A REVIEW ON SECURITY OF PERSONAL HEALTH CARE RECORDS ON CLOUD

Prabhakar Singh
Shri Shankaracharya Technical Campus
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
yadavprabhakar89@gmail.com

Prof. Samta Gajbhiye
Shri Shankaracharya Technical Campus
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
samta.gajbhiye@gmail.com

***Abstract*—** Personal Health record is a rising patient-driven model of health data information, which is frequently outsourced to be put away at an outsider, for example, to cloud suppliers. Be that as it may, there have been wide protection worries as individual health data could be presented to those outsider servers and to unapproved parties. To guarantee the patients' control over access to their own PHRs (personal health record), it is a promising technique to encode the PHRs before outsourcing. This paper reviews some of the techniques that how can the cloud most important and critical data can be stored and retrieved without any intervention of hacker.

***Keywords*—** *Personal Health Record, Cloud, Security, Health data .*

I. INTRODUCTION

As of late, personal health record (PHR) has risen as a patient-driven model of health data trade. A PHR benefit enables a patient to make, oversee, and control her own wellbeing information in one place through the web, which has made the capacity, recovery, and sharing of the restorative data more effective. Particularly, every patient is guaranteed the full control of her restorative records and can impart her wellbeing information to an extensive variety of clients, including social insurance suppliers, relatives or companions. Because of the high cost of building and keeping up specific server farms, numerous PHR administrations are outsourced to or given by outsider specialist co-ops, for instance, Microsoft HealthVault. Recently, models of putting away PHRs in distributed computing have been proposed in [6] [7].

While it is energizing to have helpful PHR administrations for everybody, there are numerous security and protection dangers which could obstruct its wide selection. The fundamental concern is about whether the patients could really control the sharing of their touchy individual health data (PHI), particularly when they are put away on an outsider server which individuals may not completely trust. From one perspective, in spite of the fact that there exist human services directions, for example, HIPAA which is as of late altered to fuse business partners, cloud suppliers are typically not secured substances [8][9]. Then again, because of the high estimation of the delicate PHI, the third party stockpiling servers are regularly the objectives of different noxious practices which may prompt introduction of the PHI. As a renowned episode, a Department of Veterans Affairs database containing touchy PHI of 26.5 million military veterans, including their government managed savings numbers and medical issues was stolen by a worker who took the information home without approval [10]. To guarantee understanding driven protection control over their own PHRs, it is basic to have fine-grained information get to control instruments that work with.

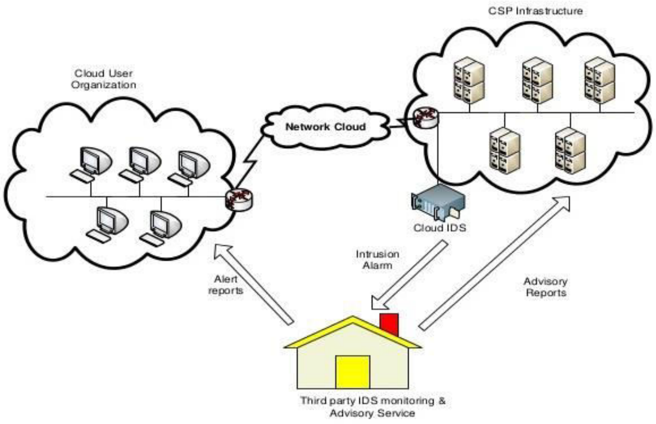

Fig.1. shows the architecture of PHR system

Regardless of various activities by industry and various principles a work in progress to give the interoperability crosswise over various PHR and EHR administrations, security and protection stay significant impediments concerning the selection of the PHRs by the people. Numerous customers don't trust business organizations to deal with their PHRs. By that, in current medicinal services, where a ton of IT usefulness gets outsourced, patients are stressed if their health information will be dealt with as classified by organizations running server farms [11, 12].

To deliver these issues identified with security and privacy of person's wellbeing data, we propose another variation of a ciphertext-arrangement characteristic based encryption (CP-ABE) conspire which empowers patients to safely store and offer their heath records on a business PHR framework. Our CPABE plot enables the patient to store her PHRs in a scrambled shape, and cryptographically implements quiet or authoritative get to approaches. The plan empowers offering of patient's information to clients from various areas, in view of traits confirmed by different specialists. For instance, a patient can scramble her information accordingly that it can be gotten to by a person from a social area (e.g. his/her grown-up youngsters) and additionally from the expert area (e.g. specialists or attendants) [14].

II. LITERATURE SURVEY

Mrinmoy Bar et. al [1], Author propose an efficient and secure patient-centric access control (PEACE) scheme for the emerging electronic health care (eHealth) system. In order to assure the privacy of patient personal health information (PHI), we define different access privileges to data requesters according to their roles, and then assign different attribute sets to the data requesters. By using these different sets of attribute, we construct the patient-centric access policies of patient PHI. The PEACE scheme can guarantee PHI integrity and confidentiality by adopting digital signature and pseudo-identity techniques. It encompasses identity based cryptography to aggregate remote patient PHI securely. Extensive security and performance analyses demonstrate that the PEACE scheme is able to achieve desired security requirements at the cost of an acceptable communication delay.

Luan Ibraimi et. al, Here author describe a new approach which enables secure storage and controlled sharing of patient's health records in the aforementioned scenarios. A new variant of a ciphertext-policy attribute-based encryption scheme is proposed to enforce patient/organizational access control policies such that everyone can download the encrypted data but only authorized users from the social domain (e.g. family, friends, or fellow patients) or authorized users from the professional domain (e.g. doctors or nurses) are allowed to decrypt it [2].

Shucheng Yu et. al., addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in finegrained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models [3].

Melissa Chase et. al, In this paper, author propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice [4].

Vipul Goyal et. al, As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for flne-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE) [5].

.

TABLE 1. Shows comparison between various existing approaches and its limitation

REF. NO.	Paper Title	Publisher Details	Author	Conclusion and Merits and Demerits
[1]	PEACE: An Efficient and Secure Patient-centric Access Control Scheme for eHealth Care System	IEEE, 2011	Mrinmoy Barua, Xiaohui Liang, Rongxing Lu, and Xuemin (Sherman) Shen	In this paper, author proposed a scheme, PEACE, to achieve patient-centric access control with security and privacy by exploiting attribute based encryption. ➢ **Merit** – PEACE scheme is able to achieve desired security requirements. ➢ **Demerit** – data storage maintaining cost is high.
[2]	Secure Management of Personal Health Records by Applying Attribute-Based Encryption	Technical Report, Univ. of Twente, 2009.	Luan Ibraimi, Muhammad Asim, Milan Petkovic	A new variant of a cipher text-policy attribute-based encryption scheme is proposed to enforce patient/organizational access control policies ➢ **Merit** –allows patients to encrypt the data according to an access policy over a set of attributes issued by two trusted authorities. ➢ **Demerit** – does not have security proof for the scheme.
[3]	Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing	IEEE INFOCOM '10, 2010	Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou	A propose a scheme to achieve this goal by exploiting KPABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption ➢ **Merit** – data access control in the emerging cloud computing environment ➢ **Demerit** – method not provide fine grandness, data confidentiality, and scalability simultaneously, which is not provide.
[4]	Improving Privacy and Security in Multi-Authority Attribute-Based Encryption	ACM, 2009	Melissa Chase, Sherman S.M. Chow	Author propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice **Merit** – it does not rely on a central authority **Demerit** – Lack of user's privacy
[5]	Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data	Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06)	Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters	Author proposed a user's keys and cipher texts are labeled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. ➢ **Merit** –data are encrypted under a set of attributes so that multiple users who possess proper keys can decrypt ➢ **Demerit** – do not able hide the set of attributes under which the data is encrypted.

III. CONCLUSION

This reviews some the new approach for secure management of personal health records which are stored and shared from an un-trusted web server. We gave an overview of various access control mechanisms and analyze which mechanisms are most useful for scenarios where data is stored on a commercial PHR systems or it is outsourced to a third party data center. Traditional access control mechanisms as well as traditional encryption techniques are not suitable to be used in these scenarios.

REFERENCES

[1] M. Barua, X. Liang, R. Lu and X. Shen, "PEACE: An efficient and secure patient-centric access control scheme for eHealth care system," 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, 2011, pp. 970-975.

[2] L. Ibraimi, M. Asim and M. Petković, "Secure management of personal health records by applying attribute-based encryption," Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health, 0slo, 2009, pp. 71-74.

[3] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1-9.

[4] J. Han, W. Susilo, Y. Mu, J. Zhou and M. H. A. Au, "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 665-678, March 2015.

[5] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. 2006. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, 89-98.

[6] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/health/ he-privacy26, 2006.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.

[8] 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.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[11] 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.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009.