Secure Data Sharing for Vehicular Ad-hoc Networks Using Cloud Computing

Mehdi Sookhak[1], F. Richard Yu[1](✉), and Helen Tang[2]

[1] Department of System and Computer Engineering,
Carleton University, Ottawa, ON, Canada
mehdi.sookhak@carleton.ca, richard.yu@carleton.ca
[2] Defence Research and Development Canada, Ottawa, ON, Canada
Helen.Tang@drdc-rddc.gc.ca

Abstract. During the last decade, researchers and developers have been attracted to Vehicular Ad-hoc Network (VANET) research area due to its significant applications, including efficient traffic management, road safety, and entertainment. Several resources such as communication, on-board unit, storage, computing, and endless battery are embedded in the vehicles, which are used for enhancing Intelligent Transportation Systems (ITSs). One of the crucial challenges for VANETs is to securely share an important information among vehicles. In some cases, the data owner is also not available and unable to control the data sharing process, i.e., sharing data with a new user or revoking the existing user. In this paper, we present a new method to address the data sharing problem and delegate the management of data to a Trusted Third Party (TPA) based on bilinear pairing technique. To achieve this goal, we use a cloud computing, as the mainstream platform of utility computing paradigm, to store the huge amount of data and perform the re-encryption process securely.

Keywords: Vehicular ad-hoc networks · Cloud computing · Data access control · Bilinear pairing technique · Proxy re-encryption

1 Introduction

Recent improvements in hardware, software, and communication technologies lead to many improvements and developments in the networking area. One of the main networking technologies that has attracted the researchers' and industries consideration over the last decades is VANETs [1]. VANET is a self-organized network composed of mobile nodes connected with wireless links where the vehicles act as nodes [2]. Vehicular network is formed between moving vehicles equipped with wireless interfaces that could be homogeneous or heterogeneous technologies. These networks are considered as one of the real-life applications of the ad-hoc network, which enable communications among nearby vehicles as well as between vehicles and nearby fixed equipment (roadside equipment). Vehicles can communicate to infrastructure in a Vehicle-to-Infrastructure (V2I) design

Y. Zhou and T. Kunz (Eds.): ADHOCNETS 2016, LNICST 184, pp. 306–315, 2017.
DOI: 10.1007/978-3-319-51204-4_25

where Road Side Unit (RSU) functions as an interface between On Board Unit (OBU) and main core network. Vehicles can also directly communicate to each other in Vehicle-to-Vehicle (V2V) design [3].

The main aim of VANET is to provide safety for drivers and passengers by developing novel applications and solutions. The idea of vehicular network has been expanded into ITS and Intelligent Vehicular Network as promising solutions to transportation and traffic-related problems in modern cities by creating safe, secure, and healthy environment [4]. However, the growth of vehicular network and its applications and services requires scalable infrastructure, computing capacity, and storage [5].

One of the main challenges of vehicular networks is to securely share the critical information among vehicles. To address this problem, the data owner who wants to share the data with other vehicles, can outsource the data to the remote servers of cloud computing [6,8]. However, delegating the management of such an important information to the untrusted cloud server is not reasonable, due to the confidentiality and integrity of outsourced files [13,14]. One way to solve this problem is using the proxy re-encryption technique that allows the data owner to encrypt the data before outsourcing to the remote servers, and delegate the management of encrypted data to the cloud server without requiring to decrypt them. Although there are several methods to support proxy re-encryption in cloud computing, the data owner must generate a re-encryption key for allowing a new user to access the data and decrypting it. Therefore, the existing methods are inapplicable when the data owner is unavailable. Moreover, sending the owner's private key to the third part to perform the management is not a usable solution.

This paper presents a new method for securely sharing data in the vehicular networks by using cloud computing and the bilinear pairing technique. After encrypting the data, the data owner, who wants to share the data, transfers it to the cloud computing, which is responsible for re-encrypting the ciphertext for the users. The data owner also delegates the key management of the encrypted data to the TPA while preserving the privacy of data by blinding the private key. As a result, when a new user requests to access the outsourced data, the TPA is able to generate the re-encryption key, which allows the user to decrypt it by the user's private key.

The rest of the paper is organized as follows: Sect. 2 presents a background on vehicular networks, and vehicular cloud computing. Section 3 explains the preliminaries and makes an overview on the bilinear pairing technique. Section 4 describes the architecture and system operation of the proposed method. The related works as well as the advantages and disadvantage of the existing methods are stated in Sect. 5. Finally, we conclude the paper in Sect. 6.

2 Background

This section explains the concept of cloud computing, mobile computing and vehicular networks, respectively, since these are the cornerstone of vehicle cloud computing concept.

2.1 Vehicular Ad-hoc Networks

In this era, by growing the new intelligent technologies as a remarkable contributor of transportation systems, the employing of ITS concept has significantly brought attention of governments and academia in this area [9]. Meanwhile, the use of VANET as a subset of Mobile Ad-hoc Network (MANET) is the significant wireless technology proposed exclusively for vehicular environment. The employment of this technology in ITS is the concept which is significantly demonstrated to enhance the road safety, efficiency, and services through real-time V2V and V2I communications [10].

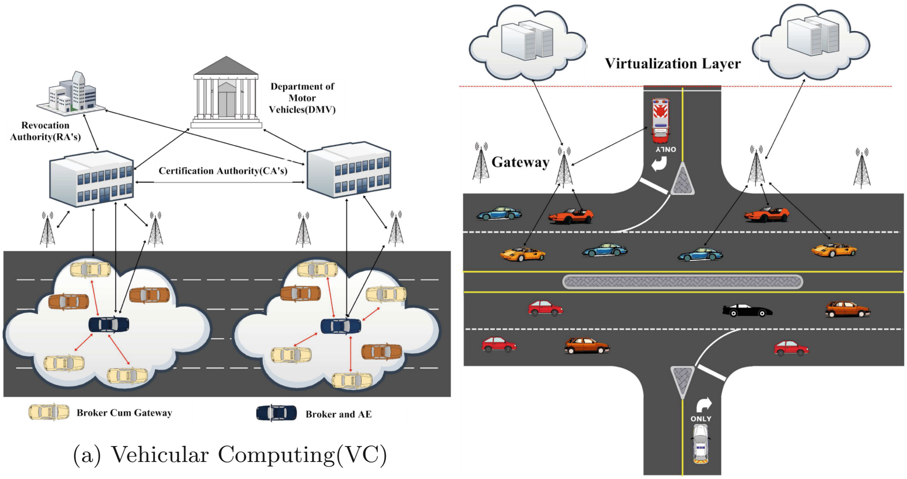
In ITSs, each vehicle plays the role of sender, receiver, and router to broadcast data to the vehicular network, which then utilizes the data to ensure safe and free-flow of traffic [11]. To take place the communication between RSUs and vehicles, vehicles must be equipped with OBU that enables short-range wireless ad-hoc networks to be formed. In addition, vehicles must be equipped with a hardware, which permits detailed position information, such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. On the other side, fixed RSUs that are linked to the backbone network must be mounted, to facilitate communication. Communication configurations in VANET contain V2V, V2I, and routing-based communications. They rely on very accurate information regarding the surrounding environment, which requires the employment of accurate positioning systems and well communication protocols for transferring information [12].

2.2 Vehicular Cloud Computing

Cloud computing is a comparatively new trend in the field of Information Technology (IT) that decreases computing, storage and other functions from traditional desktop and portable computer devices since all the functions can be virtualized in cloud computing platform [15,17]. Cloud computing provides ubiquitous, applicable, and on-demand network access to the vast shared computing resources, such as all networks, servers, storages, applications, and services. Consequently, end users only need some simple I/O devices to enjoy powerful processing ability and convenient service in cloud computing platform [18]. One of the main applications of cloud computing is in vehicular networks, as vehicular cloud computing.

Vehicular cloud computing can be divided into two categories: (1) Vehicular Computing, and (2) Vehicular using Cloud. In the first type of VCC, each vehicle can play a role as a datacenter, while in the VuC, the vehicles will be connected to the cloud for outsourcing data and augmenting the computation resources [6]. In the following, we briefly explain these two concepts:

1. Vehicular Computing (VC): The cloud computing paradigm enables the utilization of excess computing power in a way that vehicles are treated as underutilized computational resources, which can be used for providing public services. In this scenario, the parked vehicles can be counted as a huge idle



(a) Vehicular Computing(VC)

(b) Vehicular using Cloud (VuC)

Fig. 1. Vehicular cloud computing architectures

resource that is merely wasted. For instance, many people park their vehicles in the parking airports while traveling. In addition, some vehicles are stuck in congested traffic. These characters of such vehicles make them an ideal nominee for nodes in a cloud computing network [5,6]. Figure 1(a) shows three main components of VC, such as VANET infrastructure, gateways and brokers.

2. Vehicular using Cloud (VuC): It has been emerged as a new concept to efficiently solve the drivers' problem by using the cloud services instead of sharing their own resources. In VuC, vehicles utilize VANET infrastructure to connect to conventional clouds and use the real-time services, for example monitoring the real-time traffic information and infotainment. VANET infrastructure, gateways, and virtualization layer are three main components of VuC. RSUs act as gateways between the vehicles and clouds. They are also responsible to provide the virtualization layer. To connect the gateways to clouds, high speed wired communication (e.g. optical fiber) can be used, while wireless communication (e.g. V2V and V2I) is used to connect the vehicles to gateways [19,20]. It is important to mention that our proposed method is based on VuC. Figure 1b shows the general architecture of VuC.

By taking advantage of VCC, the problem of municipal traffic management centers, which is the lack of adequate computational resources, will be removed. This is because the vehicles assist local consultants to resolve traffic incidents in a timely fashion. The chief concentration of the VCC is to provide on demand solutions for unpredictable incidents in a proactive fashion. VCCs present a unified incorporation and reorganized management of on board facilities. Moreover, they adapt dynamically based on the system environments and application requirements. A federation of VCCs presents a decision support system and becomes the temporary infrastructure replacement in case of natural disaster that abolishes standing infrastructure. The Federal Communication Commission (FCC) allocated Dedicated Short-Range Communication (DSRC) for supporting the vehicular networks. Furthermore, road infrastructures such as cameras, access points, and inductive loop detectors are supportive for VCC.

3 Preliminaries and Definition

This section briefly reviews the cryptographic background about the bilinear map and the required security assumptions.

3.1 Bilinear Maps

In 2001, some researchers [21–23] introduced a special type of encryption method, which is called proxy re-encryption, on the basis of bilinear maps. Let G_1, G_2 be cyclic groups with prime order p; $g_1, g_2 \in G_1$ be the generators of the group G_1; and $a, b \in Z_p$ that indicates a, b are randomly selected from a finite set Z.

Function $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map with the following properties: (1) Bilinearity: for all $a, b \in Z_p$, it can be seen that $e\left({g_1}^a, {g_1}^b\right) = e(g_1, g_1)^{ab}$, and (2) Non-degeneracy: If $g_1, g_2 \in G_1$ have the capability to generate G_1, then $e(g_1, g_1)$ can generate G_2.

3.2 Complexity Assumptions

Most of the cryptosystems that have designed on the basis of bilinear map properties, rely on the Decisional Bilinear Diffie-Hellman (DBDH) assumption. This assumption indicates that for any $g_1 \in G_1$, $a, b, c \in Z_p$, and $Q \in G_2$, it is hard to distinguish $e(g_1, g_1)^{abc}$ from the random given that $(g_1, {g_1}^a, {g_1}^b, {g_1}^c, Q)$.

4 Proposed Method

In this section, we propose our method on the basis of proxy re-encryption technique for providing a secure mechanism to share data in vehicular-based cloud computing.

4.1 Architecture of the Proposed Method

Figure 2 shows the architecture of the proposed method, which consists of four important components, as follows: (1) Data Owner (DO): who encrypts and outsources the data to the cloud server, and delegates the re-encryption process to the cloud service provider; (2) TPA: who is responsible for adding or revoking users based on the received information from DO; (3) Cloud Service Provider (CSP): who stores the revived data from DO, checks the access control of the files, and re-encrypts data for new users; and (4) User: who asks the CSP for accessing an encrypted file.

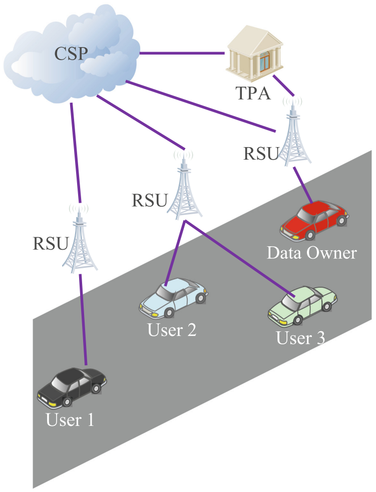


Fig. 2. The architecture of the proposed method for secure data sharing in VCC

4.2 Definition

- $KeyGen(1^k) \rightarrow (pk, sk, pp)$. This algorithm generates the public and secret key for the DO (pk_d, sk_d) and users (pk_d, sk_d) as well as some public parameters by using a security parameter 1^k.
- $KeyDelegation(sk_d) \rightarrow (Aux)$. This algorithm uses the secret key of the data owner to generate the auxiliary key that can be used by TPA to generate the re-encryption key for the users.
- $ReKeyGen(pk_u, sk_t, Aux) \rightarrow (rekey)$. The output of this algorithm is a new key that can be used by the CSP to re-encrypt the outsourced ciphertext.
- $Enc(F, pk_d, sk_d) \rightarrow (C)$. This algorithm decrypts the DO's file by using the public and secret key of the DO.
- $ReEnc(C, pk_u, rekey) \rightarrow (C')$. It is responsible to re-encrypts the outsourced ciphertext based on the users' public key and the generated key by the TPA.
- $Dec(C', sk_u)\, to\, M$. The user can use this function to decrypt the re-encrypted outsourced file (C') using her secret key.

Table 1 shows the notation of the proposed method for secure data sharing in vehicular-based cloud computing.

4.3 System Operation

The designed data sharing method for VCC consists of the following phases:

(1) *Setup.* Our method operates over two groups G_1, G_2 of order p with the bilinear map properties $e : G_1 \times G_1 \rightarrow G_2$. First of all, the system parameters $(g \in G_1, Z = e(g, g) \in G_2)$ need to be randomly generated and distributed among the users and the owners. Then, each client needs to select a random

Table 1. The notation used in explanation of the proposed method

Symbol	Description
g	A generator for G_1
Z	$e(g, g)$
x_d	Secret Key of the data owner
x_u	Secret Key of the user
g^{x_d}	Data owner public key
g^{x_u}	User public key
r	Random Number
q	Large prime Number
DO	Data Owner
TPA	Trusted Third Party
CSP	Cloud Service Provider

number as a secret key and generate her public key based on this random number, for example, $(pk_u = g^{x_u}, sk_u = x_u)$ for each user and $(pk_d = g^{x_d}, sk_d = x_d)$ for each data owner.

(2) *Data encryption and key delegation.* Assume that the DO wants to share a file $F \in G_2$ among users. The Do generates a random number r and a unique large prime number q for each file. Then, the DO encrypts F by: $C = (Z^{rq}.F, g^{r.\frac{x_d}{q}})$. Then, the owner outsources the encrypted file (C) as well as a list of the authorized users to the vehicular cloud and delegates the management of the file to the CSP. Finally, the DO makes the TPA responsible for adding a new user for this file by sending a blind version of her secret key $(\frac{q^2}{x_d})$ to the TPA.

(3) *Data re-encryption.* If a new user requests the CSP to access the encrypted file (C), firstly, the CSP has to check whether the new user has eligibility to access data. After confirming that, the CSP asks the TPA to generate the re-encryption key based on the user's public key by:

$$rekey = {pk_u}^{(\frac{q^2}{x_d})} = g^{\frac{x_u \cdot q^2}{x_d}}$$

Up on receiving the re-encryption key, the CSP re-encrypts the outsourced file (C) by using the following equation:

$$C' = (Z^{rq}.F, re - encrypt(g^{r.\frac{x_d}{q}}, g^{\frac{x_u \cdot q^2}{x_d}}))$$

$$re - encrypt(g^{r.\frac{x_d}{q}}, g^{\frac{x_u \cdot q^2}{x_d}}) = e(g^{r.\frac{x_d}{q}}, g^{\frac{x_u \cdot q^2}{x_d}}) = Z^{rqx_u}$$

(4) *Data Decryption.* After obtaining the re-encrypted file $C' = (Z^{rq}.F, Z^{rqx_u})$, the user is able to decrypt the file by:

$$F = \frac{Z^{rq}.F}{(Z^{rqx_u})^{\frac{1}{x_u}}}$$

Remark 1. It is important to mention that although the transferred parameters between DO and TPA is blinded, we can generate a session key to encrypt and decrypt the data by using the public key of the DO (pk_d) and the public key of the TPA (pk_T).

Remark 2. All of the communications between DO and TPA, DO and CSP, and User and CSP are performed by using the existing RSU and OBU.

5 Related Work

Most of the existing methods for secure data sharing have been proposed for cloud and mobile cloud computing. In this section, we make an overview on some of the proposed method based on proxy re-encryption and focus on their advantages and disadvantages.

Proxy re-encryption (PRE) is a cryptosystem, which can be used to turn a ciphertext encrypted under one key into an encryption of the same plaintext under another key by using a proxy. Blaze et al. [21] was the first to propose a PRE scheme without having to learn the plaintext and secret key based on the ElGamal cryptosystem [24]. Although this scheme is semantically secure under the Decision Diffie-Hellman assumption in G, it suffers from several issues, such as bidirectionality, collusion, and re-encryption key generation process.

Ivan and Dodis [22] presented a unidirectional PRE approach on the basis of standard public key cryptosystems in which Alices secret key is divided in two parts $sk_a = sk_1 + sk_2$ and distributed between Proxy and Bob. Although this method addressed the bidirectional problem of the first PRE scheme, it needs a pre secret-sharing, which enforces Bob to store the additional secret key.

Ateniese *et al.* [23] solved the aforementioned problems and designed a unidirectional proxy re-encryption method by using the bilinear maps. To prevent the collision attack, the authors considered a master key security without requiring the pre-sharing of secret keys between parties.

Tysowski *et al.* [25] extended the Ateniese method [23] and presented a manager-based re-encryption scheme for mobile cloud computing based on the bilinear maps. However, this method has several drawbacks, such as: considering a manager as a trusted entity to generate the public key and secret key of all other parties, and requiring the re-encryption task by changing the group membership.

We propose a first proxy re-encryption method for sharing data securely in vehicular-based cloud computing. In this method, all parties are able to generates their public and private keys. One of the main contributions of this method is that the new user can access the outsourced data even if the data owner is unavailable. This is because the data owner delegated the management of data access control to the TPA by using a blinded key results in preserving the privacy of data.

6 Conclusion and Future Work

Secure data sharing is one of the important issues in vehicular ad hoc networks. Although the vehicles are able to directly share the data using V2V communication in vehicular networks, this technique is inefficient. Recently, researchers have introduced the vehicular cloud computing, which can provide several benefits for users, such as data sharing. In this paper, we presented a secure data sharing method for vehicular-based cloud computing using a proxy re-encryption technique. When the DO encrypts the file and outsources it in the vehicular cloud, the data access management is delegated to the TPA by a blind version of her key. This method also enables a new user to request the CSP for accessing the encrypted data even if the data owner is unavailable. Future work is in progress to consider trust management in the proposed framework.

References

1. Hartenstein, H., Laberteaux, K.P.: A tutorial survey on vehicular ad hoc networks. IEEE Commun. Mag. **46**(6), 164–171 (2008)
2. Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., Zedan, H.: A comprehensive survey on vehicular ad hoc network. J. Netw. Comput. App. **37**, 380–392 (2014)
3. Toor, Y., Muhlethaler, P., Laouiti, A., Fortelle, A.D.L.: Vehicle ad hoc networks: applications and related technical issues. IEEE Commun. Surv. Tut. **10**, 74–88 (2008)
4. Dimitrakopoulos, G., Demestichas, P.: Intelligent transportation systems. IEEE Veh. Tech. Mag. **5**, 77–84 (2010)
5. Olariu, S., Hristov, T., Yan, G.: The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds Mobile Ad Hoc Networking. Wiley, Hoboken (2013)
6. Whaiduzzaman, M., Sookhak, M., Gani, A., Buyya, R.: A survey on vehicular cloud computing. J. Netw. Comput. App. **40**, 325–344 (2014)
7. Abuelela, M., Olariu, S.: Taking VANET to the clouds. In: Proceedings of the 8th International ACM Conference on Advances in Mobile Computing and Multimedia, pp. 6–13, New York (2010)
8. Yan, G., Wen, D., Olariu, S., Weigle, M.C.: Security challenges in vehicular cloud computing. IEEE Trans. Intel. Transp. Syst. **14**, 284–294 (2013)
9. Faouzi, N.-E.E., Leung, H., Kurian, A.: Data fusion in intelligent transportation systems: progress and challenges a survey. Inf. Fusion. **12**, 4–10 (2011)
10. Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETS): status, results, andchallenges. Tele Commun. Syst. **50**, 217–241 (2012)
11. Harri, J., Filali, F., Bonnet, C.: Mobility models for vehicular ad hoc networks: a survey and taxonomy. IEEE Commun. Surv. Tut. **11**, 19–41 (2009)
12. Bitam, S., Mellouk, A., Zeadally, S.: Bio-inspired routing algorithms survey for vehicular ad hoc networks. IEEE Commun. Surv. Tut. **17**, 843–867 (2015)
13. Sookhak, M., Talebian, H., Ahmed, E., Gani, A., Khan, M.K.: A review on remote data auditing in single cloud server: taxonomy and open issues. J. Netw. Comput. App. **43**, 121–141 (2014)
14. Sookhak, M., Gani, A., Talebian, H., Akhunzada, A., Khan, S.U., Buyya, R., Zomaya, A.Y.: Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues. ACM Comput. Surv. **47**, 65:1–65:34 (2015)

15. Sookhak, M., Akhunzada, A., Gani, A., Khan, M.K., Anuar, N.B.: Towards dynamic remote data auditing in computational clouds. Sci. World J., 1–12 (2014)
16. Sookhak, M., Gani, A., Khan, M.K., Buyya, R.: Dynamic remote data auditing for securing big data storage in cloud computing. Inf. Sci. (2015, in Press)
17. Yousafzai, A., Gani, A., Noor, R.M., Sookhak, M., Talebian, H., Shiraz, M., Khan, M.K.: Cloud resource allocation schemes: review, taxonomy, and opportunities. Knowl. Inf. Syst, 1–35 (2016)
18. Shiraz, M., Sookhak, M., Gani, A., Shah, S.A.A.: A study on the critical analysis of computational offloading frameworks for mobile cloud computing. J. Netw. Comput. App. **47**, 47–60 (2015)
19. Hussain, R., Abbas, F., Son, J., Oh, H.: TIaaS: secure cloud-assisted traffic information dissemination in vehicular ad hoc networks cluster. In: 13th IEEE/ACM International Symposium on Cloud and Grid Computing (CCGrid), pp. 178–179, Delft (2013)
20. Arif, S., Olariu, S., Wang, J., Yan, G., Yang, W., Khalil, I.: Datacenter at the airport: reasoning about time-dependent parking lot occupancy. IEEE Trans. Parallel Distrib. Syst. **23**, 2067–2080 (2012)
21. Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: International Conference on the Theory and Application of Cryptographic Techniques, pp. 127–144 (1998)
22. Ivan, A., Dodis, Y.: Proxy cryptography revisited. In: Proceedings of 10th Annual the Network and Distributed System Security Symposium (NDSS), pp. 1–20, California (2003)
23. Ateniese, G., Fu, K., Green, M., Hohenberger, S.: Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur. **9**, 1–30 (2006)
24. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985). doi:10.1007/3-540-39568-7_2
25. Tysowski, P.K., Hasan, M.A.: Re-encryption-based key management towards secure and scalable mobile applications in clouds. In: IACR Cryptology ePrint Archive, pp. 1–10 (2011)