

{tag}

{/tag}

IJCA Proceedings on International Conference
on Innovations in Computing Techniques (ICICT 2015)

© 2015 by IJCA Journal

ICICT 2015 - Number 2

Year of Publication: 2015

Authors:

Sathish Kumar V E

K Umamaheswari

{bibtex}icict1490.bib{/bibtex}

Abstract

Personal Health Record (PHR) sharing in cloud is a major issue in recent trends. The data stored in cloud is not secure because everything depends upon the cloud service provider. An unexpected cloud crash may expose all data in cloud. In order to overcome that a new symmetric key encryption that uses a constant key for encrypting PHR is proposed. The system developed uses a Patient Controlled Encryption (PCE), where the patients control and manage their own health record. The system developed enhances key management by storing the keys by the patient itself. The patients can share their key with whoever they want. The algorithm used here takes less computational time and memory usage for execution than existing

cryptographic algorithms.

References

ences

- Cheng Kang Chu, Sherman S. M. Chow, Wen Guey Tzeng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 468-477, Feb. 2014.
- Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan 2013.
- Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, vol 1, no. 15, pp. 0975-8887, 2010.
- J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records", Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.
- Hans Lohr, Marcel Winandy, Ahmed Regha, "Securing the E Health Cloud", International Conference on Trusted Systems 2009 (INTRUST'09), 2009.
- Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," master's thesis, Worcester Polytechnic Inst. , 2011.
- V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.
- 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," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

Index Terms

Computer Science

Security

Keywords

Personal Health Record Access Control Data Privacy Symmetric Key Encryption Data Security.

