International Journal of Control and Automation
Vol.10, No.7 (2017), pp.39-50
http://dx.doi.org/10.14257/ijca.2017.10.7.04

A Design of Vehicle Management Framework for Secure Communication in Vanet Cloud Computing Environment

Byung Wook Jin[1], Jung oh Park[2]* and [1]Moon Seog Jun[3]

Dept. of Computer Science, Soongsil University, South Korea[1]
*Dept. of Paideia, Sungkyul University, South Korea[2]**
Dept. of Computer Science, Soongsil University, South Korea[3]
[1]Quddnr4511@naver.com, [2] jopark02@sungkyul.ac.kr, [3]mjun@ssu.ac.kr*

Abstract

The development and technology of a smart car are getting more important with the convergence of IT technology and vehicle industry recently. The prospect of the convergence of IT technology and automobile industry is heightened and large corporations inside and outside of the country as well as the government and research institutions are expanding business and growing competitiveness. Vehicle communication is trying to enhance convenience by providing safety and various IT services for the users. However, there exist the attack techniques which use the weak points of ITS based system and there are few researches on this. Also, with the convergence with IT technology, it is not safe from the various attack techniques that happen in the wireless environment. This research article designed the framework for the safe communication protocol and vehicle approach/control and management. The proposed protocol evaluated the safety and the code performance based on the requirement of vehicle security. In the communication environment that passed through vehicles and infrastructure, there was approximately 60% of performance improvement in roughly 57% vehicles and vehicle communications.

Keywords: *Access Control, Authentication ,VANET Cloud, Management System*

1. Introduction

Recently, the technical cooperation through the convergence of the vehicle industry and cloud computing, the core technology of IT field, is emerging as a key issue. It aims to provide safety and convenience for the drivers through interaction with users using software flat and by installing the sensor and electronic devices in the car. And the researches to achieve this goal are being actively conducted[1]. Users can be provided with contents such as music, mail, documents, and videos also in the car. However, the convergence technique lacks the maturity and complementation enough to deal with possible attack techniques[2-4][9]. Also, it still has the weak points of the existing wireless network, and the method to efficiently deal with the new and mutated attack techniques is needed. Therefore, in the environment where cloud computing and the vehicle environment are converged, this research article suggests the security fame work that can secure the integrity for the safety messages in the car and can efficiently approach and control the car.

The composition of this research article is as follows. In chapter 2, it explains the components of the vehicle cloud computing and the requirement for security. In chapter 3, it designs the communication frame work and suggests the protocol for vehicle registration, communication, and cancellation. In chapter 4, it evaluates the security and analyzes the safety based on the proposed protocol. In chapter 5, as a conclusion of the research article, it explains the future research plan.

[*] Corresponding Author Jung-oh Park(E-mail:jopark02@sungkyul.ac.kr)

ISSN: 2005-4297 IJCA

2. Related Researches

2.1. The Components of the Vehicle Cloud Computing

The vehicle cloud computing is composed of vehicle cloud, roadside cloud, and center cloud. Examining the environment of vehicle cloud, the messages are communicated vehicle to vehicle (V2V). The automobiles that are connected through cloud server are provided with the service, possessing a lot of resources compared to the personal automobile[1][9]. The roadside cloud environment is based on vehicle-to-infrastructure (V2I), in which vehicle and RSU(Road Side Unit) communicate, and which consists of RoadSide and local server. However, the range of communication of roadside cloud is limited as it conducts communication through wireless interface within the wireless internet area. Automobiles and Road Side Unit are accessed to the center using wireless network, and it is defined as center cloud. The center cloud has more resources than vehicle cloud and roadside cloud, being used for data processing and arithmetic. [Figure 1] below is the data communication structure in the vehicle cloud computing environment[3,5,10].

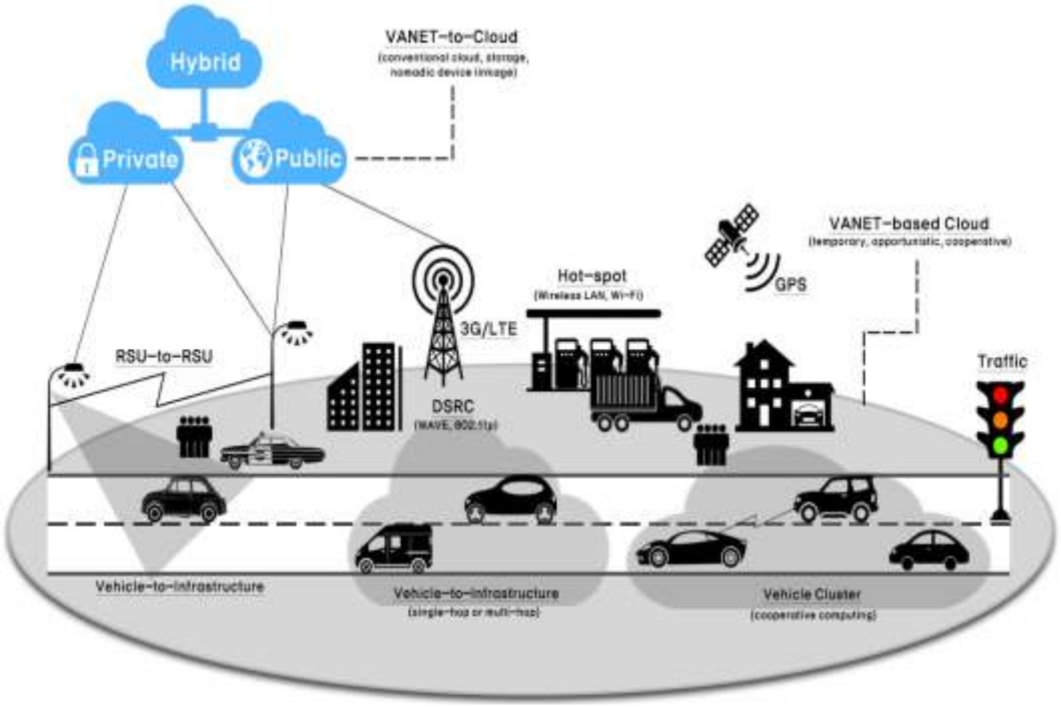
Hybrid
Private
Public
VANET-to-Cloud
(conventional cloud, storage, nomadic device linkage)
VANET-based Cloud
(temporary, opportunistic, cooperative)
GPS
Hot-spot
(Wireless LAN, Wi-Fi)
3G/LTE
RSU-to-RSU
DSRC
(WAVE, 802.11p)
Traffic
Vehicle-to-infrastructure
Vehicle-to-infrastructure
(single-hop or multi-hop)
Vehicle Cluster
(cooperative computing)

Figure 1. Data Communication Structure in the Vehicle Cloud Environment

2.2. The Requirement for the Vehicle Cloud Computing Security

There are security threats such as modulation, camouflage, sybil, service infra, tapping, and personal information leakage in the vehicle communication environment. To complement these, it needs to meet the security requirements such as integrity, certification protection of privacy, protection of data, and non-repudiation [5,7,10-11].

· **Integrity :** In the vehicle environment, the surveillance system can monitor automobiles through cameras installed on the road. In the case of accident happening, it can be used as evidence data through camera, and the integrity, which means that the recorded evidence data should not be changed, needs to be secured [4, 11].

· **Certification :** Certification includes proving the identity of users and integrity in the messages that are sent out by users. The vehicle needs to conduct certification considering characteristics that automobiles move fast in the vehicle cloud environment, and it is difficult to certify the car and the car owner due to the mobility of the location [6][12].

· **Protection of privacy :** The surveillance and management of the volume of traffic should receive and depend on correct information in the vehicle cloud service environment. The automobiles transmit the information and data of their current location through the vehicle cloud server and the problem of making the location information public can occur[4]. Also, in case that the drivers need to provide personal information for the certification of the car and the car owner, the problem of personal information leakage can occur [7,9].

· **Protection of data :** In the vehicle cloud environment, the shared resources of the vehicle can be provided for the server, other automobiles, and Road Side Uint, and if there are no restrictions about the protection, drivers can access the data in other automobiles and save them after changing the contents. To prevent this from happening and protect the data from the non-certified users, the encryption needs to be done to secure the confidentiality. And in case of using the vehicle that is parked as a data center, customers can be provided with services by accessing the data center established in the vehicle cloud. After getting the service, there can be sensitive data remaining such as personal information of the customers. To prevent this, the remaining data after the service is finished needs to be destroyed and taken care of [3-4, 8,13].

3. Proposed Protocol

3.1. The Designing of Proposed Communication Framework

This research article designed the communication frame work in the environment where the existing VANET and the cloud technology are converged. The communication frame work of the vehicle cloud environment is as shown in [Figure 2]. The vehicle communication protocol was designed after registering the automobile. And the renewed protocol of the vehicle was designed for safe communication. Also, the communication frame work was designed based on the requirements for the vehicle environment security. In the process of registering automobiles, the session key is created and the safe communication is performed through utilization in the communication protocol based on it. The safety about the data of the vehicle environment was supplemented by designing the vehicle renewed protocol and vehicle approach control of the non-certified automobiles by testing the data in the process of communication.

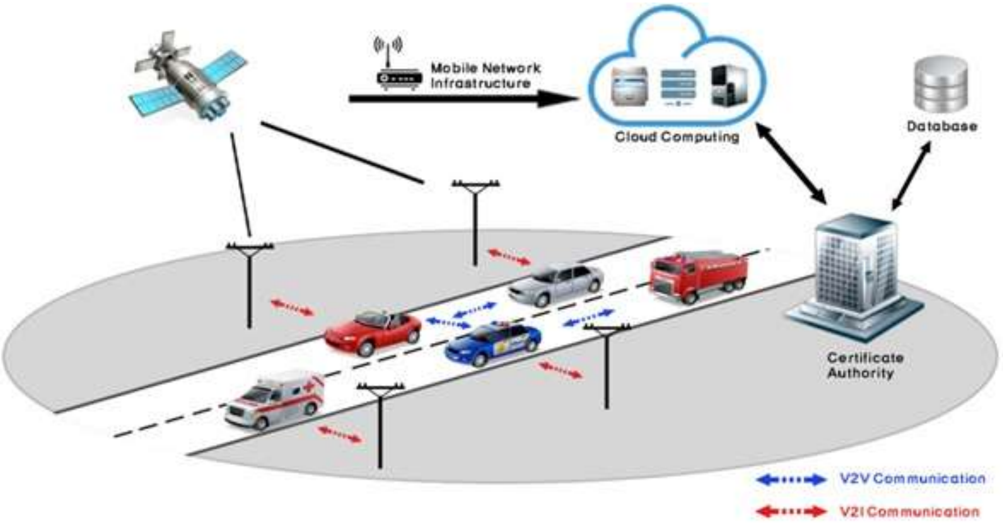

Figure 2. Design of Communication Framework in the Vehicle Cloud Environment

3.1. The Designing of Proposed Communication Framework

This research article designed the communication frame work in the environment where the existing VANET and the cloud technology are converged. The communication frame work of the vehicle cloud environment is as shown in [Figure 2]. The vehicle communication protocol was designed after registering the automobile. And the renewed protocol of the vehicle was designed for safe communication. Also, the communication frame work was designed based on the requirements for the vehicle environment security. In the process of registering automobiles, the session key is created and the safe communication is performed through utilization in the communication protocol based on it. The safety about the data of the vehicle environment was supplemented by designing the vehicle renewed protocol and vehicle approach control of the non-certified automobiles by testing the data in the process of communication.

3.2. Designing Vehicle Registration Protocol

Figure 3 shows the proposed Vehicle Registration protocol. The process of it is as follows.

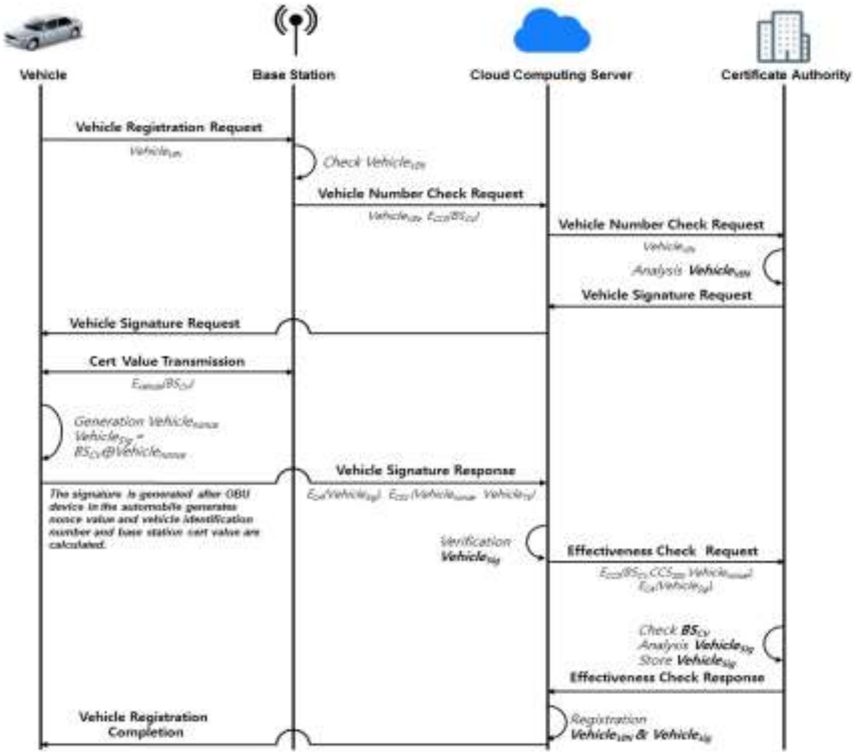
Vehicle
Base Station
Cloud Computing Server
Certificate Authority
Vehicle Registration Request
$Vehicle_{VIN}$
Check $Vehicle_{VIN}$
Vehicle Number Check Request
$Vehicle_{VIN}$, $E_{CSS}(BS_{CV})$
Vehicle Number Check Request
$Vehicle_{VIN}$
Analysis $Vehicle_{VIN}$
Vehicle Signature Request
Vehicle Signature Request
Cert Value Transmission
$E_{Vehicle}(BS_{CV})$
Generation $Vehicle_{nonce}$
$Vehicle_{Sig}$ = BS_{CV}@$Vehicle_{nonce}$
Vehicle Signature Response
$E_{CA}(Vehicle_{Sig})$, $E_{CSS}(Vehicle_{nonce}, Vehicle_{VIN})$
The signature is generated after OBU device in the automobile generates nonce value and vehicle identification number and base station cert value are calculated.
Verification $Vehicle_{Sig}$
Effectiveness Check Request
$E_{CCS}(BS_{CV}, CCS_{ID}, Vehicle_{nonce})$
$E_{CA}(Vehicle_{Sig})$
Check BS_{CV}
Analysis $Vehicle_{Sig}$
Store $Vehicle_{Sig}$
Effectiveness Check Response
Registration $Vehicle_{VIN}$ & $Vehicle_{Sig}$
Vehicle Registration Completion

Figure 3. The Protocol of Vehicle Registration

1. The vehicle is base station that transmits the message for requesting the registration including ***Vehicle***$_{VIN}$.

2. Base station transmits the message for requesting the inspection of the vehicle number from the cloud computing server after testing ***Vehicle***$_{VIN}$.

$$\boldsymbol{Vehicle_{VIN}, E_{CSS}(BS_{CV})} \qquad (1)$$

3. Cloud Computing Server transmits to certificate authority the message for requesting the inspection of the vehicle number including ***Vehicle***$_{VIN}$.

4. Certificate authority transmits the message for requesting the vehicle signature from the cloud computing server after analyzing $\boldsymbol{Vehicle_{VIN}}$.

5. The cloud computing server transmits the message for requesting the vehicle signature from the automobile, and the vehicle communicates after encrypting the base station and cert value.

$$\boldsymbol{E_{Vehicle}(BS_{CV})} \qquad (2)$$

6. The vehicle transmits the signature reply message from the cloud computing server after generating $\boldsymbol{Vehicle_{nonce}}$. The signature is generated after OBU device in the vehicle generates nonce value and then the base station cert value is XoR calculated. (The signature is generated after OBU device in the vehicle generates nonce value and vehicle identification number and base station cert value are calculated.)

$$\boldsymbol{Vehicle_{Sig} = BS_{CV} \oplus Vehicle_{nonce}, E_{CA}(Vehicle_{Sig}), E_{CSS}(Vehicle_{nonce}, Vehicle_{TS})} \qquad (3)$$

7. The cloud computing server transmits the message for the inspection of effectiveness to the certificate authority after verifying $\boldsymbol{Vehicle_{sig}}$.

$$\boldsymbol{E_{CCS}(BS_{CV}, CSS_{Sig}, Vehicle_{nonce}), ECA(Vehicle_{Sig})} \qquad (4)$$

8. The certificate authority tests BS_{CV}, analyzes $\boldsymbol{Vehicle_{sig}}$ and saves them. And then, it transmits the message for the inspection of effectiveness to the cloud computing server.

9. The cloud computing server transmits the message of completing the vehicle registration after registering $\boldsymbol{Vehicle_{VIN}}$ and $\boldsymbol{Vehicle_{Sig}}$.

3.3. Designing Vehicle Communication Protocol

Figure 4 shows the proposed Vehicle Communication protocol. The process of it is as follows.

1. $\boldsymbol{Vehicle_i}$ transmits the situation message from Road Side Unit.

$$\boldsymbol{E_{CSS}(Vehicle_{Sig}, Message), Vehicle_{VIN}} \qquad (5)$$

2. Vehicle transmits the message of vehicle request after encrypting the $\boldsymbol{RSU_{parameter}}$ of the received message.

$$\boldsymbol{E_{CSS}(Vehicle_{sig}, Message), Vehicle_{VIN}, EBS(RSU_{parameter})} \qquad (6)$$

3. Base station transmits the message for requesting the inspection of vehicle to the cloud computing server after examining $\boldsymbol{RSU_{Parameter}}$.

$$\boldsymbol{E_{CSS}(Vehicle_{sig}, Message), Vehicle_{VIN}} \qquad (7)$$

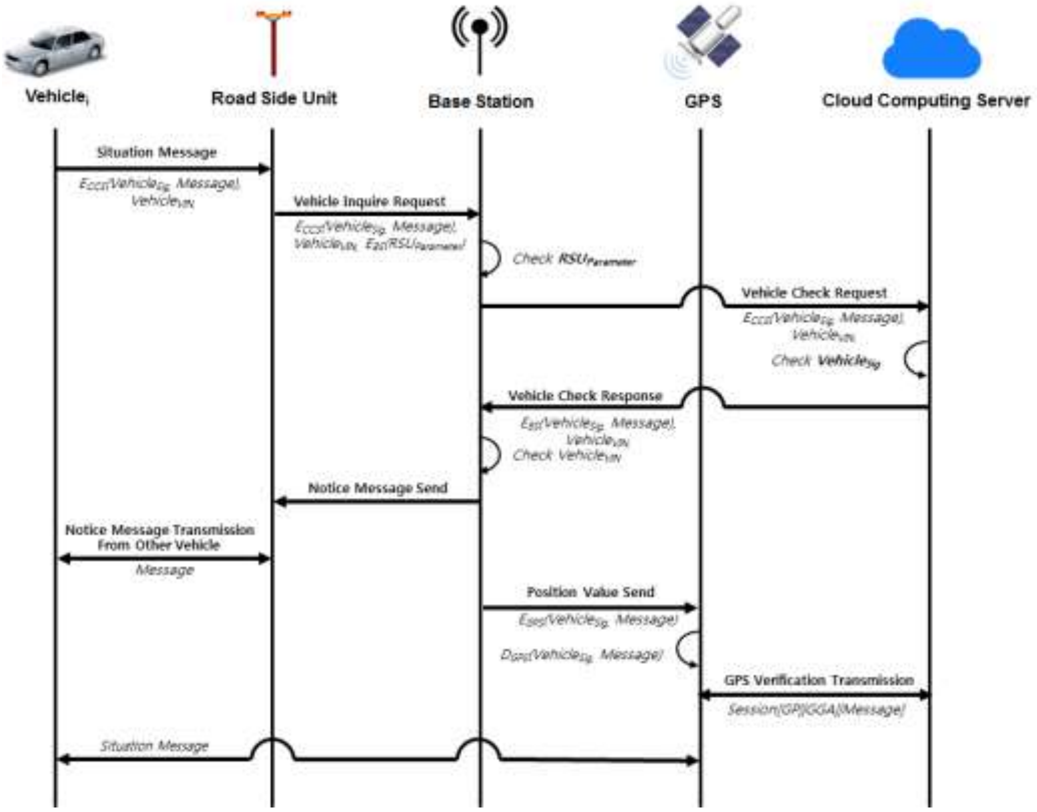
Vehicle$_i$
Road Side Unit
Base Station
GPS
Cloud Computing Server
Situation Message
$E_{CCS}(Vehicle_{Sig}, Message)$, $Vehicle_{VIN}$
Vehicle Inquire Request
$E_{CCS}(Vehicle_{Sig}, Message)$, $Vehicle_{VIN}$, $E_{BS}(RSU_{Parameter})$
Check $RSU_{Parameter}$
Vehicle Check Request
$E_{CCS}(Vehicle_{Sig}, Message)$, $Vehicle_{VIN}$
Check $Vehicle_{Sig}$
Vehicle Check Response
$E_{BS}(Vehicle_{Sig}, Message)$, $Vehicle_{VIN}$
Check $Vehicle_{VIN}$
Notice Message Send
Notice Message Transmission From Other Vehicle
Message
Position Value Send
$E_{GPS}(Vehicle_{Sig}, Message)$
$D_{GPS}(Vehicle_{Sig}, Message)$
GPS Verification Transmission
Session[GP||GGA||Message]
Situation Message

Figure 4. Design of Vehicle Communication Protocol

4. The cloud computing server transmits the reply message for vehicle inspection from base station after testing $\boldsymbol{Vehicle_{Sig}}$

5. Base station announces the message from the vehicle on the road via Road Side Unit.

6. Base station transmit the location value from GPS.

$$\boldsymbol{E_{GPS}(Vehicle_{sig}, Message)} \tag{8}$$

7. GPS communicates the GPS verification message from the cloud computing server after decoding the received location value.

$$\boldsymbol{Session[GP||GGA||Message]} \tag{9}$$

8. After this, GPS transmits the situation message from the automobiles on the location.

3.4. Designing Cancellation of Vehicle Registration

Figure 5 shows the proposed Cancellation of Vehicle Revocation protocol. The process of it is as follows.

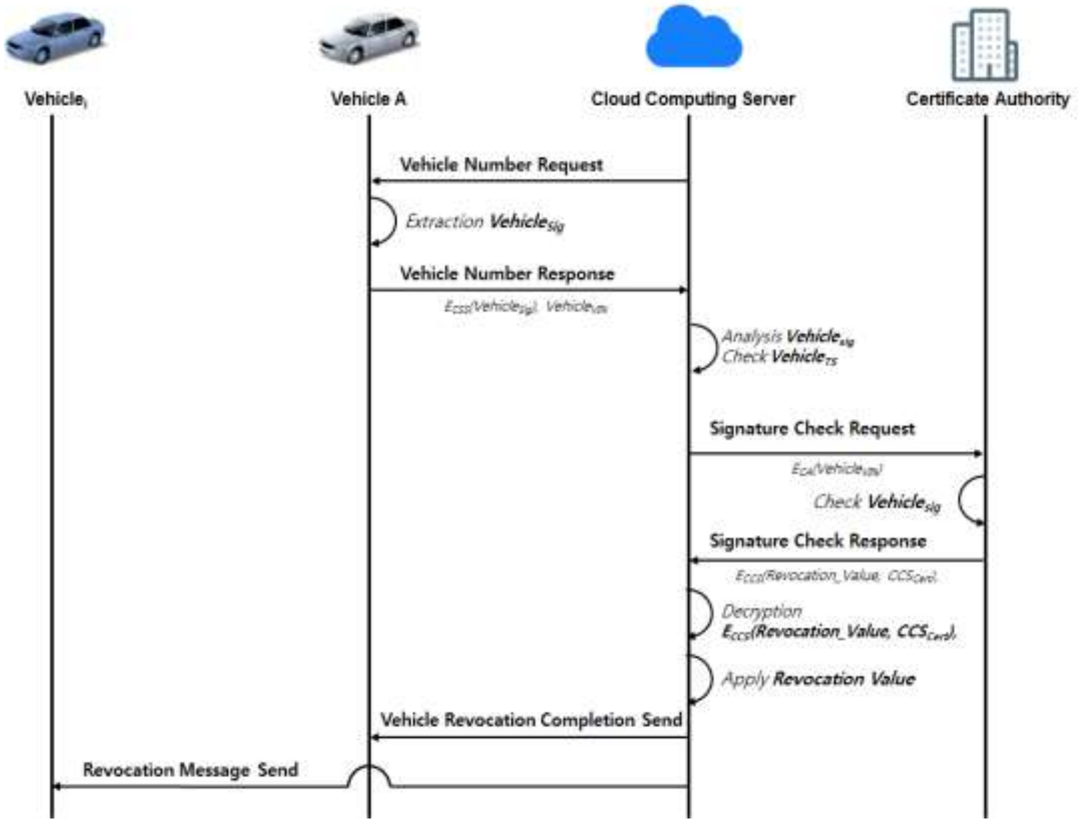

Figure 5. Design Cancellation of Vehicle Revocation

1. The cloud computing server requests the message for vehicle number request from the automobile.

2. The vehicle extracts ***Vehicle$_{Sig}$*** and then responds to the message of number request through the cloud computing server.

$$E_{CSS}(Vehicle_{Sig}),Vehicle_{VIN} \quad (10)$$

3. The cloud computing server inspects ***Vehicle$_{sig}$*** and ***Vehicle$_{TS}$***. And then it transmits the message for requesting the inspection of signature from the certificate authority.

$$E_{CA}(Vehicle_{VIN}) \quad (11)$$

4. The certificate authority transmits the replying message about signature inspection. After decoding, it applies the revocation value.

$$E_{CSS}(Revocation\text{-}Value,\ CCS_{Cert}) \quad (12)$$

5. After cancellation message is transmitted through ***Vehicle$_A$***, it is transmitted to the surrounding in the form of broadcasting from the automobile.

4. Performance Evaluation in the Vehicle Cloud Computing Environment

4.1. Safety Analysis

· **Denial of Service :** The attack on availability happens when multiple cases of hacking into OBU or RSU occur, or when one vehicle transmits infinite messages. This research article complemented safety by verifying ***Vehicle$_{VIN}$***, **E$_{CSS}$(BS$_{CV}$)** and ***Vehicle$_{Sig}$*** of the vehicle in the cloud computing server and the certificate agency to prevent the attack on availability.

· **Data modification and MITM(Man in the Middle attack) :** A man-in-the-middle attack is an attack where the attacker intercepts in the communication between two parties in the cloud environment, eavesdropping, altering and fabricating the messages between them. The man-in-the-middle attack fails as the messages are transmitted through codes based on bilinear pairing on V2I and V2V basis,

· **Repudiation :** It is an attack where a malevolent user gets on the automobile, denying and transmitting the message in the vehicle cloud environment, which causes harm. Also, it is not safe from the attack of DDoS and Dos. This research article verifies **Vehicle$_{sig}$** The denial can be prevented by transmitting safely through utilizing the session key mutually, and checking **BS$_{Cert}$**, ***GP||GGA*** for base station and GPS.

· **Impersonation attack :** It is an act in which a non-certified user access the vehicle cloud server and illegally acquires data. However, it is safe from camouflage as it certifies through the vehicle cloud server after generating **Vehicle$_{sig}$** of the vehicle in the protocol of vehicle registration and certification.

· **Information disclosure :** A non-certified user can access the vehicle cloud server and expose the information of the storage server. To complement this problem, the vehicle cloud server confirms **Vehicle$_{Sig}$** when accessing the Road Side Unit and the automobile, and the base station registers **Vehicle$_{VIN}$** of the automobile, making it possible to track down on the information leakage.

4.2 Security Evaluation (Evaluation of the Code Performance)

The environment for analysis is composed based on Inter(R) Core(TM)2 Quad CPU Q9400 @ 2.66HZz 2.66GHz, 4.00GB and Windows 7 Enterprise OS. And for the simulation, the performance speed of encryption/decryption and the message communication protocol were evaluated by utilizing Eclipse IDE for Java Developers and referring to TTAK.KO-06.0402 of the existing vehicle environment.

The communication based on V2I that passes through the interface in the proposed protocol transmitted the message after conducting encryption and decryption three times from each node, and the communication based on V2V transmitted the message after communicating the encryption 4 times. In the existing vehicle cloud environment, messages are communicated by using the RSA encryption based on PKI open key while in the proposed protocol, the performance of the encryption part can be improved by utilizing the identity-based encryption. The performance evaluation of the existing vehicle environment and the proposed frame work is as shown in [Figure 6].

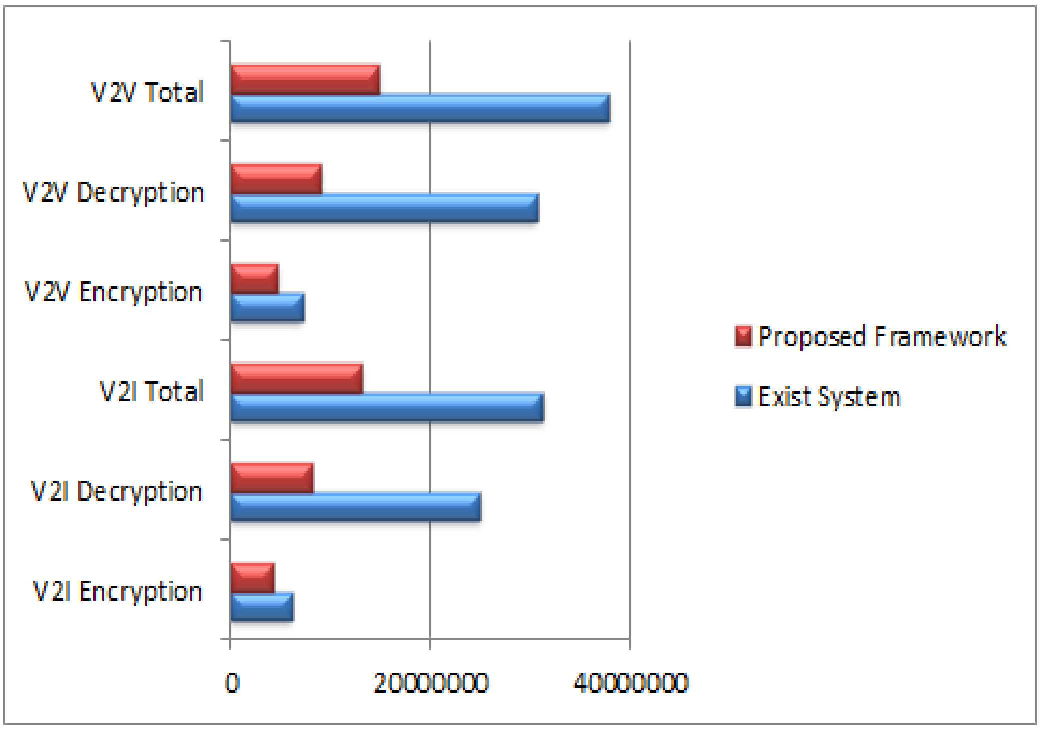

Figure 6. Comparison of Performance Speed of the Existing System and the Proposed Framework

Table 1. Analysis and Comparison of the Proposed Encryption Method and the Standard Code (Speed unit: nanosecond)

	DES	SEED	AES	RSA	Proposed Cryptography System
Key Size	56	128	128	1024	160
Average of Encryption & Decryption time (100 times)	320976959	5276676	47262008	9718287	3913663
Minimum of Encryption (100 times)	229840186	3914225	36129968	1696618	1119241
Minimum of Decryption (100 times)	1136773	162451	132040	7314533	2218762

The unit of performance speed was measured by nanosecond and in the existing system, V2I was 31154861 nanoseconds and V2V was 37844604 nanoseconds. In the proposed system, V2I basis was 13140989 nanoseconds and V2V was 14856115 nanoseconds, showing roughly 57% and 60% improvement in speed. To analyze the performance of the proposed algorithm, the research article compared it with the code algorithm of each standard and analyzed the average, maximum, and minimum hours of 10 times of each encryption and decryption except for the key generating part.

The identity-based code based on the proposed ECC had higher encryption performance than that of DES, SEED, AES, which is based on symmetric key. RSA encryption based on non-symmetry did not show differences in the encryption performance, but the performance range in the decryption performance dropped by more than 3 times roughly. The proposed encryption method showed effective operation speed in the encryption/decryption performance.

5. Conclusion

This research article designed the communication frame work to conduct safe communication based on the cloud computing technology in the vehicle environment. The proposed frame work suggested vehicle registration, communication, and cancellation protocol to complement the safety of messages that happen in the vehicle and also enhance effectiveness. The proposed frame work was analyzed in terms of its safety by applying the attack techniques that happen in the existing system. To conduct safety evaluation, the performance speed was compared by applying the identity-based code method based on PKI and ECC, which is used in the existing cloud vehicle environment. And by measuring the proposed code method and DES, AES, SEED, RSA, we could confirm that there was improved speed of approximately 57% in V2I and 60% in V2V.

So far, the researches on individual areas such as vehicle communication, cloud computing technology and message communication technology have been actively done, but there have not been many researches on the convergence technology environment. As a result, the prevention of the safety threats against the new and mutated attacks and measures for safety requirements are needed. Also, for the vehicle cloud communication, the technologies of the vehicle industry and IT industry are being converged, and in most of the self-driving cars that are currently being developed provide convenience for the users by installing various kinds of sensors. In this regard, various researches are needed to conduct this safely.

References

[1] M. H. Hu, K. H. Lee, “Vehicular And Security Requirement”, korea institute of information Security & Cryptology, vol. 24, no 2, **(2013)**.C. E. Larsen, R. Trip and C. R. Johnson, “Methods for procedures related to the electrophysiology of the heart”, U.S. Patent 5,529,067, **(1995)**.

[2] TTAK.KO-06-0402, “Data Exchange Protocol for Vehicle Road Guidance”, TTA, 2015. 12.

[3] TTAK.KO-12.0208, Security Requirements for Vehicle-to-Vehicle Communication, TTA, 2012.12.21

[4] TTAK.KO-06.0174, Requirements for Wide-Area Wireless Communication for ITS/Telematics, TTA, 2008. 6. 26.

[5] S. Olariu, T. Hristov, and G. Yan, “The Next Paradigm Shift: From Vehicular Networks to Vehicluar Cloud”, Mobile Ad Hoc Networking: Cutting Edge Directions, Second Eition, John wiley & Sons, Inc., **(2013)**.

[6] B. K. Chaurasia, “Infrastructure based Authentication in VANETs”, International Journal of Multimedia and Ubiquitous Engineering, vol. 6, no. 2, **(2011)**.

[7] G. Yan, D. B. Rawat and B. B. Bista, “Toward Secure Vehicular Clouds”, 2012 Sixth International Conference on Complex, Intelligent, and SoftWare Intensive System, **(2012)**, pp. 370-375.

[8] J.-O. Park, D.-H. Choi, “A Design of Framework for Secure Communication in Vehicular Cloud Environment”, vol. 19, no. 9, **(2015)**, pp. 2114-2010.

[9] S.-T. Yoo, S.-H. Oh, “OAuth-based User Authentication Framework for Internet of Things”, KAIS, vol.16, no.11, **(2015)**, pp.8057-8063.

[10] K.-H. Lee, J.-S. Lee, S.-Y. Min, “A design on Light-Weight Key Exchange and Mutual Authentication Routing Protocol in Sensor Network Environments”, KAIS, vol.16, no.11, **(2015)**, pp. 7541-7548.

[11] B.-K. Lee, E.-H. Lee, “Design of UIGRP(Urban Intersection based Geographic Routing Protocol) considering the moving direction and density of vehicles”, KAIS, vol.16, no.1, **(2015)**, pp. 703-712.

[12] H.-J. Shin, “Design and Implementation of Network Access Control based on IPv6”, KAIS, vol.15 no.10, **(2015)**, pp. 6310-6316.

[13] J.-W. Kim, J.-H. Park, M.-S. Jun, “A Design of Smart Banking System using Digital Signature based on Biometric Authentication”, KAIS, vol.16, no.9, **(2015)**, pp. 6282-6289.

Authors

Byung Wook Jin received his B.S. degree in Multimedia Science from ChungWoon University, Chungnam, Korea. in 2011, and M.S. degree in Computer Science from Soongsil University, Seoul, Korea, in 2013. He is Currently a Ph.D Course in the Computer Science, Soongsil University. His research interests include Internet Of Thing, Authentication System, Network Security.

Jung-Oh Park is a Professor of Department of Paideia, Sungkyul University, Korea. His research interests include: PKI and Ubiquitous Computing. His address is: Sungkyuldaehakro-53, Manan-gu, Anyang-City, Gyeonggi-Do, 430-742, South Korea. His phone number is +82-10-3357-8873 and the email address is jopark02@sungkyul.ac.kr

MoonSeog Jun, He has Ph.D. degree in Computer Science from Maryland University, United State of America, in 1989. He is currently an Professor in SoongSil University, Seoul, Korea. His research interests include Information Protectm Aythentication system, Cryptography.