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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Securely Managing the Personal Health Records Using Attribute Based Encryption in Cloud Computing

S.Aarthika[1]

Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India[1]

ABSTRACT— Personal Health Record (PHR) is stored in cloud server for confidential purpose. In past works Identity Based Encryption (IBE) is used. Since twentieth Century Attribute Based Encryption process is used for securely store the PHR data in cloud.PHR is a developing patient-centric model of health information exchange which is often outsourced to be stored at a third party, such as cloud provider. To assure the PHR security, PHR data can be encrypted before outsource. In this process ABE is used to secure data outsourcing. In previous work single owner process is used so that key management is complex. Here proposing a multi owner scenario and divide the user into multiple security domains that reduces the key management complexity for owners and users. A high degree of PHR security is assured by using Multi Authority-Attribute Based Encryption (MA-ABE).By enhancing the MA-ABE, the public user domain security has introduced Distributed Attribute Based Encryption (DABE) concept to independently maintain attribute authorities who contains arbitary number of attributes. The key values are maintained and distributed to authorities. The data privacy is assured in DABE process in PHR

KEYWORDS— Personal health records, cloud computing, multi authority attribute based encryption

I. INTRODUCTION

Technically , cloud computing is regarded as an ingenious combination of a series of technologies, establishing a novel business model by offering IT services and using economies of scale Participants in the business chain of cloud computing can benefit from this novel model. Cloud customers can save huge capital investment of IT infrastructure, and concentrate on their own core business. Therefore, many companies or organizations have been migrating or building their business into cloud. However, numerous potential customers are still hesitant to take advantage of cloud due to security and privacy concern In recent years, personal health record has emerged as a patient-centric model of health information exchange. It enables the patient to create and control her medical data. This may be placed in a single place such as data center, from where access can be made by different individuals. Dues, to the high cost of building and maintaining specialized datacenters, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft Health Vault, Google Health. The need of security and privacy in personal health records brings the idea of encrypting the data before outsourcing to the servers. To ensure best policy, it is the patient herself who encrypts the data and determines which users shall have access in what manner. This often conflicts with scalability since there are a wide variety of personnel who try to access the PHR data. The data access may be for professional purposes or personal purposes which are categorized as professional users and personal users. Professional users include doctors, researchers, lab technician setc whereas personal users include family members and friends. This large scale of users may lead to key management overhead upon the patient. In order to overcome this, a central authority (CA) has been appointed to perform key management of professional users. But this again requires too much trust on single authority Hence we move to a new

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

encryption pattern namely Attribute Based Encryption (ABE). In ABE, it is the attributes of the users or the data that selects the access policies, which enable patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism.

II. LITERATURE REVIEW

Personal Health Record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing

1) Securing Personal Health Records

M. Li, S. Yu, K. Ren, and W. Lou [1] proposes a novel and practical framework for fine-grained data access control to PHR data in cloud computing environments, under multi owner settings. To ensure that each owner has full control over her PHR data, they leverage Attribute-Based Encryption (ABE) as the encryption primitive, and each owner generates her own set of ABE keys. his way, a patient can selectively shaIn tre her PHR among a set of users by encrypting the file according to a set of attributes, and her encryption and user management. complexity is linear to the number of attributes rather than the number of authorized users in the system

2) Securing Personal Health Records

M. Li, S. Yu, K. Ren, and W. Lou [1] proposes a novel and practical framework for fine-grained data access control to PHR data in cloud computing environments, under multi owner settings. To ensure that each owner has full control over her PHR data, they leverage Attribute-Based Encryption (ABE) as the encryption primitive, and each owner generates her own set of ABE keys. his way, a patient can selectively shaIn tre her PHR among a set of users by encrypting the file according to a set of attributes, and her encryption and user management complexity is linear to the number of attributes rather than the number of authorized users in the system. To avoid from high key management complexity for each owner and user, they divide the system into multiple Security Domains (SDs), where each of them is associated with a subset of all the users. Each owner and the users having personal connections to her belong to a personal domain, while for each public domain they rely on multiple auxiliary Attribute Authorities (AA) to manage its users and attributes. Each AA distributive governs a disjoint subset of attributes, while none of them alone is able to control the security of the whole system. In addition, they discuss methods for enabling efficient and on-demand revocation of users or attributes, and break-glass access under emergence scenarios.

3) Authorized Private Keyword Search

M. Li, S. Yu, N. Cao, and W. Lou [3] proposes the systematic study the problem of authorized private keyword searches (APKS) over encrypted PHRs in cloud computing. They make the following main contributions. First, they propose a fine-grained authorization framework in which every user obtain search capabilities under the authorization of local trusted Authorities (LTAs), based on checking for user's attributes. The central TA's task is reduced to minimum, and can remain semi-offline after initialization. Using an obtained capability, a user can let the cloud server search through all owners' encrypted PHRs to find the records that match with the query conditions. Their framework enjoys a high level of system scalability for PHR applications in the public domain. To realize such a framework, they make novel use of a recent cryptographic primitive, hierarchical predicate encryption (HPE), which features delegation of search capabilities. Based on

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

HPE they propose two solutions for searching on encrypted PHR documents, APKS and APKS+. The first solution enhances search efficiency, especially for subset and a class of simple range queries, while the second enhances query privacy with the help of proxy servers. Both schemes support multi-dimensional multi-keyword searches and allow delegation and revocation of search capabilities. Finally, they implement their scheme on a modern workstation and carry out extensive performance evaluation. Through experimental results they demonstrate that their scheme is suitable for a wide range of delay-tolerant PHR applications. To the best of their knowledge, their work is the first to address the authorized private search over encrypted PHRs within the public domain.

4) Privacy of Electronic Medical Records

J. Benaloh, m. Chase, e. Horvitz, and k. Lauter [3] proposes the encryption schemes with strong security properties will guarantee that the patient's privacy is protected. However, adherence to a simple encryption scheme can interfere with the desired functionality of health record systems. In particular, they would like to employ encryption, yet support such desirable functions as allowing users to share partial access rights with others and to perform various searches over their records. In what follows, they consider encryption schemes that enable patients to delegate partial decryption rights, and that allow patients (and their delegates) to search over their health data. They shall propose a design that refers to as Patient Controlled Encryption (PCE) as a solution to secure and private storage of patients' medical records. PCE allows the patient to selectively share records among doctors and healthcare providers. The design of the system is based on a hierarchical encryption system. The patient's record is partitioned into a hierarchical structure, each portion of which is encrypted with a corresponding key. The patient is required to store a root secret key, from which a tree of sub keys is derived. The patient can selectively distribute sub keys for decryption of various portions of the record. The patient can also generate and distribute trapdoors for selectively searching portions of the record. Their design prevents unauthorized access to patients' medical data by data storage providers, healthcare providers, pharmaceutical companies, insurance companies, or others who have not been given the appropriate decryption keys. Prevents unauthorized access to patients' medical data by data storage providers, healthcare providers, pharmaceutical company's insurance companies, or others who have not been given the appropriate decryption keys.

III. EXISTING SYSTEM

In the existing system our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its 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. In both types of security domains, we utilize ABE to realize cryptographically enforced, patient-centric PHR access. Especially, in a PUD multi-authority ABE is used, in which there are multiple "attribute authorities" (AAs), each governing a disjoint subset of attributes. *Role attributes* are defined for PUDs, representing the professional role or obligations of a PUD user. Users in PUDs obtain their attribute-based secret keys from the AAs, without directly interacting with the owners. To control access from PUD users, owners are free to specify role-based fine-grained access policies for her PHR files, while do not need to know the list of authorized users when doing encryption. Since the PUDs contain the majority of users, it greatly reduces the key management overhead for both the owners and users. Each data owner (e.g., patient) is a trusted authority of her own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in her PSD. Since the users are personally known by the PHR owner, to realize patient-centric access, the owner is at the best position to grant user access privileges on a case-by-case basis. For PSD, *data attributes* are defined which refer to the intrinsic properties of the PHR data, such as the category of a PHR file.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

For the purpose of PSD access, each PHR file is labeled with its data attributes, while the key size is only linear with the number of file categories a user can access. Since the number of users in a PSD is often small, it reduces the burden for the owner. When encrypting the data for PSD, all that the owner needs to know is the intrinsic data properties. The multi-domain approach best models different user types and access requirements in a PHR system. The use of ABE makes the encrypted PHRs self-protective, i.e., they can be accessed by only authorized users even when storing on a semi-trusted server, and when the owner is not online. In addition, efficient and on-demand user revocation is made possible via our ABE enhancements.

Drawbacks of Existing System

The expressibility of our existing encryptor's access policy is somewhat limited by that of MA-ABE's, since it only supports conjunctive policy across multiple AAs.

The credentials from different organizations may be considered equally effective, in that case distributed ABE schemes will be needed. We designate those issues as proposed works

IV. PROPOSED SYSTEM

In this proposed system this paper contains the concept of Distributed Attribute-Based Encryption (DABE), i.e., a fully distributed version of CP-ABE, where multiple attribute authorities may be present and distribute secret attribute keys. There are three different types of entities in a DABE scheme a master, attribute authorities and users. The master is responsible for the distribution of secret user keys. The latter task can independently be performed by the attribute authorities. Attribute authorities are responsible to verify whether a user is eligible of a specific attribute. In our scheme every attribute is associated with a single attribute authority, but each attribute authority can be responsible for an arbitrary number of attributes. To encrypt a message, a user first formulates his access policy in the form of a Boolean formula by attribute. To decrypt a cipher text, a user needs at least access to some set of attributes. The following diagrams shows that the authority to each users.

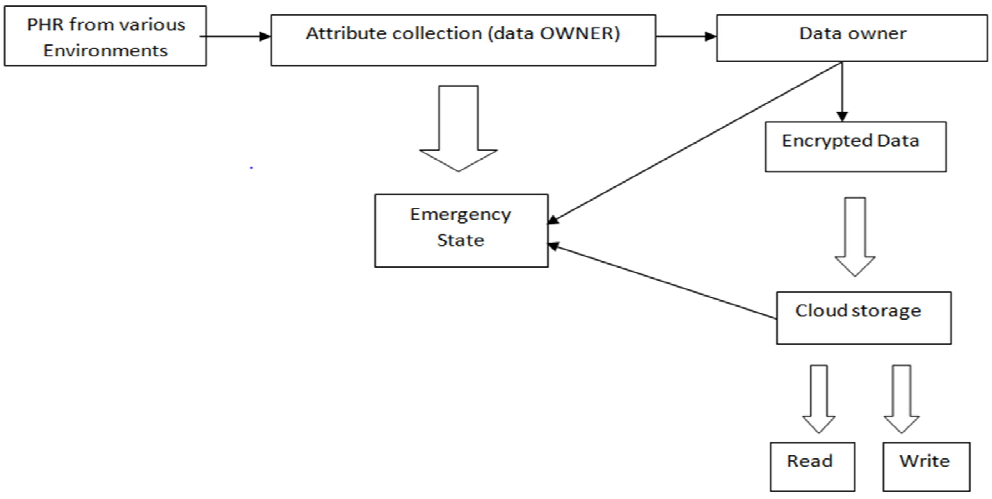

Fig.1. Architecture

Advantages of Proposed System

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

It supports practical and flexible data sharing scheme by handling both read and write operations in the access control model.

In this system attribute based encryption reduce the complexity of key management is greatly.

Personal Health Records are maintained with security and privacy.

The PHRs are accessed only by the authorized parties which makes this model provides more data confidentiality.

Even the cloud database owner can not able to modify the personal health record in this model.

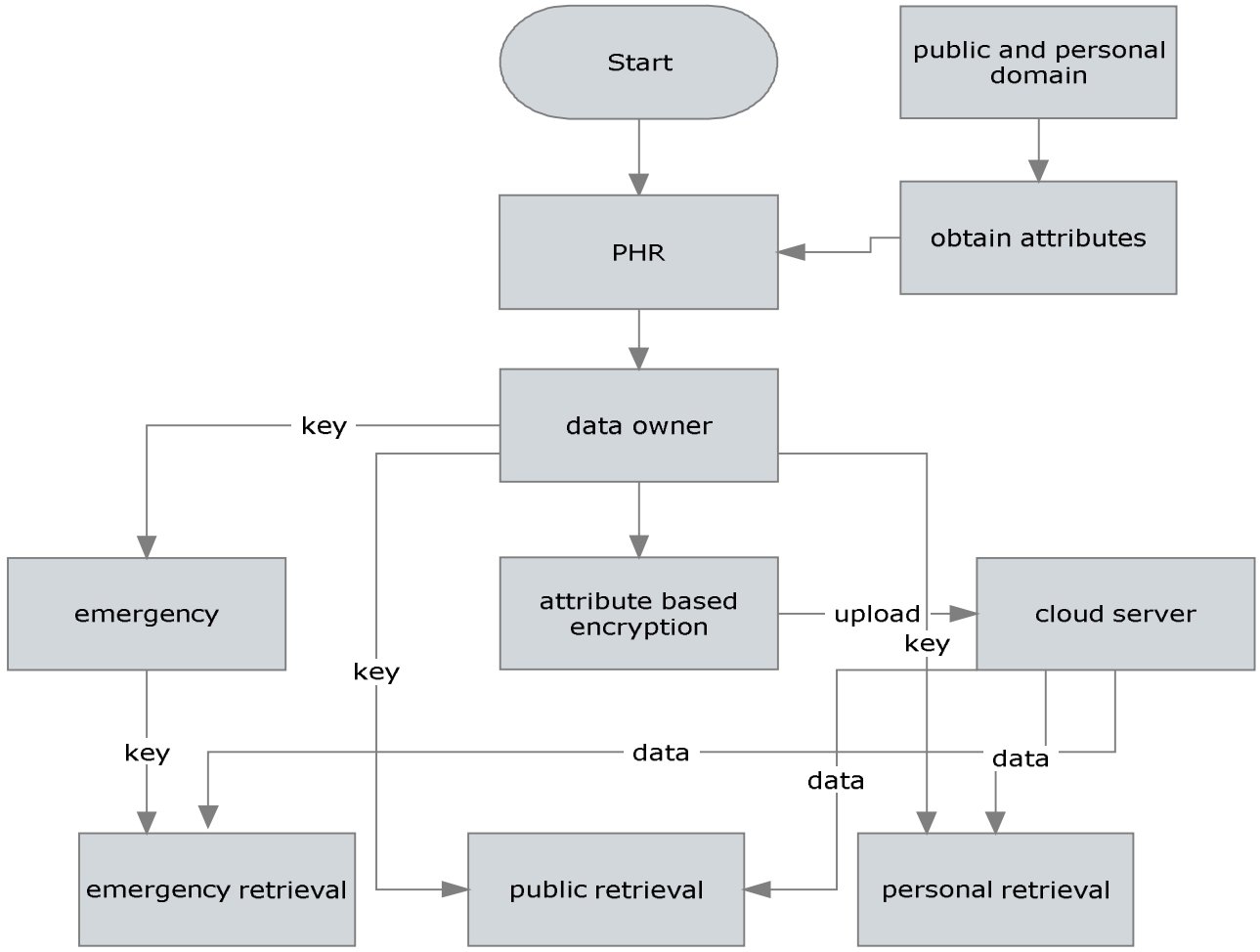

Fig. 2.Flow diagram

To achieve the secrecy of PHR in DABE scheme the following components are required

Attribute based Access Policy Module:

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

In this framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition, two ABE systems are involved. The users having read and write access as data readers and contributors, respectively. PHR can be select for encrypt as per the attribute of the personnel records These attributes are sets of labels or properties that can be used to describe all the entities that must be considered for authorization purposes i.e., access is controlled not by the rights that are possessed by the user, but by the attributes of the user.

DataOwner For PHR:

The data owner module is designed to maintain the patient details. The attribute selection model is used to select sensitive attributes. Patient Health Records (PHR) is maintained with different attribute collections. Data owner assigns access permissions to various authorities(PUD) and (PSD).The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)).

Distributed Attribute based Encryption –key Management:

In this framework, service provider distribute the personal health record file to its corresponding users. The public and personal user are get their actual key from service provider through key distribution process.The distribution process make at end of the file uploading.Each data owner (e.g., patient) is a trusted authority of her own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in her PSD.Since the users are personally known by the PHR owner,to realize patient-centric access, the owner is at the best position to grant user access privileges on a case-by-case basis.

Outsource the encrypted data in cloud:

In this paper, we consider the server to be semi-trusted, i.e., honest but curious as those action. 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. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

Data confidentiality Module:

The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files, excluding the server. The user get their personal health record from cloud server and get actual key from data owner.

V. CONCLUSION AND FUTURE WORKS

This system proposed a novel framework of secure sharing of personal health records in cloud computing environment by using DABE. Authorized parties shall have complete control of their privacy through encrypting their PHR files to allow fine-grained access. The unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees. PHRs are securely accessed using this model in the cloud servers. Further enhancement could be done on an existing DABE scheme to handle efficient and on-demand user revocation, and prove its security.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

REFERENCES

[1] 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.

[2] 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

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

[4] 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

[5] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[7] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEEWireless Communications Magazine, Feb. 2010.

[8] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp.417–426.

[9] 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.

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

[11] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving system using attribute-based infrastructure," ser. CCSW '10,2010, pp. 47–52.

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

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

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

[15] J.Bethencourt,A.Sahai, and B. Waters, "Ciphertext-policyattribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.

[16] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, and A. D. Rubin, "Self-protecting electronic medical records using attribute-based encryption," Cryptology ePrint Archive, Report 2010/565, 2010, http://eprint.iacr.org/.