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 Techniques for Storing Personal Health Details (PHR) In Privacy Cloud

Priya.C[1], Chandra Sekaran.S[2]

M.E, Department of CSE, P.S.V College of Engineering and Technology, Krishnagiri, Tamilnadu, India[1]

Associate Professor, Department of CSE, P.S.V College of Engineering and Technology, Krishnagiri, Tamilnadu, India[2]

Abstract: Personal Health Record is an emerging patient – centric model of health information exchange, which is often outsourced to be stored at the 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, it is a promising method to encrypt the health records before outsourcing. Yet, issue such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose novel patient centric framework. This paper is to address this important problem and design for health record in privacy of the involved parties and their data's. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the Health record systems into multiple security domains that greatly reduce the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority .Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

Keywords: Health care, Identity Based Encryption, Key private proxy re-encryption, Outsourcing decryption, Personal Health Record, Privacy.

I. INTRODUCTION

1.1 SECURITY AND PRIVACY IN THE CLOUD

Security is the biggest concern when it comes to cloud computing. By leveraging a remote cloud based infrastructure, a company essentially gives away private data and information, things that might be sensitive and confidential. It is then up to the cloud service provider to manage, protect and retain them, thus the provider's reliability is very critical. A company's existence might be put in jeopardy, so all possible alternatives should be explored before a decision. On the same note, even end users might feel uncomfortable surrendering their data to a third party. Similarly, privacy in the cloud is another huge issue. Companies and users have to trust their cloud service vendors that they will protect their data from unauthorized users. The various Stories of data loss and password leakage in the media do not help to reassure some of the most concerned users. Proving secure and performance analysis demonstrates the effectiveness in Cloud Computing environment

1.2 ABOUT THE SYSTEM

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient 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. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized

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

data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed. While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary.

Although health record could offer a great opportunity to improve the quality of healthcare services and potentially reduce healthcare costs, there is a stumbling block in making this technology a reality. The existing privacy laws such as HIPAA (Health Insurance Portability and Accountability Act) provide baseline protection for personal health record, they are generally considered not applicable or transferable to cloud computing environments. The current law is more focused on protection against adversarial intrusions while there is little effort on protecting clients from business collecting private information. privacy protection mechanisms by simply removing clients' personal identity information (such as names or SSN) or by using anonymization technique fails to serve as an effective way in dealing with privacy of Health systems due to the increasing amount and diversity of personal identifiable information.

The proposed mobile health monitoring scenario provides a good opportunity for adversaries to obtain a large set of medical information, which could potentially lead to identifying an individual user. We then provide an improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the Health service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To relieve the computational complexity on the company's side, which is proportional to the number of clients, we propose a further improvement, leading to our final scheme. It is based on a new variant of key private proxy re-encryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud.

1.3. OVERVIEW

In this paper, we endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a 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. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date [4]. To this end, we make the following main contributions: We propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her

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

personal domain. In this way, our framework can simultaneously handle different types of PHR sharing applications' requirements, while incurring minimal key management overhead for both owners and users in the system.

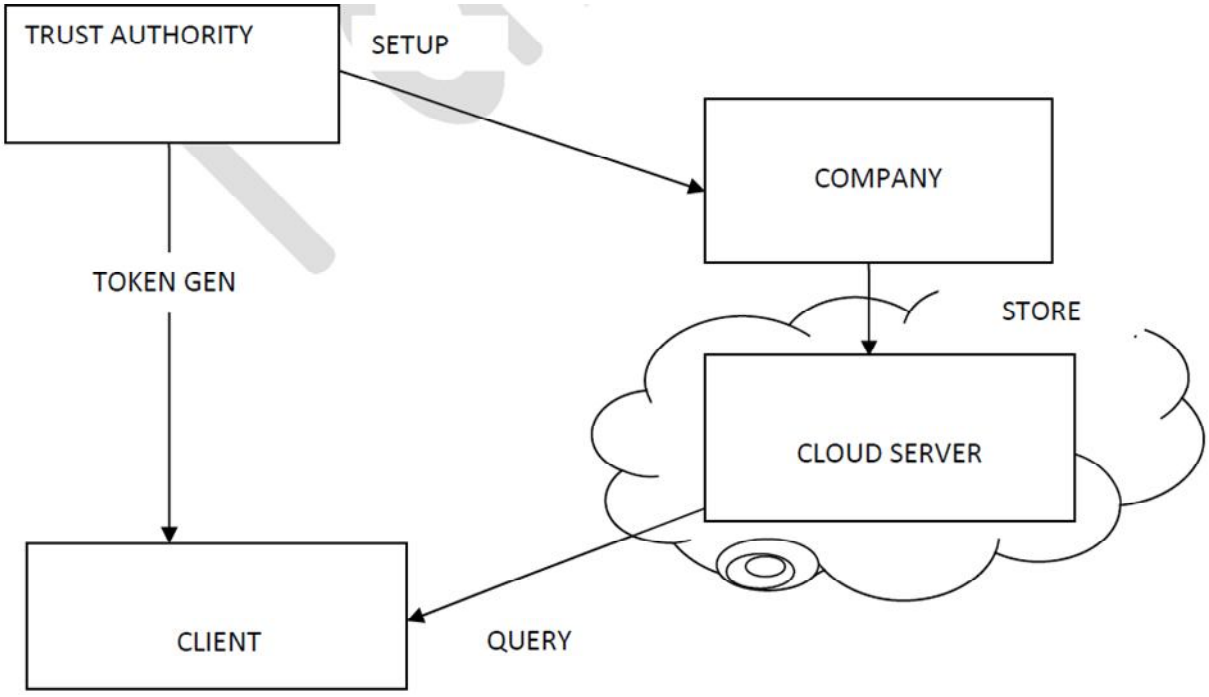

FIG 1. ARCHITECTURE DESIGN

In addition, the framework enforces write access break-glass access to PHRs under emergence scenarios. In the public domain, we use multi-authority ABE (MA-ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes. Furthermore, we enhance MA-ABE by putting forward an efficient and on-demand user/attribute revocation scheme, and prove its security under standard security assumptions [4]. In this way, patients have full privacy control over their PHRs. We provide a thorough analysis of the complexity and scalability of our proposed secure PHR sharing solution, in terms of multiple metrics in computation, communication, storage and key management. We also compare our scheme to several previous ones in complexity, scalability and security. Furthermore, we demonstrate the efficiency of our scheme by implementing it on a modern workstation and performing experiments/simulations. Compared with the preliminary version of this paper there are several main additional contributions: We clarify and extend our usage of MA-ABE in the public domain, and formally show how and which types of user defined file access policies are realized. We clarify the proposed revocable MA-ABE scheme, and provide a formal security proof for it. We carry out both real-world experiments and simulations to evaluate the performance of the proposed solution in this paper.

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

1.4 SYSTEM ANALYSIS

We consider a PHR system where there are 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; for example, 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. A typical PHR system uses standard data formats. For example, continuity-of-care (CCR) .based on XML data structure, which is widely, used in representative PHR systems including Indivo, an open-source PHR system adopted by Boston Children's Hospital. Due to the nature of XML, the PHR files are logically organized by their categories in a hierarchical way.

II. LITERATURE SURVEY

Genome-wide association studies aim at discovering the association between genetic variations, particularly single-nucleotide polymorphism(SNP) and common diseases which is well recognized to be one of the most important and active areas in biomedical research[8]. The attacker is assumed to already have a high density SNP profile to the victim, which can be extracted from a small amount of blood sample. This assumption is realistic, as the cost of genotyping is becoming increasingly affordable. Recent advances in DNA sequencing technologies have put ubiquitous availability of fully sequenced human genomes within research. Widespread and affordable availability of fully sequenced genomes immediately opens up important in a number of health related fields [7]. Operators of online social networks are increasingly sharing potentially sensitive information about user and data mining researches .privacy is typically protected by anonymization, i.e., removing names, address, etc. [1]. Attribute Based Encryption (ABE) is a new vision for public key encryption that allows users to encrypt and decrypt messages based on user attribute. ABE is currently being considered for many cloud storage and computing applications. However, one of the main efficiency drawbacks of ABE is that the size of the cipher text and the time required to decrypt it grows with the complexity of the access formal [3]. Further a new paradigm for ABE that largely eliminates this overhead for users. We present an efficient protocol for privacy preserving evaluation of diagnostics programs represented as binary decision or branching programs. The protocol the label assigned by the program to his vector. The programs owner does not learn anything [6]. A fully functional identity based encryption scheme (IBE). The scheme as chosen cipher text security in the random oracle model assuming a variant of the computational Diffie Hellman problem [4].

III. ALGORITHM AND TECHNIQUES

3.1 TOKEN GENERATION ALGORITHM

We propose a new ID-based key private proxy encryption scheme with lower cost of rekey generation comparing with the original encryption algorithm. Different from the traditional Identity-based PRE system, our rekey generation algorithm is run by TA rather than the company. The company is required to obtain the secret keys for the identity from TA in the traditional ID based PRE scheme.

3.2 KEY PRIVATE PROXY RE-ENCRYPTION

Proxy re-encryption (PRE) allows a proxy to convert a cipher text encrypted under one key into an encryption of the same message under another key. The main idea is to place as little trust and reveal as little information to the proxy as necessary to allow it to perform its translations.[5] However, in all prior PRE schemes, it is easy for the proxy to determine between which participants a re-encryption key can transform cipher texts.

Allows un-trusted proxy server with a re-encryption key to transform a cipher text encrypted for Alice into one that could be decrypted by bob. In our scheme, we emphasize two most relevant properties: uni-directionality and key privateness.

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

IV. MODELS AND DEFINITIONS

4.1 BRANCHING PROGRAM

We formally describe the branching programs, which include binary classification or decision trees as a special case. We only consider the binary branching program for the ease of exposition since a private query protocol based on a general decision tree can be easily derived from our scheme. Let v be the vector of clients' attributes.

4.2 TOKEN GENERATION

To generate the private key for a client first computes the identity representation set of each element in v and delivers all the *n* identity representation sets to TA. Then TA runs the extracted keys and delivers all the respective private keys to the client.(TA-Trust Authority).

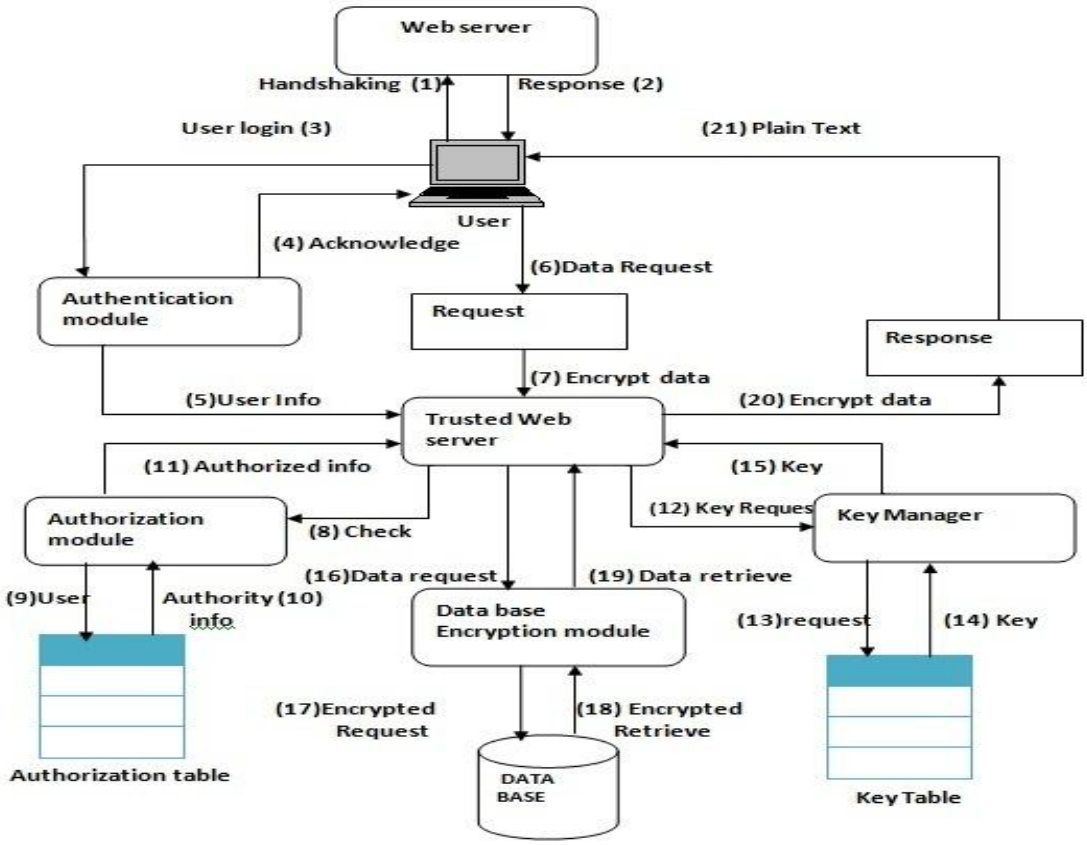

FIG 2. RUNNING PROCESS

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

4.3 QUERY

A client delivers the private key sets obtained from the Token Gen algorithm to the cloud, which runs the Anon Decryption algorithm on the cipher text generated in the Store algorithm. Starting from p1, the decryption result determines which cipher text should be decrypted next. For instance, if, then the decryption result indicates the next node index $L(i)$. The cloud will then use $sk_v(L(i))$ to decrypt the subsequent cipher text $CL(i)$. Continue this process iteratively until it reaches a leaf node and decrypt the respective attached information.

4.4 SEMI TRUSTED AUTHORITY

A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors.

V. CONCLUSION AND FUTURE ENHANCEMENT

5.1 CONCLUSION

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses 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 compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations.

5.2 FUTURE ENHANCEMENT

In Future, user's attribute is no longer valid; the user should not be able to access future PHR files using that attribute. 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. It has been observed that the adoption of automated decision support algorithms in the cloud-assisted mHealth monitoring has been considered as a future trend. It is also observed that future mobile health monitoring and decision support systems might have to deal with other much more privacy-sensitive features such as DNA profiles, from which an adversary may be able to reidentify an individual user.

VI. ACKNOWLEDGEMENT

First and Foremost, I would like to thank my graduate advisor, Prof. Chandra sekaran .S, for his guidance and encouragement throughout my graduate studies. His vast knowledge and working experience in computer science and engineering have proven invaluable in my quest to learn and grow.

I would also like to thank my other professors and advisors, Prof. Sakthivel .B, for their constructive support, camaraderie, and teamwork. My studies would not have been the same without their contributions.

Finally, but definitely not least, I want to thank my parents for their loving encouragement and grounding support at home which allowed me to concentrate and complete my work.

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] Arvind Narayanan and Vitaly Shmatikov ,"De-anonymizing social networks," in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2009, pp. 173–187.

[2] A.Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008, pp. 111–125.

[3] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in Usenix Security, 201110.

[4] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO, 2001, pp. 213–229.

[5] Giuseppe Ateniese, Karyn Benson, Susan Hohenberger "Key-Private Proxy Re-Encryption", JAN 22,2009.

[6] J. Brickell, D. Porter, V. Shmatikov, and E. Witchel, "Privacy-preserving remote diagnostics," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 498–507.

[7] P. Baldi, R. Baronio, E. D. Cristofaro, P. Gasti, and G. Tsudik, "Countering gattaca: efficient and secure testing of fully-sequenced human genomes," in ACM Conference on Computer and Communications Security, 2011, pp. 691–702.

[8] R. Wang, Y. Li, X. Wang, H. Tang, and X. Zhou, "Learning your identity and disease from research papers: information leaks in genome wide association study," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 534–544.