An ID-Based Group Key Agreement Scheme for Controlling Access and Privacy in Cloud

Jen-Ho Yang[1, a], Iuon-Chang Lin[2, 3, b], Po-Ching Chien [2]

[1] Department of Multimedia and Mobile Commerce, Kainan University, No. 1, Kannan Rd., Luzhu, Taoyuan County, 33857, Taiwan, R.O.C.
[2]Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan.
[3]Department of Photonics and Communication Engineering, Asia University, Taichung, Taiwan, R.O.C.

* Corresponding author. Email: [a]jenhoyang@mail.knu.edu.tw, [b] iclin@nchu.edu.tw
Manuscript submitted Nov. 23, 2017; accepted January 28, 2018.
doi: 10.17706/ijcce.2018.7.1.1-7

Abstract: As the population of cloud service, more and more people concerns the privacy and security of cloud service. Therefore, an ID-based group key agreement scheme is proposed. In this paper, the group key agreement scheme is applied to the access control of cloud service. For achieving the access control and the privacy of data, the data owner can determine who can decrypt the encrypted data. In the aspect of computation cost, the bilinear pairing is used to compute the session key and the symmetric encryption is used to encrypt data in the scheme because of the bilinear pairing and symmetric encryption have lower computation cost than others. In the aspect of security, the scheme proposed in this paper not only can assist two attacks: impersonation attack and man-in-the-middle attack, but also can satisfy four security attributes: known-key security, key control, unknown key-share and key compromise impersonation.

Key words: Bilinear pairing, ID-based group key agreement, access control, cloud service.

1. Introduction

The applications of cloud service have a great growth in the recent years. There provides three services in cloud service [1]: (1) Software as a Service (SaaS), (2) Platform as a Service (PaaS), and (3) Infrastructure as a Service (IaaS). SaaS provides customers software applications from web, without downloading and installing at user end. PaaS is a service which offers a platform on cloud that the customers can develop systems or applications. And customers can rent the physical or virtual machine from the providers of IaaS. In spite of the advantages of cloud service, the privacy of sensitive data is a significant challenge. Therefore, the access control in cloud service has become more important in these days [2], [3].

In group key agreement, multiple participants form a group, and every participant in the group negotiates a session key to make communication confidentiality and integrity [4]. Data owner can use session key to encrypt the data and the receivers can decrypt the encrypted data by session key. The security of group key agreement relates to the member change is important [5], it means that when a participant leaves group, he/she cannot compute the after sessions' session key, in the same way, when there is a new participant joins group, he/she cannot compute the previous sessions' session key, it is known-key security.

In this paper, the group key agreement scheme is applied to the access control of cloud service. This scheme achieves the access control by determining who can compute the session key of the encrypted data. Any member in the group can be the data owner by computing a session key. The most important is the data

owner can determine who can decrypt the encrypted data as he/she pleases.

For decreasing the computation cost of the proposed scheme, we apply bilinear pairing to generate session key, and symmetric cryptography to encrypt the sensitive data. Compared with asymmetric cryptography, symmetric cryptography requires lesser memory and runs faster [6,7]. Besides, bilinear pairing does not employ a cost-intensive operation, such as modular exponentiation [8]. Therefore, the computation cost of the proposed scheme is efficient.

Furthermore, the scheme proposed in this paper not only assists two attacks: impersonation attack and man-in-the-middle attack, but also satisfies four security attributes: known-key security, key control, unknown key-share and key compromise impersonation.

The rest of this paper is organized as follows: Section 2 mentions the preliminaries, including bilinear pairing and desirable attributes. Section 3 describes the proposed scheme. The security analysis is presented in Section 4. Finally Section 5 concludes the paper.

2. Preliminaries

2.1. Bilinear Pairing and Some Problems

Bilinear pairing is the extended application of elliptic curve. Such as group signature schemes, ID-based encryption schemes are using bilinear pairing to make the proposed schemes achieve more efficiency and security [9]-[12].

Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group of prime order p. The bilinear pairing $\hat{e}: G_1 \times G_1 \to G_2$ is with the following properties [13].

1. Bilinearity: For all $g_1, g_2, g_3 \in G_1$ and $a, b \in Z_q^*$,

$\hat{e}(g_1, g_2 + g_3) = \hat{e}(g_1, g_2) \cdot \hat{e}(g_1, g_3)$,

$\hat{e}(g_1 + g_2, g_3) = \hat{e}(g_1, g_3) \cdot \hat{e}(g_2, g_3)$, and

$\hat{e}(ag_1, bg_2) = \hat{e}(abg_1, g_2) = \hat{e}(g_1, abg_2) = \hat{e}(g_1, g_2)^{ab}$.

2. Non-degeneracy: There exists $g_1, g_2 \in G_1$, such that $\hat{e}(g_1, g_2) \in G_2$.
3. Computability: For $g_1, g_2 \in G_1$, there is an efficient algorithm that can compute $\hat{e}(g_1, g_2)$ in polynomial time.

Suppose the following problems relate to bilinear pairing.

1. Discrete Logarithm Problem (DLP): For $Y = nX$, and $n \in Z_q^*$. Given $X, Y \in G_1$ to compute n. It is discrete logarithm problem.
2. Decision Diffie-Hellman Problem (DDHP): For $X \in G_1$ and $a, b, c \in Z_q^*$. Given X, aX, bX, cX to determine whether $c = ab \bmod q$ holds or not is decision Diffie-Hellman problem.
3. Computational Diffie-Hellman Problem (CDHP): Computational Diffie-Hellman problem is given X, aX, bX to compute abX, where $X \in G_1$ and $a, b \in Z_q^*$.

The DLP ,DDHP, and CDHP are supposed to be the hard problem is G_1 and G_2 in this paper.

2.2. Desirable Attributes

The proposed scheme in this paper can defend two attacks and satisfy four security attributes. And the definitions of these attributes were re-defined as follow [14, 15, and 16].

Two Attacks:

1. Impersonation attack: There are two scenarios of impersonation attack in our scheme. One is the adversary tries to impersonate data owner, and the other is the adversary tries to impersonate the receiver.
2. Man-in-the-middle attack: Man-in-the-middle attack is an attacker intercepts the data which is sent by legal data owner, and then the attacker sends the data to the receivers after the contents of data is altered.

Four Security Attributes:

1. Known-key security: Even the decryption key is leak, there is no one can compute the previous decryption key by knowing other sessions' decryption key. In this paper, we have two aspects of know-key security, one is when a participant leaves group, the participant cannot compute the after sessions' session key, the other one is when a new participant join this group, in the same way, the new participant cannot compute the previous sessions' session key from new session key, it is known-key security.
2. Key control: The session key cannot be preselected by any receivers.
3. Unknown key-share: The session key is shared with the illegal member without the data owner knowing it.

Key compromise impersonation: If the attacker knows the private key of the member U_j, then the adversary only can pretend him/her to be U_j. But the adversary cannot impersonate other members in the presence of U_j.

3. Proposed Scheme

In this paper, the proposed ID-based key agreement scheme is constructed of three phases: (1) the Setup Phase, (2) the Key Agreement Phase, and (3) the Retrieving Phase. Besides, there are three roles in the proposed scheme. CA is responsible for the generation of parameters, data owner is one of the group members who would like to send data, and the data owner can determine the other group members who can receive data as the receivers.

In the setup phase, CA generates the knowledge for key agreement phase, such as group member's public/private key pair, and the parameters of bilinear pairing. The broadcast process happens in the second phase. The data owner computes a session key and encrypts the data by this session key, and encrypts the session key by his/her private key, then the data owner computes a signature for the encrypted data and the session key, hence receivers can verify the integrity of data in next phase. In the retrieving phase, receivers decrypt the session key by their private key, and verify the integrity of the encrypted data and session key. After the verification is done, receivers decrypt the encrypted data by session key. The flowchart of the proposed scheme is shown in Figure 1.

The Setup Phase: Suppose that the group size is n. The CA determines two hash function $H_1(.):\{0,1\}^* \to G_1$ and $H_2(.):\{0,1\}^* \to \{0,1\}$, two cyclic groups G_1 and G_2, one bilinear mapping $\hat{e}$, a generator x of G_1, and a master key $g \in Z_q^*$, then compute $q = x \times g^{-1}$, choose a symmetric encryption scheme for encrypting data, and generates the key pair (P_i , S_i) for each member in the group, where $P_i = H_1(ID_i) \in G_1$, and $S_i = gP_i \in G_1$. After that, CA sends $(G_1, G_2, \hat{e}, H_2, P_i, S_i, q, x)$ by secure channel to every member in the group.

The Key Agreement Phase: After the data owner i chooses the receivers to whom he/she would like to

send the data, data owner i creates a set G to store the receivers' public key. Such as $G=\{P_i,P_j,P_k,...,P_n\}$. And the data owner i performs the session key agreement processes as follows.

1. Select a random number $r \in Z_q^*$.
2. Compute a parameter $Q = r\prod_{l=i}^{n} P_l$.
3. Compute a session key $K = \hat{e}(Q/P_i, S_i)$.
4. Encrypt the data M by session key K, $C = E_K(M)$.
5. Compute $h = H_2(K \| C)$ and a signature $v = \hat{e}(h, qS_i)$.
6. Upload C, Q, and v to cloud.

The Retrieving Phase: When the receivers acquire C, Q, and v in cloud, they performs the retrieving process for computing session key and verifying the integrity of session key and encrypted data as follow.

1. Receiver j computes the session key $K' = \hat{e}(S_j, Q/P_j)$.

$$
\begin{aligned}
K' &= \hat{e}(S_j, Q/P_j) \\
&= \hat{e}(gP_j, \tfrac{r(\prod_{l=i}^{n} P_l)}{P_j}) \\
&= \hat{e}(gP_j, r\times P_i \times P_j \times P_k \times \ldots \times \tfrac{P_n}{P_j}) \\
&= \hat{e}(r\times gP_j, P_i \times P_k \times \ldots \times P_n) \\
&= \hat{e}(r\times P_j, gP_i \times P_k \times \ldots \times P_n) \\
&= \hat{e}(r\times P_j \times P_k \times \ldots \times P_n, gP_i) \\
&= \hat{e}(\tfrac{r(\prod_{l=i}^{n} P_l)}{P_i}, gP_i) \\
&= \hat{e}(Q/P_i, S_i) \\
&= K
\end{aligned}
$$

2. Compute $h' = H_2(K' \| C)$, and $v' = \hat{e}(h', xP_i)$.
3. Verify whether $v' = v$ or not. If it is valid, it means that the integrity of the session key and the encrypted data are unquestioned.

$$
\begin{aligned}
v &= \hat{e}(h, qS_i) \\
&= \hat{e}(h, g\times H_1(ID_i)\times x \times g^{-1}) \\
&= \hat{e}(h, H_1(ID_i)\times x) \\
&= \hat{e}(h, xP_i)
\end{aligned}
$$

After the integrity of session key and encrypted data are verified, receiver j can decrypt the encrypted data by computing $M = D_K(C)$.

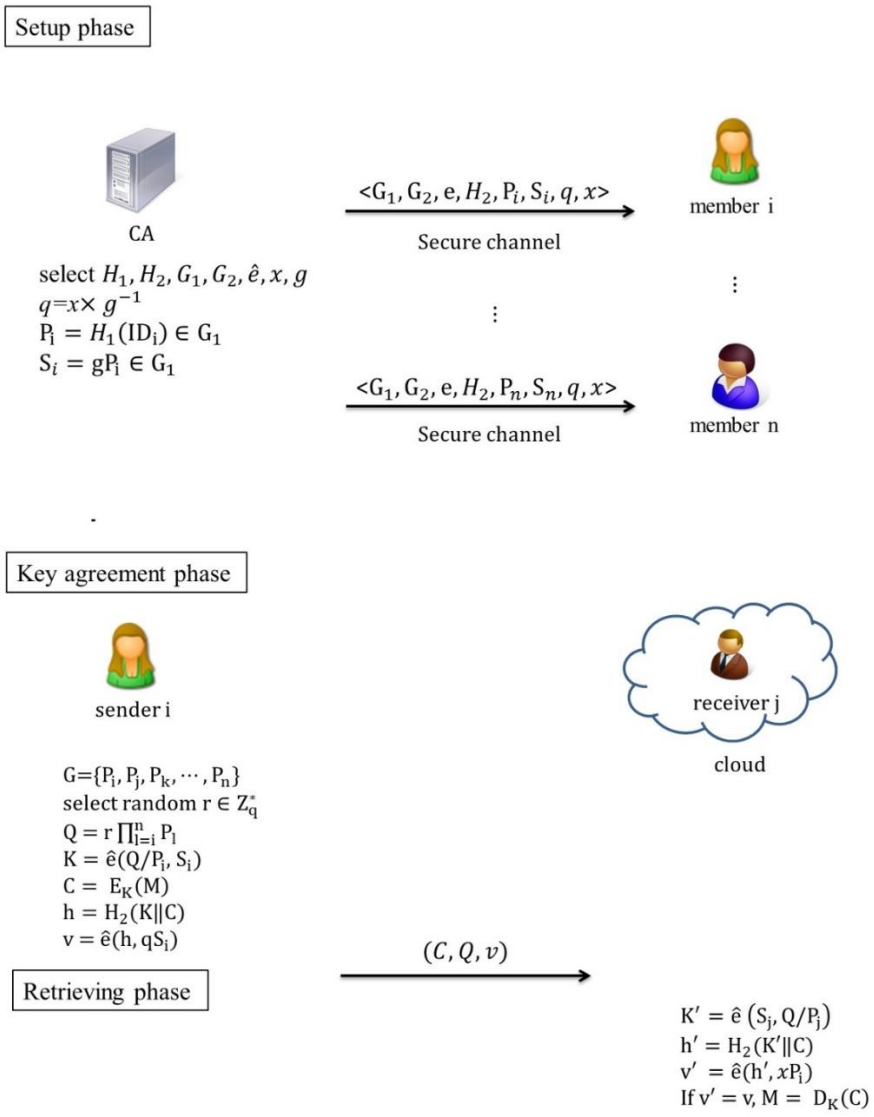

Fig. 1. The flowchart of the proposed scheme.

4. Security Analysis

Two Attacks:

1. Impersonation attack: Suppose that the attacker wants to impersonate the data owner U_i in the proposed scheme. The attacker has to generate the session key and the signature via U_i's private key. Without knowing U_i's private key, the adversary cannot compute the session key and signature of U_i. It means the impersonation attack is failed. In the same way, if the attacker knows nothing about the private key of U_j, the attacker cannot derive the session key. Therefore, the proposed scheme can resist the impersonation attack.
2. Man-in-the-middle attack: Every data owner will compute a signature for the encrypted data and session key. Therefore, the receivers can check the integrity of the encrypted data and session key by verifying the signature.

Four Security Attributes:

1. Known-key security: Due to $K = \hat{e}(Q/P_i, S_i)$, $Q = r\prod_{l=i}^{n} P_l$, and r is selected randomly in every session in the proposed scheme. Because of the discrete logarithm problem (DLP), *r* is hard to compute. As a result, no matter the previous session members or new session entrants, all of them cannot compute other sessions' session key except the session they involved in.
2. Key control: The session key is constructed by every participant's public key and a random number. Public key is generated by CA. For this reason, the session key cannot be forced to a preselected value by receivers or attackers.
3. Unknown key-share: Due to the session key is computed by all receivers' public key, hence the data owners must know the session key is shared with who.

Key compromise impersonation: Due to the discrete logarithm problem (DLP) of bilinear pairing, the attacker cannot compute the master key g via U_j's private key. And without knowing the master key g, the adversary cannot compute the private key of U_i. As this reason, the adversary cannot generate a valid signature S on behalf of U_i even U_j's private key is compromised. Therefore, the adversary only can pretend to be U_j, but cannot in the presence of U_i.

5. Conclusion

An efficiency and security ID-based group key agreement scheme is proposed in this paper. In the aspect of efficiency, bilinear pairing has less computational overheads and high security. Therefore, bilinear pairing is used to compute the session key in the proposed scheme. And the symmetric encryption has lower computation cost than asymmetric encryption. Hence, the receivers decrypt the data which is encrypted by symmetric encryption with session key. Therefore, the computation cost will not increase too much with the growth of the encryption data.

In the aspect of security, the proposed scheme resists impersonation attack and man-in-the-middle attack by the signature of the data owner, avoids key compromise impersonation by discrete logarithm problem (DLP), generates a random number to satisfy known-key security, and computes the session key by using every receiver's public key to achieve key control and unknown key-share these two security attributes, that proves the proposed scheme in this paper is efficiency and security indeed.

References

[1] Um-e-Ghazia, & Masood, R. (2012). Comparative analysis of access control systems on cloud. *Proceedings of ACIS Int'l Conf. on Software Engineering, Artificial Intelligence, Networking and Parallel & Distributed Computing (SNPD)* (pp. 8-10).

[2] Mon, E. E., & Naing, T. T. (2011). The privacy-aware access control system using attribute and role based access control in private cloud. *Proceedings of Int'l Conf. Broadband Network and Multimedia Technology(IC-BNMT)* (pp. 447-451).

[3] Subashini, S., & Kavitha, V. (2010). A survey on security issues in service delivery models of cloud computing, *Journal of Network and Computer Applications*, *34,* 1-11.

[4] Wu, C. (2012). A provable authenticated certificate less group key agreement with constant rounds. *Journal of Communication and Networks*, *14*, 104-110.

[5] Muthumayil, K., Rajamani, V., Manikandan, S., & Buvana, M. (2011). A group key agreement protocol based on stability and power using elliptic curve cryptography, *Proceedings of Int'l Conf. on Emerging Trends in Electrical and Computer Technology (ICETECT)*.

[6] Agrawal M., & Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. *International Journal on Computer Science and Engineering (IJCSE), 4(5)*, 877-882.

[7] Salama, D., Elminaam, A., Mohamed, H., Kader, A., & Hadhoud, M. M. (2008). Performance evaluation of symmetric encryption algorithms. *International Journal of Computer Science and Network Security*, 8(12).

[8] Islam, S. H., & Biswas, G. P. (2012). An efficient and provably-secure digital signature scheme based on elliptic curve bilinear pairings. *Theoretical and Applied Informatics*, *24(2)*, 109-118.

[9] Zhang, F., Safavi-Naini, R., & Susilo, W. (2004). An efficient signature scheme from bilinear pairings and its applications. *Proceedings on Lecture Notes in Computer Science (LNCS)*, *2947*, 277–290.

[10] Joux, A. (2002). The Weil and Tate AAIRINGS as building blocks for public key cryptosystems. *Proceedings of the Algorithmic Number Theory Symposium (ANTS-V) 2002, Vol. 2369*, *Lecture Notes in Computer Science* (pp. 20–32). London, UK.

[11] Barreto, P. S. L. M., Kim, H. Y., & Scott, M. (2002). Efficient algorithms for pairing-based crytosystems. *Proceedings of Advances in Cryptology-Brypto 2002*, *Vol. 2442, Lecture Notes in Computer Science* (pp. 354-368).

[12] Bonehand, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairings. *Proceedings of Advances in Cryptology-Crypto 2001*, *Vol. 2139, Lecture Notes in Computer Science* (pp. 213-229).

[13] Lin, I. C., Chang, P. Y., & Chang, C. C. (2010). A key management scheme for sensor networks using bilinear pairings and gap Diffie-Hellman group. *International Journal of Innovative Computing, Information and Control*, *6(2)*, 809-816.

[14] Zhang, L., Wu, Q., Qin, B., Domingo-Ferrer, J., & González-Nicolás, U. (2011). Asymmetric group key agreement protocol for open networks and its application to broadcast encryption. *Computer Networks*, *55, 3246-3255*.

[15] Burmester, M., & Desmedt, Y. (1995). A secure and efficient conference key distribution system. *Proceedings on Lecture Notes in Computer Science (LNCS)*, *950, 275-286*.

[16] Blake, S., Johnson, D., & Menezes, A. (1997). Key agreement protocols and their security analysis. *Proceedings on IMA Conference on Cryptography and Coding* (pp. 30-45).

Jen-Ho Yang received the B.S. degree in computer science and information engineering from I-Shou University, Kaoshiung in 2002, and the Ph.D. degree in computer science and information engineering from National Chung Cheng University, Chiayi County in 2009. Since 2009, he has been an associate professor with the Department of Multimedia and Mobile Commerce in Kainan University, Taoyuan. His current research interests include electronic commerce, information security, cryptography, authentication for wireless environments, digital right management, and fast modular multiplication algorithm.

Iuon-Chang Lin received the Ph.D. in computer science and information engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently a professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan. His current research interests include electronic commerce, information security, RFID information systems, and cloud computing.