$$\tilde{R}_3 = \left(\frac{e(T_3,W)}{e(P,P)}\right)^c e(T_3,P)^{s_x} e(H,W)^{-s_\alpha - s_\beta} e(H,P)^{-s_{\delta_1} - s_{\delta_2}}$$
$$= \left(\frac{e(T_3,W)}{e(P,P)}\right)^c e(T_3,P)^{r_x + cx_i} e(H,W)^{-r_\alpha - c\alpha - r_\beta - c\beta}$$
$$e(H,P)^{-r_{\delta_1} - cx_i\alpha - r_{\delta_2} - cx_i\beta}$$
$$= \left(\frac{e(T_3,W)}{e(P,P)}\right)^c e(T_3, x_i P)^c e(-(\alpha+\beta)H, W + x_i P)^c$$
$$e(T_3,P)^{r_x} e(H,W)^{-r_\alpha - r_\beta} e(H,P)^{-r_{\delta_1} - r_{\delta_2}}$$
$$= \left(\frac{e(T_3,W)}{e(P,P)}\right)^c e(T_3, x_i P)^c e(-(\alpha+\beta)H, W + x_i P)^c$$
$$R_3 = \left(\frac{e(T_3,W)}{e(P,P)}\right)^c e(T_3 - (\alpha+\beta)H, W + x_i P)^c e(T_3, W)^{-c} R_3$$
$$= \left(\frac{e(A_i, W + x_i P)}{e(P,P)}\right)^c R_3 = R_3.$$

Lemma 1.2. Revoked users cannot utilize the cloud after their revocation.

Proof. Lemma 1.2 is equivalent to the accuracy of Algorithm 3 (revocation verification). The accuracy of revocation verification is based on the following relation:

$$e(T_3 - A_i, H_0) = e(A_i + (\alpha+\beta)\cdot H - A_i, H_0)$$
$$= e(\alpha H, H_0) e(\beta H, H_0)$$
$$= e(\alpha U, \xi_1 H_0) e(\beta V, \xi_2 H_0)$$
$$= e(T_1, H_1) e(T_2, H_2).$$

Lemma 1.3. An attacker is unable to access the cloud server based on the statement of the intractability of q-SDH problem in G1.

Proof. The brief security analysis can be shown as follows: Suppose that an attacker A succeeds to forge a valid group signature with a non negligible probability in polynomial time. In addition to that we think f is a random oracle. With the help of Forking Lemma [21], by using the oracle replay method, the attacker A obtains two suitable signatures $(M, \sigma_0, c, \sigma_1)$ and $(M, \sigma_0, c', \sigma_1')$ as follows:

$$\begin{cases} \sigma_0 = (T_1, T_2, T_3, c, R_1, R_2, R_3, R_4, R_5) \\ c = f(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \\ c' = f'(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \\ \sigma_1 = (s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2}) \\ \sigma_1' = (s_\alpha', s_\beta', s_x', s_{\delta_1}', s_{\delta_2}') \end{cases} \quad (5)$$

$$\begin{cases} s_\alpha = r_\alpha + c\alpha, s_\alpha' = r_\alpha + c'\alpha \\ s_\beta = r_\beta + c\beta, s_\beta' = r_\beta + c'\beta \\ s_x = r_x + cx, s_x' = r_x + c'x \\ s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_1}' = r_{\delta_1} + c'\delta_1 \\ s_{\delta_2} = r_{\delta_2} + c\delta_2, s_{\delta_2}' = r_{\delta_2} + c'\delta_2. \end{cases} \quad (6)$$

Then, A can compute an SDH tuple $(\hat{x} = \Delta s_x / \Delta c, \hat{A} = T_3 - ((\Delta s_\alpha + \Delta s_\beta)/\hat{\Delta c}) \cdot H)$ such that $A = \frac{1}{\gamma + \hat{x}}$ and $e(\hat{A}, W + \hat{x}P) = e(P,P)$, where $\Delta s_x = s_x - s_x'$, $\Delta c = c - c'$, $\Delta s_\alpha = s_\alpha - s_\alpha'$, an $\Delta s_\beta = s_\beta - s_\beta'$. Obviously, this contradicts with q-SDH assumption.

Theorem 2. The proposed scheme supports traceability and privacy preserving.

Proof. The display of this theorem is double. On one hand, the group manager has the capability to identify the real signer. Given a valid group signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ and the private tuple (ξ_1, ξ_2), the group manger can compute the private key of the signer through the equation $A_i = T_3 - (\xi_1 \cdot T_1 + \xi_2 \cdot T_2)$. The correctness of the equation holds based on the following relation:

$$T_3 - (\xi_1 \cdot T_1 + \xi_2 \cdot T_2) = A_i + (\alpha+\beta)\cdot$$
$$H - (\xi_1\alpha \cdot U + \xi_2\beta \cdot V) = A_i.$$

On the other hand, other entities cannot reveal the signer's identity from a group signature, if not, DL assumption will be in inconsistency. Additional proofs on the accuracy, anonymity, unforgeability and traceability of group signatures can be found in [12].

Theorem 3. The proposed scheme protects data confidentiality under the hardness of theWBDHEproblem andGDHEproblem.

Proof. Theorem 3 can be deduced from the following two lemmas:

Lemma 3.1. The cloud server is unable to learn the content of the stored files.

Proof. To prove this lemma, we take a data file (C_1, C_2, C) as an example to demonstrate the data confidentiality, where $C_1 = k \cdot Y, C_2 = k \cdot P, K = Z^k, C = Enc_K(M)$ and no user has been revoked before the data file is uploaded. Suppose if the cloud server can calculate $K = Z^k$, i.e., "given $C_1 = k \cdot Y, C_2 = k \cdot P, P,$ for unidentified γ, computing $e(C_1, P)^{\frac{1}{\gamma}} = e(G,P)^k = K$."This contradicts with the WBDHE statement. On other hand, given the revocation list, and the cloud server can learns the incomplete private key of a revoked user i, i.e $(A_i, x_i)$for a revoked user. Without the knowledge of the other part private key Bi, it is also not capable to calculate the decryption key through the equation $e(C_1, A_i) e(C_2, B_i) = Z^k$. Thus, the accuracy of Lemma 3.1 can be ensured.

Lemma 3.2. Even under the collusion with revoked users, this cloud server can also not capable of learning the content of the files stored after their revocation.

Proof. We first define two polynomial functions $f(X) = \Pi_{i=1}^{r}(X + x_i)$ and $g(X) = \Pi_{i=1}^{n-r}(X + x_i')$. Let G0 and P0 denote two elements in group G1. Then, we set G = $f(\gamma)G_0$and $P = f(\gamma)g(\gamma)P_0$.To retain the confidentiality against the revoked users, the data owner calculate the header information C1, C2 and the encryption key K as follows:

$$\begin{cases} C_1 = kY = k\gamma f(\gamma)\cdot G_0 \\ C_2 = kP_r = \dfrac{k}{(\gamma+x_1)(\gamma+x_2)\cdots(\gamma+x_r)}P = kg(\gamma)P_0 \\ K = Z_r^k = Z^{\frac{k}{(\gamma+x_1)(\gamma+x_2)\cdots(\gamma+x_r)}} = Z^{\frac{k}{f(\gamma)}} \\ = e(G,P)^{f(\gamma)} = e(G_0,H_0)^{kf(\gamma)g(\gamma)}. \end{cases} \quad (7)$$

We can observe that it is not possible for revoked users to compute the encryption key K, since "given $k\gamma f(\gamma)\cdot G_0$ and $kg(\gamma)P_0$, computing $e(G_0,H_0)^{kf(\gamma)g(\gamma)}$, is an instance of (t,n)-GDHE problem, which has been demonstrated to be intractable in polynomial time [14]. By the analysis above, we conclude that the proposed scheme get the security goals including access control, data confidentiality as well as traceability and anonymity.

6. Conclusion

In this paper, we design a secure data sharing method, Mona, for the dynamic groups in an untrusted cloud. In Mona, a user is capable to the share data with others in the group with no revealing identity privacy to the cloud. Additionally, Mona can supports efficient user revocation and new user joining. More especially, efficient user revocation can be achieved from side to side a public revocation list without inform the private keys of the remaining users, and new users can straight decrypt files stored in the cloud before their participation. Also, the storage transparency and the encryption computation cost are constant. Wide analyses show that our future scheme satisfies the desired security requirements and guarantees efficiency as well.

References

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.
[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.
[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.
[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.
[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.
[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.
[12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
[13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.
[14] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

Author Profile

A. Jyothi MCA, M.Tech [Ph.D.] working as assistant professor in Computer Science Engineering from CVSR COLLEGE OF ENGINEERING from ANURAG GROUP OF INSTITUTIONS Venkatapur (V), Ghatkesar (M), Ranga Reddy District, Hyderabad-500088, Telangana State.

Deeti Naga Vijay received the B.Tech degree in Information Technology from JNTU hyderabad 2012 and pursuing M.Tech. degree in Computer science and Engineering from JNTU Hyderabad.