ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Secure Sharing of Personal Health Record in Cloud Environment

E.Saranya, V.Tamilarasi, E.Thavamani, E.Vigneshwari, T.Sathis Kumar*

U.G Student, Department of Computer Science and Engineering, Saranathan College of Engineering, Trichy, Tamilnadu, India

Assistant Professor, Department of Computer Science and Engineering, Saranathan College of Engineering , Trichy, Tamilnadu, India*

ABSTRACT: In cloud secure personal data sharing is the important issues because it creates several securities and data confidentiality problem while accessing the cloud services. Many challenges present in personal data sharing such as data privacy protection, flexible data sharing, efficient authority delegation, computation efficiency optimization, are remaining toward achieving practical fine-grained access control in the Personal Health Information Sharing system. Personal health records must be encrypted to protect privacy before outsourcing to the cloud. Aiming at solving the above challenges, here propose an efficient data sharing mechanism for Personal Data Sharing, which not only achieves data privacy, fine-grained access control and authority delegation simultaneously, but also optimizes the computation efficiency and is suitable for resource constrained servers. Most of the data consumers are honest, while few of them are corrupt and will leakage their secret keys in the collusion. On the contrary, PKG and data owner are assumed to be fully trusted. Besides, public cloud 1 and public cloud 2 cannot collude with each other. The non-collusive assumption is reasonable, because the client can demand that two cloud servers cannot reveal users' information by contract. In proposed work, PR-ABE (Attribute Based Encryption with Proxy Re-encryption) technique implements to provide secure encryption of medical data. To improve the access control, here partial key sharing scheme will be implement. Using this, data owner can send partial secret key for the requested user. This approach overcomes the key guessing attack in data retrieval process.

KEYWORDS: PR-ABE(Attribute Based Encryption with Proxy Re-encryption), PKG(Private Key Generator), OMD(Original Medical Database), DMD(Duplicate Medical Database), KGC(Key Generation Centre), EMR(Electonic Medical Record).

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks ,to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. It is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principles of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. Forrester [1] defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption". It is a technology that uses the internet and central remote servers to maintain data and applications and allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing examples are Yahoo email, Gmail, or Hotmail.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization.

Public Cloud

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

Private Cloud

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud:

- ✓ On-premise Private Cloud
- ✓ Externally hosted Private Cloud

Hybrid Cloud

Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

II.LITERATURE SURVEY

Authors: Kaitai Liang1, Liming Fang, Duncan S. Wong, and Willy Susilo

Proposed work is to construct a new CP-ABPRE in the random oracle model with CCA security. Prior to proposing the scheme, we first introduce some intuition behind our construction. We choose Waters ABE (the most efficient construction proposed in [26]) as a basic building block of our scheme due to the following reasons. The construction of Waters ABE scheme enables us to convert the scheme to be an ABE Key Encapsulation in the random oracle model. Specifically, in our construction a content key that is asymmetrically encrypted under an access policy is used to hide a message in a symmetric way. Furthermore, Waters ABE scheme utilizes LSSS to support any monotonic access formula for ciphertexts. It is a desirable property for CP-ABPRE systems when being implemented in practice. In addition, the construction for ciphertexts, whose size is linear in the size of formula, is able to help us relieve the communication cost incurred by re-encryption and the generation of re-encryption key. To make data sharing be more efficiently, Proxy Re-Encryption (PRE) is proposed. PRE extends the traditional Public Key Encryption (PKE) to support the delegation of decryption rights. It allows a semi-trusted party called proxy to transform a ciphertext intended for a party A into another ciphertext of the same plaintext intended for party B. The proxy, however, learns neither the decryption keys nor the underlying plaintext. PRE is a useful cryptographic primitive and has many applications, such as secure distributed files systems and email forwarding.

Proposed scheme provides a new authorization method to specify who can do a plaintext equality test based on ciphertexts. Then, a new concept of PKEwET and identity-based encryption was proposed, under the name identity based encryption with equality test (IBEET). To decrease the computational time cost in the previous scheme, designed a scheme for this purpose. Recently, ABE supports the concept of equality test, because it supports the functionality of search and tests on the ciphertext based on different access policies. A KP-ABE with equality test (ET) scheme was proposed, which provides testing if the ciphertexts include the same information based on the sets of different attributes. But, it only realizes one-way against chosen-ciphertext attacks. Proposed scheme isn't secure for a test under chosen ciphertext attack. They proposed a new scheme to solve one-way against chosen-ciphertext attack. As we know, there is no explicit CP-ABE fine-grained access control scheme with equality test. The data owner encrypts his private data with corresponding trapdoors and stores it in the cloud. Suppose there is a user intends to search in the data owner's ciphertexts, he sends a request using specific trapdoor to the cloud. When the cloud receives the request of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

searching, it can decide whether two different ciphertexts are encryptions of the same plaintext. The aim of this work is to allow the users an easy search of ciphertexts, to reach secure fine-grained, and access control in the cloud.

III.THEORITICAL FRAMEWORK

EXISTING SYSTEM:

Compared with traditional model of ABE the existing system was adopted with two different public cloud servers to achieve secured outsourced computation. In this system public cloud 1 and public cloud 2 are honest-but-curious more precisely, they will follow the protocol but try to find out as much private information as possible. Most of the consumers are honest, while few of them are corrupt and will leakage their secret keys in collusion. It is a fine grained data sharing mechanism for EMR system which achieves non interactive fine grained access control and authority delegation simultaneously.

PROPOSED SYSTEM:

Design Considerations:

- To implement two cloud based secure EMR sharing scheme.
- PKG is to provide system parameters.

PRE an ABE for new access policy without revealing the plaintext.

- Develop an extensible security with the help of two cloud servers.
- Server 1 has the files that are uploaded by user itself.
- Server 2 has the fake copy of the original file.

Advantages of Proposed System:

- Communication cost is small and fixed.
- Prevent public cloud servers from learning secret information.
- Improved computation efficiency for PKG and USER.
- No collusion between two clouds.

Algorithm Used:

Attribute Based Encryption: 320 bits

- **Setup (λ, U) → (PK, MK):**
  - The setup algorithm takes as input a security parameter λ and a universe description U, which defines the set of allowed attributes in the system. It outputs the public parameters PK and the master secret key MK.
- **Encrypt (PK, M, S) → CT:**
  - The encryption algorithm takes as input the public parameters PK, a message M and a set of attributes S and outputs a ciphertext CT associated with the attribute set.
- **KeyGen (MK, A) → SK:**
  - The key generation algorithm takes as input the master secret key MK and an access structure A and outputs a private key SK associated with the attributes.
- **Decrypt (SK, CT) → M:**
  - The decryption algorithm takes as input a private key SK associated with access structure A and a ciphertext CT associated with attribute set S and outputs a message M if S satisfies A or the error message ⊥ otherwise.

IV.IMPLEMENTATION

Proposed system will be implementing using PHP as front end and SQL is for back end process. This approach has modules like frame work creation, Medical files uploading ,Data Encryption, Duplicate storage, File access and alert system. Input process has file storage and output was provide secure to medical files using two cloud.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

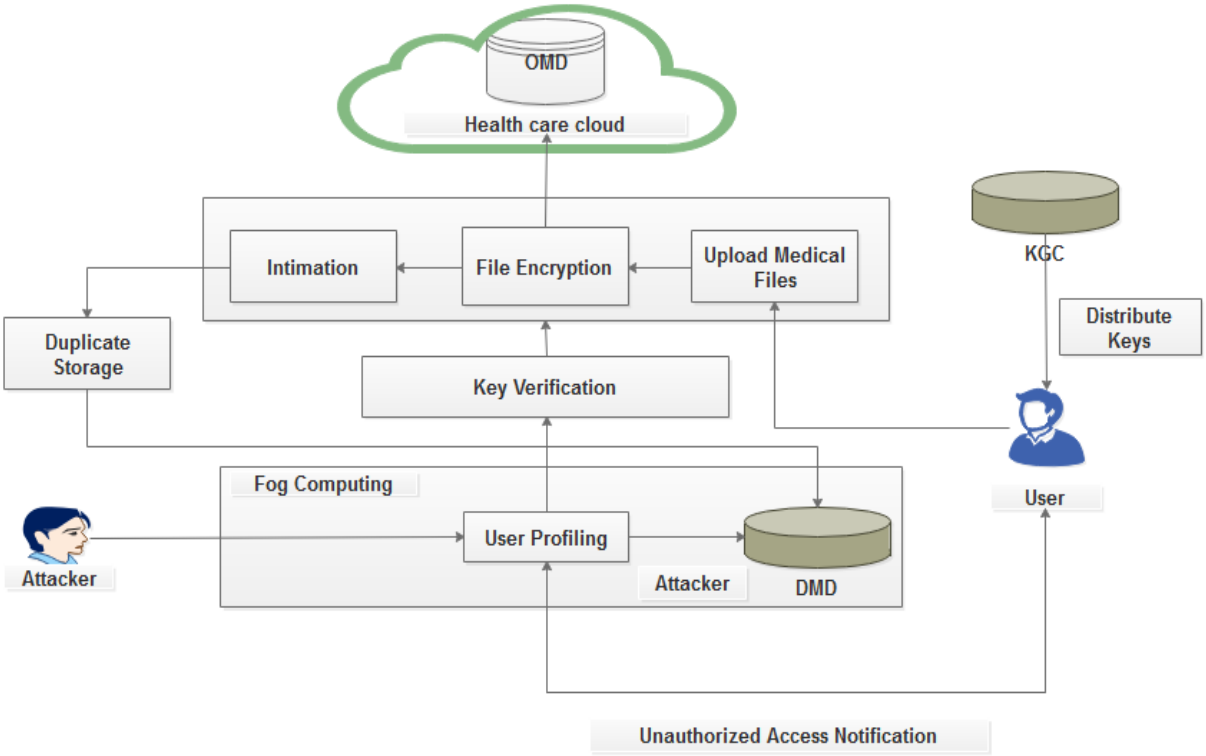

Fig 1.Architecture diagram

V.RESULTS

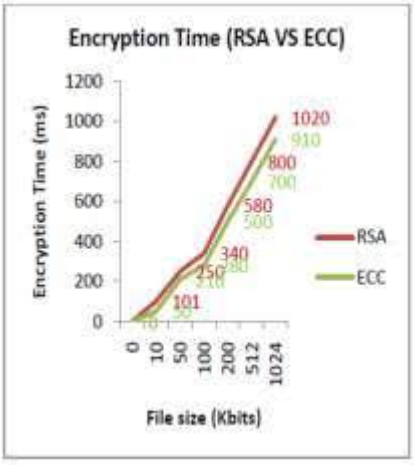

Fig 2.Encryption time of RSA and ECC

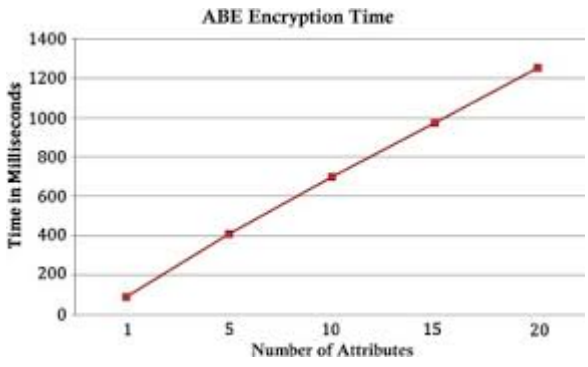

Fig 3.Encyption time of ABE

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

As shown in the above figure 2 and 3 **RSA algorithm** and Attribute Based Encryption (**ABE**) is used for encryption and decryption of messages in which **ABE** tends to be more efficient than **RSA** based **algorithm**. **ABE** is a new public key based on one-to-many encryption that allows users to decrypt the message based on set of attributes and access policies.

VI.CONCLUSION

The results shows that the implemented algorithm handles the security of the data strictly, that it provides security in sake that hackers could not reach as easy as they try to. The proposed algorithm provides security efficient clouds with non colluding properties. Our proposed scheme achieves better performance in outsourced key generation, Encryption, Re-encryption key generation and Decryption simultaneously.

REFERENCES

[1]J. Alderman, N. Farley, and J.Crampton, "Tree-based cryptographic access control," in Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, pp. 47–64.
[2]R. Zhang, H. Ma, and Y. Lu, "Fine-grained access control system based on fully outsourced attribute-based encryption," Journal of Systems and Software, vol. 125, pp. 344–353, 2017.
[3]H. Ma, R. Zhang, Z. Wan, Y. Lu, and S. Lin, "Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 6, pp. 679–692, 2017.
[4]A. Castiglione, A. D. Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, and X. Huang, "Hierarchical and shared access control," IEEE Transactions Information Forensics and Security, vol. 11, no. 4, pp. 850–865, 2016.
[5] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1-6, 2008.
[6] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24,July/Aug. 2010.
[7] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on Computer and Communications Security, pp. 756-758, 2010.
[8] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," World Wide Web, vol. 15, no.4, pp. 409-428, 2012.
[9]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.
[10] A.Sahai and B. Waters. "Fuzzy Identity-Based Encryption." In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.
[11]E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management–part 1: General (revision 3)," NIST special publication, vol. 800, p. 57, 2011.
[12] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, and P. L.Montgomery, "On the security of 1024-bit rsa and 160-bit elliptic curve cryptography.," IACR Cryptology ePrint Archive, p. 389, 2009.
[13] S.Hemalatha, Dr.R.Manickachezian, "Present and Future of Cloud Computing: A Collaborated Survey Report"., International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-2, July 2012.
[14] S.Hemalatha, Dr.R.Manickachezian, "Implicit Security Architecture Framework in Cloud Computing Based on Data Partitioning and Security Key Distribution"., International Journal of Emerging Technologies in Computational and Applied Sciences, ISSN (Online): 2279-0055 , pp. 76-81, Feb.2013.
[15] S.Hemalatha, Dr.R.Manickachezian " Dynamic Auditing Protocol using Improved RSA and CBDH for Cloud Data Storage".,International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1, January 2014.