International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 10, December- 2012

# Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing

S. Vidya[1]

*Assistant Professor,
Computer Science and Engineering,
SNS College of Technology, India.*

K. Vani[2]

*Assistant Professor,
Computer Science and Engineering,
SNS College of Technology, India.*

D. Kavin Priya[3]

*Assistant Professor,
Computer Science and Engineering,
SNS College of Technology, India.*

## Abstract

*Recently Personal Health Records (PHRs) has emerged as a patient centric model of health information management and exchange. It stores the PHRs electronically in one centralized place in Third Party Cloud Server. It greatly facilitates the management and sharing of patient's health information and also has serious privacy concerns about whether these service providers can be fully trusted. To facilitates rapid development of cloud data storage and maintain the security assurances with outsourced PHRs, the efficient method have been designed. To ensure the patients control over their own privacy homomorphic encryption has been proposed with data auditing to verify the correctness of PHRs stored in cloud server.*

**Index Terms- Cloud computing, PHRs, Homomorphic Encryption**

## 1. Introduction

Cloud computing is an emerging computing technology where applications and all the services are provided via Internet. It is a model for enabling on-demand network access to pool resources. Cloud computing can be considered as a computing paradigm with greater flexibility and availability at lower cost[2]. Because of these characteristics, cloud computing has been receiving a great nowadays. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other efficiencies. The Internet has grown into a world of its own, and its huge space now offers capabilities that could support Physicians in their duties in numerous ways. Nowadays software functions have moved from the individual's local hardware to a central server that operates from a remote location. In recent years, is an emerging trend and PHR is a patient-centric model of health information exchange and management. A PHR is an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in her own health care.

Generally, PHR service allows a user to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. The general principles of the security rule include that a covered entity must maintain "reasonable and appropriate" administrative, technical, and physical safeguards to protect Electronic Personal Health Information (e-PHI),[8] which include requirements to ensure confidentiality, integrity, and availability of information; anticipation and protection against possible threats to the privacy of the information or against inappropriate use; and compliance by the entity's workforce. Generally information is recorded on secured systems, backups, hard drives, flash drives, shared folders, professional networks etc.

As health care professionals, physicians know that ensuring the accuracy of confidential information involves more technical approaches, to avoid the security pitfalls. Privacy laws that speak to the protection of patient confidentiality are complex and often difficult to understand in the context of an ever-growing cloud-based technology[4]. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault, Samedi, and Medicine Brain. While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption[1].

Cloud computing is the term used for the concept of operating from a remote server, without information or executable files in the physical hardware that is being manipulated by the user. PHR outsourcing relieves the owners of the burden of local data storage and maintenance; it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements. In order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on-demand data correctness verification on behalf of cloud data owners have to be designed.

Cloud service providers (CSP) are separate administrative entities; data outsourcing actually relinquishes the owner's ultimate control over the fate of their data[12]. The survey says half of the medical transcription and data processing of the United States, estimated at $20 billion, is outsourced. These offshore processors are considered business associates of HIPAA-covered entities. Transmission of data or monitoring of the offshore security parameters may not be optimal[3].

## 2.Usage of Cloud Computing in Health Care

In general, not only the patients but doctors also could deceive by perceptions that their practices were the right ones for managing common hospitals events.

In medical field cloud computing offers great prospective for speedy access to medical information. Health IT infrastructure is very complex and for this reason organization has taken additional actions to shield the organization has taken additional resources to shield the potential private data under HIPAA[3].

Maintaining secrecy and truthfulness of information stored in all forms and providing data backup and recovery processes in extreme cases are extremely important.

Quick access to medical history of each person at any location can speed up diagnosis and treatment quality avoiding complications increasing quality and saving life.

## 3. Problem Statement

Generally PHR system has multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. The users may come from various aspects; like, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. Correctness of the PHI in the cloud is put at risk due to the following reasons. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they still face a broad range of both internal and external threats to data integrity[1].

Outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may spoil the successful deployment of the cloud architecture. To fully ensure data security and save PHR owners computation resources, we propose to the framework, where data owners can resort to an external third party auditor (TPA) to verify the outsourced data when needed. Third party auditing provides a transparent yet cost-effective method for establishing trust between PHR owner and cloud server[2]. In fact , based on the audit result from a TPA, the released audit report would not only help PHR owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform [11].

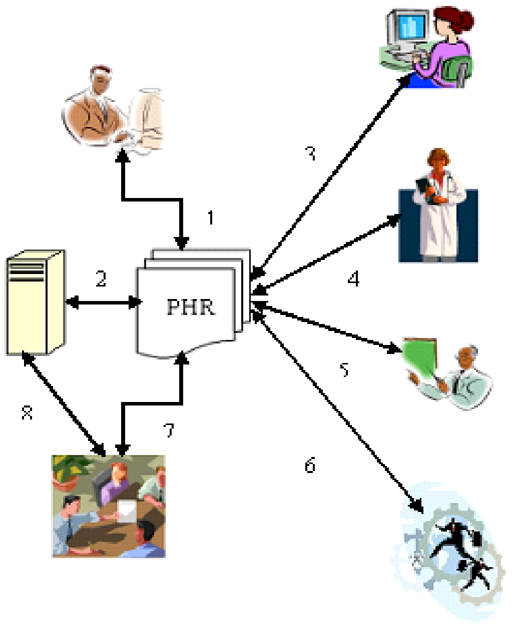
## 4. Security Model

Always the server to be semi-trusted that is honest but curious as malicious access. That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges[3].

.

## 5. Proposed Architecture

The main goal of our framework is to provide secure patient-centric PHR access and efficient security and management of that data at the same time. The User data consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a USER DATA can be mapped to an independent sector in the society, such as the health care, government or insurance sector.



1: PHR owner access and manipulate data
2: PHR is stored in cloud server
3: Sharing with friend
4: Physician access the PHR
5: insurance company
6: emergency staff
7: third party auditing
8: cloud server

Figure 1. Proposed Architecture of PHR management

It also consists of, users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner of PHR. The architecture consists of four different entities: *PHR owner*, *PHR user*, *cloud server* and *Third Party Auditor*.

PHR owner is the person whose medical information is present in that record and he has the complete rights on that data. Owner can share his information with his friends or to the doctors, nurses to get clinical suggestions.

PHR user may be in personal sector or private sector[1] who have rights according to their positions with PHR owner. User can be a health care people like physicians or Friends and family members or emergency staff.

Cloud server is the storage where the sensitive clinical data is stored and manipulated. It requires greater concern to maintain the data privacy and correctness.

TPA is the trusted entity that has expertise and capabilities to assess cloud storage security and correctness on behalf of a PHR owner upon request. The PHR owner relies on the cloud server for remote data storage and maintenance of their records, and thus is relieved of the burden of building and maintaining local storage infrastructure. In most cases cloud data storage services also provide benefits like availability, scalability, low cost and on demand sharing of data among a group of trusted users [2], such as physicians, insurance company, emergency staff, family and friends in a collaboration team or employees in the enterprise organization. As the data owner no longer possesses physical control of the data, it is of critical importance to allow the data owner to verify that his data is being correctly stored and maintained in the cloud.

We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the Cloud Servers(CS) [2]or the owners during the auditing process. The TPA should be able to efficiently audit the cloud data storage without local copy of data and without any additional online burden for data owners. Besides, any possible leakage of an owner's outsourced PHR toward a TPA through the auditing protocol should be prohibited [2]. We consider both malicious outsiders and a semi-trusted CS as prospective adversaries interrupting cloud data storage services. Malicious outsiders can be economically motivated, and have the capability to attack cloud storage servers and subsequently pollute or delete owners' data while remaining undetected [12].

An encryption scheme has algorithm consists of three steps[2].

1. Key Generation - creates two keys i.e. the privacy key prk and the public key puk.
2. Encryption - encrypts the plaintext P with the public key puk to yield ciphertext C.
3. Decryption - decrypts the ciphertext C with the privacy key prk to retrieve the plaintext P.
4. Evaluation - outputs a ciphertext C of f(P) such that Decrypt (prk,P) = f(P).

The scheme becomes homomorphic if f can be any arbitrary function, and the resulting ciphertext of Eval is compact. That means it does not grow too large regardless of the complexity of function f). The Eval algorithm in essence means that the scheme can evaluate its own decryption algorithm[2].

Utilizing Homomorphic Authenticators [12]to significantly reduce the arbitrarily large communication Overhead for public auditability without introducing any online burden on the data owner, we resort to the homomorphic authenticator technique Homomorphic authenticators are unforgeable metadata generated from individual data blocks, which can be securely aggregated in such a way to assure a verifier that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator[2].

## 6. Protecting Data Privacy

To protect data and maintain privacy proper approach is to combine the homomorphic authenticator with random masking[9]. This way, the linear combination of sampled blocks in the server's response is masked with randomness generated by the server. With random masking, the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the owner's data content, no matter how many linear combinations of the same set of file blocks can be collected. This improved technique ensures the privacy of owner data content during the auditing process, regardless of whether or not the data is encrypted, which definitely provides more flexibility for different application scenarios of cloud data storage. Besides, with the homomorphic authenticator, the desirable property of constant communication overhead for the server's response during the audit is still preserved[2].

## 7. Supporting Data Dynamics

To satisfy this special requirement, the first intuition would be using authenticated data structures, such as the well studied Merkle hash tree (MHT) which is intended to efficiently and securely prove that a set of elements is undamaged and unaltered. To further support secure and efficient data operations, one approach would be integrating the MHT with the homomorphic- authenticator-based technique taking advantage of both. the integrity of the authenticator themselves is protected by the MHT, while the authenticators further protect the integrity of the blocks This gives two immediate advantages[2]:

Unchanged blocks: The individual data operation on any file block, especially block insertion and deletion, will no longer affect other unchanged blocks.

Accountability: from the viewpoint of the threat model, all above discussions only regard the cloud server as untrusted, and the TPA's auditing result only indicates the honestness of cloud server.

Multi-Writer Model : As mentioned, cloud data storage not only provides dynamic and scalable storage services, but also allows easy on-demand file sharing.

Performance: Performance is always an important concern for practical system deployment

## 8.Conclusion and Future Enhancement

In this paper we have discussed about the Development in patient centric model and cloud computing in PHR management. this also requires the trustworthy service in cloud to protect the valuable patient data.PHR is used by multiple users so it requires the more security and privacy to reduce the complexity. here we proposed the TPA auditing to verify the cloud server which used to store and process the PHR and homomorphic encryption with data auditing is used to verify the trustworthiness of TPA.In this paper we are proposed architecture for PHR management with TPA , cloud server and potential users of PHR. We provide the architecture for providing secured PHR access. Cloud computing security is very challenging and also very essential one because it attracts numerous applications.Future work will improve the solution and fully implement the requirements of HIPAA .

## 9. References

[1] A. Vetro, H. Sun, P. DaGraca, and T. Poon, "Minimum drift architectures for three-layer scalable DTV decoding," IEEE Trans. Consumer Electron., vol. 44, no. 3, pp. 527-536, Aug. 1998.

[2] Ming Li, Shucheng Yu, Yao Zheng, , Kui Ren, Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption"IEEE Transactions on Parallel and Distributed Systems,2012.

[3] Carolina A. Klein, MD, "Cloudy Confidentiality: Clinical and Legal Implications of Cloud Computing in Health Care" The Journal of the American Academy of Psychiatry and the Law ,pp.571-578,2011.

[4] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, Pp. 743-754, April 2012

[5] Cong Wang and Kui Ren, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network ,pp. 19-24, July/August 2010.

[6] Carlos Oberdan Rolim, Fernando Luiz Koch, Carlos Becker Westphall,
Jorge Werner, Armando Fracalossi, Giovanni Schmitt Salvador, "A Cloud Computing Solution for Patient's Data Collection in Health Care
Institutions", Journal of Emerging Trends in Computing and Information Sciences"

[7] Aderemi A. Atayero*, Oluwaseyi Feyisetan, "Security Issues in Cloud Computing:
The Potentials of Homomorphic Encryption", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10,,pp. 546-552, October 2011

[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 *SecureComm'10*, Sept. 2010, pp. 89–106.

[9] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, ser. IHI '10, 2010, pp. 220–229.

[10] M.Li, S.Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in *ICDCS '11*, Jun. 2011.

[11] C.Wang et al.,"Ensuring Data Storage Security in Cloud Computing," Proc. IWQoS '09, July 2009, pp. 1–9.

[12] Q.Wang et al.,"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. ESORICS '09, Sept. 2009, pp. 355–70. [14] C. Erway et al., "Dynamic Provable Data Possession," Proc. ACM CCS '09, Nov. 2009, pp. 213–22.

[13] C.Wang et al.,"Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[14] R.C.Merkle,"Protocols for Public Key Cryptosystems," Proc. IEEE Symp.Security Privacy, 1980

**Bibliography**

Prof.S.Vidya is an Assistant Professor of Computer Science and Engineering at SNS College of Technology, India. She received a B.E degree in Computer Science and Engineering from Anna University, India in 2007 and M.E degree in Computer Science and Engineering from Karpagam University , India in 2011.She has 5 years experience in teaching and guided many projects particularly on cloud computing. Her research work focuses on cloud computing security and improving the performance.

Prof. K.Vani is an Assistant Professor of Computer Science and Engineering at SNS College of Technology, India. She received her B.E in Information Technology at Avinashilingam University, India in 2009 and completed her Masters in Computer Science and Engineering at Karunya University in 2011. She has published many papers in various International Journals and Conferences.

Prof. D.Kavinpriya working in SNS College of Technology as an Assistant Professor in Computer Science and Engineering. She completed her B.E in 2008 and M.E in Computer Science and Engineering in Anna University, India, 2011. She has published many papers in various International and National Journals and Conferences.