INFORMATICA, 2017, Vol. 28, No. 2, 375–386

DOI: http://dx.doi.org/10.15388/Informatica.2017.134

Data Sharing Scheme for Cloud Storage Service Using the Concept of Message Recovery

Jen-Ho YANG[1], Iuon-Chang LIN[2]*, Po-Ching CHIEN[2]

[1]*Department of Multimedia and Mobile Commerce, Kainan University*
No. 1, Kannan Rd., Luzhu, Taoyuan County, 33857, Taiwan
[2]*Department of Photonics and Communication Engineering, Asia University*
Department of Management Information Systems, National Chung Hsing University
Taichung, Taiwan
e-mail: jenhoyang@mail.knu.edu.tw, iclin@nchu.edu.tw

Received: September 2015; accepted: November 2016

Abstract. The popularity of sharing data through cloud services has increased these days. As a result, the security of data sharing has become an important issue. The security mechanism has to ensure that the shared data would not be intercepted or altered by illegal members during transmission. A data sharing scheme for cloud services is proposed in this paper to achieve the following four security requirements: 1) forward secrecy and backward secrecy, 2) source authentication, 3) data integrity, and 4) confidentiality. In addition, message recovery is applied to improve the efficiency of encryption and signature computation. The computation cost is reduced by computing a common key for all data. Thus, the data owner only needs to encrypt the shared data once before sending it in this proposed scheme.

Key words: bilinear pairing, message recovery, data sharing, cloud storage.

1. Introduction

Cloud service has become a trend nowadays. There are three common cloud service architectures (Ghazia and Masood, 2012): Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS provides applications as a service from the web without needing the user to download or install software at the user's end. The cloud applications can be accessible through a thin client interface, such as a web browser or a program interface. The consumer does not need to manage or control the cloud infrastructures such as network, servers, operating systems, storage, or even individual application capabilities. Salesforce is an example of SaaS in the area of Customer Relationship Management (CRM), which is an approach to managing a company's interaction with current and potential future customers.

PaaS offers platform as a service where clients can develop systems or applications. It provides the client to deploy their systems or applications onto the cloud infrastructure

*Corresponding author.

supported by the provider. The client does not manage or control the cloud infrastructures such as network, servers, operating systems, or storage. However, the client has the ability to control the deployed applications and possibly configuration settings using the application-hosting mode. Examples of PaaS are Google App Engine and Windows Azure.

IaaS offers physical or virtual machine as a service to the client. It provides processing, storage, networks, and fundamental computing resources to the client. And thus the client can deploy the software, which includes operating systems and applications. The consumer does not need to manage or control the cloud infrastructure but has control over operating systems, storage, and deployed applications. An example of IaaS is Amazon EC2.

Although the above cloud services provide convenient and flexible way to utilize resources, security is considered one of the most important open issues in cloud computing as reported by International Data Corporation (IDC) (Almorsy *et al*., 2011), which is an American market research, analysis and advisory company for information technology and telecommunications. An increasing security concern in cloud is the possibility of unintended resource sharing with competitors or malicious users due to insecure channels. Therefore, it is critical to ensure the confidentiality and integrity of the data in cloud services.

Data sharing is a widely used cloud service, and the examples are Google Drive and Dropbox. To address the security concerns mentioned above, we proposed a data sharing scheme which satisfies the following four security requirements: 1) *forward secrecy* and *backward secrecy* to ensure even if the encryption key is leaked, no one can decrypt the data; 2) *source authentication* to verify whether the data is send by the data owner; 3) *data integrity* to verify whether the data has been altered by attackers or not; 4) *confidentiality* to make sure that the data cannot be read by illegal members.

To achieve source authentication, data integrity, and confidentiality, we applied Lin and Yang's source authentication scheme (Lin and Yang, 2012) to propose the data sharing scheme. However, using their scheme for the source authentication has some security problems as follows. Once a receiver can decrypt a data, and then the receiver can decrypt every data encrypted by the same data owner because the encryption key is in the same finite field of elliptic curve. As a result, Lin and Yang's scheme cannot achieve the forward secrecy and backward secrecy. On the other hand, Lin and Yang's source authentication scheme has large computation costs. This is because the data needs to be encrypted according to the number of receivers. If the number of receivers becomes large, then the computation costs are greatly increased.

To solve the above problems, we propose a new data sharing scheme for cloud services using message recovery in this paper. We compute the encryption key by using bilinear pairing and adding a random number before the encryption key is computed to achieve the forward secrecy and backward secrecy. In addition, we reduce the computation costs by using a common key for all data which has to be encrypted. Moreover, the proposed scheme only has to encrypt the shared data once regardless the number of the receivers. According to our computation analysis, the computation cost of the proposed scheme is less than those of the related works. Therefore, the proposed scheme is very efficient for the data sharing in cloud services.

The rest of the paper is organized as follows. Section 2 presents the preliminaries, including introductions of message recovery, elliptic curve cryptosystem, bilinear pairing, and security requirements. Section 3 describes the proposed data sharing scheme. The security and computation cost analysis is presented in Section 4. Finally, Section 5 concludes the paper.

2. Preliminaries

2.1. *Message Recovery*

Message recovery concept is first proposed by Nyberg and Ruppel (1993). They showed that if the message encryption and digital signature computation can be done together, the sender only has to transmit a set of cipher text to achieve both authentication and encryption. The receivers can authenticate the data of the sender by checking whether the recovered message makes sense or not, and only the legal receiver has the key to correctly recover the original data. Thus, the message recovery scheme can encrypt the original message and generate its digital signature at the same time.

Lin and Chang (2008) used this concept to propose a new digital signature scheme for linearly hierarchical organization. In Lin and Yang's (2012) scheme, the elliptic curve cryptosystem is applied to improve the computation efficiency of source authentication. The parameters used in Lin and Yang's scheme are defined as follows: p is a large prime number, g is a point on the elliptic curve in the finite field $GF(p)$, where $g \in Z_p$; M_i is the message in packet i, where i is the packet's sequence number; k_i is a random number for the ith packet, and $H(.)$ is a one-way hash function; $GF(p) \rightarrow R$. (y_s, x_s) is the public and private key pair for the sender, where $y_s = x_s \times g \bmod p$; (y_{r_j}, x_{r_j}) is the public and private key pair for the receiver j, where $y_{r_j} = x_{r_j} \times g \bmod p$.

In Lin and Yang's scheme, when the sender wants to send a message, and the sender has to generate the information set (r_i, s_i, i) using the following equations:

$$r_i' \equiv k_i \times g \bmod p,$$

$$R_i \equiv i \times r_i' \bmod p,$$

$$m_i \equiv M_i + (k_i \times i \times y_{r_j})_x \bmod p,$$

where $(k_i \times i \times y_{r_j})_x$ is the x-coordinate of the point P.

$r_i \equiv m_i + H(R_i) \bmod p$, and

$$s_i \equiv k_i - x_s \times r_i \bmod p.$$

After the information set (r_i, s_i, i) is generated, it is sent to the receivers. When the receivers receive the information set, each receiver will authenticate the sender and check the integrity of the message. Each receiver computes r_i' by using its private key with the

equation below:

$$r_i' \equiv s_i \times g + r_i \times y_s \bmod p,$$
$$R_i \equiv i \times r_i' \bmod p,$$

$m_i \equiv r_i - H(R_i) \bmod p$, and

$$M_i \equiv m_i - (r_i' \times x_r \times i)_x \bmod p.$$

The recovered message will be meaningless if the sender or the receiver is illegal. That is, this scheme can achieve both source authentication and message encryption at the same time. However, there are two disadvantages in their scheme. First, their scheme cannot satisfy the forward secrecy and backward secrecy. According to the equations presented above, if a receiver's public key is in the finite field of elliptic curve, the receiver can decrypt any data encrypted by the sender. This is a big problem when it applies to data sharing in cloud services because the malicious receiver can access the confidential data in this scenario. Second, when the sender wants to send a message to more than one receiver, the sender has to encrypt the message once for each receiver. This causes the high computation cost problem.

2.2. *Bilinear Pairing and Some Problems*

To achieve the higher efficiency and security, the bilinear pairing (Miller, 1986; Koblitz, 1987) is applied to the group signature schemes and ID-based encryption schemes (Zhang *et al*., 2004; Joux, 2002; Barreto *et al*., 2002; Bonehand and Franklin, 2001). Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group of prime order p. The bilinear pairing $\widehat{e}: G_1 \times G_1 \to G_2$ has the following three properties (Lin *et al*., 2010).

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

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

   and

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

2. Non-degeneracy: There exists $g_1, g_2 \in G_1$, such that $\widehat{e}(g_1, g_2) \in G_2$.
3. Computability: $g_1, g_2 \in G_1$, $\widehat{e}(g_1, g_2)$ can be computed in polynomial time.

Suppose the following problems relating to bilinear pairing.

1. Discrete Logarithm Problem (DLP) (Lin *et al*., 2010): for $Y = nX$ and $n \in Z_q^*$; given $X, Y \in G_1$; compute n.

2. Decision Diffie–Hellman Problem (DDHP): for $X \in G_1$ and $a, b, c \in Z_q^*$; given X, aX, bX, cX; determine whether $c = ab \bmod q$ holds or not.
3. Computational Diffie–Hellman Problem (CDHP): given X, aX, bX; compute abX where $X \in G_1$ and $a, b \in Z_q^*$.

According Lin *et al*. (2010), the DLP is supposed to be the hard problem is G_1 and G_2 in this paper.

2.3. *Security Requirements*

Cloud service offers many benefits; it enables users to share their data with anyone on the cloud. However, the security, privacy, and integrity of the cloud services are the main challenges (Hay *et al*., 2011). To address these challenges, we propose a scheme in this paper that can satisfy the four security requirements as defined in Wang and Wu (2005) as follows.

1. *Forward secrecy and backward secrecy*: forward secrecy says if the decryption key is leaked, the receivers cannot recover any data by the previous encryption key except when the data owner allows. Similarly, backward secrecy says when a data is shared with a new receiver, the new receiver cannot recover any of the previous data using the new decryption key unless the data owner allows.
2. *Source authentication*: to avoid impersonation attacks, the sender should provide a way for the receivers to authenticate whether the data is sent from the legal sender.
3. *Data integrity*: the data might be intercepted and altered by attackers when the data is transmitted through an unsecure channel; therefore, the accuracy of the data should be confirmed by the receivers after recovering the data.
4. *Confidentiality*: to avoid eavesdropping when the data is in transmission through an unsecure channel, the confidentiality is also an important requirement in data sharing.

3. The Proposed Scheme

In the proposed scheme, M is the data shared in the cloud service, n is the shared data's sequence number, and r is a random number which is chosen by the data owner for the shared data. The proposed scheme consists of three phases: (1) the Setup Phase, (2) the Initialization Phase, and (3) the Verification Phase. The three phases are described below. The notations used in the proposed scheme are listed as follows:

The setup phase: suppose the group size is n. CA determines two hash functions $H_1(.) : \{0, 1\}^* \rightarrow G_1$ and $H_2(.) : \{0, 1\}^* \rightarrow \{0, 1\}$, an additive cyclic group G_1 of order q, where q is a large prime number, a multiplicative group G_2 of the same order, one bilinear mapping $\widehat{e}$, a generator g of G_1, and a master key $x \in Z_q^*$. Then, CA computes $w = x \times g$ and generates the key pair (P_i, S_i) for every member in the cloud service, where $P_i = H_1(ID_i) \in G_1$, and $S_i = gP_i \in G_1$. After that, CA sends $(G_1, G_2, \widehat{e}, H_2, P_i, S_i, g, q)$ through a secure

Table 1
The notations used in the proposed scheme.

Notations	Descriptions
M	Shared data in the cloud service
n	Sequence number of the shared data
k	Random number, $k \in Z_p^*$
r	Random number for the shared data, $r \in Z_p^*$
$H_1()$	Hash function, $H_1() : \{0,1\}^* \rightarrow G_1$
$H_2()$	Hash function, $H_2() : \{0,1\}^* \rightarrow \{0,1\}$
G_1	A cyclic additive group of a large prime order p
G_2	A cyclic multiplicative group of a large prime order p
$\widehat{e}$	Bilinear mapping, $\widehat{e} : G_1 \times G_1 \rightarrow G_2$
x	Master key, $g \in Z_p^*$
g	Generator of G_1
P_i	The public key of cloud storage service member, $P_i = H_1(ID_i) \in G_1$
S_i	The private key of cloud storage service member, $S_i = x P_i \in G_1$

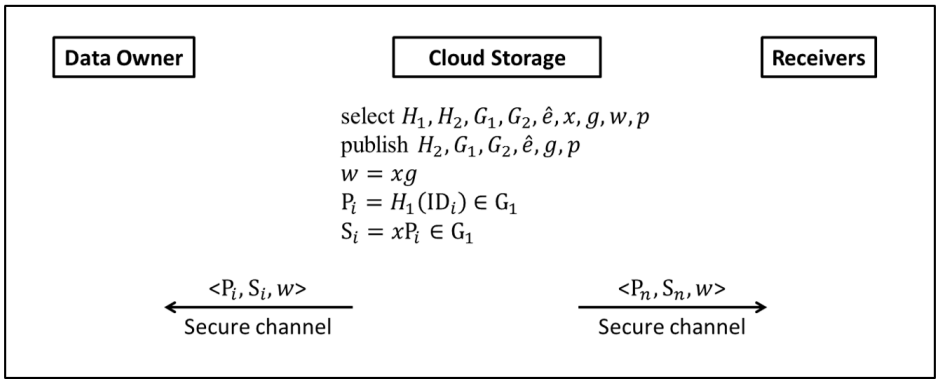

Fig. 1. The steps of the setup phase.

channel to every member who registers on the cloud service. Figure 1 illustrates the steps of the setup phase.

The initialization phase: when the data owner i wants to share his data with other members on the cloud service; the data owner creates a set G to store the public keys of the members whom the data will be shared with, e.g. $G = \{P_j, P_k, \ldots, P_n\}$. Then the data owner i performs the following initialization phase.

1. Select two random numbers $k, r \in Z_q^*$.
2. Compute a parameter $Q = k \prod_{l=i}^{n} P_l$.
3. Compute a session key $K = \widehat{e}(Q/P_i, S_i)$.
4. Compute $z \equiv r \times g \bmod q$.
5. Compute $R \equiv n \times z \bmod q$.
6. Compute $m \equiv M + (r \times n \times K \times g) \bmod q$.
7. Compute $v \equiv m + H_2(R) \bmod q$.
8. Compute $u \equiv (r - S_i \times v) \times g \bmod q$.
9. Share v, u, n, Q on the cloud service. The above steps are shown in Fig. 2.

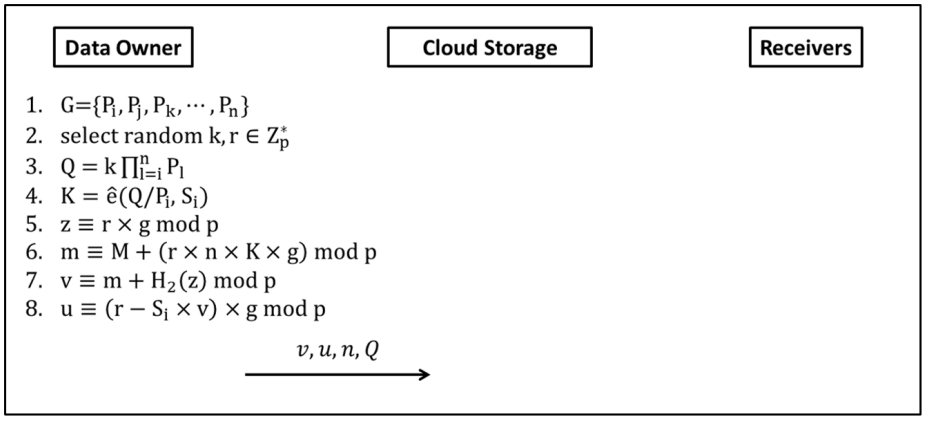

Fig. 2. The steps of the initialization phase.

The verification phase: when the member j of the cloud service wants to read data shared by data owner i, the following verification phase is performed.

1. Compute z by:

$$\begin{aligned} z &\equiv u + v \times P_i \times w \bmod q \\ &\equiv (r - S_i \times v) \times g + v \times P_i \times x \times g \bmod q \\ &\equiv r \times g - x \times P_i \times v \times g + v \times P_i \times x \times g \bmod q \\ &\equiv r \times g \bmod q. \end{aligned}$$

2. Compute $R \equiv n \times z \bmod q$.
3. Compute $m \equiv v - H_2(R) \bmod q$.
4. Compute K by:

$$\begin{aligned} K' &= \widehat{e}(S_j, Q/P_j) \\ &= \widehat{e}\left(g P_j, \frac{r\left(\prod_{l=i}^{n} P_l\right)}{P_j}\right) \\ &= \widehat{e}\left(g P_j, r \times P_i \times P_j \times P_k \times \cdots \times \frac{P_n}{P_j}\right) \\ &= \widehat{e}(r \times g P_j, P_i \times P_k \times \cdots \times P_n) \\ &= \widehat{e}(r \times P_j, g P_i \times P_k \times \cdots \times P_n) \\ &= \widehat{e}(r \times P_j \times P_k \times \cdots \times P_n, g P_i) \\ &= \widehat{e}\left(\frac{r\left(\prod_{l=i}^{n} P_l\right)}{P_i}, g P_i\right) \\ &= \widehat{e}(Q P_i, S_i) \\ &= K. \end{aligned}$$

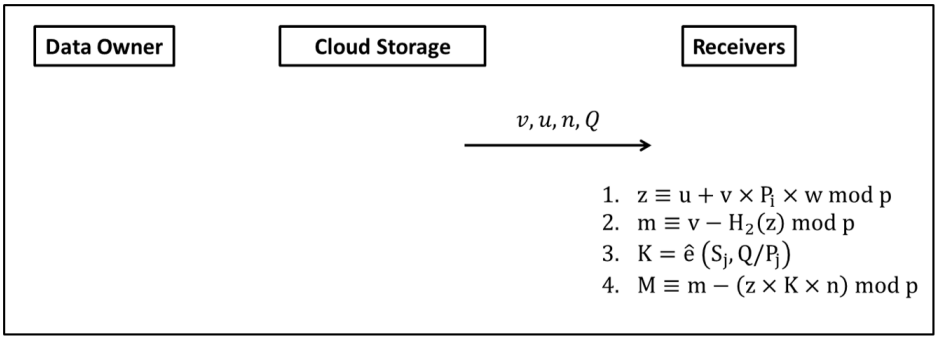

Fig. 3. The steps of the verification phase.

5. Compute M by:

$$\begin{aligned} m - (z \times K \times n) \bmod q &\equiv M + (r \times n \times K \times g) - (r \times g \times K \times n) \bmod q \\ &\equiv M. \end{aligned}$$

4. Analyses

In this section, we give the security and computation cost analyses as follows.

4.1. *Security Analysis*

Forward secrecy and backward secrecy: the encryption key is computed by $K = \widehat{e}(Q/P_i, S_i)$, where $Q = k\prod_{l=i}^{n} P_l$. The parameter k is selected randomly in every session in the proposed scheme. Due to the discrete logarithm problem (DLP), k is hard to be computed. Therefore, neither previous members nor new entrants can compute other keys except the session they are involved in. As a result, forward secrecy and backward secrecy are achieved in this proposed scheme.

Source authentication: when a legal member wants to authenticate the data, the member can compute $z \equiv u + v \times P_i \times w \bmod q$. Assume an attacker attempts to impersonate the legal data owner, then the attacker uses its public key P_a to compute its private key S_a and $u_a \equiv (r - S_a \times v) \times g \bmod q$. Then, the attacker uploads (v, u_a, n, Q) to the cloud service. When a receiver recovers the data send by the attacker, the following equations are used:

$$\begin{aligned} z_a &\equiv (r - S_a \times v) \times g + v \times P_i \times x \times g \bmod q \\ &\equiv r \times g - x \times P_a \times v \times g + v \times P_i \times x \times g \bmod q, \\ R_a &\equiv n \times z_a \bmod q, \\ M &= m - (z_a \times K \times n) \bmod q. \end{aligned}$$

The receiver can verify whether the data is from the legal data owner by determining if the result, M, is meaningless or not.

Data integrity: legal members can verify the integrity of the data using the following equations:

$$z \equiv u + v \times P_i \times w \bmod q,$$
$$R \equiv n \times z \bmod q,$$
$$m \equiv v - H_2(R) \bmod q,$$

and

$$M \equiv m - (z \times K \times n) \bmod q.$$

According to the equations above, if the sequence number n is altered to a, or v is altered to v_a by an attacker during transmission; the recovered data will become meaningless. When a legal member decrypts a packet, the member has to compute R by z and get m by computing R. As a result, without the right sequence number and the original m, the recovered data will be meaningless.

Confidentiality: besides the integrity of data, data confidentiality is also considered in the proposed scheme. Data should be recoverable only by the members whom the data owner wants to share with. If an attacker tries to recover the data using the following equations without the correct private key or the random number r, the recovered message will be meaningless.

$$z \equiv u + v \times P_i \times w \bmod q,$$
$$R \equiv n \times z \bmod q,$$
$$m \equiv v - H_2(R) \bmod q,$$
$$K' = \widehat{e}(S_j, Q/P_j),$$

and

$$M \equiv m - (z \times K \times n) \bmod q.$$

With regard to the privacy and the security in cloud storage service, the security requirements of the proposed scheme is compared with Zhao *et al.*'s and Han *et al.*'s scheme in Table 2. As Table 2 shows, the proposed scheme and Han *et al.*'s scheme can achieve forward secrecy and backward secrecy, authentication of the data source, integrity of the data, and the confidentiality of the data. However, Zhao *et al.*'s scheme cannot satisfy the source authentication requirement.

Table 2
The comparisons of security requirements.

Security requirements			
Schemes	Zhao *et al*. (2010) scheme	Han *et al*. (2013) scheme	The proposed scheme
Forward secrecy and backward secrecy	Yes	Yes	Yes
Source authentication	No	Yes	Yes
Data integrity	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes

Table 3
Comparison of time complexity.

Computational costs			
Schemes	Zhao *et al*. (2010) scheme	Han *et al*. (2013) scheme	The proposed scheme
Data owner	$15T_A$	$6T_B + 8T_E$	$(n+10)T_A + T_B + 2T_M$
Receiver	$2T_A$	$2T_B + 4T_E$	$8T_A + T_B$
Cloud storage	$3T_A$	$2T_B + T_E$	$2T_A$
PKG	–	$5T_B + 11T_E$	–

4.2. *Computation Cost Analysis*

In the aspect of computational cost analysis, the proposed scheme is compared with Zhao *et al*.'s scheme and Han *et al*.'s scheme in Table 3. T_A is the time complexity of point addition, T_B is the time complexity of bilinear paring, T_M is the time complexity of real number multiplication, and T_E is the time complexity of exponential operation. There is no exponential operation in the proposed scheme; therefore, it is obvious that the proposed scheme is more efficient than the scheme proposed by Han *et al*.

5. Conclusions

In this paper, we proposed a new data sharing scheme for cloud services. In the aspect of security, we achieved authentication of data source as well as data integrity and confidentiality. Furthermore, forward secrecy and backward secrecy are satisfied by using bilinear pairing to compute a common encryption key. In the aspect of efficiency, we use the concept of message recovery to address the problem that signed information might be lost during transmission. This approach also reduces the computation cost without using any exponential operation. Moreover, we compute a common key for every data to reduce the encryption time. Although the computation cost of the proposed scheme is higher than Zhao *et al*.'s scheme, but Zhao *et al*.'s scheme cannot achieve the security requirement of source authentication. Therefore, the proposed scheme is more secure and more efficient than the related works.

References

Almorsy, M., Grundy, J., Ibrahim, A.S. (2011). Collaboration-based cloud computing security management framework. In: *IEEE 4th International Conference on Cloud Computing*, pp. 364–371.

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

Bonehand, D., Franklin, M. (2001). Identity-based encryption from the weil pairings. In: *Proceedings of Advances in Cryptology-Crypto 2001*, *Lecture Notes in Computer Science*, vol. 2139, pp. 213–229.

Ghazia, U., Masood, R. (2012). Comparative analysis of access control systems on cloud. In: *Proceedings of ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel & Distributed Computing (SNPD)*, pp. 8–10.

Han, J., Susilo, W., Mu, W. (2013). Identity-based data storage in cloud computing. *Future Generation Computer Systems*, 29, 673–681.

Hay, B., Nance, K.L., Bishop, M. (2011). *Storm Clouds Rising: Security Challenges for IaaS Cloud Computing*. HICSS, IEEE Computer Society, pp. 1–7.

Joux, A. (2002). The weil and tate airings as building blocks for public key cryptosystems. In: *Proceedings of the Algorithmic Number Theory Symposium (ANTS-V2002)*, *Lecture Notes in Computer Science*, Vol. 2369, pp. 20–32.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203–209.

Lin, I.C., Chang, C.C. (2008.) A novel digital signature scheme for application of document review in a linearly hierarchical organization. In: *Proceedings of the 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1367–1370.

Lin, I.C., Yang, J.H. (2012). Improving computation efficiency of source authentication by elliptic curve cryptosystem. *Journal of Electronic Science and Technology*, 10(3), 227–231.

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

Miller, V.S. (1986). Use of elliptic curves in cryptography. In: Williams H.C. (Ed,), *Advances in Cryptology – CRYPTO '85 Proceedings, CRYPTO 1985, Lecture Notes in Computer Science*, Vol. 218. Springer, Berlin.

Nyberg, K., Ruppel, R.A. (1993). A new signature scheme based on the DSA giving message recovery. In: *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 58–61.

Wang, L., Wu, C.K. (2005). Efficient identity-based multicast scheme from bilinear pairing. *IEE Proceedings Communications*, 152(6), 877–882.

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)*, Vol. 2947, pp. 277–290.

Zhao, G., Rong, C., Li, J., Zhang, F., Tang, Y. (2010). Trusted data sharing over untrusted cloud storage providers. In: *Proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 97–103.

J.H. Yang received the BS degree in computer science and information engineering from I-Shou University, Kaoshiung in 2002, and the PhD 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.

I.C. Lin received the BS in computer and information sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the MS in information management from Chaoyang University of Technology, Taiwan, in 2000. He received his PhD 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, and Department of Photonics and Communication Engineering, Asia University, Taichung, Taiwan, ROC. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

P.C. Chien received the MS in the Department of Management Information Systems, National Chung Hsing University, Chiayi, Taiwan. The main research interest is connected with the problem of information security.