Modern Techniques for Providing Security in Cloud Computing Environment

Dinesh Kumar Bhayal[1] Prof. Gajendra Singh[2]
[1,2]SSSIST, Sehore (MP)

Abstract-- Cloud security is nowadays is a burning research topic. In this paper, we present an survey overview of existing cloud security algorithms. All these algorithms are described more or less on their own. Cloud security is a very popular task. We also explain the fundamentals of sequential rule mining. We describe today's approaches for cloud security. From the broad variety of efficient algorithms that have been developed we will compare the most important ones. We will systematize the algorithms and analyse their performance based on both their run time performance and theoretical considerations. Their strengths and weaknesses are also investigated. It turns out that the behaviour of the algorithms is much more similar as to be expected.

I. LITERATURE SURVEY

Attribute-Based Encryption (ABE) was first proposed by Sahai and Waters [4] with the name of Fuzzy Identity-Based Encryption, with the original goal of providing an error-tolerant identity-based encryption [5] scheme that uses biometric identities. In [6], Pirretti et al. proposed an efficient construction of ABE under the Random Oracle model and demonstrated its application in large-scale systems. Goyal et al. enhanced the original ABE scheme by embedding a monotone access structure into user secret key. The scheme proposed by Goyal et al. is called Key-Policy Attribute-Based Encryption (KP-ABE) [7], a variant of ABE. In the same work, Goyal et al. also proposed the concept of Cipher text-Policy Attribute Based Encryption (CP-ABE) without presenting a concrete construction. CP-ABE is viewed as another variant of ABE in which cipher texts are associated with an access structure. Both KP-ABE and CP-ABE are able to enforce general access policies that can be described by a monotone access structure. In [8], Ostrovsky et al. proposed an enhanced KP-ABE scheme which supports non-monotone access structures. Chase [9] enhanced Sahai-Waters ABE scheme and Goyal et al. KP-ABE scheme by supporting multiple authorities. Further enhancements to multi-authority ABE can be found. Bettencourt et al. [10] proposed the first CP-ABE construction with security under the Generic Group model. In [11], Cheung et al. presented a CCA-secure CP-ABE construction under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. In [12], the CCA secure scheme just supports AND gates in the access structure. Towards proposing a provably secure CP-ABE scheme supporting general access structure, Goyal et al. [13] proposed a CP-ABE construction with an exponential complexity which can just be viewed as theoretic feasibility. For the same goal, Waters [30] proposed another CP-ABE scheme under various security assumptions. Aside from providing basic functionalities for ABE, there are also many works proposed to provide better security/privacy protection for ABE. These works include CP-ABE with hidden policy, ABE with user accountability [14], ABE with attribute hierarchy [15] and etc.

Techniques/ Parameters	**KP-ABE**	**EKP-ABE**	**CP-ABE**	**CP-ASBE**	**HIBE**
Access Control	Low High if associated with re-encryption technique	Better than KP-ABE	Average Realization of complex Access Control	Better than CP-ABE	Comparatively low
Efficiency	Average High for broadcast type encryption	Higher thanKP-ABE Only allow constant cipher text	Average Not efficient for modern enterprise environments	Better than CP-ABE Less collusion attacks	Better Lower when compared with ABE schemes
Computational overheads	High	Reduces the computations	Average	Lower than CP-ABE	Higher

Table 1: Comparison of various security schemes

II. CONCLUSION

In this paper, we surveyed the list of existing cloud security techniques. We also analyzed the performance of various attribute based security mechanisms. There strength and weakness are also compared in a table. In a forthcoming paper, we pursue the development of a complete methodology for the proposed model.

All rights reserved by *www.ijsrd.com*

REFERENCES

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25, pp. 599–616, 2009.
[2] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/
[3] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws. com/
[4] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.
[5] D. Boneh and M. Franklin. Identity-Based Encryption from The Weil Pairing. In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.
[6] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2006.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data. In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.
[8] R. Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with
non-monotonic access structures". In Proc. of CCS'06, New York, NY, 2007.
[9] M. Chase. "Multi-authority attribute based encryption". In Proc. of TCC'07,
Amsterdam, Netherlands, 2007.
[10] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA, 2007.
[11] L. Cheung and C. Newport. Provably Secure Ciphertext Policy ABE. In Proc. of CCS'07, New York, NY, USA, 2007.
[12] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization", http://eprint.iacr.org/2008/290.
[13] V. Goyal, A. Jain, O. Pandey and A. Sahai, "Bounded Ciphertext-Policy Attribute based Encryption", In Proc. of ICALP'08, Reykjavik, Iceland, 2008
[14] M. J. Hinek, S. Jiang, R. Safavi-Naini, and S. F. Shahandashti, "Attribute-Based Encryption with Key Cloning Protection", http://eprint.iacr.org/2008/478
[15] Jin Li, Qian Wang, Cong Wang, and Kui Ren, "Enhancing Attribute-based Encryption with Attribute Hierarchy," In Proc. of ChinaCom'09, Xi'an, China, 2009.
[16] Vandana birle " State of the art in cloud security", IJSRD, volume 1, issue 2, 2013

All rights reserved by *www.ijsrd.com*