Ali, Mohammad; **Mohajeri, Javad**; **Sadeghi, Mohammad-Reza**; **Liu, Ximeng**
A fully distributed hierarchical attribute-based encryption scheme. (English) Zbl 1436.68094
Theor. Comput. Sci. 815, 25-46 (2020).

The paper studies scalability and flexibility in key delegation and user revocation mechanisms in attribute-based encryption (ABE) systems. First, the important results in the field and the general notions required next are presented. One section is dedicated to problem formulation: definition of revocable CP-HABE (Ciphertext Policy-Hierarchical ABE) systems and fully distributed revocable CP-HABE (FDR-CP-HABE) systems consisting of architecture, definition, security. Most of the paper is devoted to the detailed description of the system and the analysis of its performance compared to other known ones, and the conclusion is that the performance is acceptable compared with other similar schemes.

Reviewer: Ion Iancu (Craiova)

MSC:

68P25 Data encryption (aspects in computer science)
68M11 Internet topics
68M25 Computer security
94A60 Cryptography

Keywords:

cloud computing; cryptosystem; hierarchical attribute-based encryption; ciphertext-policy attribute-based encryption; access control; computational complexity

Software:

OOABKS; PBC Library

Full Text: DOI

References:

[1] Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A., Cloud computing—the business perspective, Decis. Support Syst., 51, 1, 176-189 (2011)

[2] Webster, J., An enterprise cloud 'survey of surveys' (2016), Forbes [online]. Available:

[3] Canard, S.; Phan, D. H.; Pointcheval, D.; Trinh, V. C., A new technique for compacting ciphertext in multi-channel broadcast encryption and attribute-based encryption, Theor. Comput. Sci., 723, 51-72 (2018) · Zbl 1390.94829

[4] Rao, Y. S.; Dutta, R., Computational friendly attribute-based encryptions with short ciphertext, Theor. Comput. Sci., 668, 1-26 (2017) · Zbl 1367.94341

[5] Xu, S.; Yang, G.; Mu, Y., Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation, Inf. Sci., 479, 116-134 (2019)

[6] Goyal, V.; Pandey, O.; Sahai, A.; Waters, B., Attribute-based encryption for fine-grained access control of encrypted data, (Proceedings of the 13th ACM Conference on Computer and Communications Security (October 2006), ACM), 89-98

[7] Bethencourt, J.; Sahai, A.; Waters, B., Ciphertext-policy attribute-based encryption, (IEEE Symposium on Security and Privacy, SP'07 (May 2007), IEEE), 321-334

[8] Wang, G.; Liu, Q.; Wu, J.; Guo, M., Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, Comput. Secur., 30, 5, 320-331 (2011)

[9] Liu, Q.; Wang, G.; Wu, J., Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inf. Sci., 258, 355-370 (2014)

[10] Li, Q.; Ma, J.; Li, R.; Liu, X.; Xiong, J.; Chen, D., Secure, efficient and revocable multi-authority access control system in cloud storage, Comput. Secur., 59, 45-59 (2016)

[11] Huang, Q.; Yang, Y.; Shen, M., Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing, Future Gener. Comput. Syst., 72, 239-249 (2017)

[12] Wan, Z.; Liu, J. E.; Deng, R. H., HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans. Inf. Forensics Secur., 7, 2, 743-754 (2012)

[13] Deng, H.; Wu, Q.; Qin, B.; Domingo-Ferrer, J.; Zhang, L.; Liu, J.; Shi, W., Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts, Inf. Sci., 275, 370-384 (2014) · Zbl 1341.68043

[14] Shamir, A., Identity-based cryptosystems and signature schemes, (Workshop on the Theory and Application of Cryptographic Techniques (August 1984), Springer: Springer Berlin, Heidelberg), 47-53 · Zbl 1359.94626

[15] Boneh, D.; Franklin, M., Identity-based encryption from the Weil pairing, (Annual International Cryptology Conference (August 2001), Springer: Springer Berlin, Heidelberg), 213-229 · Zbl 1002.94023

[16] Waters, B., Efficient identity-based encryption without random oracles, (Annual International Conference on the Theory and Applications of Cryptographic Techniques (May 2005), Springer: Springer Berlin, Heidelberg), 114-127 · Zbl 1137.94360

[17] Hong, H.; Liu, X.; Sun, Z., A fine-grained attribute based data retrieval with proxy re-encryption scheme for data outsourcing systems, Mob. Netw. Appl., 1-6 (2018)

[18] Chunpeng, G.; Liu, Z.; Xia, J.; Liming, F., Revocable identity-based broadcast proxy re-encryption for data sharing in clouds, IEEE Trans. Dependable Secure Comput. (2019)

[19] He, D.; Zhang, Y.; Wang, D.; Choo, K. K.R., Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography, IEEE Trans. Dependable Secure Comput. (2018)

[20] Zhang, Y.; Yu, J.; Hao, R.; Wang, C.; Ren, K., Enabling efficient user revocation in identity-based cloud storage auditing for shared big data, IEEE Trans. Dependable Secure Comput. (2018)

[21] Hassan, A.; Omala, A. A.; Ali, M.; Jin, C.; Li, F., Identity-based user authenticated key agreement protocol for multi-server environment with anonymity, Mob. Netw. Appl., 24, 3, 890-902 (2019)

[22] Horwitz, J.; Lynn, B., Toward hierarchical identity-based encryption, (International Conference on the Theory and Applications of Cryptographic Techniques (April 2002), Springer: Springer Berlin, Heidelberg), 466-481 · Zbl 1056.94514

[23] Seo, J. H.; Emura, K., Revocable hierarchical identity-based encryption via history-free approach, Theor. Comput. Sci., 615, 45-60 (2016) · Zbl 1338.94082

[24] Boneh, D.; Boyen, X.; Goh, E. J., Hierarchical identity based encryption with constant size ciphertext, (Annual International Conference on the Theory and Applications of Cryptographic Techniques (May 2005), Springer: Springer Berlin, Heidelberg), 440-456 · Zbl 1137.94340

[25] Waters, B., Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions, (Annual International Cryptology Conference (August 2009), Springer: Springer Berlin, Heidelberg), 619-636 · Zbl 1252.94101

[26] Sahai, A.; Waters, B., Fuzzy identity-based encryption, (Annual International Conference on the Theory and Applications of Cryptographic Techniques (May 2005), Springer: Springer Berlin, Heidelberg), 457-473 · Zbl 1137.94355

[27] Lewko, A.; Okamoto, T.; Sahai, A.; Takashima, K.; Waters, B., Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption, (Annual International Conference on the Theory and Applications of Cryptographic Techniques (May 2010), Springer: Springer Berlin, Heidelberg), 62-91 · Zbl 1279.94095

[28] Cui, J.; Zhou, H.; Xu, Y.; Zhong, H., OOABKS: online/offline attribute-based encryption for keyword search in mobile cloud, Inf. Sci. (2019)

[29] Song, Y.; Li, Z.; Li, Y.; Li, J., Attribute-based signcryption scheme based on linear codes, Inf. Sci., 417, 301-309 (2017)

[30] Miao, Y.; Ma, J.; Liu, X.; Li, X.; Liu, Z.; Li, H., Practical attribute-based multi-keyword search scheme in mobile crowdsourcing, IEEE Int. Things J., 5, 4, 3008-3018 (2017)

[31] Bobba, R.; Khurana, H.; Prabhakaran, M., Attribute-sets: a practically motivated enhancement to attribute-based encryption, (European Symposium on Research in Computer Security (September 2009), Springer: Springer Berlin, Heidelberg), 587-604

[32] Gentry, C.; Silverberg, A., Hierarchical ID-based cryptography, (International Conference on the Theory and Application of Cryptology and Information Security (December 2002), Springer: Springer Berlin, Heidelberg), 548-566 · Zbl 1065.94547

[33] Wang, S.; Yu, J.; Zhang, P.; Wang, P., A novel file hierarchy access control scheme using attribute-based encryption, Appl. Mech. Mater. (2014)

[34] Wang, S.; Zhou, J.; Liu, J. K.; Yu, J.; Chen, J.; Xie, W., An efficient file hierarchy attribute-based encryption scheme in cloud computing, IEEE Trans. Inf. Forensics Secur., 11, 6, 1265-1277 (2016)

[35] Liu, X.; Ma, J.; Xiong, J.; Liu, G., Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data, Int. J. Netw. Secur., 16, 6, 437-443 (2014)

[36] Li, J.; Wang, Q.; Wang, C.; Ren, K., Enhancing attribute-based encryption with attribute hierarchy, Mob. Netw. Appl., 16, 5, 553-561 (2011)

[37] Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W., Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst., 24, 131-143 (2013)

[38] Yu, S.; Wang, C.; Ren, K.; Lou, W., Attribute based data sharing with attribute revocation, (Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (April 2010), ACM), 261-270

[39] Liu, F.; Ng, W. K.; Zhang, W.; Han, S., Encrypted set intersection protocol for outsourced datasets, (2014 IEEE International Conference on Cloud Engineering (March 2014), IEEE), 135-140

[40] Kamara, S.; Mohassel, P.; Raykova, M.; Sadeghian, S., Scaling private set intersection to billion-element sets, (International Conference on Financial Cryptography and Data Security (March 2014), Springer: Springer Berlin, Heidelberg), 195-215

[41] Abadi, A.; Terzis, S.; Metere, R.; Dong, C., Efficient delegated private set intersection on outsourced private datasets, IEEE Trans. Dependable Secure Comput. (2017)

[42] Ruj, S.; Nayak, A.; Stojmenovic, I., DACC: distributed access control in clouds, (2011 IEEE 10th International Conference

on Trust, Security and Privacy in Computing and Communications (November 2011), IEEE), 91-98

[43] Yang, K.; Jia, X.; Ren, K.; Zhang, B.; Xie, R., DAC-MACS: effective data access control for multi-authority cloud storage systems, IEEE Trans. Inf. Forensics Secur., 8, 11, 1790-1801 (2013)

[44] The python pairing based cryptography library

[45] Lynn, B., PBC Library Manual 0.5.11 (2006)

[46] Lewko, A.; Waters, B., Decentralizing attribute-based encryption, (Annual International Conference on the Theory and Applications of Cryptographic Techniques (May 2011), Springer: Springer Berlin, Heidelberg), 568-588 · Zbl 1290.94106

[47] Hur, J., Improving security and efficiency in attribute-based data sharing, IEEE Trans. Knowl. Data Eng., 25, 10, 2271-2282 (2011)

[48] Jung, T.; Li, X. Y.; Wan, Z.; Wan, M., Privacy preserving cloud data access with multi-authorities, (2013 Proceedings IEEE INFOCOM (April 2013), IEEE), 2625-2633