IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

# E-Healthcare Privacy data sharing with Fine-Grained Access Control

**Miss. S. Saranya[1], V. Sandhiya[2], U. Rakshana Kumar[3]**
Assistant Professor, Department of Computer Science and Engineering[1]
Research Student, Department of Computer Science and Engineering[2,3]
Dhanalakshmi College of Engineering, Chennai, Tamil Nadu, India

**Abstract:** *The E-Healthcare Cloud system has shown that it can improve healthcare quality as well as individual quality of life. Unfortunately, concerns about security and privacy prevent it from being widely adopted and used. Several studies have been carried out in order to protect the privacy of electronic health record (EHR) data. We start with a two-layer encryption scheme. We create first-layer encryption to ensure efficient and fine-grained access control over EHR data, in which we create a highly specialised access policy for each data attribute in the EHR and encrypt them individually with high efficiency. To protect the privacy of role attributes and access policies used in the first-layer encryption, we construct the second-layer encryption systematically. We made a recommendation. User revocation is commonly supported in such schemes, as users' group memberships may change for a variety of reasons. Prior to now, the computational overhead for Auto user revocation. Binary key generation is included for file storage. We proposed enabling file encryption alongside proxy re encryption.*

**Keywords:** E-Healthcare.

## REFERENCES

**[1].** Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227– 238, 2013.
**[2].** H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, pp. 1–10, 2015.
**[3].** W. Zhang, Y. Lin, S. Xiao, Q. Liu, and T. Zhou, "Secure distributed keyword search in multiple clouds," in Proc. IEEE/ACM IWQOS'14. Hongkong: IEEE/ACM, May 2014, pp. 370–379.
**[4].** W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014). Atlanta, USA: IEEE, jun 2014, pp. 276–286.
**[5].** D. Nascimento and M. Correia, "Shuttle: Intrusion recovery for paas," in Proc. IEEE Distributed Computing Systems (ICDCS'15), Ohio, USA, Jun. 2015, pp. 10–20.
**[6].** At risk of exposure -in the push for electronic medical records, concern is growing about how well privacy can be safeguarded. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/heprivacy26
**[7].** J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 103–114.
**[8].** M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Security and Privacy in Communication Networks. Springer, 2010, pp. 89– 106.
**[9].** J. Sun, X. Zhu, C. Zhang, and Y. Fang, "Hcpp: Cryptography based secure ehr system for patient privacy and emergency healthcare," in Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011, pp. 373–382.
**[10].** J. Zhou, Z. Cao, X. Dong, and X. Lin, "Tr-mabe: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems," in INFOCOM, 2015 Proceedings IEEE. Hong Kong: IEEE, 2015, pp. 2398–2406.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252