Scientific Journal Impact Factor (SJIF) : 1.711

IJMTER

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

Cloud Aided handy admission Of Health Records with privacy and Audit facility

S.Govintharaj[1], G.Vinoth Kumar[2], K.Prasanth[3], T.K.P.Rajagopal[4]

[1,2,3,4]*Computer Science and Engineering,Kathir College of Engineering,Coimbatore*

Abstract -Fast access to health data enables better healthcare service provisioning, improve value of life, and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in our daily life. Services support by movable campaign, such as home care and remote monitoring, enable patients to retain their alive style and cause minimal disruption to their daily behavior. In addition, it considerably reduces the hospital tenancy, allowing patients with higher need of in-hospital treatment to be admitted.

I.INTRODUCTION

E-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are concerned, and people start to realize that they would totally lose control over their private information once it enters the cyberspace. According to the government website, around 8 million patients' health information was leak in the earlier period two years. There are good reasons for maintenance medical data secret and warning the access. An company may decide not to employ someone with positive diseases. An insurance company may refuse to provide life cover knowing the disease times gone by of a patient. Despite the paramount importance, privacy issues are not addressed sufficiently at the technical level and efforts to keep health data secure have often fallen short. This is because defensive privacy in the cyberspace is considerably more challenging. Thus, there is an urgent need for the growth of viable protocols, architectures, and systems assuring privacy and security to defend responsive and personal digital information.

II.LITERATURE SURVEY

A literature review is a text of a scholarly paper, which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic. Literature reviews use secondary sources, and do not report new or original experimental work.

A systematic review is a literature review focused on a research question, trying to identify, appraise, select and synthesize all high quality research evidence and arguments relevant to that question. A meta analysis is typically a systematic review using statistical methods to effectively combine the data used on all selected studies to produce a more reliable result.

The process of reviewing the literature and writing a literature review can be difficult and lengthy. It is helpful to bring a system of association and planning to the task. When an orderly system can be designed, it is easier to keep track of the articles, books, materials read, notes, outlines and drafts.

G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis, "Medical information privacy assurance: Cryptographic and system aspects," presented at the 3rd Conf. Security Commun. Netw., Amalfi, Italy, Sep. 2002.

The firsthand experience of experts in information security and assurance who studied or worked with health applications has been of a different sort: While general principles of security still apply in the medical information field, a number of unique characteristics of the health care business environment suggest a more tailored approach. Electronically-managed information touches almost all aspects of our daily life in modern society. Cryptographic techniques can be used to assure that sensitive information is kept secure and, in general, to protect communication systems. The communication infrastructure is made secure, all privacy problems will not disappear. While making the Internet as secure as possible is necessary for privacy, it is not sufficient in and of itself. Security is not synonymous with privacy. The intelligence and financial industries are likely to be used for criminal purposes, such as the sale of military secrets or fraud, respectively. With medical information such breaches and uses may be more insidious, and the damages less over.

2.1.Advantages

- Improving the security and privacy of electronic medical data.
- MIPA project has sponsored the design of credential transfer systems to support requirements of minimum disclosure.
- The design of a system for anonymous electronic prescriptions.

2.2.Disadvantages

- linkable anonymity is no anonymity
- In security would hinder efficiency, decrease performance, and increase costs.
- Measure of risk to the security of our medical records as a better alternative to pricing health care beyond the reach of many.

D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing. Extended abstract in CRYPTO 2001,”SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

A fully functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational DiffieHellman problem. Our system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. We give precise definitions for secure identity based encryption schemes and give several applications for such systems. A public key encryption scheme in which the public key can be an arbitrary string. In such a scheme there are four algorithms:

(1) Setup generates global system parameters and a master-key

(2) Extract uses the master-key to generate the private key corresponding to an

arbitrary public key string ID $\in \{0, 1\}^*$

(3) Encrypt encrypts messages using the public key ID, and

(4) Decrypt decrypts messages using the corresponding private key .

Advantages

- Ciphertext security for identity-based systems and proposed a fully functional IBE system.
- Ciphertext security in the random oracle model.
- IBE system whose security is based on the difficulty of distinguishing quadratic residues from non-residues in the ring.

Disadvantages

- The problem is to build chosen ciphertext secure identity based systems that are secure in the standard computation model.
- Need to provide chosen ciphertext security based on DDH.
- DDH assumption is false in the group of points on the curve E, need of re-work
- two distributions appear to be computationally indistinguishable

Nicholas G. McDonald, "Past, Present, and Future Methods of Cryptography and Data Encryption" A Research Review.

Cryptography and encryption have been used for secure communication for thousands of years. Throughout history, military communication has had the greatest influence on encryption and the advancements thereof. The need for secure commercial and private communication has been led by the Information Age, which began in the 1980's. Although the Internet had been invented in the late 1960's, it did not gain a public face until the World Wide Web was invented in 1989. The World Wide Web is an electronic protocol which allows people to communicate mail, information, and commerce through a digital medium. This new method of information exchange has caused a tremendous need for information security. A thorough understanding of cryptography and encryption will help people develop better ways to protect valuable information as technology becomes faster and more efficient. Encryption is one specific element of cryptography in which one hides data or information by transforming it into an undecipherable code. Encryption typically uses a specified parameter or key to perform the data transformation.

Advantages

- Easy understanding of encryption can also help individuals with securing private data and information.

Disadvantages

- Severely unethical, our communication with one another is constantly being monitored.
- Need Monitor our communication can include governments, internet service providers, hackers, identity thieves, and more.

III. PROPOSED SYSTEM

The proposed cloud-assisted portable health networking is stimulated by the authority, flexibility, expediency, and cost competence of the Cloud-based data/computation outsourcing paradigm. We introduce the private cloud which can be measured as a service offered to portable users. Mobile users outsource data dispensation tasks to the private cloud which stores the processed results on the public cloud.

The cloud-assisted service model supports the completion of practical privacy mechanism since intensive calculation and storage can be shifted to the cloud, leaving portable users with lightweight tasks. Our planned pattern hiding scheme just somewhat increase the calculation and storage costs at the public cloud compare to the most efficient construction.

ADVANTAGES OF PROPOSED SYSTEM

- safe mechanism
- Flexible
- expediency

- Efficiency & accuracy
- No malicious attacks
- Trustable

Implementation

This project consists of four modules,

1. Storage Privacy

2. Symmetric Encryption
3. eHealth Access Control
4. Privacy Data Sharing

Storage Privacy

The user can be linked with the storage and recovery process, i.e., these process should be anonymous. unofficial parties should not be able to link numerous data files to profile a user. It indicates that the file identifiers should appear chance and leak no useful in sequence. Public Storage only collects information from you that is compulsory for us to provide service and information that we believe will interest you. We collect the following three categories of information from you: (a) Personally Identifiable Information; (b) Non-Personal Information; and (c) Passive Anonymous Information. All three of these categories are collectively referred to as "Information" in this Privacy Policy.

- To offer a report to our advertisers or business partners that tells them who respond to a meticulous offer to facilitate the fulfillment of an order that you have made with an advertiser or business partner;
- To customize, personalize, analyze, evaluate, adjust and improve the Site and our services to meet your needs and expectation and those of our business partners;
- To describe our customer audience, products and services;
- To develop partnerships with third parties to offer products or services which we believe will interest our customers;
- To anonymize or aggregate PII for various purposes, such as market or traffic flow analysis and reporting; and
- To process job applications and for recruitment purposes.

Symmetric Encryption

The covert distribution needs to be perform once and for all, and the ABE encryption of the shares needs to be performed only for a limited number of general roles. Encrypting a message does not assurance that this message is not changed while encrypted. Hence often a message authentication code is added to a ciphertext to ensure that changes to the ciphertext will be noted by the receiver. Message authentication codes can be constructed from symmetric ciphers.

The shared secret is either shared beforehand between the communicating parties, in which case it can also be called a pre-shared key, or it is created at the start of the communication session by using a key-agreement protocol, for-instance using public-key cryptography such as Diffie-Hellman or using symmetric-key cryptography such as Kerberos

eHealth Access Control

The access control is achieved by our ABE-control threshold signing scheme, where the expensive ABE operations are only used for encrypting small secret values and the majority of data encryption is fulfilled by efficient symmetric key scheme. the access structure is specified. We will show that this cryptosystem gives us a powerful tool for encryption with fine-grained access control for applications such as sharing audit log information. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users.

Privacy Data Sharing

The ability to share the same data resource with multiple request or users. It implies that the data are stored in one or more servers in thenetwork and that there is some software locking mechanism that prevents the same set of data from being changed by

Two people at thesame time. Data sharing is a primary feature of a database management system.
The privacy protection for e-health data concentrate on the framework design including the demonstration of the significance of privacy for e-health systems, the authentication based on existing wireless infrastructure

REFERENCES

1. T. Albert. Doctors ask AMA to assure some privacy for their prescription pads. http://www.ama-assn.org/sci-pubs/amnews/pick 00/prl11225.htm, American Medical News. 2000.
2. WebMD Health. My Health Re c or d, http://my.webmd.com/my health record
3. Office for Civil Rights. Standards for privacy of individually iden tifiable health information. http://www.hhs.gov/ocr/hipaa/finalmaster.html. 2001
4. D. Chaum, Security Without Identific ation: T r ansactions Systems to Make Big Brother Obsolete, CACM Vol. 28, No. 10, October 1985.
5. Damg ˚ ard. Payment systems and credential mechanisms with prov able security against abuse by individuals. In Advanc es in Cryptology – CR YPTO '88, pp. 328–335, Springer-V erlag, 1988.
6. G. Ateniese, M. Joye, J. Camenisch, and G. Tsudik. A Practical and Prov ably Secure
7. Coalition-resistant Group Signature Scheme. In In Advances in Cryptology - CR YPTO 2000. V olume 1880 of LNCS, pages 255-270, Springer V erlag, August 2000.
8. J. Baek and Y. Zheng, "Identity-Based Threshold Signature Scheme from the Bilinear Pairings,"Proc. Int'l Conf. Information Technology (ITCC '04), Information Assurance and Security Track (IAS '04), pp. 124-128, 2004.
9. IEEE Std 1609.2-2006,IEEE Trial-Use Standard for Wireless Access in Vehicular Environmentsł Security Services for Applications and Management Messages,http://ieeexplore.ieee.org/servlet/opac? punumber=11000, 2006.
10. T. Leinmu¨ller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks,"Proc. IEEE Wireless Comm.,pp. 16-21, Oct. 2006.