A Homomorphic Encryption Technique for Scalable and Secure Sharing of Personal Health Record in Cloud Computing

Soubhagya B
ME Computer Science and Engineering
Noorul Islam University
India

Venifa Mini G
Department of Computer Science and Engineering
Noorul Islam University
India

Jeya A. Celin J
Department of Computer Science and Engineering
Noorul Islam University
India

ABSTRACT

Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computers with internet access. Personal Health Record(PHR) is an emerging patient centric model of health information exchange, which is outsourced to be stored at a third party, such as cloud providers. Issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation have remained the most important challenges towards fine-grained, cryptographically enforced data access control. In the proposed work, a novel patient centric framework and a mechanism for data access control to PHRs stored in semi structured servers. A high degree of patient privacy is ensured by exploiting Homomorphic Encryption technique. It also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break glass access under emergency scenarios without revealing the content of original data. For secure data outsourcing, the users are divided in the PHR system into multiple security domains that greatly reduces the key management for owners and users.

General Terms

Cloud Computing, Personal Health Record (PHR), Homomorphic Encryption (HE).

Keywords

Personal Health Record (PHR), Cloud Computing, Homomorphic Encryption (HE)

1. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing 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. The main issues are related to loss of privacy and business value of private data by the adoption of cloud services by consumers and businesses.

A patient usually goes to hospital near by their home for health services and their health information is stored in their local database. Sometimes the patient need to go another health care centre for several reason due to unavailability of service on holidays, need for specialized health centers, emergency occurred while out of station or change of residence . The health information stored in the health care centers is only accessible to the employees of that centre and information flow is limited since the health information is stored in their own systems [18].

Personal Health Record (PHR) is a patient centric model of health information storage and exchange. A PHR is an electronic record created by a PHR Owner i.e., patient and stored in a cloud server and uses the analytical service of service providers. Each patient has full control over their own record and can effectively share with a wide range of users including doctors, family, friends and insurance agents. The cost of building and difficulty in maintaining of data centers cause the PHR services to be provided by third party service providers such as Microsoft Health Vault, Google Health respectively. These service providers cannot be fully trusted; since the patients lose physical control over their PHRs when they are stored in cloud servers cannot provide strong privacy assurance. The PHR data could be leaked if an employee of the cloud provider’s organization misbehaves. Since cloud computing is an open platform, the servers are subjected to malicious outside attacks [1]. However, concerns over loss of privacy, secure and scalable sharing of PHR data among multiple PHR users is an important problems to address [2].

The goal of patient centric privacy is often conflict with scalability in a PHR system. A PHR owner should decide how to encrypt their own files and which set of users should be allowed to view his file. The PHR users get the access right from the owner by providing the corresponding decryption key. The owner has the only right to accept and reject the users and determine which part of his PHR file can be viewed by the user. Most of the existing works contain the single data owner scenario in a PHR system [4], [5]. There are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner whose PHR they wants to read would limit the accessibility since patients are not always online.

An excellent way to assuage the privacy concerns is to store Personal Health Record (PHR) data in the cloud encrypted, and perform computations on encrypted data. To deal with the potential risks of privacy exposure, instead of letting the PHR service providers encrypt patients’ data, PHR services should give patients (PHR owners) full control over the selective sharing of their own PHR data. To this end, need an encryption scheme that allows meaningful computation on encrypted data, namely a Homomorphic Encryption (HE) scheme. With HE, the cloud can compute functions on the encrypted data and send the patient updates, alerts, or recommendations based on the received data.

2. LITERATURE REVIEW

E-health clouds offer easy access to medical data, and offer new opportunities for business models. In [3] the overall security of e-health systems needs client platform security. Security architecture is used for privacy concerns in e-health infrastructures. To decrease cost in health care, uses e-health systems like electronic health records (EHRs) and to improve personal health management. E-health systems store and process very important and secret data and proposed proper security and privacy framework. E-health system offers a more cost efficient service and improved service quality to manage data security and privacy. Electronic Health Records (EHR) is managed by health professionals only [4][20]. The main demerits of this system is, it is not efficient when the patient is absent or unable to authenticate and doesn't provide an effective scenario for emergency access.

An authorization framework for searching on encrypted PHR uses authorized private keyword searches (APKS), where users obtain query capabilities from localized trusted authorities according to their attributes [9]. Based on checking for user's attributes, every user obtain search capabilities under the authorization of local trusted authorities (LTAs). A user can search over an encrypted PHR using this method. Hierarchical predicate encryption (HPE) is used for efficient search capabilities [9]. The main issue is, it support only exact keyword search and sometimes query length may increases for fine-grained search.

Another encryption method, Ciphertext-Policy Attribute Based Encryption (CP-ABE) is a cryptographic primitive for fine-grained access control of shared data. Each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a ciphertext with the obtained attributes if it satisfy the ciphertext access structure [12]. It explains patient access control policies such that everyone can download the encrypted data but only authorized users are allowed to decrypt it. The main issue is that It lacks Key Management Scalability [12].

In [10] CP-ABE enables the authority to revoke user attributes with minimal effort and achieve this by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enable the authority to delegate most of laborious tasks to proxy servers. It is provably securing against chosen cipher text attacks. It integrates the proxy re-encryption technique with CP-ABE, and enables the authority to delegate most laborious tasks of user revocation to proxy servers without leaking any confidential information to them. On each revocation event, the authority just generates several proxy re-encryption keys and transmits them to proxy servers. Proxy servers will update secret keys for all users but the one to be revoked. CP-ABE schemes places minimal load on the authority upon each revocation event, and the authority is able to freely revoke any attribute of users at any time [10], [11].

A framework for fine-grained data access control to PHR data in cloud computing environments are proposed under multi owner settings using Attribute-based encryption (ABE)[13][7] ,is the encryption primitive used to ensure that each owner has full control over their PHR data, and each owner generates their own set of ABE keys [13]. A patient can selectively share their PHR among a set of users by encrypting the file according to a set of attributes, and encryption and user management complexity is linear to the number of attributes rather than the number of authorized users in the system[7][13]. But ABE doesn't support more expressive owner- defined access policies and doesn't enable users to processes on encrypted data without decrypting it.

Cloud storage is effective for reducing cost and long term data storage but doesn't provide any guarantee on data integrity and availability. This problem should be properly addressed otherwise it may affect the cloud architecture. An external third party auditor (TPA) is used to verify the outsourced data when needed [6] [7]. Based on the audit result from a TPA, it help PHR owners to evaluate the risk of their subscribed cloud data services and also help cloud service provider to improve their cloud based service platform [8]. The TPA cannot be fully trusted since the members in it can access the sensitive data.

In [12] allows patients to encrypt the data by two trusted authorities who issues access policy over a set of attributes. The scheme does not require the presence of a central authority to coordinate the work of the trusted authorities. It supports very expressive access policies and policies written in disjunctive normal form (DNF) or conjunctive normal form (CNF). The main issue is it doesn't provide a security proof. In our scheme Homomorphic Encryption is used for securing patients personal health record. A high degree of privacy is ensured while sharing data between different set of users

3. SYSTEM MODEL

In the proposed work, a mechanism for secure data sharing, access control to PHRs which is stored in cloud servers are fully controlled by the patient. A high degree of patient privacy is ensured by exploiting Homomorphic Encryption technique. For secure data outsourcing, the users are divided in the PHR system into multiple security domains that greatly reduces the key management for owners and users.

The paper proposes mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. The owners directly assign access privileges for personal users and encrypt a PHR file. This paper provides a thorough analysis of the complexity and scalability of the proposed secure PHR sharing solution. The proposed architecture uses Homomorphic Encryption technique for scalable and secure sharing of PHR among different set of users. A Homomorphic Encryption is the conversion of data into cipher text that can be analyzed and worked with as if it were still in its original form. Homomorphic encryption is expected to play an important part in cloud computing, allowing patients to store encrypted PHR files in a public cloud and take advantage of the cloud provider's analytic services. The scheme would prevent rogue insiders from violating privacy and would prevent accidental leakage of private information. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When decrypt the result of any operation, it is the same as if it had carried out the calculation on the raw data.

The application of Homomorphic encryption is an important stone in Cloud Computing security; more generally, we could outsource the calculations on confidential data to the Cloud server, keeping the secret key that can decrypt the result of calculation. The advantages are a high degree of patient privacy is ensured, enables dynamic modification of access policies, and supports efficient user revocation, access control and allows processing on the encrypted data without the need to decrypt.

If the data stored in the cloud were encrypted, that would effectively solve issues like availability, data security and third party access control. A user can access the PHR file from the cloud to carry out computation on data without first decrypting it. The cloud provider thus has to decrypt the data, perform the computation then send the result to the user. If the user could carry out any arbitrary computation on the accessed data without the cloud provider knowledge, the user's data - computation is done on encrypted data without prior decryption [14].

All data for a patient's medical record is encrypted and stored in the cloud storage system. The patient controls sharing and access to the record by sharing secret keys with specific provider .With Homomorphic Encryption the cloud can compute functions on the encrypted data and send the patient updates, alerts, or recommendations based on the received data. The functions to be computed in this scenario which can help predict certain dangerous health episodes. Encrypted input to the functions could include blood pressure or heart monitor or blood sugar readings [15].

The main goal of the framework is to provide secure and scalable patients PHR access and provide efficient security and management of the data at the same time. The Users make access based on their personal and professional roles, example of the former is family member and friends while latter can be doctors, nurses, medical researchers, government or insurance sector. Fig 1 shows the tree structure of proposed work.

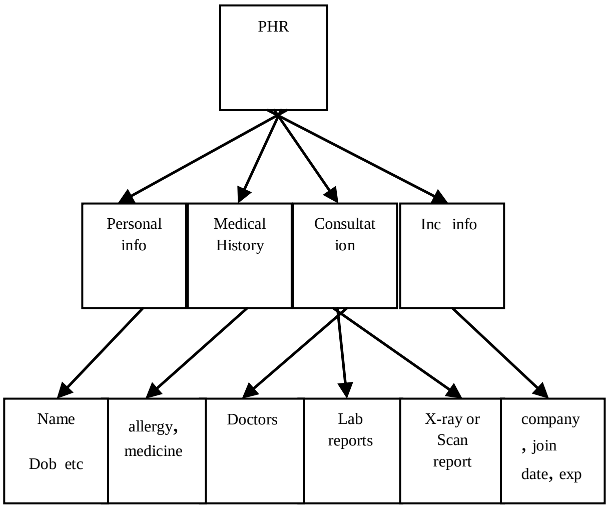


Fig 1: The hierarchy of PHR

The PHR Owner creates a PHR file which contains Personal information, Medical History both details can be accessed by Personal user. The personal users like friends or family members only need the basic information not the detailed information of PHR owner's health details. The doctors can access personal information, medical history for examining early health related issues and can update current examination result like lab or x-ray report, while the insurance agent can only access the insurance information (both users come under Professional users). Each user is associated with different access rights which are provided by the PHR Owner itself. The PHR owner can revoke the access rights of a PHR user and also can update access policies. Fig 2 explains our proposed architecture.

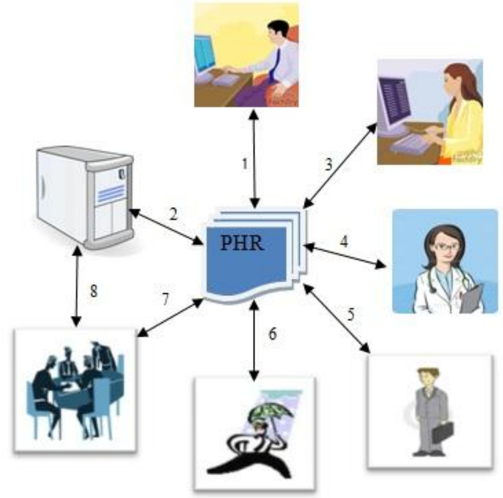


Fig2: Proposed architecture of PHR Data Sharing

1. PHR Owner create, manage and access PHR file
2. PHR stored in cloud server
3. PHR sharing with family or friend
4. Sharing with health care providers
5. Sharing with insurance company
6. Emergency staff access
7. Access by Cloud providers
8. Cloud Server

PHR Owner is the person who creates his medical 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 and insurance agent. Each owner's PHR's access right is also delegated to an emergency department ED. The emergency staffs needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys.

PHR user may be in personal sector or public sector, have rights according to their positions with PHR owner. The users in personal sector include family members or friends and public sector includes doctors, insurance agent or emergency staff.

Cloud server is the storage where the sensitive PHR is stored and manipulated. It requires greater concern to maintain the data privacy and correctness. 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 [19].

The PHR owner uses the cloud server for data storage and maintenance of their PHR, and thus building and maintaining local storage infrastructure is not needed. 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 [7], such as physicians, insurance company, emergency staff, family and friends in a collaboration team or employees in the enterprise organization. It is importance to allow the data owner to verify that his data is being correctly stored and maintained in the cloud since the data owner no longer possesses physical control of the data.

In some cases a trusted third party auditing is conducted to ensure secrecy of the patient's data [6]. But this third party cannot be fully trusted. Malicious outsiders can be economically motivated, and have the capability to attack cloud storage servers and subsequently pollute or delete owner's data while remaining undetected [17]. In the proposed architecture, each PHR owner's client application generates its corresponding public keys. A PHR owner can specify the access privilege of a data reader and let his application generate and distribute corresponding key. A reader could also obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner, and the owner will grant her a subset of requested data types.

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

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

4. EXPERIMENTAL ANALYSIS

A prototype for PHR systems are developed in this section. The username and password is used to login and shows in fig3.

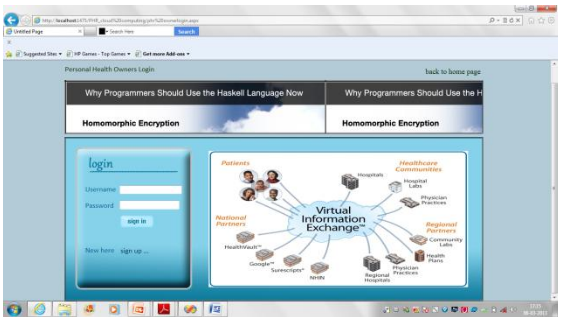
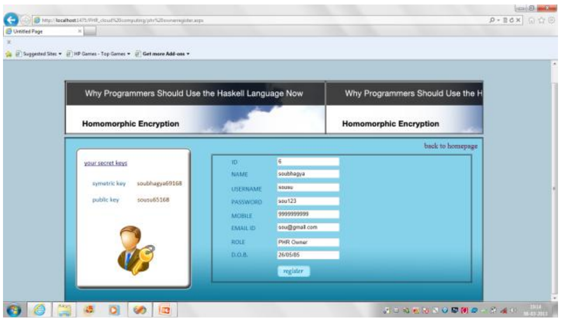


Fig 3: Patient Authentication screen

The patient or user can login only after completing the registration procedure. Fig 4 shows the screenshots of registration.

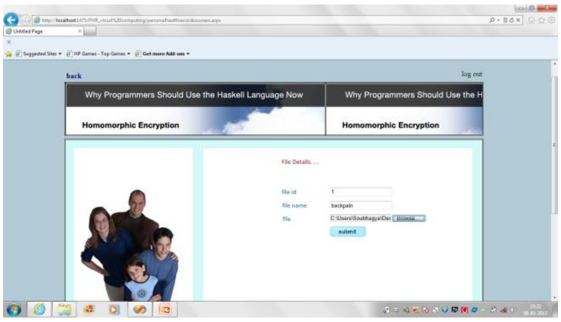


symetric key soubhagya69168
public key sousu65168

ID 6
NAME soubhagya
USERNAME sousu
PASSWORD sou123
MOBILE 9999999999
EMAIL ID sou@gmail.com
ROLE PHR Owner
D.O.B. 26/05/85

Fig 4: Patient registration screen

Fig 5 shows the uploading of the health record which is to be encrypted and stored.



file id 1
file name backpain
file C:\Users\Soubhagya\Des

Fig5: Uploading Health Record

The Homomorphic Encryption has the best encryption method to ensure security and privacy of shared data. Security performance of different encryption method is plotted in fig 6

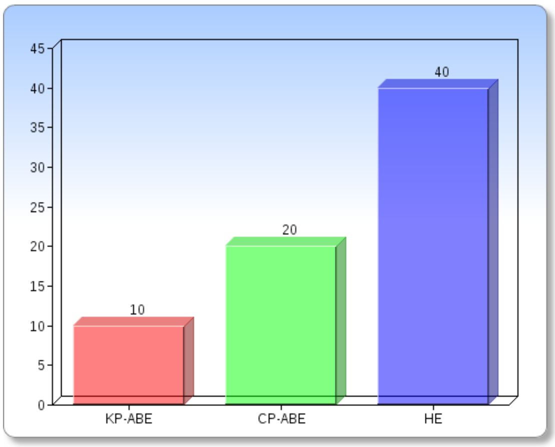


Fig6: Security Comparison

The main difference in homomorphic encryption compared to other encryption technique is it allows processing in ciphertext without decrypting the original text. The following table shows how our scheme is different from others.

The table1 shows the properties of encryption methods

SCHEME	KEYGEN	ENC	DEC	EVAL
ABE	√	√	√	––
CP-ABE	√	√	√	––
HE(our scheme)	√	√	√	√

Fig 7 shows the comparison of efficiency between different encryption techniques. This scheme is more efficient than other methods since its cipher text size, public and private key size is smaller, easy to generate and cost effective.

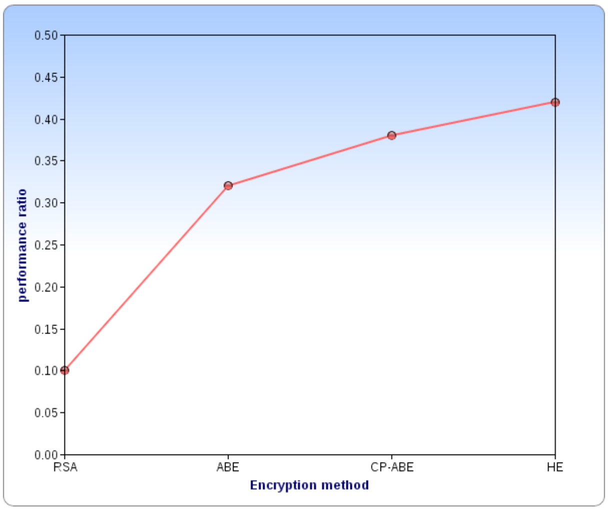


Fig 7: Efficiency comparison

5. CONCLUSION & FUTUREWORK

In the proposed work, addresses the security and privacy concerns of cloud-based PHR system by integrating advanced cryptographic technique, such as Homomorphic Encryption, into PHR system. The paper demonstrate that, by using appropriate cryptographic techniques, patients can protect their valuable healthcare information against partially trustworthy cloud servers, by assigning fine-grained, access privileges to selected data users. In the future work, a better description method can further reduce key management complexity and policy complexity. Combining other privacy-enhancing techniques with cryptographic techniques may enhance more efficient way to address the security and privacy issue of PHR systems.

6. REFERENCES

[1] "At Risk of Exposure-in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online]. Available:http://articles.latimes.com/2006/jun/26/health/he-privacy26

[2] "The health insurance portability and accountability act." [Online]Available: http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp.

[3] 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, pp. 220–229, 2010.

[4] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, pp. 103–114, 2009.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

[6] S.Vidya, K.Vani and D. Kavin Priya, " Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing**,**" International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 10, December- 2012.

[7] 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.

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

[9] 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.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

[11] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.

[12] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.

[13] 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, pp. 89–106, Sept.2010.

[14] 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, October 2011.

[15] Michael N, Kristin Lauter, Vinod Vaikuntanathan, "Can Homomorphic Encryption be Practical?" Proceedings of the 3rd ACM workshop on Cloud computing security workshop, CCSW '11

[16] "Indivo." [Online]. Available: http://indivohealth.org/

[17] Q.Wang et al.,"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. ESORICS , pp. 355–70, Sept. 2009.

[18] MD. Nurul Huda, Noboru Sonehara, Shigeki Yamada.,"A Privacy Managemaent Architecture For Patient-Controlled Personal Health Record System," Journal of Engineering Science and Technology Vol. 4, No. 2 , 154 – 170,2009.

[19] 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.

[20] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC 2010, 2010.

.