Sustainability **2015**, *7*, 2028-2044; doi:10.3390/su7022028

OPEN ACCESS

sustainability

ISSN 2071-1050

www.mdpi.com/journal/sustainability

Article

VCC-SSF: Service-Oriented Security Framework for Vehicular Cloud Computing

Won Min Kang [1], Jae Dong Lee [1], Young-Sik Jeong [2] and Jong Hyuk Park [1,3,*]

[1] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 139-743, Korea; E-Mails: wkaqhdsk0@seoultech.ac.kr (W.M.K.); jdlee731@seoultech.ac.kr (J.D.L.)

[2] Department of Multimedia Engineering, Dongguk University, Seoul 100-716, Korea; E-Mail: ysjeong@dongguk.edu

[3] Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology, Seoul 139-743, Korea

* Author to whom correspondence should be addressed; E-Mail: jhpark1@seoultech.ac.kr.

Academic Editor: Marc A. Rosen

Received: 20 December 2014 / Accepted: 6 February 2015 / Published: 13 February 2015

Abstract: Recently, as vehicle computing technology has advanced, the paradigm of the vehicle has changed from a simple means of transportation to a smart vehicle for safety and convenience. In addition, the previous functions of the Intelligent Transportation System (ITS) such as traffic accident prevention and providing traffic volume information have been combined with cloud computing. ITS services provide user-oriented broad services in the Vehicular Cloud Computing (VCC) environment through efficient traffic management, traffic accident prevention, and convenience services. However, existing vehicle services focus on providing services using sensing information inside the vehicle and the system to provide the service through an interface with the external infrastructure is insufficient. In addition, because wireless networks are used in VCC environments, there is a risk of important information leakage from sensors inside the vehicle, such as driver personal identification and payment information at the time of goods purchase. We propose the VCC Service-oriented Security Framework (VCC-SSF) to address the limitations and security threats of VCC-based services. The proposed framework considers security for convenient and efficient services of VCC and includes new user-oriented payment management and active accident management services. Furthermore, it provides authentication, encryption, access control, confidentiality, integrity, and privacy protection for user personal information and information inside the vehicle.

Keywords: vehicular cloud computing; payment service; accident management service

1. Introduction

The advancement of Intelligent Traffic Systems (ITS) technology now provides functions to prevent accidents for vehicles and pedestrians as well as quickly find destinations. Furthermore, it also provides conveniences such as public transportation arrival alarms, among others. In ITS, V2X communication (composed of Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Nomadic devices (V2N), and In-Vehicle Networking (IVN) communication) provides convenient services such as collision prevention, traffic lane maintenance, and traffic information collection through mobile terminals [1–4]. In order to provide convenience for the user, ITS is able to communicate between vehicles or between a vehicle and the infrastructure without network disconnection. For this communication, the Vehicular Ad hoc NETwork (VANET) protocol is used to minimize network disconnection caused by vehicle movement and to provide services to drivers or other users [5–8]. In addition, in the VANET environment, cloud computing provides services through the VANET routing protocol. However, message forgery, modification, and extortion by man-in-the-middle attacks are possible, and there is the possibility that a black hole attack could cause a fatal traffic accident. Furthermore, the existing services provided by intelligent traffic systems are applied only inside the vehicle, and studies on services that use traffic infrastructure are insufficient. Thus, we need to simultaneously provide user-oriented active services and secure important data.

Therefore, for secure Vehicular Cloud Computing (VCC), we propose the VCC Service-oriented Security Framework (VCC-SSF) in this paper. VCC-SSF provides the authentication, encryption, access control, and privacy protection required to protect private information, payment, and other important information inside the vehicle from security threats that may occur in the VCC environment. In addition, VCC-SSF includes a new active payment service that meets user requirements through the Payment as well as Accident Management Services to actively provide traffic accident prevention and accident response and management.

This paper is organized as follows: In Section 2, we describe the VCC's architecture and security requirements as well as review previous studies. Section 3 proposes the VCC-SSF architecture and application, and, in Section 4, the conclusion is presented.

2. Related Works

While previous ITSs established an overall communication infrastructure to provide traffic information as well as communication between vehicles or between vehicles and the infrastructure, ITS now has the goal of providing various services to drivers or pedestrians based on a communication infrastructure. In addition, it is combined with cloud computing technology to utilize storage embedded in the vehicle by the previous ITS, or processes sensitive information for use in traffic accident management and accident prevention [1,9,10]. In this section, we discuss the VCC and cloud computing architecture, VCC security requirements, and previous related works.

2.1. Architecture of VCC

The following description of VCC architecture is based on studies such as [1,11–13]. VCC architecture is composed of five layers: Physical, Communication, Cloud, Cloud Service, and VCC Application Layers.

The *Physical Layer* is divided into the traffic control center and transportation infrastructure that is installed on the road. The traffic control center manages the relationship between the vehicle and infrastructure and determines traffic conditions through periodic communication. In addition, it maintains a friendly relationship with services such as police, fire, and emergency services and copes quickly with any traffic accidents that may occur. The transportation infrastructure enables communications between the vehicle and itself. It collects traffic information such as the location of the vehicle or volume of traffic and transmits this collected information to the traffic control center and other vehicles. In addition, Wireless-Fidelity (Wi-Fi) is provided for drivers and pedestrians.

The *Communication Layer* includes all of the communication required by the VCC for communication between vehicles and between vehicles and the traffic infrastructure, as well as inside the vehicle. In addition, it manages periodic communication between objects. Particularly for communication inside the vehicle, the Communication Layer sends speed and location information, fuel status, driver behavior, driver health status, external environment information, *etc.* obtained from the sensors mounted in the vehicle to the Cloud Layer.

The *Cloud Layer* is composed of Cloud Storage to store data sent from the Communication Layer and the Cloud Server to process the data. Cloud Storage stores road traffic information, vehicle location, surrounding vehicle location information, and driver or user personal information. The Cloud Server processes the data in Cloud Storage for use in applications.

The *Cloud Service Layer* is combined of cloud computing technology to manage and enable services in the VCC environment. Cloud-based services in the vehicle computing environment are: Network as a Service (NaaS), Storage as a Service (SaaS), Cooperation as a Service (CaaS), and Computing as a Service (CompaaS).

The *VCC Application Layer* is the layer that manages the Cloud Service-based applications that can be applied to the VCC environment. Based on the internal and external information of a vehicle, it measures traffic volume and provides functions to prevent the vehicle concentration that often occurs in inner-city areas. In addition, it prevents accidents and manages emergency situations, parking, public transportation, *etc.*

2.2. Security Requirements for VCC

In the VCC environment, communications such as inside the vehicle, between vehicles, and between vehicles and the infrastructure utilize wired and wireless communications. Hence, there is a security threat in the existing VANET or cloud environment.

The essential security requirements for VCC based services are Confidentiality, Integrity, Availability, and Privacy Protection, which we discuss in detail as follows:

- **Confidentiality:** In a VCC environment, attackers can easily extort sensitive personal information such as the unique details of a vehicle or email address of driver, phone number, or residential address using man-in-the-middle (MITM) attacks. This is because the unique information of a vehicle or private information are used for application services, and in these cases, the attacker may tap the data using a Sniffing attack in-the-middle. Hence, this information should be encrypted to protect the data from MITM attacks.
- **Integrity:** Integrity should be provided for the information sent in a VCC environment. If the integrity of the driver's personal identification information, payment information, or location information is compromised by message forgery or a falsification attack, it could cause financial damage to the user or have fatal consequences in emergency situations. To defend against attacks on data integrity, important data should have its integrity guaranteed by hash functions and digital signatures.
- **Availability:** In VANET communication, a wireless network is used to communicate between vehicles. In the case of Cluster-based Routing (CBR), a header vehicle and adjacent vehicles form a cluster for mutual communication, and among these vehicles, a malicious user could interrupt or stop the service of the target vehicle with a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack such as Flooding or Jamming. Additionally, an attack on availability could occur if a malicious user hinders the routing of the vehicle network with a black hole attack [14–16]. To ensure availability, a vehicle should be authenticated through an authentication mechanism, and only the authenticated vehicle should be able to access the corresponding object.
- **Privacy Protection:** Because various applications are now provided inside the vehicle, privacy invasions can occur. When the black box data inside the vehicle is exposed, privacy is exposed. Additionally, because of the exposure of personal information, vehicle location information, and vehicle route provided by the navigation service, privacy invasion occurs. To prevent privacy invasions, encryption should be applied to important information. In addition, for identification or authentication of a vehicle or user, instead of using a unique ID, a random ID should be used to provide anonymity.

2.3. Previous Research on VCC

This subsection reviews previous works related to VCC services and security. Wan *et al.* [12] integrated the Vehicular Cyber-Physical System (VCPS) with Mobile Cloud Computing (MCC) and proposed the VCPS and MCC Integration Architecture (VCMIA) to support ITS and cloud services for fluent traffic. VCMIA provided a mobile service to the user to access a mobile traffic cloud. In addition, using GIS with Traffic-Aware Capability and Cloud-Supported Dynamic Vehicle Routing, it provided real time traffic information to the user and shared road traffic information with other users. In addition, it utilized MCC and location information to provide optimal Vehicle Routing to the user.

Wan *et al.* [17] proposed the VCPS for fluent and integrated communication between the vehicle network and customer center, and proposed situation recognition VCPS architecture using the cloud. Context-aware VCPS modified the parking service according to the situation and assigned computing resources to users in the VCPS data center. In addition, it provided functions such as Vehicle to Clouds

(VTC) and Vehicle as Clouds (VAC) that are formed and provided by the Vehicle with Clouds (VWC) infrastructure and its users.

VCC uses various computing capabilities of cloud computing paradigm. Vehicles with more stationary than moving time could use many public services on the road and parking lots. In addition, through cloud computing, various services such as traffic management, accident management, and entertainment are provided. Ma *et al.* [18] proposed the user-oriented Cloud Transportation System (C_TS) using a driving path guide. Crowdsourcing methods and cloud computing architecture are utilized to establish a traffic model that predicts by collecting, filtering, and modeling user data. User data (location and speed) are collected to determine user patterns based on a crowdsourcing method. The data are then calculated again, and, to provide real-time guidance, services are provided using an external data source.

Gerla *et al.* [19] distributed content efficiently to consumers through Named Data Networking (NDN), using names instead of IP addresses. They proposed a model consisting of the consumer requesting content and providers providing the information to the consumers in response. The cloud services that are generated and maintained by the cloud information providers were classified into existing cloud and vehicle cloud services. The cloud resources in the vehicle cannot only share data through storage, sensing, and computing, but can also detect and control event occurrences within the physical limits of the sensor capabilities.

Dressler *et al.* [20] used the network or storage of stationary vehicles in VCC to use idle resources. This system uses a Virtual Cord Protocol (VCP) to enroll a new vehicle or exclude an existing vehicle from the network. Driving and Parking modes are defined, and when a vehicle is in Driving mode, it accesses the VCP domain using an inter-domain routing for data exchange. The vehicle is enrolled using the existing code in parking mode. Inter-domain routing selects a vehicle to play the role of gateway for communication among multiple VCP cords, or decides which protocol to use when data is saved to a local VCP cord.

Hussain and Oh [21] addressed the problems of privacy, anonymous withdrawal, and route tracing via VANET using Clouds (VuC). The proposed technique protects privacy through multiple anonymities guaranteeing conditional anonymity. Beacon messages are saved in the cloud to use for route tracing and anonymous withdrawal. Institutions with authority can work together to trace a route selected by a user for a certain period of time. In addition, the institution can identify the user.

Sur *et al.* [22] proposed a new VCC-based secure and privacy-preserving navigation protocol. The proposed protocol uses a hash-sign-switch paradigm with a trapdoor hash function. To provide safe navigation service, a single-use anonymous certificate and hash key are used for the signing, and the route to the destination is provided from a Road Side Unit (RSU) to the vehicle. In addition, for privacy protection, zero-knowledge proof is used.

3. VCC-SSF

In this section, the following aspects of the proposed VCC-SSF are discussed in detail: the VCC-SSF Architecture, Application Service Layer, and Security Layer.

3.1. Architecture of VCC-SSF

VCC-SSF for the VCC environment is composed of three layers: Core Technology, Security, and Application Services. Figure 1 shows the architecture of VCC-SSF.

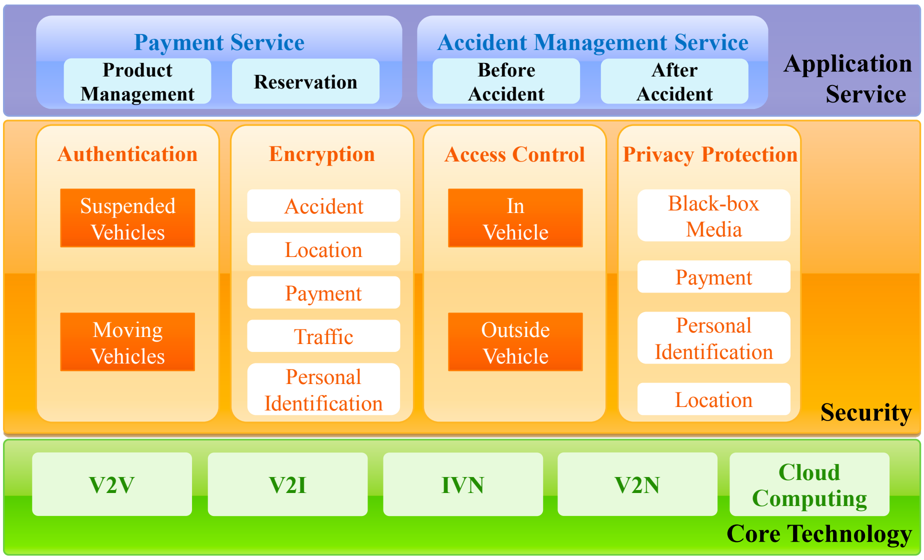

Figure 1. Architecture of VCC-SSF.

The *Core Technology Layer* is the layer handling the V2X of vehicle computing and Cloud Computing technologies, *i.e.*, the core technology of VCC-SSF. The V2X comprises the V2V, V2I, IVN, and V2N technologies, and it facilitates communication between vehicles and between the vehicle and infrastructure. In addition, its technologies are related to Cloud Computing, such as storage virtualization, server virtualization, and cloud storage management.

The *Security Layer* is the layer providing functions such as authentication, encryption, access control, and privacy protection. Furthermore, it authenticates stationary and driving vehicles and encrypts personal identification and sensitive information (e.g., location, payment, traffic, and accident information). In addition, it provides access control to the internal and external systems of the vehicle for permitted objects, and protects personal privacy such as video and voice data in the vehicle black box, payment information, personal identification information, location information, *etc.*

The *Application Service Layer* provides services to the driver or user utilizing V2X communication to access the collected data in a VCC environment. Two services are provided: Payment Service and Accident Management Service. The Payment Service allows the user to automatically pay for desired goods and consumables inside the vehicle in advance. The Accident Management Service prevents accidents that may occur on the road, provides response when an accident occurs, and provides management for vehicles involved in the accident.

3.2. Application Service Layer

We discuss the proposed Payment and Accident Management Services provided by the VCC-SSF in this subsection.

Payment Service: In the proposed Payment Service, Product Management receives the user's purchase requirements or utilizes sensor information inside the vehicle to automatically list the goods to purchase. It then finds nearby shops and searches their inventory. In addition, it checks the information inside the vehicle using the sensors and automatically asks for confirmation by the user before making payment. Product Management carries out the goods purchase and payment in the VCC environment, using V2I communication to receive the user's receipt. The receipt lists the purchased goods information (groceries, home appliances, meats, clothes, vegetables, *etc.*), vehicle consumables information (fuel in the vehicle, engine oil, brake oil, tire wear conditions, drive belt, battery, *etc.*), or reservation information (hotel, parking lot, hospital reservations, *etc.*). Only authenticated users can use the Payment Service, and the registered private information, payment information, and payment list are protected by encryption. In addition, to verify transaction and payment actions and prevent denial of the transaction, the communication is verified through hash algorithms and digital signatures. Figure 2 shows the concept of a payment service.

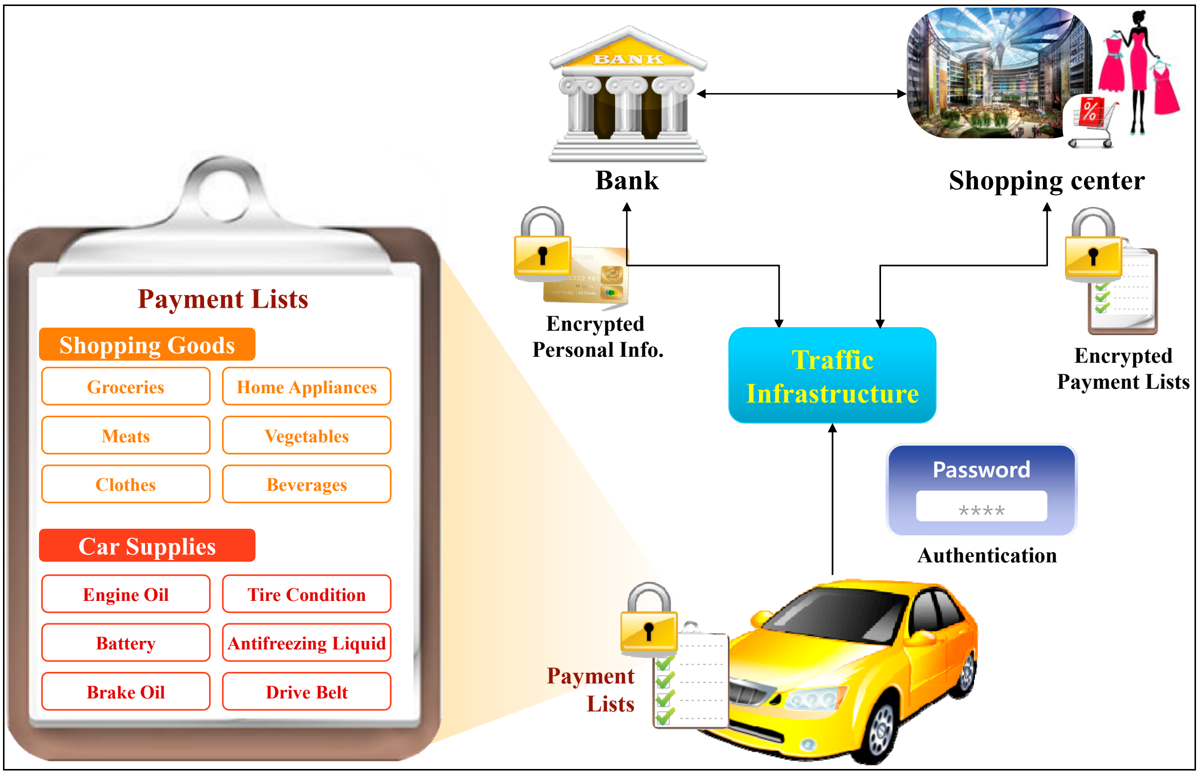

Figure 2. Payment service.

Accident Management Service: The Accident Management Service protects the life of accident victims by enabling quick first aid responses when a traffic accident occurs. Furthermore, it eases traffic congestion by managing the accident vehicle, and, in many cases, can prevent the fundamental cause of accidents. Using active accident management, it notifies nearby vehicles of the accident occurrence and conditions in real time, and when an emergency vehicle requires access, it broadcasts this communication to all vehicles. Figure 1 shows the architecture of the proposed Accident Management Service.

The proposed Accident Management Service uses VCC. It has two modes: before and after an accident. Before an accident occurrence, it utilizes a human body detection sensor inside the vehicle to monitor the health status and driving capability of the driver. In addition, using V2V and V2I communication during driving, it periodically checks the maintenance of the traffic lane and status of the vehicle. In addition, V2V communication is utilized to recognize vehicles approaching at a certain distance and, by notifying the driver, it helps to prevent a secondary accident occurrence.

After an accident occurs, it checks the driver for injuries, and through communication inside the vehicle such as the Electronic Control Unit (ECU), it determines the damage status. This information is sent to the traffic control center, and, by connecting to the nearest hospital and police station, it supports quick dispatch of emergency services and takes action for transportation to a nearby hospital according to the status of the accident victim. These processes, from active response and action to the management of the accident vehicle, are carried out utilizing VCC. The architecture of Accident Management System is shown in Figure 3.

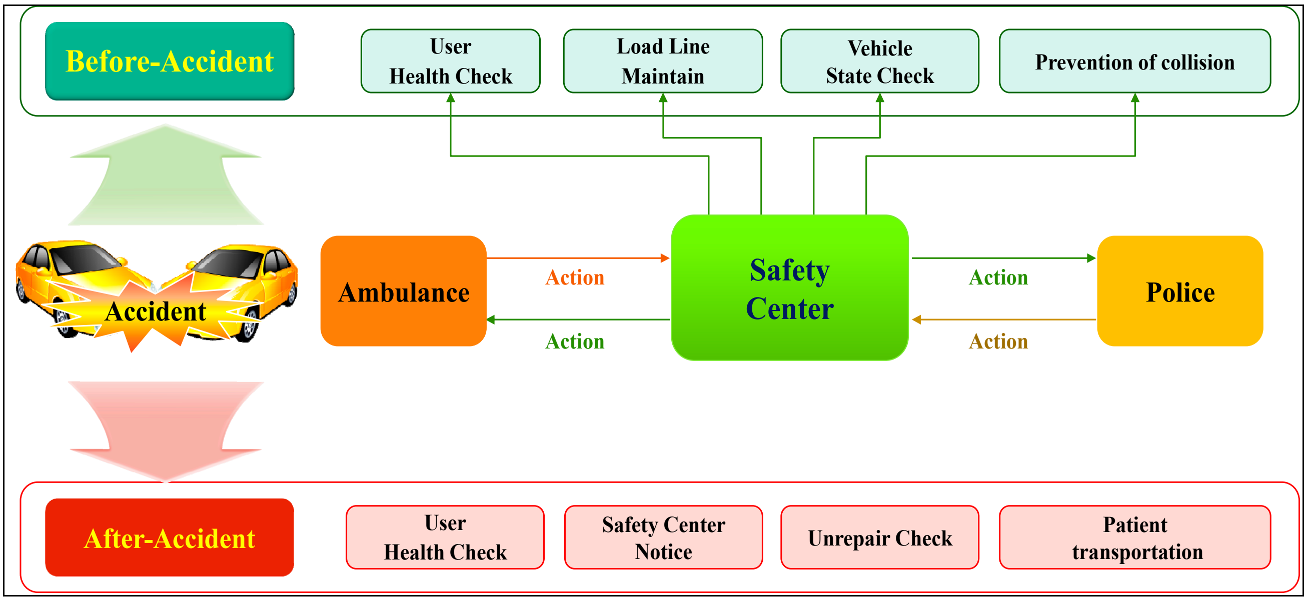

Figure 3. Architecture of accident management system.

3.3. Security Layer

As vehicle computing advances, vehicles are also able to process sensitive information such as vehicle location and unique information as well as driver personal information and health status through the sensors. If the information is extorted or manipulated by a malicious attacker, it may cause financial or physical damage to the user. In this subsection, we discuss the Security Layer, which is a core part of the proposed framework. The Security Layer is composed of Authentication, Data Integrity, Encryption, Access Control, and Privacy Protection. We define the terms used in Table 1 for security layer.

Authentication: Vehicle authentication can prevent malicious attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), and black hole attacks. When a person tries to access information inside the vehicle or the driver's personal information, this information should be provided only to users with permission. Vehicle authentication is considered separately depending on whether the vehicle is stationary or moving. The reason for this is that Storage as a Service (SaaS) and Computing as a Service (CompaaS) only utilize the storage and computing resources of a stationary or parked vehicle using vehicle authentication in shopping malls and parking lots. In addition, services to provide real time information such as Emergency or Accident Management Services need to send information to the police station, hospital, or other vehicles very quickly.

Table 1. Definition of terms.

Terms	Definition
V_S/V_M	Stationary vehicle/Moving vehicle
CA/U/SP	Certificate Authority/User/Service Provider
RSU/ECU	Road Side Unit/Electronic Control Unit
Hash ( )/Shift ( )	Hash Algorithm/Circular Shift Operation
E_x ( )/D_y ( )	Encryption algorithm using x key/ Decryption algorithm using y key
Sig_x ( )/$Very_y$ ( )	Signature algorithm using x key/ Verification algorithm using y key
C/P/Cert	Encrypted Message/Plain Text/Certificate
K_{x_prv}/K_{x_pub}	Private Key of X/Public Key of X
PVID/RID	Pseudo Vehicular ID/Road Side Unit ID
R_K	Random Values
DN/VN	Driver Number/Vehicle Number
X_TS	Time Stamp Values of X
ET	Expiry Time of Certificate
AcNo	Number of Accesses
VC_Int_Info/VC_Ext_Info	Internal/External Information

The definition of stationary and moving vehicles is as follows. The boundary of an RSU is defined as $RSU_n = [RSU_1, RSU_2, RSU_3, \ldots, RSU_n]$, n = 1, 2, 3, …, n. If the vehicle is stationary, the Vehicular Time Stamp (V_TS) value becomes 0. If the vehicle is moving, V_TS value has a value of 1 or greater. The V_TS is the time the vehicle passes each RSU. Using the difference of V_TS values, the RSU determines the movement of the vehicle. The V_TS value is used to authenticate a moving vehicle. The areas within which each RSU recognizes the vehicle overlap, and hence vehicle authentication is possible without network disconnection.

$$V\_TS = V\_TS_{RSUn} - V\_TS_{RSUn-1}$$

- **Authentication procedure:** Vehicle authentication utilizes V2I communication. Using the Pseudo Vehicular ID (PVID) and driver's Driver Number (DN) issued by the RSU, certificates are issued from the Certificate Authority (CA). The issued certificates are signed with K_{ca_prv}, and the vehicle verifies the certificate with K_{ca_pub}.

  If (V_TS = 0) then

  Deliver CA → V_S: Cert V_S = [Hash(PVID $\oplus$ DN), C_TS, ET, RID, AcNo] K_{ca_prv}

  else

  Deliver CA → V_M: Cert V_M = [Hash(PVID $\oplus$ DN), RID, C_TS, ET, RID, AcNo] K_{ca_prv}

If V_TS is 0, the vehicle is considered to be stationary. The stationary vehicle is marked as V_S, and the CA issues the certificate to V_S. The certificate includes the PVID and DN hash value, Time Stamp values of Certificate (C_TS), Expiry time of Certificate (ET), Road Side Unit ID (RID), and the Number of Accesses (AcNo). The C_TS is the time when the certificate is issued, and the ET is the expiration time of the certificate. The RID is the unique ID of the previous RSU, and by storing the IDs of RSU that vehicle has already passed, the system can verify the previous route. AcNo is the number of authentication attempts allowed. If there are more than AcNo access attempts, access and authentication to the corresponding vehicle is restricted.

Data Integrity: Information encryption, along with integrity, should be provided. Hash functions and digital signatures are used to provide data integrity.

- **Data integrity procedure:** Data integrity is provided for the Critical Info (*i.e.*, Personal Information, Payment Information, Location, User Information, and User State), which is sensitive information used both inside and outside the vehicle. This procedure is as follows.

  Signing V_S, V_M → RSU: Sig $_{K_{v\_prv}}$ (Hash(Critical Info)) || P

  To maintain data integrity inside the vehicle, the user hashes the Critical Info and signs it with K_{v_prv} to generate a hash value. This is then sent to the RSU along with the original information P.

  Verifying RSU: H = Very $_{K_{v\_pub}}$ (Hash(Critical Info))

  The signed data is verified using K_{v_pub}, registered in the CA. In addition, the hash value is compared with hashing P. Hash value H is obtained after the mutual verification to check whether data integrity is guaranteed.

Encryption: In VCC, sensitive information inside the vehicle, such as the private information and financial payment information as well as the ECU information that is collected using the On Board Unit (OBU) and On Board Equipment (OBE), should be protected through encryption.

- **Encryption of the information inside the vehicle:** The Drive System, Braking System, Steering System, *etc.* inside the vehicle are controlled through the ECU. This information is frequently used inside the vehicle for service or function, and hence fast encryption is required. In this system, a symmetric key encryption method is used. Key generation is as follows:

  Generate Key = Shift(VN) $\oplus$ R_K

  The 128-bit unique number (VN) assigned by the manufacturer is used as the key for the symmetric key encryption. We perform a circular shift operation by seven bits on the VN, and eXclusive-OR the result with R_K, generated using a random number generator inside the vehicle, to generate the final key.

  Encrypt OBD, OBU → U: C = E_{Key} (VC_Int_Info)

  VC_Int_Info (*i.e.*, Speed, Fuel, Oil Pressure, Tire Condition, GPS, Temperature, *etc.*) is displayed to the user inside the vehicle by the OBD. The OBU is also encrypted using a symmetric key encryption algorithm.

- **Encryption for information using infrastructure:** In the Application Layer, services are frequently provided through infrastructure, and the VC_Ext_Info (*i.e.*, Personal Information, Payment Information, Location, User Information, and User State) is encrypted using a public key encryption algorithm.

  Encrypt V_S, V_M → RSU: $C = E_{K_{sp\_pub}}$ (Hash(VC_Ext_Info))

  VC_Ext_Info is sent to an RSU by encrypting the hash value obtained by hashing the key of the Service Provider (SP) K_{sp_pub}. Key K_{sp_pub} is managed in the CA.

  SP decrypts the encrypted data using K_{sp_prv}, and hashes it to finally obtain and use VC_Ext_Info.

  Decrypt RSU → SP: $P = D_{K_{sp\_prv}}$ (Hash(VC_Ext_Info))

Access Control: In the VCC environment, access to sensitive information should be restricted when there is no legitimately granted authority. The access control monitors attempts to access the vehicle information system from inside and outside the vehicle in VCC.

- **Access control for the internal system:** The internal system displays the sensor information visually to the user through the OBU. There are various subjects that attempt to access this information. For example, car mechanics attempting to repair the vehicle, the vehicle owner, drivers other than the owner, and malicious attackers. When objects try to access this information, the role-based access controls access according to the situation information. In addition, we consider the time and place. No subjects except the vehicle owner can access the personal identification information. The example of role-based access control for time and location is shown in Table 2.

Table 2. Example of role-based access control for time and location.

Situation Information	Role	Permission
Time	R1: 06:00–24:00	P1, P2, P3
	R2: 00:00–06:00	P1, P2 (Optional)
Location	R3: Parking lot	P1, P2 (Optional)
	R4: Road	P1, P2 (Optional)
	R5: Repair shop	P1, P3

Role-based access control that takes into account situation information permits access to information inside the vehicle from 6:00–24:00 h by all subjects except others. Access control information for each subject is listed in Table 3. The vehicle owner has permission P1 to access all information. A guest driver is provided with P2 permission, and is given only the information required for driving the vehicle. A car mechanic has the P3 rights, and is provided only the information required for maintenance. Others have P4 rights, the lowest level of permission, and cannot access any information. For example, the vehicle owner can register a guest driver on the system, and access is limited to the location or traffic information required for the driving. A car mechanic can access the information during R1 hours, since this type of work is done during the day, and the information is limited to start-up, steering, or braking system information as required for vehicle repair. Finally, persons who are not registered by the vehicle owner are considered to be "others," and they have no authority. The owner and guest drivers have access to their allowed information at any hour.

Table 3. Access control information for each object.

Object		Access
Vehicle owner	P1	Can access all information
Guest driver	P2	Driving information, traffic information
Car mechanic	P3	Information of Drive System, Braking System, Steering System, *etc.*
Others	P4	No access

Role-based access control considers three locations: parking lot, road, and repair shop. For example, in a parking lot or on the road, only the vehicle owner and the guest driver can access information. In contrast, in the repair shop, only the car mechanic and owner have access to information.

- **Access control for outside the vehicle:** From outside the vehicle, using V2V and V2I communication, traffic infrastructure and external vehicles also attempt to access the internal information. The traffic infrastructure attempts to access the location for traffic analysis or vehicle authentication. External vehicles attempt to access the information for services such as collision prevention or traffic lane maintenance as well as V2V communication. In both cases, the corresponding vehicle should also control the access of the traffic infrastructure and external vehicles. Only correctly authenticated vehicles can exchange information, but the other vehicles cannot access the information without permission.

Table 4. Access control from outside the vehicle.

Classification	Role	Description
Authentication completed	A1: Full access permitted	Can access all information
	A2: Only authenticated vehicles inside the cluster can access the information (e.g., location, destination, and traffic information sharing)	Information can be shared only within the cluster
	A3: Only the authenticated traffic infrastructure can access the information	Information transmission to the traffic infrastructure
Partial authentication completed	P1: Information is shared with emergency vehicles	First aid, rescue, police vehicles, *etc.*
Authentication is not possible	N1: Cannot access the information	Vehicles without permission cannot access any information

Access control from outside the vehicle is divided into access for subjects that complete authentication and access for subjects that cannot. Table 4 shows the access control from outside the vehicle. For example, only when authenticated subjects with roles A1, A2, or A3 and partially authenticated subjects (first aid, rescue, police, *etc.*) try to access the information is the access to the vehicle location or traffic information permitted. Unauthenticated subjects take on role N1; for them, access to all information is restricted. For role A1, access to all information is permitted for vehicles that complete authentication. For role A2 in the VANET environment, a small logical cluster is generated and V2V communication between subjects inside the cluster is possible. However, only location, destination, traffic, and entertainment information can be shared inside the cluster. The VN or DN of each vehicle cannot be accessed. For role A3, because of the characteristics of the VCC environment, communication with nearby RSUs is frequent. In this case, an RSU requests access or sends data to the vehicle for authentication or traffic information collection. The corresponding vehicle checks the RID of the requesting RSU, bestows A3 authority, and blocks access to the DN. It permits access to other information for traffic analysis. However, access is restricted for unauthenticated RSUs.

Privacy Protection: Among the information transmitted in the VCC environment, privacy protection should be considered for the driver or user identification information, vehicle location information, video or voice recorded by the vehicle black box, payment information used in Payment Services, *etc.* This information is used for the convenience of the driver or the user, but when it is exposed to malicious attackers, this could cause the user financial damage or defamation. We address privacy protection in the following two ways:

- **Privacy protection with a vehicle alias ID:** In the VCC environment, the vehicle authentication process uses the PVID. Instead of using the VN, we use a PVID assigned by an RSU during authentication. The VN is the unique number of each vehicle. Hence there is a risk of exposure of the vehicle owner's personal information through inquiry to the management system. However, if a PVID is used, authentication can be performed without exposing the VN.
- **Privacy protection with data encryption:** An invasion of privacy occurs when the private identification information, location information, or video captured by the black box inside the vehicle are exposed to others. However, if this information is encrypted inside or outside the vehicle and not displayed to others, invasion of privacy does not occur. As mentioned above, the privacy of the DN, payment information, location information, and data in the black box can be protected using encryption.

3.4. Analysis of VCC-SSF

In this section, we analyze VCC-SSF to compare with methods that are proposed in previous studies based on security concerns—Confidentiality, Integrity, Availability, and Privacy Protection in the VCC environment. The security comparison is shown in Table 5.

Table 5. Security comparison.

Classification	Wan *et al.* [12]	Wan *et al.* [17]	Ma *et al.* [18]	Hussain and Oh [21]	Sur *et al.* [22]	VCC-SSF
Confidentiality	Δ	O	X	O	O	O
Integrity	Δ	O	X	O	X	O
Availability	X	X	X	X	X	Δ
Privacy Protection	Δ	O	X	O	O	Δ

(O: strong, Δ: medium, X: weak).

Confidentiality: Data are generated through many sensors in the vehicle. In addition, private identification information, payment information, location information, *etc.* are provided from or sent to the traffic infrastructure. In this case, only permitted vehicles should be able to receive services, and user access to important information should be separated through access control. In addition, the information should be encrypted to prevent exposure to external users. The VCC-SSF system proposed in this paper can separate users via role-based access control inside and outside the vehicle along with the vehicle authentication to control information usage. In addition, the data sent from inside or outside the vehicle is encrypted to defend against tapping, falsification, or other malicious activities. The framework proposed in [17] comprises context-aware vehicular security mechanisms (CVSMs), and collects data from sensors. The information is protected through encryption, authentication, and access control. The system proposed in [12] protects location or map information, but the protection of other important information is limited. The framework proposed in [21] protects vehicle speed, location, and personal information based on GeoLock. The framework proposed in [22] uses hashed ElGamal encryption to encrypt vehicle location and personal information. The framework in [18] does not mention any technology to provide confidentiality.

Integrity: Integrity should be provided for private identification information, payment information, and location information. Just as for important information extortion, integrity invasion also causes financial damage to the user. VCC-SSF disables the identification of the vehicle or the user by hashing the unique information or ID of the object. In addition, integrity is provided for important information such as Personal Information, Payment Information, *etc.*, through the hash function. However, in the framework in [12], the information for which data integrity is provided is limited. Integrity is applied only to geographical or location information, and details for other information such as personal identification or payment is limited. The framework in [21] uses beacons to provide the integrity. A beacon includes the current time, location, and speed, and it uses HMAC to periodically transmit it. The frameworks in [17,22] are undergoing development for integrity protection.

Availability: In the VCC environment, it is important to provide services without network disconnection. Because of the characteristics of wireless network environments, attacks that degrade availability such as Denial of Service (DoS), Distributed Denial of Service (DDoS), or black hole attacks may occur. VCC-SSF only provides services between the vehicle and infrastructure and between vehicles to permitted vehicles in order to defend against these attacks. The number of authentication attempts is limited to block access attempts from external malicious users. In cases of the existing frameworks [12,17,18,21,22], studies on attacks against availability are undergoing.

Privacy Protection: Privacy protection is a very important element in the VCC environment. VCC-SSF authorizes using a PVID for the vehicle. It does not use the VN or user unique identification, hence exposure of additional personal information does not occur. In addition, VCC-SSF encrypts important data to prevent leakage. In [12], privacy protection is considered, but the protected data is limited to location or map information. In [17,21,22] data is encrypted for possible privacy protection, and [18] is still undergoing development with respect to privacy protection.

4. Conclusions

As ITS and cloud computing technology are combined, services convenient to users are being provided; however, there are insufficient studies on an ITS framework that can provide security for information used in the services. Therefore, this study proposed VCC-SSF, a framework based on VCC that provides security services to guarantee Confidentiality, Integrity, Availability, and Privacy Protection for its users. In addition, for the convenience of the user as well as active accident management, it also proposed Payment and Accident Management Services. However, there are still problems with key distribution and management in VCC environments. Vehicle and user authentication is also limited. Future studies will address effective methods for key distribution and management in the framework. Moreover, we will solve the vehicle and user authentication without certificates.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the vehicle IT Convergence cooperation project supervised by the NIPA (National IT Industry Promotion Agency)—(Various content services and security framework that is optimized for vehicle technology works in the connected-car platform).

In addition, this research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2013-H0301-13-4007) supervised by the NIPA (National IT Industry Promotion Agency).

Author Contributions

Won Min Kang: mainly writing; Jae Dong Lee: design of the total system; Young-Sik Jeong: research for the related works, analyzing and improving for the proposed system; Jong Hyuk Park: total supervision for the paper work, review and comments, *etc*.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Whaiduzzaman, M.; Sookhak, M.; Gani, A.; Buyya, R. A survey on vehicular cloud computing. *J. Netw. Comput. Appl.* **2014**, *40*, 325–344.
2. Dias, J.A.F.F.; Rodrigues, J.J.P.C.; Zhou, L. Cooperation advances on vehicular communications: A survey. *Veh. Commun.* **2014**, *1*, 22–32.
3. Dua, A.; Kumar, N.; Bawa, S. A systematic review on routing protocols for Vehicular Ad Hoc Networks. *Veh. Commun.* **2014**, *1*, 33–52.
4. Taysi, Z.C.; Yavuz, A.G. ETSI compliant GeoNetworking protocol layer implementation for IVC simulations. *Hum.-Centric Comput. Inf. Sci.* **2013**, *3*, 1–12.

5. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular Ad Hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392.
6. Zeadally, S.; Hunt, R.; Chen, Y.-S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241.
7. Grant-Muller, S.; Usher, M. Intelligent Transport Systems: The propensity for environmental and economic benefits. *Technol. Forecast. Soc. Chang.* **2014**, *82*, 149–166.
8. Hussain, R.; Oh, H. Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks. *J. Inf. Process. Syst.* **2014**, *10*, 103–118.
9. Yu, Z.; Gao, W.; Zuo, X. Design of Novel Intelligent Transportation System based on Wireless Sensor Network and ZigBee Technology. *Sens. Transducers* **2013**, *166*, 95–102.
10. Abid, H.; Phuong, L.T.T.; Wang, J.; Lee, S.; Qaisar, S. V-Cloud: Vehicular cyber-physical systems and cloud computing. In Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL '11), Barcelona, Spain, 26–29 October 2011; Article 165, pp. 1–5.
11. Gu, L.; Zeng, D.; Guo, S. Vehicular Cloud Computing: A Survey. In Proceedings of the 2013 IEEE Globecom Workshops (GC Workshops), Atlanta, GA, USA, 9–13 December 2013; pp. 403–407.
12. Wan, J.; Zhang, D.; Sun, Y.; Lin, K.; Zou, C.; Cai, H. VCMIA: A Novel Architecture for Integrating Vehicular Cyber-Physical Systems and Mobile Cloud Computing. *Mob. Netw. Appl.* **2014**, *19*, 153–160.
13. He, W.; Yan, G.; Xu, L.D. Developing Vehicular Data Cloud Services in the IoT Environment. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1687–1695.
14. Sandhu, G.; Dasgupta, M. Impact of Blackhole Attack in MANET. *Int. J. Recent Trends Eng. Technol.* **2010**, *3*, 183–186.
15. Tseng, F.-H.; Chou, L.-D.; Chao, H.-C. A survey of black hole attacks in wireless mobile ad hoc networks. *Hum.-centric Comput. Inf. Sci.* **2011**, doi:10.1186/2192-1962-1-4.
16. Singh, R.; Singh, P.; Duhan, M. An effective implementation of security based algorithmic approach in mobile adhoc networks. *Hum.-Centric Comput. Inf. Sci.* **2014**, doi:10.1186/s13673-014-0007-9.
17. Wan, J.; Zhang, D.; Zhao, S.; Yang, L.T.; Lloret, J. Context-Aware Vehicular Cyber-Physical Systems with Cloud Support Architecture, Challenges, and Solutions. *IEEE Commun. Mag.* **2014**, *52*, 106–113.
18. Ma, M.; Huang, Y.; Chu, C.-H.; Wang, P. User-Driven Cloud Transportation System for Smart Driving. In Proceedings of the IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), Taipei, Taiwan, 3–6 December 2012; pp. 658–665.
19. Gerla, M.; Lee, E.-K.; Pau, G.; Lee, U. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 241–246.
20. Dressler, F.; Handle, P.; Sommer, C. Towards a Vehicular Cloud—Using Parked Vehicles as a Temporary Network and Storage Infrastructure. In Proceedings of the 2014 ACM international workshop on Wireless and mobile technologies for smart cities (WiMobCity-14), Philadelphia, PA, USA, 11–14 August 2014; pp. 11–18.

21. Hussain, R.; Oh, H. A Secure and Privacy-Aware Route Tracing and Revocation Mechanism in VANET-based Clouds. *J. Korea Inst. Inf. Secur. Cryptol.* **2014**, *24*, 795–807.
22. Sur, C.; Park, Y.H.; Rhee, K.H. An efficient and secure navigation protocol based on vehicular cloud. *Int. J. Comput. Math.* **2014**, *2014*, 1–20.