

---

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

---

Thesis Summary.....	iv
Acknowledgement.....	vii
Table of Contents.....	viii
List of Figures.....	xiii
List of Tables.....	xxvi
List of Abbreviations.....	xxviii
<b>1. Chapter ONE: Introduction .....</b>	<b>1</b>
1.1 <b>Introduction to Wireless Ad-hoc Network .....</b>	<b>2</b>
1.2 <b>Introduction to VANET .....</b>	<b>5</b>
1.2.1   Overview of VANET .....	8
1.2.2   VANET Characteristics.....	10
1.2.3   VANET Applications .....	12
1.2.4   Overview of VANET Non-safety Applications .....	15
1.2.4.1   Non-safety Applications Analysis Framework .....	16
1.2.4.2   Examples of Non-safety Applications .....	18
1.2.5   VANET Challenges.....	24
1.3 <b>Problem Definition.....</b>	<b>24</b>
1.4 <b>Objectives of Thesis .....</b>	<b>26</b>
1.5 <b>Contributions of Thesis .....</b>	<b>28</b>
1.6 <b>Outline of Thesis .....</b>	<b>30</b>

## Table of Contents

---

<b>2. Chapter TWO: VANET Security and Privacy .....</b>	<b>34</b>
<b>2.1 Threat Model.....</b>	<b>36</b>
2.1.1 Types of Adversaries .....	37
<b>2.2 Security and Privacy Requirements.....</b>	<b>39</b>
2.2.1 Security Requirements.....	41
2.2.2 Privacy Requirements.....	44
2.2.3 Other System Requirements .....	46
<b>2.3 VANET Attacks and Attackers .....</b>	<b>48</b>
2.3.1 Types of Attacks.....	48
2.3.2 Types of Attackers.....	54
<b>2.4 Public Key Infrastructure .....</b>	<b>56</b>
2.4.1 Key Distribution .....	57
2.4.2 Trusted Parties .....	58
<b>2.5 Security-related VANET Projects.....</b>	<b>59</b>
2.5.1 IEEE 1609 standard for WAVE .....	60
2.5.2 Vehicle Safety Communications Project.....	60
2.5.3 PRESERVE Project.....	61
2.5.4 Other Projects .....	62
<b>3. Chapter THREE: Approaches for VANET Security and Privacy 65</b>	
<b>3.1 Approaches versus Security and Privacy Requirements .....</b>	<b>68</b>
3.1.1 Message Authentication and Privacy .....	68
3.1.1.1 Group Signature Scheme.....	69
3.1.1.2 Pseudonymous Authentication.....	71
3.1.2 Message Authentication and Data Integrity .....	75
3.1.3 Anonymity and Unlinkability.....	75
3.1.4 Accountability, Traceability and Non-Repudiation .....	76
3.1.5 Misbehavior Detection and Revocation .....	78

## Table of Contents

---

<b>3.2</b>	<b>Schemes based on Group Signatures .....</b>	<b>82</b>
3.2.1	GSIS: Secure Vehicular Communications with Privacy Preserving.....	83
3.2.2	Efficient and Robust Pseudonymous Authentication in VANET .....	85
3.2.3	Balanced Trustworthiness, Safety, and Privacy in V2V .....	88
3.2.4	Threshold Anonymous Announcement in VANET .....	91
<b>3.3</b>	<b>Schemes based on Pseudonyms .....</b>	<b>93</b>
3.3.1	Securing Vehicular Ad-hoc Networks.....	94
3.3.2	Efficient and Spontaneous Privacy-Preserving Protocol.....	98
3.3.3	Security Framework with Strong Non-Repudiation and Privacy.....	100
<b>3.4</b>	<b>Other Approaches.....</b>	<b>103</b>
3.4.1	Balancing Auditability and Privacy in Vehicular Networks .....	103
3.4.2	Trustworthy Privacy-Preserving Car-Generated Announcements.....	106
<b>3.5</b>	<b>Summary.....</b>	<b>106</b>
<b>4.</b>	<b>Chapter FOUR: A Secure Privacy-Preserving RSU-Aided System for VCC.....</b>	<b>111</b>
<b>4.1</b>	<b>Preliminaries .....</b>	<b>113</b>
4.1.1	Motivation of Proposed System .....	115
4.1.2	RSU Cluster Formation .....	116
<b>4.2</b>	<b>Outline of Phases of Proposed System .....</b>	<b>118</b>
<b>4.3</b>	<b>Description of Roles of Entities of Proposed System .....</b>	<b>121</b>
<b>4.4</b>	<b>Description of Phases of Proposed System .....</b>	<b>130</b>
4.4.1	Phase I: Vehicle Bootstrapping Phase.....	132

## Table of Contents

---

4.4.2	Phase II: Vehicle and LBS Provider Certificate Provisioning Phase.....	134
4.4.2.1	Vehicle Certificate Provisioning Process.....	134
4.4.2.2	LBS Provider Certificate Provisioning Process .....	141
4.4.2.3	Pseudonym Certificate Renewal .....	146
4.4.3	Phase III: Vehicle and LBS Provider Certificate Revocation Phase.....	147
4.4.3.1	Vehicle Certificate Revocation Process .....	148
4.4.3.2	LBS Provider Certificate Revocation Process .....	154
4.4.4	Phase IV: LBS Request in Vehicular Cloud Computing Phase.....	159
4.4.4.1	RSU Clouds.....	171
<b>4.5</b>	<b>Security and Privacy Analysis of Proposed System.....</b>	<b>171</b>
4.5.1	Security and Privacy Analysis of Proposed System Entities.....	172
4.5.2	Security and Privacy Considerations of Proposed System.....	175
4.5.3	Security Services versus System Attacks.....	176
<b>5.</b>	<b>Chapter FIVE: Performance Evaluation and Results.....</b>	<b>184</b>
<b>5.1</b>	<b>State-of-the-art Cryptosystems.....</b>	<b>186</b>
<b>5.2</b>	<b>RSA-based Cryptosystem.....</b>	<b>188</b>
<b>5.3</b>	<b>Cryptographic Overhead of Proposed System.....</b>	<b>190</b>
5.3.1	Cryptographic Overhead of Phase II for Vehicle and RSU .....	191
5.3.2	Cryptographic Overhead of Phase III for Vehicle and RSU.....	197
5.3.3	Cryptographic Overhead of Phase IV for Vehicle and RSU.....	202

## Table of Contents

---

5.3.4	Cryptographic Overhead of all System Phases .....	208
5.3.4.1	Cryptographic Overhead for a Vehicle .....	208
5.3.4.2	Cryptographic Overhead for a RSU .....	214
5.3.5	Average Cryptographic Overhead of all System Phases ...	221
5.3.5.1	Average Cryptographic Overhead for Vehicle and RSU .....	221
5.3.5.2	Average Cryptographic Overhead for a Vehicle.....	228
5.3.5.3	Average Cryptographic Overhead for a RSU .....	234
<b>5.4</b>	<b>Relationship between Overheads of Proposed Protocol Algorithms.....</b>	<b>241</b>
<b>5.5</b>	<b>Percentage Decrease of Overhead using L.S. Consideration.....</b>	<b>245</b>
<b>5.6</b>	<b>Overhead Comparison with other Approaches .....</b>	<b>249</b>
5.6.1	Overhead Comparison for a Vehicle .....	250
5.6.1.1	Percentage Decrease of Vehicle Overhead using Proposed System. ....	258
5.6.2	Overhead Comparison for a RSU .....	267
5.6.2.1	Percentage Decrease of RSU Overhead using Proposed System.....	272
<b>5.7</b>	<b>Security and Privacy Comparison with other Approaches.</b>	<b>276</b>
<b>6.</b>	<b>Chapter SIX: Conclusion .....</b>	<b>279</b>
<b>6.1</b>	<b>Summary and Outcomes .....</b>	<b>280</b>
<b>6.2</b>	<b>Future Work.....</b>	<b>283</b>
	<b>References.....</b>	<b>285</b>

---

# List of Figures

---

<b>Fig. 1.1.</b> Hierarchy of Wireless Networks.....	4
<b>Fig. 1.2.</b> Illustration of a VANET Model.....	6
<b>Fig. 1.3.</b> Illustration of VANET Communication .....	6
<b>Fig. 1.4.</b> Illustration of a Modern Smart Vehicle .....	8
<b>Fig. 1.5.</b> Categories of VANET Applications .....	13
<b>Fig. 1.6.</b> Examples of VANET Applications Scenarios .....	14
<b>Fig. 1.7.</b> Non-safety VANET Applications Analysis Framework .....	17
<b>Fig. 2.1.</b> Interrelations of security, privacy, and other system requirements. The “red-solid” are the “constraining” requirements and the “green-dotted” are the “supporting” requirements.....	40
<b>Fig. 2.2.</b> A forgery attack where A2 and A3 are colluding attackers that disseminate fake information in order to free the way of attacker A1 by affecting other vehicles’ (V) decisions.....	52

## List of Figures

---

<b>Fig. 2.3.</b> Illustration of Denial-of-Service Attack .....	52
<b>Fig. 2.4.</b> Illustration of a typical Sybil Attack .....	54
<b>Fig. 2.5.</b> Illustration of a typical Selfish Driver Attitude .....	55
<b>Fig. 3.1.</b> Vehicle <i>A</i> updates its pseudonym for each new message sent.....	72
<b>Fig. 3.2.</b> A <i>Mix-Zone</i> : two vehicles met at the same place, known as an intersection, at time $t_0$ .....	74
<b>Fig. 3.3.</b> A group of vehicles, $k$ -users, forming a $k$ -anonymous region.....	74
<b>Fig. 4.1.</b> Illustration of VANET Communications: V2V and V2I, R2R, RSU Cloud and RSU Cluster.....	118
<b>Fig. 4.2.</b> Illustration of Proposed System Entities.....	122
<b>Fig. 4.3.</b> Functions of Misbehaviour Authority (MA) in Vehicle Certificate Revocation Process.....	126
<b>Fig. 4.4.</b> Example of Phases II, III and IV of Proposed System.....	131
<b>Fig. 4.5.</b> Illustration of the System Entities involved in the Vehicle Certificate Provisioning Process.....	135
<b>Fig. 4.6.</b> Illustration of the Vehicle Certificate Provisioning Process .....	135