International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

Protecting E-Health Record with Data Sharing in Public Cloud

Miss. Pansare Kalyani Baban[1], Prof-Kurhade N.V[2]

[1,2]Sharadchandra Pawar College of Engineering, Dumberwadi, Tal-Junnar, Dist-Pune

Abstract - *In the recent years, distributed computing grows rapidly. A lot of knowledge square measure transferred and place away in remote open cloud servers that cannot utterly be trusty by shopper especially, a regularly expanding number of endeavors may need to manage their data by the guide of the cloud servers. In any case, when the data re-appropriated in the cloud are unstable, the troubles of security and assurance winds up squeezing for wide game plan of the cloud frameworks. This paper proposes an ensured data sharing intend to ensure the security of data proprietor and the security challenges for information sharing. The security and productivity examination exhibit that the set upend plan is feasible and effective. Finally, we talk about its application in electronic well-being record.*

Key Words: Attribute-based encryption, Cloud computing, Data sharing, Searchable encryption

1. INTRODUCTION

The technique of cloud computing relieves consume of data management, data processing, and capital use on equipment, programming, and work force systems of support, etc. Public cloud is owned and controlled by public cloud servers (PCS), which cannot be trusted. PCS might steal or get the data information stored by the users. Thus, many different security notions are proposed to ensure the security in cloud such as remote data integrity, remote data sharing, etc. Data sharing is one of important applications in cloud computing, especially for enterprise. Usually, an enterprise may authorize some entities to share its remote data under its defined policy.

2. Related work

C. Chu, S. Chow, W. Tzeng, J. Zhou, R. Deng, Key-aggregate crypto system for scalable data sharing in cloud storage," [1] IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, Feb. 2014

The private key holder can discharge a steady size total key for adaptable decisions of cipher-text set in distributed storage, however the other encoded records outside the set stay classified. This compact mixture key is handily sent to others or be keep in a {very} revolving credit with very restricted secure storage. We provide formal privacy observation of our schemes within the customary model. We likewise depict other use of our plans. In explicit, our schemes offer the primary public-key patient controlled secret writing for versatile hierarchy that was nevertheless to be notable.

Y. Tong, J. Sun, S. Chow, P. Li, Cloud-assisted mobile-access of health data with privacy and audit ability", [2] IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, Mar. 2014.

To incorporate key administration from pseudorandom variety generator for unlink capacity, a protected compartmentalization technique for privacy protective keyword search that hides each inquiry and access designs supported excess, and incorporate the thought of attribute primarily based coding with threshold language for giving job based access management with audit ability to stop potential misconduct, in each tradition and emergency cases.

C. Fan, V. Huang, H. Rung, Arbitrary-state attribute-based encryption with dynamic membership", [3] IEEE Transactions on Computers, vol. 63, no. 8, pp. 1951-1961, Apr. 2013.

An ABE theme that is that the 1st ABE theme that aims at dynamic membership management with arbitrary states, not binary states solely, for each attribute. Our work likewise keeps high adaptability of the limitations on properties and influences clients to have the capacity to powerfully join, leave, and refresh their traits. It is pointless for those clients who don't change their credit statuses to reestablish their private keys when some client updates the values of her/his attributes. Finally, we tend to conjointly formally prove the safety of the planned theme while not victimisation random oracles.

D. Boneh, G. Crescenzo, R. Ostrovskyy, G. Persianoz, "Public key encryption with keyword search", [4] in Eurocrypt 2004, Interlaken, Switzerland, May 2-6, 2004, pp.506-522.

Consider a mail server that stores distinctive messages openly mixed for Alice by others. Using our framework Alice can send the mail server a key that will engage the server to recognize all messages containing a few watchwords, however get the hang of nothing else. We define the idea of open key encryption with catchphrase chase and give a couple of improvements.

N. Cao, C. Wang, M. Li, K. Ren, W. Lou, \Privacy-preserving multi keyword ranked search over encrypted cloud data",[5] IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222-233, Nov. 2013.

The economical similarity live of coordinate matching," i.e., as several matches as attainable, to capture the connectedness of information documents to the search question. We further use "In ward thing comparability" to quantitatively survey such resemblance measure. We at first propose a key idea for the MRSE subject to anchor inside thing count, and after that give two basically upgraded MRSE wants to achieve diverse stringent assurance requirements in two particular threat

3. Proposed algorithm

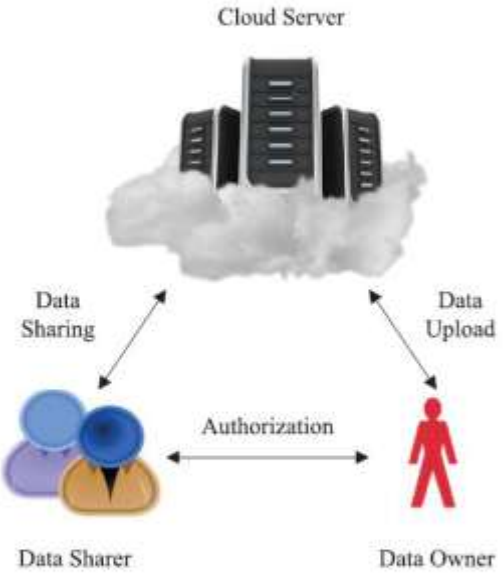

Fig-1:-System Architecture

The data sharing scheme comprises of three different entities, Cloud Server, Data owner and Data sharer.

1) Data Owner: Data owner is an entity whose massive data will be uploaded to the cloud servers for storage and processing. It is either the patients or the hospital.

2) Data Sharer: Data sharer is an entity who will share the data owners' remote data. It may be the medical/health researcher, the medical/health research organization or the relatives of the data owner.

3) Cloud Server: Cloud server is an entity who is managed by cloud service provider. It has enormous storage space and computation resource which are used to process the data owners' data.

4. Algorithm

1. ABE

Which users can decrypt a cipher text will be decided by the attributes and policies related with the message and the client

A focal expert will make mystery keys for the clients (like in IBE) in view of traits/arrangements for every client

Steps:

1. Setup: The AA acts a PKG for AN IBE theme, running Setup to come up with the non-public key master –key and therefore the public values params.
2. Attribute List: (Optional) Alice obtains list of ordinary attribute varieties. (Note: no certificates.)
3. Policy: Alice determines her access policy f for a resource key κ in terms of the attribute set.
4. Encrypt: Alice computes cipher-text c = f[κ] using the AND & OR constructions described above.
5. Decryption: If he has private IBE keys ("verifiable" testaments) relating to characteristics fulfilling f, at that point Bob can unscramble c, yielding κ.
6. Authorization Request: Otherwise, Bob may request from the AA the secret IBE keys ("verifiable" testaments for attributes to which Bob is entitled.

5. CONCLUSION

In the propose system, data sharing scheme which can achieve the anonymity and data confidentiality in public clouds. We formalize the definition and the protection model. Then, we designed a concrete data sharing scheme and gave the security proof. Security examination demonstrated our plan is provably secure in the proposed security show. Execution investigation demonstrated that our plan is relevant.

REFERENCES

[1] HUAQUN WANG1, 2 1Jiangsu Key Laboratory, \Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-health Record," IEEE Transactions on Parallel Data Security Intelligent Processing, School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

[2] C. Chu, S. Chow, W. Tzeng, J. Zhou, R. Deng, \Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, Feb. 2014.

[3] Y. Tong, J. Sun, S. Chow, P. Li, Cloud-assisted mobile-access of health data with privacy and audit ability", IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, Mar. 2014.

[4] C. Fan, V. Huang, H. Rung, Arbitrary-state attribute-based encryption with dynamic membership", IEEE Transactions on Computers, vol. 63, no. 8, pp. 1951-1961, Apr. 2013.

[5] D. Boneh, G. Crescenzo, R. Ostrovskyy, G. Persianoz, \Public key encryption with keyword search", in Euro crypt 2004, Interlaken, Switzerland, May 2-6, 2004, pp.506-522.