











we are able to prevent the system from collusion attack even if the security of the cloud is compromised. Even if the attacker is able to get into the cloud and steal the information, he cannot comprehend it because the data cannot be decrypted. Even if he conspires with the cloud storage system, the attacker will not be able to acquire the required data and information.

Moreover, we also point out that there is no single perfect method to achieve perfect audit for the cloud data. Therefore, it might be imperative to set some new trends to design much more effective schemes.

#### References

- [1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50-58, April 1, 2010.
- [2] Gurinder Kaur, Vinay Bhardwaj, "A Review of VM Placement Strategies," *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 6, Issue 5, May 2016.
- [3] Subramanian S, Nitish Krishna G, Kiran Kumar M, Suresh P and G R Karpagam, "An Adaptive Algorithm for Dynamic Priority Based Virtual machine scheduling in cloud", *IJCSI International Journal of Computer Science Issues*, Vol. 9, Issue 6, No 2, November 2012 ISSN (Online): 1694-0814
- [4] Eu-jin Goh, Hovav Shacham, Nagendra Modadugu, and Dan Boneh, "Sirius: Securing Remote Untrusted Storage," *Proc. Network and Distributed Systems Security (NDSS) Symposium*, pp. 131-145, 2003.
- [5] Meenakshi Sharma, Pankaj Sharma, Dr. Sandeep Sharma, "Efficient Load Balancing Algorithm in VM Cloud Environment" *IJCST Vol. 3, Issue 1, Jan. - March 2012*.
- [6] Z. Zhu, Z. Jiang, and R. Jiang, "The attack on Mona: Secure multi-owner data sharing for dynamic groups in the cloud," in *Proc. Int. Conf. Inf. Sci. Cloud Comput.*, Dec. 7, 2013, pp. 185–189.
- [7] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving Secure role-based access control on encrypted data in cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.
- [8] X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," in *Proc. IEEE Conf. Comput. Commun.*, 2008, pp. 1211–1219.
- [9] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," *IEEE Trans. Know. Data Eng.*, vol. 25, no. 11, pp. 2602–2614, Nov. 2013.
- [10] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
- [11] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography*, 2008, pp. 53–70.
- [12] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1182–1191, Jun. 2013.
- [13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity-based encryption with constant size ciphertext," in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 2005, pp. 440–456.
- [14] C. Delerangle, P. Paillier, and D. Pointcheval, "Fully collusion-secure dynamic broadcast encryption with constant-size ciphertext or decryption keys," in *Proc. 1st Int. Conf. Pairing-Based Cryptography*, 2007, pp. 39–59.
- [15] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.