Hindawi
Mobile Information Systems
Volume 2017, Article ID 2925465, 5 pages
https://doi.org/10.1155/2017/2925465

Research Article

Certificateless Public Auditing with Privacy Preserving for Cloud-Assisted Wireless Body Area Networks

Baoyuan Kang, Jiaqiang Wang, and Dongyang Shao

School of Computer Science and Software, Tianjin Polytechnic University, Tianjin 300387, China

Correspondence should be addressed to Baoyuan Kang; baoyuankang@aliyun.com

Received 9 January 2017; Accepted 11 April 2017; Published 6 July 2017

Academic Editor: Stefania Sardellitti

With cloud computing being integrated with wireless body area networks, the digital ecosystem called cloud-assisted WBAN was proposed. In cloud-assisted medical systems, the integrity of the stored data is important. Recently, based on certificateless public key cryptography, He et al. proposed a certificateless public auditing scheme for cloud-assisted WBANs. But He et al.'s scheme is not a scheme with privacy preserving. After many checks on some of the same data blocks, the auditor can derive these data blocks. In this paper, we propose a certificateless public auditing scheme with privacy preserving for cloud-assisted WBANs. In the proof phase of the proposed scheme, the proof information is protected from being directly exposed to the auditor. So, the curious auditor could not derive the data blocks. We also prove that the proposed scheme is secure in the random oracle model under the assumption that the Diffie-Hellman problem is hard, and we give a comparison of the proposed scheme with He et al.'s scheme in terms of security and computation cost.

1. Introduction

Advances in wireless communication technologies, microcontroller systems, and sensor technologies have enabled the design and development of wireless body area networks (WBANs) that are playing an increasingly important role in healthcare systems because of their ability to provide continuous measurements and to monitor a patient's health status by using medical sensors implanted inside the patient's body [1].

To make a fast diagnosis and store and process sensing data in real time, cloud computing is being integrated with traditional WBANs to propose the digital ecosystem called cloud-assisted WBAN. In cloud-assisted medical systems, the data stored in the cloud-based store resource are the basis of all diagnoses. So, the integrity of the stored data is important. As a cryptographic technique, public auditing scheme [2] could provide effective data integrity check service in cloud-assisted WBANs. In a typical public auditing scheme in cloud service, there are three entities: a data user, a cloud server, and a third-party auditor. Data file from the data user is outsourced to the cloud server, and the auditor provides the data integrity check service for the data user. The data user is a resource-constrained entity, but the auditor has certain computation ability and expertise for integrity checking. After Ateniese et al.'s pioneering work [2], many auditing schemes were proposed [3–18]. But these schemes were constructed on a public key cryptographic system; data users and the auditor need more storage space or computation cost in key management and verification.

In ID-based cryptography [19], the public key of any user is his/her identity. So, it is clear that the auditing schemes on the ID-based cryptography system will reduce the costs of the data users and the auditor. Many ID-based public auditing schemes are proposed [20–23]. But, in ID-based public auditing schemes, the PKG (private key generator) knows any user's private key. It is clear that, for patient privacy information process in cloud-assisted medical systems, ID-based public auditing schemes are not secure. Recently, based on certificateless public key cryptography [24], He et al. proposed a certificateless public auditing scheme for cloud-assisted WBANs [1]. In certificateless public key cryptography, the private key of a user consists of two parts. One is the partial private key generated by the PKG, and the other is a secret key generated by the user. So, certificateless public

key cryptography simultaneously overcomes the drawback of public key cryptography and ID-based cryptography. Certificateless public auditing scheme is very applicable for cloud-assisted WBANs with energy-limited sensors and a large amount of personal sensitive information. In [1], the proposed certificateless public auditing scheme is proved to be secure and very suitable for use in cloud-assisted WBANs. But He et al.'s scheme is not a scheme with privacy preserving. After many checks on some of the same data blocks, the auditor can derive these data blocks from the proof information that the cloud server submitted.

In this paper, we propose a certificateless public auditing scheme with privacy preserving. In the proof phase of the proposed scheme, the proof information is protected from being directly exposed to the auditor. So, the curious auditor could not derive the data blocks. We also prove that the proposed scheme is secure in the random oracle model under the assumption that the Diffie-Hellman problem is hard.

The rest of the paper is organized as follows. In Section 2, we propose the system and security model. In Section 3, we review bilinear pairing and computational Diffie-Hellman problem relevant to the security of the proposed scheme. A certificateless public auditing scheme with privacy preserving is proposed in Section 4. In Section 5, we provide security proofs of the proposed scheme. In Section 6, we compare the proposed scheme with He et al.'s scheme in terms of security and computation cost. Conclusion is given in Section 7.

2. The System and Security Model

2.1. The System Model. There are four entities included in a certificateless public auditing scheme:

(1) A data user (DU) who possesses a data file needed to be stored on the cloud.

(2) A cloud server (CS) that provides data storage service to the data user.

(3) A third-party auditor (AU) who has capacities to check data integrity on behalf of the data user.

(4) A private key generator (PKG) that is responsible for setting up the system parameter and generating the partial private key for any entity by using the entity's identity information.

To reduce the burden of data file storage, the data user (DU) uploads his/her data file to the cloud server (CS) for storage, and the DU no longer possesses his/her data file locally. To ensure the data file is correctly stored in the cloud server, DU entrusts the trusted third-party AU who has expertise and computation capabilities to periodically check his/her data file integrity.

2.2. The Security Model. In a certificateless public auditing scheme, PKG is a trusted authority, DU is honest, and AU is honest but curious. CS is a semitrusted party; he/she might change or delete the data user's file for his/her benefit and forge the proof information for passing data integrity checking. We will also investigate whether AU can get any information about the data file content during the auditing process.

Our design goals are three aspects:

(1) Public auditability: AU can verify the correctness of the cloud data file blocks on demand without retrieving a copy of the whole data file or introducing additional online burden to the cloud users.

(2) Storage correctness: no cheating cloud server can pass AU's audit.

(3) Privacy preserving: AU cannot derive data user's file content from the information collected during the auditing process.

3. Preliminary

3.1. The Bilinear Pairing. Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and let G_2 be a cyclic multiplicative group of the same order. Let $e : G_1 \times G_1 \to G_2$ be a pairing map which satisfies the following conditions.

(1) Bilinearity. For any $P, Q, R \in G_1$, then

$$\begin{aligned} e(P+Q,R) &= e(P,R)\, e(Q,R), \\ e(P,Q+R) &= e(P,Q)\, e(P,R). \end{aligned} \tag{1}$$

In particular, for any $a, b \in Z_q$, $e(aP, bP) = e(P, abP) = e(abP, P) = e(P,P)^{ab}$.

(2) Nondegeneracy. There exists $P, Q \in G_1$, such that $e(P,Q) \neq 1$.

(3) Computability. There is an efficient algorithm to compute $e(P,Q)$ for all $P, Q \in G_1$.

3.2. Computational Diffie-Hellman (CDH) Problem. There is a generator P of an additive cyclic group G with order q, and there is (aP, bP) for unknown $a, b \in Z_q^*$ to compute abP.

4. The Proposed Scheme

The proposed certificateless public auditing scheme consists of seven algorithms: *setup, partial-private-key extraction, set-public key, tag generation, challenge phase, prove phase, and verify phase*.

Setup. Given a security parameter $k \in Z$, the algorithm works as follows:

(1) Run the parameter generator on input k to generate a prime q, an additive cyclic group G_1 and a multiplicative cyclic group G_2 of the same order q, a generator P of G_1, and a bilinear map $e : G_1 \times G_1 \to G_2$.

(2) Pick a random $s \in Z_q^*$ as master key of PKG and set system public key $P_{\text{pub}} = s \cdot P$.

(3) Choose four cryptographic hash functions

$$\begin{aligned} H_1 &: \{0,1\}^* \longrightarrow G_1, \\ H_2 &: \{0,1\}^* \longrightarrow Z_q, \\ H_3 &: \{0,1\}^* \longrightarrow G_1, \\ H_4 &: \{0,1\}^* \longrightarrow G_1. \end{aligned} \tag{2}$$

The system parameters are $\langle q, G_1, G_2, e, P, P_{\text{pub}}, H_1, H_2, H_3, H_4 \rangle$.

Partial-Private-Key Extraction. When any one wants to register his/her identity ID_i to PKG, the algorithm works as follows:

(1) Compute $Q_i = H(\text{ID}_i) \in G_1$.

(2) Set the partial private key $S_i = s \cdot Q_i$, where s is the master key of PKG.

Set-Public Key. Given a user's identity ID_i, this algorithm picks a random $x_i \in Z_q^*$ as the user's secret value and computes his/her public key as $P_i = x_i P$.

Tag Generation. For a data file $M = m_1 \parallel \cdots \parallel m_n$, $m_i \in Z_q$, this algorithm works as follows:

(1) For each data block m_i, choose $r_i \in_R Z_q^*$ and compute

$$\begin{aligned} R_i &= r_i \cdot P, \\ h_i &= H_2\left(m_i, R_i, \text{ID}_{\text{DU}}, P_{\text{DU}}\right), \\ Z_i &= H_3\left(m_i, R_i, \text{ID}_{\text{DU}}, P_{\text{DU}}\right), \\ T &= H_4\left(P_{\text{pub}}\right). \end{aligned} \tag{3}$$

(2) Compute

$$\sigma_{m_i} = h_i S_{\text{DU}} + x_{\text{DU}} Z_i + \left(r_i + m_i\right) T. \tag{4}$$

Let $\varphi = ((\sigma_{m_1}, R_1), \ldots, (\sigma_{m_n}, R_n))$.

(3) DU sends $(\text{ID}_{\text{DU}}, M, \varphi)$ to CS.

(4) DU sends

$$\begin{aligned} &\text{RE}_{\text{DU}} \\ &= \left(\text{ID}_{\text{DU}}, \text{ID}_{\text{CS}}, \omega = \left(\left(h_1, Z_1, R_1\right), \ldots, \left(h_n, Z_n, R_n\right)\right)\right) \end{aligned} \tag{5}$$

to AU.

Challenge Phase. To check the integrity of the outsourced data file M, AU randomly chooses a set $I \subseteq [1, n]$ and a number $a \in Z_q$ to generate the challenging information

$$\text{Chall} = \left[\text{ID}_{\text{DU}}, a, I\right] \tag{6}$$

and sends it to the CS.

Prove Phase. Upon receiving $\text{Chall} = [\text{ID}_{\text{DU}}, a, I]$, CS produces set $\omega = \{(i, v_i)\}$, $i \in I$.

Here, $v_i = a^i \bmod q$. Then, using $M = m_1 \parallel \cdots \parallel m_n$ and φ, CS picks a random number $l \in Z_q^*$, computes

$$\begin{aligned} \sigma &= \sum_{i \in I} v_i \sigma_{m_i}, \\ \mu &= \left(\sum_{i \in I} v_i m_i - l \cdot H_2(L)\right) \bmod q, \end{aligned} \tag{7}$$

and sends proof information (σ, μ, L) to the AU. Here, $L = l \cdot P$.

Verify Phase. Upon receiving the proof information (σ, μ, L), based on stored information RE_{DU}, AU computes

$$\begin{aligned} h &= \sum_{i \in I} v_i h_i, \\ Z &= \sum_{i \in I} v_i Z_i, \\ R &= \sum_{i \in I} v_i R_i. \end{aligned} \tag{8}$$

Then, it checks the equation

$$\begin{aligned} e(\sigma, P) = e\left(h Q_{\text{DU}}, P_{\text{pub}}\right) \cdot e\left(Z, P_{\text{DU}}\right) \\ \cdot e\left(R + \mu \cdot P + H_2(L) \cdot L, T\right). \end{aligned} \tag{9}$$

If the equation holds, AU accepts the proof.

The correctness of the above verification equation can be demonstrated as follows:

$$\begin{aligned} e(\sigma, P) &= e\left(\sum_{i \in I} v_i \sigma_{m_i}, P\right) = \prod_{i \in I} e\left(v_i \sigma_{m_i}, P\right) \\ &= \prod_{i \in I} e\left(v_i h_i S_{\text{DU}} + v_i x_{\text{DU}} Z_i + v_i \left(r_i + m_i\right) T, P\right) \\ &= e\left(\sum_{i \in I} v_i h_i S_{\text{DU}}, P\right) \cdot e\left(\sum_{i \in I} v_i x_{\text{DU}} Z_i, P\right) \\ &\quad \cdot e\left(\sum_{i \in I} v_i \left(r_i + m_i\right) T, P\right) \\ &= e\left(h Q_{\text{DU}}, P_{\text{pub}}\right) \cdot e\left(Z, P_{\text{DU}}\right) \\ &\quad \cdot e\left(R + \mu P + H_2(L) \cdot L, T\right). \end{aligned} \tag{10}$$

5. Security

In this section, we discuss the security of the proposed scheme in unforgeability and privacy preserving.

5.1. Unforgeability

Theorem 1. *If the CDH assumption is hard, then the proposed scheme is secure against proof information existential forgery attack from the CS.*

Proof of Theorem 1. We will show that if CS can forge valid proof information, the challenger will use the forged proof information to solve the CDH problem.

Because CS has the signature of any one file block, CS needs not do tag oracle. So, we only look at hash functions H_1, H_2 as random oracles. For given CDH problem instance (aP, bP), the challenger lets the system public key $P_{\text{pub}} = aP$, and in partial-private-key-extract phase, for two times oracles, let $Q_i = H_1(\text{ID}_i) = \beta_j(bP)$, $j = 1, 2$. β_j, selected by the challenger, is a random number. In the proof process, for the same Chall information and same random number l, let (σ_1, μ_1, L) and (σ_2, μ_2, L) be two pieces of valid proof information under two times different H_2 oracles, $H_2(L) = \eta_i, i = 1, 2$. Then, the following two equations hold:

$$\begin{aligned} e(\sigma_1, P) &= e(h\beta_1(bP), aP) \cdot e(Z, P_{\text{DU}}) \\ &\quad \cdot e(R + \mu_1 \cdot P + \eta_1 \cdot (lP), T), \\ e(\sigma_2, P) &= e(h\beta_2(bP), aP) \cdot e(Z, P_{\text{DU}}) \\ &\quad \cdot e(R + \mu_2 \cdot P + \eta_2 \cdot (lP), T). \end{aligned} \tag{11}$$

Then,

$$\begin{aligned} &e(\sigma_2 - \sigma_1, P) \\ &\quad = e(h(\beta_2 - \beta_1)(bP), aP) \\ &\qquad \cdot e((\mu_2 - \mu_1) \cdot P + (\eta_2 - \eta_1) \cdot (lP), T). \end{aligned} \tag{12}$$

So,

$$\begin{aligned} \sigma_2 - \sigma_1 &= h(\beta_2 - \beta_1)(abP) \\ &\quad + ((\mu_2 - \mu_1) + (\eta_2 - \eta_1)l) \cdot T. \end{aligned} \tag{13}$$

The challenger derives

$$\begin{aligned} abP &= (h(\beta_2 - \beta_1))^{-1} \\ &\quad \cdot (\sigma_2 - \sigma_1 - ((\mu_2 - \mu_1) + (\eta_2 - \eta_1)l) \cdot T). \end{aligned} \tag{14}$$

□

5.2. Privacy Preserving

Theorem 2. *In the proposed scheme, AU cannot derive any information about DU's data blocks during the whole auditing procedure.*

Table 1: Comparison of security.

	Unforgeability	Privacy preserving
He et al. [1]	Yes	No
Ours	Yes	Yes

Proof of Theorem 2. In the whole auditing procedure, AU can get information

$$\begin{aligned} &\text{RE}_{\text{DU}} \\ &\quad = (\text{ID}_{\text{DU}}, \text{ID}_{\text{CS}}, \omega = ((h_1, Z_1, R_1), \ldots, (h_n, Z_n, R_n))), \\ &\text{Chall} = [\text{ID}_{\text{DU}}, a, I], \\ &\sigma = \sum_{i \in I} v_i \sigma_{m_i}, \\ &\mu = \left(\sum_{i \in I} v_i m_i - l \cdot H_2(L) \right) \bmod q. \end{aligned} \tag{15}$$

But Chall $= [\text{ID}_{\text{DU}}, a, I]$ are irrelevant to the file content, and AU cannot derive any information about the data blocks from h_i, Z_i since the hash functions are secure.

AU cannot derive any information about the data blocks from equation $\mu = (\sum_{i \in I} v_i m_i - l \cdot H_2(L)) \bmod q$, since there is an unknown random number l.

Finally, AU cannot derive file content information from σ. □

6. Comparisons

In this section, we compare the proposed scheme with He et al.'s scheme [1] in terms of security and computation cost. In the comparison of computation cost, we use P, H, and E as scalar multiplication computation, hash computation, and bilinear pairings computation, respectively. We show the comparison results in Tables 1 and 2. According to Table 1, our scheme demonstrates better security, and according to Table 2 there is notable low hash computation cost in the proposed scheme. Of course, in some phases, there are high computation costs in multiplication and bilinear pairings computation.

7. Conclusion

In this paper, we propose a certificateless public auditing scheme with privacy preserving for cloud-assisted wireless body area networks. In the proof phase of the proposed scheme, the proof information is protected from being directly exposed to the auditor. So, the curious auditor could not derive the data blocks. We also prove that the proposed scheme is secure in the random oracle model under the assumption that the Diffie-Hellman problem is hard. The comparison indicates that the proposed scheme is more secure and suitable for cloud-assisted wireless body area networks.

Table 2: Comparison of computation cost.

	$A1$	$A2$	$A3$	$A4$	$A5$	$A6$
He et al. [1]	$1P$	$1P + 1H$	$1p$	$2P + 3H$	$\|I\|P$	$(\|I\| + 3)P + (\|I\| + 3)H + 2E$
Ours	$1P$	$1P + 1H$	$1P$	$4P + 3H$	$\|I\|P + 1$	$(2\|I\| + 3)P + 1H + 4E$

$A1$: setup; $A2$: partial-private-key extraction; $A3$: set-public key; $A4$: tag generation; $A5$: proof phase; $A6$: verify phase.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the Applied Basic and Advanced Technology Research Programs of Tianjin (no. 15JCYBJC15900).

References

[1] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Systems Journal*, no. 99, 2015.

[2] G. Ateniese, R. Burns, R. Curtmola et al., "Provable data possession at untrusted stores," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 598–609, Virginia, Va, USA, November 2007.

[3] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in *Proceedings of the International Conference on Theory and Application of Cryptology and Information Security: Advances in Cryptology*, pp. 319–333, 2009.

[4] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: an effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012.

[5] N. Kaaniche, A. Boudguiga, and M. Laurent, "ID based cryptography for cloud data storage," in *Proceedings of the IEEE 6th International Conference on Cloud Computing*, pp. 375–382, July 2013.

[6] Q.-A. Wang, C. Wang, K. Ren, W.-J. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2011.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proceedings of the IEEE INFOCOM*, pp. 525–533, 2010.

[8] J. Yuan and S. Yu, "Public integrity auditing for dynamic data sharing with multiuser modification," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1717–1726, 2015.

[9] J. H. Zhang and X. B. Zhao, "Privacy-preserving public auditing scheme for shared data with supporting multi-function," *Journal of Communications*, vol. 10, no. 7, pp. 535–542, 2015.

[10] K. Zeng, "Publicly verifiable remote data integrity," in *Proceedings of the 10th International Conference on Information and Communications Security*, pp. 419–434, 2008.

[11] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 12, pp. 2231–2244, 2012.

[12] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in *Proceedings of the ACM Symposium on Applied Computing*, pp. 1550–1557, 2011.

[13] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," *Computers and Electrical Engineering*, vol. 40, no. 5, pp. 1703–1713, 2014.

[14] Y. Li, Y. Yu, B. Yang, G. Min, and H. Wu, "Privacy preserving cloud auditing with efficient key update," *Future Generation Computer Systems*, 2016.

[15] L. Xue, J. Ni, Y. Li, and J. Shen, "Provable data transfer from provable data possession and deletion in cloud storage," *Computer Standard & Interfaces*, 2016.

[16] D. He, H. Wang, J. Zhang, and L. Wang, "Insecurity of an identity-based public auditing protocol for the outsourced data in cloud storage," *Information Sciences*, vol. 375, pp. 48–53, 2017.

[17] D. Kim, H. Kwon, C. Hahn, and J. Hur, "Privacy-preserving public auditing for educational multimedia data in cloud computing," *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13077–13091, 2016.

[18] T. Yang, B. Yu, H. Wang, J. Li, and Z. Lv, "Cryptanalysis and improvement of Panda—public auditing for shared data in cloud and internet of things," *Multimedia Tools and Applications*, vol. 8, 2015.

[19] H. Jin, K. Zhou, H. Jiang, D. Lei, R. Wei, and C. Li, "Full integrity and freshness for cloud data," *Future Generation Computer Systems*, 2015.

[20] B. Kang and D. Xu, "Secure electronic cash scheme with anonymity revocation," *Mobile Information Systems*, vol. 2016, Article ID 2620141, 10 pages, 2016.

[21] H. Wang, J. Domingo-Ferrer, Q. Wu, and B. Qin, "Identity-based remote data possession checking in public clouds," *IET Information Security*, vol. 8, no. 2, pp. 114–121, 2014.

[22] J. Zhang and Q. Dong, "Efficient ID-based public auditing for the outsourced data in cloud storage," *Information Sciences*, vol. 343-344, pp. 1–14, 2016.

[23] Y. Yu, L. Xue, M. H. Au et al., "Cloud data integrity checking with an identity-based auditing mechanism from RSA," *Future Generation Computer Systems*, vol. 62, pp. 85–91, 2016.

[24] S. AI-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptology and Information Security*, pp. 452–473, 2003.