Information **2014**, *5*, 526-534; doi:10.3390/info5040526

OPEN ACCESS

information

ISSN 2078-2489

www.mdpi.com/journal/information

Article

VBSM: VCC-Based Black Box Service Model with Enhanced Data Integrity

Won Min Kang, Jae Dong Lee and Jong Hyuk Park *

Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, SeoulTech, 172 Gongreung 2-dong, Nowon-gu, Seoul 139-743, Korea;
E-Mails: wkaqhdsk0@seoultech.ac.kr (W.M.K.); jdlee731@seoultech.ac.kr (J.D.L.)

* Author to whom correspondence should be addressed; E-Mail: jhpark1@seoultech.ac.kr;
Tel.: +82-2-970-6702; Fax: +82-2-977-9441.

External Editor: Jason C. Hung

Received: 25 June 2014; in revised form: 10 October 2014 / Accepted: / 13 October 2014
Published: 17 October 2014

Abstract: Recently, intelligent transport systems have been applied to vehicle cloud environments. Such technology is especially useful for the systematic management of road traffic. Moreover, automobiles are increasingly equipped with a black box for accident prevention and preservation of evidence. Vehicle black boxes have become mandatory because black box images and voice data have served as forensic evidence in courts. However, the data from black boxes can be forged or modified by man-in-the-middle (MITM) attacks and message hijacking. In this paper, we propose a vehicle cloud computing-based black box service model that can provide integrity for black box data through digital signatures in vehicle cloud computing (VCC) environments. Our proposed model protects against MITM attacks and message hijacking using only a hash value and digital signature. Moreover, a mirroring technique (RAID 1) provides backup and recovery to protect the data from a traffic accident.

Keywords: vehicle black box; hash function; vehicle cloud computing; digital signature

1. Introduction

The concept of an automobile has changed from simply providing faster transportation to ensuring safe and convenient transportation in modern society. In addition, intelligent transport systems (ITS) are being introduced to the world to resolve problems related to traffic congestion and collisions [1,2].

Recently, vehicle cloud computing (VCC) technology has come to the fore as a smart service, combining ITS with cloud computing. With VCC technology, users can drive more efficiently, utilizing vehicle networks and storage.

Nowadays, vehicles with black boxes are increasingly common. However, there are some limitations to this technology, mostly relating to insufficient storage capacity and the inability to provide data integrity. Ample research is being carried out to resolve these limitations by using VCC to expand the storage capacity in black boxes and to ensure data integrity.

Black box technology has long been used ubiquitously in airplanes, serving, among other things, as a device to identify the cause of a major accident. This concept is now being applied to automobile black box devices, so that traffic accidents can be recorded and the driver's voice and crash images are preserved [2–4]. As the installation of a black box becomes mandatory, it will prove advantageous for identifying the cause of a collision, helping to resolve conflicts between victims and offenders in traffic accidents, as well as providing forensic evidence [5,6]. Currently, however, black boxes installed in vehicles raise a security issue, because videos, pictures and voice data recorded for traffic accidents can be forged or modified, invalidating it as evidence in court. In response to this, we propose a VCC-based vehicle black box service model (VBSM) that can ensure the integrity of black box data.

The remainder of this paper is organized as follows: In Section 2, we discuss related works, including the security requirements for VCC, existing research and the core technology behind vehicle black boxes for ensuring data integrity. Section 3 presents our VBSM, which provides data integrity and permits the recovery of data in the event of any damage to the system. In Section 4, we conclude and discuss the direction of our future research.

2. Related Works

2.1. Security Considerations in VCC

In this section, we consider security threats and requirements.

(1) MITM attack: Because VCC makes use of cloud technology, users download black box data using an Internet connection. However, this process is currently done without encryption, such that an attacker could intercept the data or eavesdrop in the middle of the process, compromising the data in a black box. We should therefore consider a protection scheme against man-in-the-middle (MITM) attacks.

(2) Data integrity: Black box data can be forged or modified, thus suggesting the need for a method to preserve the integrity of black box data. If a malicious user attempts to forge or modify downloaded black box data, such as images or voice data, the forged data cannot be guaranteed as forensic evidence. Even if the original data is forged or modified, data integrity should be established by some method, such as a digital signature. Due to this potential problem, the integrity of the data in a black box must be ensured [1].

(3) Data backup and recovery: A vehicle black box should be prepared in the event that damage to the data results. Vehicle black boxes are always exposed to the risk of a traffic accident. When a major accident occurs, a vehicle black box that is installed on the front side of a vehicle is likely to be damaged. Accordingly, we should consider an alternative scheme for a damaged vehicle black box by mirroring the data contained in it.

2.2. Existing Research

Kim *et al.* [5] proposed a real-time technique to guarantee the integrity of data. This technique involves supplying users with a smart card from a trusted third party upon purchasing a black box. A unique signature key is stored in the smart card. Using this signature key, a public key is employed, and data integrity is provided via the digital signature. However, this method cannot guarantee data management and protection, or even data integrity, if the smart card or the black box is damaged.

Kim and Yeong [7] proposed a method for encryption and integrity with respect to vehicle black box data. In the data-security storage module, vehicle information generated in a black box is protected using an encryption module. This module combines the data located in the memory event folder and a normal folder with a secure hash algorithm (SHA-1) and an algorithm providing an advanced encryption standard (AES). When a predefined effect is detected, the result is stored in the secure data folder of the memory. Integrity validation is subsequently conducted by comparing the encrypted data stored in the secure data folder with the encrypted data previously generated by the encryption module. If the two values are identical, validation is completed. In this scheme, data is protected and data integrity is ensured. However, this scheme cannot guarantee the integrity of data in a black box that is transferred from the device.

An e-black box system, proposed by Nguyen *et al.*, is a device that can be mounted in any vehicle. This device uses an On Board Diagnostics-II (OBD-II) protocol to communicate with the electronic control unit (ECU) to identify information internal to the vehicle. It furthermore records vehicle information via cameras and a GPS. Users can identify the location of the e-black box using a smartphone, and black box information is provided through a computer. However, under such circumstances, the e-black box poses a security threat, exposing the data to forgery or modification [8].

2.3. Core Technologies

A hash function processes an arbitrary long input value to produce a short result value. It is a function for receiving as input a message of arbitrary length and outputting a fixed-length hash value. One of the reasons for using such a function is to ensure data integrity by extracting an evidence value for input messages that cannot be changed, thereby detecting errors in messages or modifications to them. It can also be used with a digital signature, using a private and public key as a method for reducing the length of the signature text via the hash value obtained through a hash function. This ensures the integrity of the data in a black box, thereby maximizing its resource efficiency [9,10].

A vehicle black box should always be operational whenever the vehicle is running. A vehicle black box mounted at the front of a vehicle is at a high risk of damage should a traffic accident occur. Once the black box is damaged, its data is destroyed and no longer retrievable. Thus, a mirroring technique is warranted to guarantee the availability of the system. Such a technique redirects the input/output

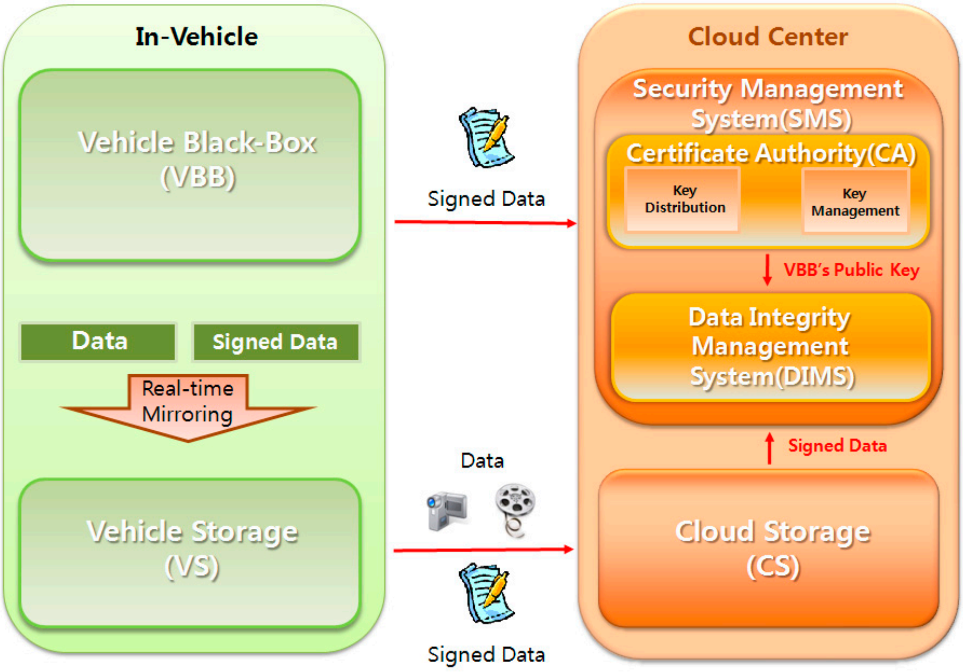
(I/O) operations to a mirror disk as soon as a physical defect is discovered in the primary disk. Even if the primary disk experiences I/O problems, a backup mirror disk provides the required I/O services, ensuring operational continuity [11,12].

3. The Proposed VBSM

In this section, we introduce a VCC-based vehicle black box service model (VBSM) that provides enhanced data integrity.

The most significant security problem in a vehicle black box is the risk that a malicious user can forge or modify black box data. The data cannot be used as legal evidence under such circumstances. Figure 1 shows the architecture for the proposed VBSM.

Figure 1. Architecture of the vehicle black box service model (VBSM).



There are three main parts constituting the proposed model: the cloud center (CC), the vehicle black box (VBB) and the vehicle storage (VS).

First, the CC consists of a security management system (SMS) and cloud storage (CS). Specifically, the SMS is composed of a certificate authority (CA) and a data-integrity management system (DIMS). The CA is implemented to manage and distribute the encryption key, and the DIMS manages the hash values and related data. Furthermore, the DIMS compares the hash values to provide data integrity. Finally, the CS stores and manages data and signed data in the VS.

Second, the VBB, once the hash values for video, pictures and voice data are generated, extrapolates the digital signature with the hash values of data and stores both the data and signed-data in the VS.

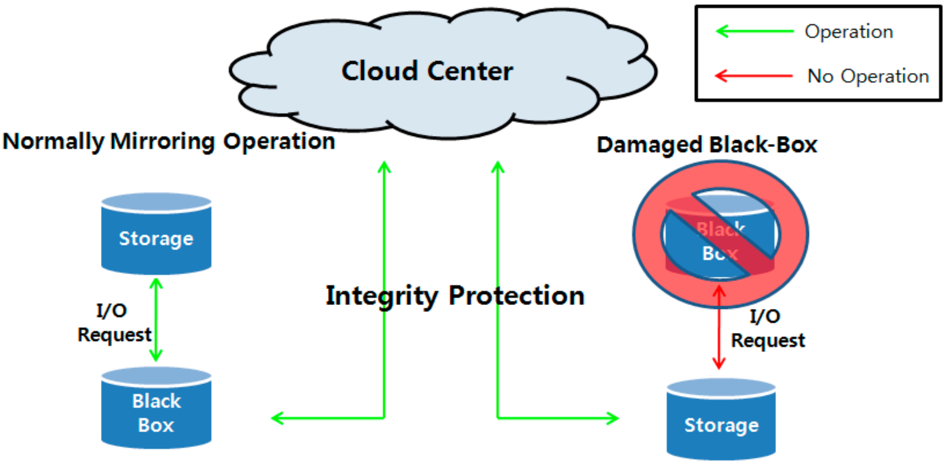
Third, should a user choose to store data and park a car, the VS transfers the stored data to CS facilitated by the CC. Moreover, should the vehicle be involved in an accident, the data is immediately transferred into CS through the CC.

3.1. Black Box Data Mirroring

One of the important requirements for a vehicle black box is to ensure that data is not destroyed. Video, pictures and voice data captured by the black box play an important role in the identifying the cause of a traffic accident. If the black box is sufficiently damaged, data loss is sure to occur. Therefore, data loss from black box damage should be taken into consideration.

The data in the proposed VBSM is protected by mirroring the black box data using a vehicle storage system located at the rear of the vehicle. When vehicle storage cannot communicate with the black box, it is assumed that the black box is damaged, and integrity validation is performed between the vehicle storage and the cloud center. Figure 2 shows the mirroring operation for data backup into storage mounted at the rear of a vehicle with an internal network.

Figure 2. Mirroring operation for black box data.



3.2. VBSM Service Scenario

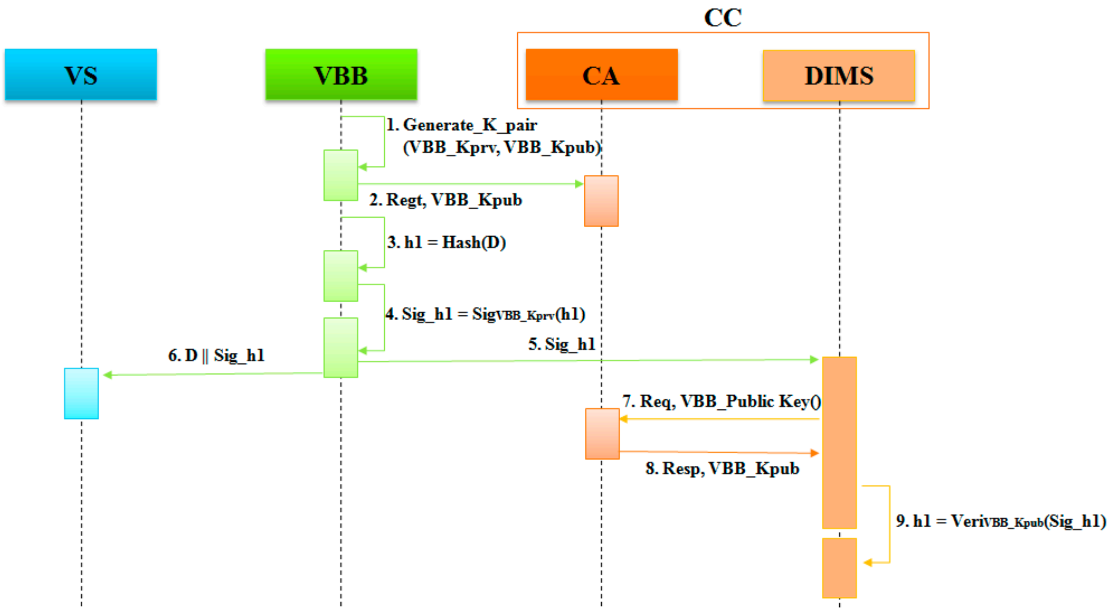
3.2.1. VBSM of General Operation

Figure 3 illustrates the general operation of the VBSM with defined functions shown in Table 1.

Table 1. Explanation of terms.

Terms	**Explanation**
Regt ()	Register function
Hash ()	Hash function
Sig ()	Digital signature algorithm
Veri ()	Verify function
Cmp ()	Compare function
D	Data: vehicle black box (VBB)
h1	Hash value of the data
Sig_h1	Digital signature for h1 data
h2	Hash value of the verified Sig_h1

Figure 3. The VBSM's general operation.



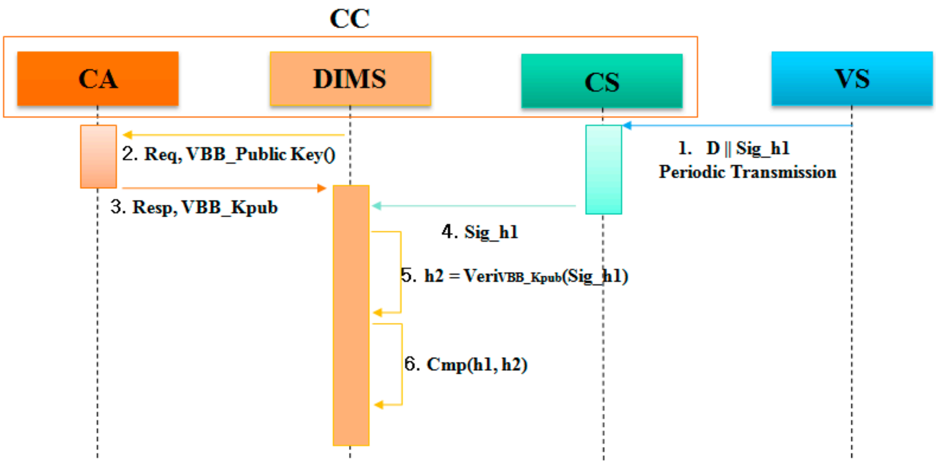
Step 1 VBB: Generate_K_pair (VBB_Kprv, VBB_Kpub)
The black box generates a key pair, such as the VBB's private and public keys.
Step 2 VBB→CA: Registering the VBB_Kpub
The black box registers the VBB's public key at the certificate authority.
Step 3 VBB: h1 = Hash(D)
The black box calculates a hash value for data such as video, pictures and voice data in the VBB.
Step 4 VBB: Sig_h1 = SigVBB_Kprv(h1)
The black box generates a digital signature using the VBB's private key and the hash value from Step 3.
Step 5 VBB→DIMS: Sig_h1
The Sig_h1 is transferred from the vehicle black box to a data integrity management system.
Step 6 VBB→VS: D || Sig_h1
Data, such as video, pictures and voice data, in the VBB and Sig_h1, are transferred from the black box into vehicle storage.
Step 7 DIMS→CA: Requesting the VBB_Kpub
The data integrity management system requests the VBB's public key from the certificate authority.
Step 8 CA→DIMS: Responding with the VBB_Kpub
The certificate authority distributes the VBB's public key to the data integrity management system.
Step 9 DIMS: h1 = VeriVBB_Kpub(Sig_h1)
The data integrity management system verifies the Sig_h1 and stores the h1.

3.2.2. VBSM's Special Cases Operation

Figure 4 demonstrates the operation of the VBSM in special cases. If a user chooses to store the data and park the car, the VS periodically transfers the data and signed data into CS through the CC.

Furthermore, if the vehicle sustains damage in the event of an accident, the VS sends both the data and signed data into CS through the CC, ensuring data integrity.

Figure 4. VBSM of special cases operation.



Step 1 VS→CS: D || Sig_h1
From the CC, data and Sig_h1 in the vehicle storage are periodically transferred to cloud storage.
Step 2 DIMS→CA: Requesting the VBB_Kpub.
The data integrity management system requests the VBB's public key from the certificate authority.
Step 3 CA→DIMS: Responding with the VBB_Kpub
The certificate authority distributes the VBB's public key to the data integrity management system.
Step 4 CS→DIMS: Sig_h1
Cloud storage transfers a Sign_h1 to the data integrity management system for data integrity.
Step 5 DIMS: h2 = VeriVBB_Kpub(Sig_h1)
The data integrity management system verifies the Sig_h1 and stores h2.
Step 6 DIMS: Cmp(h1, h2)
The data integrity management system compares the hash values of h1 and h2.

3.3. Efficiency Analyses of VBSM

In this subsection, we present the results of comparative analyses of our proposed VSBM with existing models. The following security threats were considered, as described in Section 2.1: protection from MITM attacks, protection from data forgery and modification and data recovery. The proposed VBSM is secure from MITM attacks that can expose data via wiretapping by malicious users who intervene in the communication between the black box and the cloud center. The existing research did not consider external environments, such as connections with other devices. We considered that signed data is communicated between the cloud center and the vehicle black box, and the stored data in a black box is secure from MITM attacks. The VBSM also protects against data forgery and modification. The VBSM generates a digital signature using hash values for data integrity. The process for ensuring data integrity in the VBSM is detailed in Sections 3.2.1 and 3.2.2. Finally, the existing research did not use external storage. However, the VBSM prevents data loss from damaging the black box. In addition, the VBSM provides the restoration of data. Backup data is stored in the vehicle storage located at the rear of the vehicle utilizing a mirroring technique known as "RAID 1". Even if the black box is damaged in a traffic collision, the storage system communicates with the cloud center to retrieve the data preserved in cloud storage.

Table 2. Analyses of performance.

Category	**VBSM**	**[3]**	**[4]**	**[5]**
Protection from MITM attacks	O	X	O	X
Protection from data forgery and modification	O	O	O	X
Data recovery	O	X	X	X

(O, good; X, weak)

4. Conclusions

In this paper, we proposed a VCC-based vehicle black box service model. Our model solved an existing problem related to data integrity in vehicle black boxes. We used cloud computing technology with digital signatures to ensure that the data stored in our proposed device is secure. We furthermore considered data backup and recovery in damaged black boxes providing data storage at the rear of the vehicle, implementing a RAID 1 mirroring technique. Existing black boxes do not provide data integrity. However, by providing integrity, data from black boxes can be used as evidence in court trials relating to traffic accidents. Our model provides this opportunity with security and reliability. In future research, we will study how to improve the processing speed during integrity validation in the vehicle black box. We further intend to research security issues arising from backup data at the front of the vehicle and the data stored at the vehicle's rear.

Acknowledgments

This study was supported by the Research Program funded by the Seoul National University of Science and Technology (U2014-0092).

Author Contributions

Won Min Kang developed the concept and drafted the manuscript, which was revised by Jae Dong Lee. Jong Hyuk Park supervised the overall work. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Han, J.W.; Lee, B.G.; Son, M.H.; Choi, B.C.; Kim, M.S.; Na, J.C.; Cho, H.S. Security Trends in Intelligent Vehicle Transport System. In *Electronics and Telecommunications Trends*; Electronics and Telecommunications Research Institute: Daejeon, Korea, 2013; pp. 86–94.

2. Kim, M.S.; Choi, S.G.; Jeong, C.Y.; Han, J.W. Security Issues and Trends in Vehicle Black box. In *Electronics and Telecommunications Trends*; Electronics and Telecommunications Research Institute: Daejeon, Korea, 2012; pp. 123–129.
3. Jeong, S.-W.; Park, Y.-H. Integrated video management system for vehicle black box using the mobile cloud. *J. Korea Inst. Inf. Commun. Eng.* **2013**, *17*, 2352–2358.
4. Kim, M.; Nam, J.-H.; Jang, J.-W. Implementation of smart car infotainment system including black box and self-diagnosis function. *Int. J. Softw. Eng. Appl.* **2014**, *18*, 267–274.
5. Kim, Y.Y.; Kim, B.H.; Lee, D.H. Real-time integrity for vehicle black box system. *J. Korea Inst. Inf. Secur. Cryptol.* **2009**, *19*, 49–61.
6. Choi, S.-O.; Kim, Y.-P.; Im, Y.-S.; Kim, Y.-J.; Kang, E.-Y. Smart Moblie Blackbox DVR in car Environment. *J. Inst. Internet Broadcast. Commun.* **2013**, *13*, 9–15.
7. Kim, M.S.; Jeong, C.Y. An Efficient Data Integrity Scheme for Preventing Falsification of Car Black box. In Proceedings of the 2013 International Conference on ICT Convergence (ICTC), Jeju, Korea, 14–16 October 2013.
8. Nguyen, D.L.; Lee, M.-E.; Lensky, A. The Design and Implementation of New Vehicle Black box Using the OBD Information. In Proceedings of the 2012 7th International Conference on Computing and Convergence Technology (ICCCT), Seoul, Korea, 3–5 December 2012.
9. Verkhovsky, B.S. Public-key cryptosystems with secret encryptor and digital signature. *Int. J. Innov. Technol. Explor. Eng.* **2013**, *2*, 321–325.
10. Noroozi, E.; Daud, S.M.; Sabouhi, A. Secure digital signature schemes based on hash functions. *Int. J. Commun. Netw. Syst. Sci.* **2013**, *6*, 1–6.
11. Wan. H.; Cho, H.E.; Heon, Y.; Yeom, A. Study on mirroring for high-availability cloud storage. *J. Korean Inst. Inf. Sci. Eng.* **2011**, *38*, 273–276.
12. Meckel, H.; Stephan, C.; Bunse, C.; Krafzik, M.; Reher, C.; Kohl, M.; Meyer, H.E.; Eisenacher, M. The amino acid's backup bone—storage solutions for proteomics facilities. *Biochim. Biophys. Acta* **2014**, *1844*, 2–11.