Article

Vehicular Cloud Network and Information Security Mechanisms

Hsin-Te Wu [1] and Gwo-Jiun Horng [2,*]

[1] Department of Computer Science and Information Engineering , National Penghu University of Science and Technology , Penghu , Taiwan; wuhsinte@gms.npu.edu.tw

[2] Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology, Tainan, Taiwan; grojium@gmail.com

* Correspondence: grojium@gmail.com; Tel.: 886- 6-253-3131#3227

Abstract: This project designed a set of network security mechanisms for cloud applications in VANETs. At present, cloud computing is one of the government's development priorities in the industry. We divide cloud into public, private, and hybrid clouds in this project. Vehicles or passengers can access road conditions or public transport information through the public cloud; public transportation can access current driving records and users can access relevant enterprise information on the private cloud and hybrid cloud is a combination of public and private clouds. Both cloud computing or VANETs require network and information security. At present, many researches on VANETs security only focus on message communication, and neglect information storage. Researches on cloud computing security only focus on information protection, and neglect user privacy and anonymity. This project designed a set of network and information security mechanisms in line with the requirements of Confidentiality, Authentication, Non-repudiation, Conditional Anonymity, and Conditional Untraceability. This project primarily needs to achieve the following: 1.an authentication mechanism to verify the identity of each other between the passenger and the vehicle and to verify the identity with Single Sign-On; 2. vehicle or user privacy and anonymity, which need to be able to replace the anonymous ID and related parameters for the vehicle or the user; 3. a private communication mechanism, which enables any vehicle or user to communicate privately; and 4. an information security encryption method, which can encrypt the information on a cloud server to avoid unauthorized access by internal personnel or hackers.

Keywords: Vehicular Ad Hoc Network (VANET); Cloud Computing; privacy preservation; security and privacy.

1. Introduction

Today, a lot of public transportation means are equipped vehicular wireless communication devices, and the network is constructed by these devices is called Vehicular Ad Hoc Network (VANET). Recently, many topics of VANET are surveyed. For example, travel records of public transportation means can be transferred to a server for transportation companies to master the route and number of passengers of these means for further management. Passengers can send email or access value-added information services through these devices [1-4]. These network access behaviors construct a hybrid cloud mechanism based on cloud computing. Public transportations and passengers can access not only information in public clouds, such as weather and news, but also those in private clouds, such as number of passengers and travel records of means. The cloud computing pays attention to the information and network security of these transferred information, including user anonymity, privacy, and identity authentication, complying with the network security requirements of VANETs. The project aims to apply cloud computing in VANETs for users to access applications through vehicular devices, and proposes a network security mechanism in this article for each device to keep the information anonymity and security when transferring data through cloud network.

There are two vehicular communication modes in VANETs, vehicle-to-vehicle communication (IVC) and RSU (Roadside Unit) -to-vehicle communication (RVC). IVC allows each vehicle to broadcast information to other vehicles or send information to one specific vehicle via others. RVC allows vehicles to exchange information with one another within the broadcast range or communicate with and obtain information from other vehicles via wireless-device equipped RSUs. VANETs enable vehicles to exchange up-to-date traffic information, which improves the flow of traffic and driving safety. However, if the information is modified or falsified by a malicious vehicle user, serious consequences such as traffic congestion and even a traffic accident can occur. A scheme for ensuring information security is proposed in the present study.

The proposed cloud computing network and information security mechanism in VANETs adopts bilinear pairings and chameleon hash function for a RSU and a mobile device of vehicle or user to authenticate the identity of each other. It protects the privacy of user data transferred in the cloud against the decryption by the others. Moreover, it fulfills the requirements of confidentiality, authentication, non-repudiation, conditional anonymity, and conditional untraceability in the VANET. Finally, the project analyzes the performance of the mechanism and those stated in related works and analysis results show that the performance of the mechanism is better.

2. Related Work

The delay of long-term authentication in centralized AAA architectures is reduced in [5]. The article aims to protect privacy of vehicle and network security of portable electronic currency, and proposes a network security mechanism based on the Bilinear Diffie-Hellman (BDH) problem. However, based on the mechanism, each vehicle should generate key once in a while for privacy, and it costs a great of loadings for each vehicle.

A network security mechanism based on the chameleon hashing method is proposed in [6]. It can protect privacy and network communication of vehicles in VANETs. However, the greater calculation complexity and longer packet length of chameleon hashing method costs a lot of loadings for VANETs.

A network security mechanism based on the Bilinear pairing method is proposed in [7]. Although the mechanism can protect network communication of vehicles in VANETs, there is no private communication between the vehicles. Moreover, renewed parameters of related vehicles should be updated to the Trusted Authority (TA), and it causes centralized authentication issues.

The batch authentication and group signature method is proposed in [8]. Through the group signature to protect message anonymity and security, a vehicle will form a group with its neighboring ones. Vehicles in the same group will construct a set of correlated keys, and then they will encrypt messages with these keys. Since the other vehicles can not trace the sender of message, the method can protect vehicle privacy. However, the method causes that the sender of a malicious message can not be traced, too.

The architecture proposed in [9] is appropriate to vehicular networks. However, no any related network security mechanism is proposed. It causes interception or fake risks for transferred data. Moreover, since existing cloud computing network security mechanisms can not fulfill the requirements of vehicle anonymous ID and privacy, they are not appropriate to the cloud applications in VANETs. The project aims to propose a set of cloud computing network and information security mechanism in VANETs.

In literature [15], a set of network security mechanisms based on chameleon hashing was proposed to ensure vehicle privacy and network communications security in VANETs. However, owing to computational complexity and packet length of chameleon hashing, it constitutes a big burden for VANETs.

3. Background

This section will introduce the technologies used in the method developed in this study. Section 3.1 introduces system model, and Section 3.2 bilinear pairing and hard problems.

3.1. System Model

In system environment, as shown in Figure 1, we assume that the overall environment only has one TA and TA is the legally binding unit mechanism and in charge of controlling the whole network's security, which will provide the real identities of malicious nodes for legal prosecution when malicious nodes attack. On the one hand, the role of TA takes charge of validating vehicles or RSU's identities and on the other hand RSU and relevant coefficients are set by TA and RSU is set up on some common traffic facilities, such as traffic lights. TA and RSU are provided with wire/wireless communication. The communication between TA and RSU adopts wire communication, such as backbone. TA, RSU, and vehicles use short distance wireless communication equipment and the communication between RSU and vehicles adopts wireless communication. The parameters used in the method are described in the Notation section.

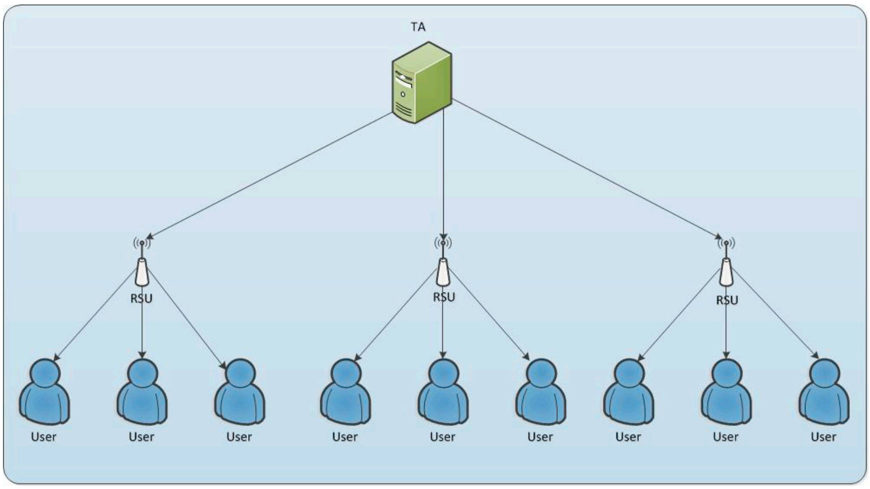

Figure 1. System Environment

3.2. Bilinear Pairings and Hard Problems

Let G₁ and G₂ denote an additive and a multiplicative group, and both them with prime order q. Let P be generator of G₁, and $\hat{e}: G_1 \times G_1 \rightarrow G_2$ be a bilinear mapping with the following properties.

1. Bilinear:

$\hat{e} = (aP, bP) = \hat{e}(P, P)^{ab}$, $\hat{e}(a \cdot P + b \cdot P, P) = \hat{e}(a \cdot P, P)\hat{e}(b \cdot P, P)$, for all $P \in G_1$ and $a, b \in Z_q^*$.

2. Non-degeneracy:

$\exists P \in G_1$ such that $\hat{e}(P, P) \neq 1$. That is, the mapping does not send all pairs in $G_1 \times G_1$ to the identity in G_2.

3. Computable:

There exists an efficient algorithm to compute $\hat{e}(P, P)$ for all $P \in G_1$.

The bilinear map $\hat{e}$ can be implemented using the Weil [14] and Tate [15] pairings on elliptic curves. We consider the implementation of a Tate pairing on a Miyaji–Nakabayashi–Takano (MNT) curve [16] with embedding degree 6, where G_1 is represented by 161 bits, and the order q is represented by 160 bits.

4. Proposed Method

The proposed mechanism consists of three stages: preliminary system establishment, identity authentication, and private communication construction.

4.1. Preliminary System Establishment

For system initialization, TA generates the parameters of each communication device, and CA initializes the parameters of RSU and vehicle. The parameters of each device consist of the public key, private key, data key, and message signature. The parameters of TA are set through the following procedure:

1. TA selects a random number, $s_{ID_{t,TA}} \in Z_q^*$, as the secret value.
2. TA adopts three hash functions, $\mathrm{H}:\{0,1\}^* \to Z_q^*$, $\mathrm{H}_1:\{0,1\}^* \to G_1$, and $\mathrm{H}_2:G_2 \to \{0,1\}^*$.
3. TA sets the $PU_{ID_{t,TA}} = \mathrm{H}_1\left(ID_{t,TA}\right)$ as the public key, where $ID_{t,TA}$ is the real ID of CA.
4. TA sets the $PR_{ID_{t,TA}} = s_{ID_{t,TA}} \mathrm{H}_1\left(ID_{t,TA}\right)$ as the private key,
5. TA sets the $D_{ID_{t,TA}} = s_{ID_{t,TA}} \cdot P$ as the data key, and
6. TA sets the $B_{ID_{t,TA}} = \hat{e}\left(C_{ID_{t,TA}} P, P\right)$ as the public value, where the $C_{ID_{t,TA}} = \hat{e}\left(m_{ID_{t,TA}} P, -\alpha_{ID_{t,TA}} \cdot \gamma_{ID_{t,TA}} P\right)$.

Second, TA announces the parameters $\left(ID_{t,TA}, B_{ID_{t,TA}}, D_{ID_{t,TA}}, \mathrm{H}, \mathrm{H}_1, \mathrm{H}_2\right)$ and hide $s_{ID_{t,TA}}$. The parameters of each RSU are set through the following procedure:

1. A RSU, R_R, selects a random number, $s_{ID_{t,R_R}} \in Z_q^*$, as the secret value,
2. R_R calculates the $B_{ID_{t,R_R}} = \hat{e}\left(C_{ID_{t,R_R}} P, P\right)$ and $-s_{ID_{t,TA}} \cdot s_{ID_{t,R_R}} P$ as the public value, where $C_{ID_{t,R_R}} = \hat{e}\left(-s_{ID_{t,TA}} \cdot s_{ID_{t,R_R}} P, s_{ID_{t,TA}} \cdot ID_{t,R_R} P\right)$,
3. R_R calculates the $D_{ID_{t,R_R}} = s_{ID_{t,R_R}} \cdot P$ as the data key,
4. R_R calculates the $PU_{ID_{t,R_R}} = \mathrm{H}_1\left(ID_{t,R_R}\right)$ as the public key, where ID_{t,R_R} is the unique ID of RSU R_R, and
5. R_R calculates the $PR_{ID_{t,R_R}} = s_{ID_{t,R_R}} \mathrm{H}_1\left(ID_{t,R_R}\right)$ as the private key.

Third, the parameters of each vehicle are set through the following procedure:

1. A vehicle, V, selects a random number, $s_{ID_{t,V}} \in Z_q^*$, as the secret value,
2. V calculates the $B_{ID_{t,V}} = \hat{e}\left(C_{ID_{t,V}} P, P\right)$ and $-s_{ID_{t,TA}} s_{ID_{t,V}} P$ as the public value, were

doi:10.20944/preprints201610.004.v1

$C_{ID_{i,V}} = \hat{e}\left(-s_{ID_{t,TA}} s_{ID_{i,V}} P, s_{ID_{t,TA}} \cdot ID_{i,V} P\right)$, and

3. *V* calculates the $D_{ID_{i,V}} = s_{ID_{i,V}} \cdot P$ as the data key.

Then the vehicle, *V,* calculates the anonymous ID, $ID_{i,V}$=H($ID_{t,V}$), where $ID_{t,V}$ is its delivery engine number. Finally, the parameters of each user device are set through the following procedure:

1. A user device, *U*, selects a random number, $s_{ID_{i,U}} \in Z_q^*$, as the secret value,

2. *U* calculates the $B_{ID_{i,U}} = \hat{e}\left(C_{ID_{i,U}} P, P\right)$ and $-s_{ID_{t,TA}} s_{ID_{i,U}} P$ as the public value, were

$C_{ID_{i,U}} = \hat{e}\left(-s_{ID_{t,TA}} s_{ID_{i,U}} P, s_{ID_{t,TA}} \cdot ID_{i,U} P\right)$, and

3. *U* calculates the $D_{ID_{i,U}} = s_{ID_{i,U}} \cdot P$ as the data key.

Then the user device, *U,* calculates the anonymous ID, $ID_{i,U}$=H($ID_{t,U}$), where $ID_{t,U}$ is its identification code.

4.2. Identity Authentication

A user device, *U*, (or a vehicle, *V*) will requests identity authentication from a RSU, and obtains a temporary anonymous ID and a parameter. Then the *U* encrypts the parameter with the public key provided by the RSU, and send the result to the RSU for identity authentication. The verification process is described as follows:

1. The user device, *U*, verify the RSU: If the calculated value,

   $D_{ID_{t,R_R}} \cdot ID_{t,R_R} = \hat{e}\left(-s_{ID_{t,TA}} \cdot s_{ID_{t,R_R}} P, s_{ID_{t,TA}} \cdot ID_{t,R_R} P\right)$, based on the known values, $-s_{ID_{t,TA}} \cdot s_{ID_{t,R_R}} P$,

   $D_{ID_{t,R_R}}$, and ID_{i,R_R}, is correct, the RSU is legal.

2. *U* encrypts the parameter with the public key provided by the RSU by calculating

   $PK_{ID_{t,R_R}}\left(-s_{ID_{t,TA}} s_{ID_{i,U}} P \,\|\, D_{ID_{i,U}} P \,\|\, ID_{i,U} \,\|\, ID_{i',U} \,\|\, SK_{ID_{i',U}}\right)$ and sends the result to the RSU.

3. After receiving and decrypting the result, the RSU checks the legitimacy of the user device, *U*, by

   calculating $D_{ID_{i,U}} \cdot ID_{i,U} = \hat{e}\left(-s_{ID_{t,TA}} \cdot s_{ID_{i,U}} P, s_{ID_{t,TA}} \cdot ID_{i,U} P\right)$.

RSU stores $ID_{i',U} \,\|\, SK_{ID_{i',U}}$, where $SK_{ID_{i',U}}$ is the common session key of the RSU and the user device, U.

4.3. Private Communication Construction

Cloud Information Query:

A user device, *U*, can query cloud information through the procedure as follows:

1. *U* encrypts the message with the private key,

   $ID_{i',U} \,\|\, SE\left(ID_{i',U} \,\|\, ID_{i,U} \,\|\, SE(ID_{i,U} \,\|\, Info_{ID_{i,U}})_{SK_{ID_{i,U}}}\right)_{SK_{ID_{i',U}}}$, and sends it to the RSU.

2. RSU decrypts the message with the common session key, $SK_{ID_{i',U}}$, and send the result to TA since the identity authentication of *U* has completed.
3. After receiving and decrypting the result, TA process the query, and then encrypts the query result with the private key of $ID_{i,U}$ and sends it to the RSU.

4. RSU encrypt the query result with the common session key, $SK_{ID_{i',U}}$, and send it to $ID_{i',U}$. $ID_{i',U}$ can decrypt it by itself and obtain the query result.

Upload Data:

A user device, *U*, can upload data to cloud through the procedure as follows:

1. *U* encrypts the message with the private key, $ID_{i',U} \| SE\left(ID_{i',U} \| ID_{i,U} \| SE(ID_{i,U} \| Info_{ID_{i,U}})_{SK_{ID_{i,U}}}\right)_{SK_{ID_{i',U}}}$, and sends it to the RSU.
2. RSU decrypts the message with the common session key, $SK_{ID_{i',U}}$, and send the result to TA since the identity authentication of *U* has completed.

After receiving result, TA decrypts it with the private key of $ID_{i,U}$ and save the data in cloud.

The proposed method in the article adopts symmetric encryption to reduce the calculation of encryption/decryption and the time complexity in private communications.

5. SECURITY AND PERFORMANCE ANALYSIS

The article performs the security and performance analysis of the proposed mechanism and those stated in related works. The proposed mechanism fulfills the requirements of confidentiality, authentication, non-repudiation, conditional anonymity, and conditional untraceability.

5.1. Security analysis

1. Confidentiality: TAs, RSUs, vehicles, and mobile devices can adopts the proposed mechanism to perform private communications with their private keys.

2. Authentication: Each unit of a communication can process the identity authentication for each other without the third party.

3. Non-repudiation: Since the keys of each unit can not be faked, the sender of each message can be identified for non-repudiation.

4. Conditional Anonymity and Conditional Untraceability: A vehicle or a mobile device can obtains a different and anonymous ID when entering the region of a RSU. Therefore, a RSU can trace the real identity of a vehicle or a mobile device with the anonymous ID for its malicious behavior.

5.2. Performance analysis

The article performs the performance analysis of the proposed mechanism and those stated in related works [5-7]. The table 1 shows the Bilinear pairing [10-12] for time complexity, the table 2 shows the encryption/decryption calculations of RSA[13] and the others, and the table 3 shows the performance analysis results of the proposed mechanism and those stated in [5-7]. According to these results, the proposed mechanism requires a pairing operation time in identity authentications, and an AES encryption time and an AES decryption time in private communications. Therefore, the performance of the proposed mechanism is better than those stated in [5-7].

Table 1、Bilinear pairing Execution Time in milliseconds

Notations	Descriptions	Execution Time
T_p	Pairing operation	≈ 4.5
T_m	Point Multiplication	≈ 0.6
T_e	Field Exponentiation	≈ 0.54

Table 2、RSA/HMAC Execution Time in milliseconds

Notations	**Descriptions**	**Execution Time**
ASE	RSA encryption	0.19
ASD	RSA decryption	4.65
HMAC	HMAC	0.002
SE	ASE encryption	<0.19
SD	ASE decryption	<4.65

Table 3、performance analysis

Method **Property**	**Proposed Method**	**[5]**	**[6]**	**[7]**
Identity Authentication	4.5ms	9ms	6.04ms	4.5ms
Handoff	9.34ms	5.1ms	5.85ms	5.7ms
Private Communication Construction	ASE encryption: 0.19ms ASE decryption: 4.65ms	encryption: 9ms decryption: 9ms	encryption: 5.25ms decryption: 5.25ms	encryption: 4.5ms decryption: 4.5ms

6. Conclusions

The proposed mechanism in the article costs less encryption/decryption time in private communications. In addition, the proposed mechanism fulfills confidentiality, authentication, non-repudiation, conditional anonymity, and conditional untraceability in terms of security analysis, and it is better than those stated in the related works [5-7] based on their performance analysis results. For privacy, all data transferred in cloud should be encrypted. However, the data search with keyword can be performed after decrypting these data. In the future, the article will aim to speed up the search of encrypted data.

References

1. U.S. Dept. Transp., " Nat. Highway Traffic Safety Admin.", Vehicle Safety Communications Project. 2006.
2. S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu, " Secure incentives for commercial ad dissemination in vehicular networks", in Proc. ACM IntSymp. MobiHoc ,pp. 150-159, 2007.
3. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services.IEEE 1609, 2006.
4. IEEE P802.11p/D11.0, "Draft Amendment for Wireless Access in Vehicular Environments (WAVE)," IEEE 802.11 Working Group of the IEEE 802 Committee, Mar. 2010.
5. Lo-Yao Yeh and Jiun-Long Huang, "PBS: A Portable Billing Scheme with Fine-Grained Access Control for Service-Oriented Vehicular Networks", IEEE Transactions on Mobile Computing, Vol. 13, No. 11, November 2014.
6. Song Guo, Deze Zeng and Yang Xiang, "Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 11, November 2014.
7. T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," IEEE Transactions on Computers, vol. 63, no. 2, pp. 510–524, 2014.
8. S.-J.Horng, S.-F. Tzeng, Y. Pan et al., "B-SPECS+: batch verification for secure pseudonymous authentication in VANET," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1860–1875, 2013.

9. Jiafu Wan, Daqiang Zhang, Shengjie Zhao, Laurence T. Yang, and Jaime Lloret, "Context-Aware Vehicular Cyber-Physical Systems with Cloud Support: Architecture, Challenges, and Solutions", Context-Aware Networking and Communications 2014.
10. M. Scott, "Implementing cryptographic pairings," Lecture Notes in Computer Science, vol. 4575, pp. 177-196, 2007.
11. S. D. Galbraith, K. Harrison, D. Soldera, "Implementing the Tate pairing," Proc. of ANTS'02, LNCS 2369, Springer-Verlag, 2002, pp.324-337.
12. A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, vol. E84-A, pp. 1234-1243, May 2001.
13. Long M, Chwan-Hwa JW, and Irwind JD "Reducing communication overhead for wireless roaming authentication: methods and performance evaluation", 2008, Int J Netw Secur 6(3):331–341.
14. D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," presented at the Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, 2001.
15. M. Scott, "Computing the tate pairing," in Proceedings of the 2005 international conference on Topics in Cryptology, San Francisco, CA, 2005, pp. 293-304.
16. M. Scott, "Computing the Tate pairing," in Topics in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 293–304.
17. S. Guo, D. Zeng, and Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 2794–2803, 2014.