e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

Securely Sharing of Personal Health Records in Distributed System Using Attribute Based Encryption

Padmavati D. Lakdeuthors
The Institution of Engineers (India), MSC, AMIE
Mahalaxmi, Mumbai, India

Abstract— Cryptography is one of the best solutions to provide security to (PHR). It is first decided by American Medical Association (AMA) that PHR is also one type of asset and it should get protected from unauthorized user. If data is get leaked by any doctor or the IT professional which work on behalf of patient then it is one type of crime for that responsible person may have to face several penalties. Here I am planning to use attribute based encryption (ABE). Attributes like name, contact number, address like this few more attributes are used which will give more information that are educational qualification, location, diseases, etc. Further ABE is categorized as key policy attribute based encryption KP-ABE, Multi authority attribute based encryption MA-ABE.
Keywords—Encryption;decryption;attribute;MA-ABE,sensitive data

I. INTRODUCTION

Now a day's personal health record (PHR) has emerged as a patient centric model of health information exchange. In our country people are not aware about PHR. It is required to create awareness about PHR system. The application of information technology to healthcare (healthcare IT) has become increasingly important in many countries in the recent years. There are continuing efforts on national and international standardization for interoperability and data exchange. Many different application scenarios are investigated in electronic healthcare (e-health) e.g., electronic health records, accounting and billing, medical research, and trading intellectual property. In particular e-health systems like electronic health records (EHR) are believed to decrease costs in healthcare e.g. avoiding expensive double diagnoses or repetitive drug administration and to improve personal health management in general.

The e-health approach in Austria, the electronic Health Card (eHC) system and Taiwan Electronic Medical Record Template (TMT) [5] are the examples of centralized data. In Germany each insured person will get a smartcard that not only contains administrative information (name, health insurance company) , but also can be used to access and store medical data like electronic prescriptions, emergency information like blood group, medication history, and electronic health records. The smartcard contains cryptographic keys and functions to identify the patient and to encrypt sensitive data. The TMT in Taiwan concentrates on a standardized document data structure to ease information sharing, but also contains a similar infrastructure based on smartcards allowing sharing and transferring electronic health records (HER). A common approach in all these systems is to store medical data in central data centers, which build the core concept of a centrally managed healthcare infrastructure [5].

II. LITRATURE SURVEY

TABLE I. IN SHORT SUMMARY REFERRED PAPERS [6][7][11]

Paper 1. Securing the e-health cloud		
What exactly given in abstract	***What are the achievements***	***Possible future directions***
This paper gives idea about the use of information technology to improve medical services and reduce cost. Further it is explained that the medical records stored on cloud storage that can be useful for other businesses at the same time. As health records are get used for other businesses means it is one type of risk, client's data is not secure. With the help of eHC and TMT this paper explained the secure sharing of e-health record in cloud. In this system e-health manages cryptographic keys, certificates. Management of hardware and software components.	This paper focuses on data storage and data processing, Management of e-health infrastructure usability aspect of end user. Main focus is on client security. Data availability and accessibility.	As this paper says the health data is used for other businesses to avoid this TVD is useful. TVD is trusted virtual domain it is one type of security frame- work for distributed multi domain enviro- nment.
Paper 2.Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine Grained Data Access Control in Multi-Owner Settings		
Here new crypto system concept is introduced i.e.MA-ABE. This scheme allows any number of independent authorities to monitor attribute and distribute secret keys. This paper explained security with the help of confidentiality, integrity and availability. This paper says that data confidentiality is not only a security or privacy issue but also of juristic concern. First Chase and Chow used multi authority attribute based encryption. This paper says that when multiple users are sharing data for multi user KP-ABE is used. To protect file GID and KP-ABE policies, proxy re-encryption, SSL and pair of private-public keys are used.	With the help of MA-ABE sharing of data is get available and confidentiality is achieved without any central authority. Fine grained access control that means data is get accessed only by authorized users. Re-key generation and distribution.	Here future work will be enhancing multi authority attribute based scheme (MA-ABE)
Paper 3.Authorized Private Keyword Search Over Encrypted Data In Cloud Computing		
Many people having doubt in their mind when they are storing their data on a server owned by a third party CSP's. Content of this paper shows its work in multi owner, multiuser environment. This paper is useful to study systematically problem of authorized private keyword searches (APKS) over encrypted data in cloud computing.	In this system patient can get information if patient's disease match otherwise he or she cannot learn any information. From this paper it is get concluded that though APKS takes more time for	In future pairing based cryptography scheme utilisation and APKS utilisation for fast search.

In this paper they used attribute hierarchies over different type of fields like numerical and non-numerical. In this paper hierarchy structure is used. The basic idea behind this is to include the path using is index values. This paper has implemented basic solution of APKS using pairing based cryptography (PBC).	setup and encryption it is much faster in search operation.	

III. OVERVIEW OF PHR

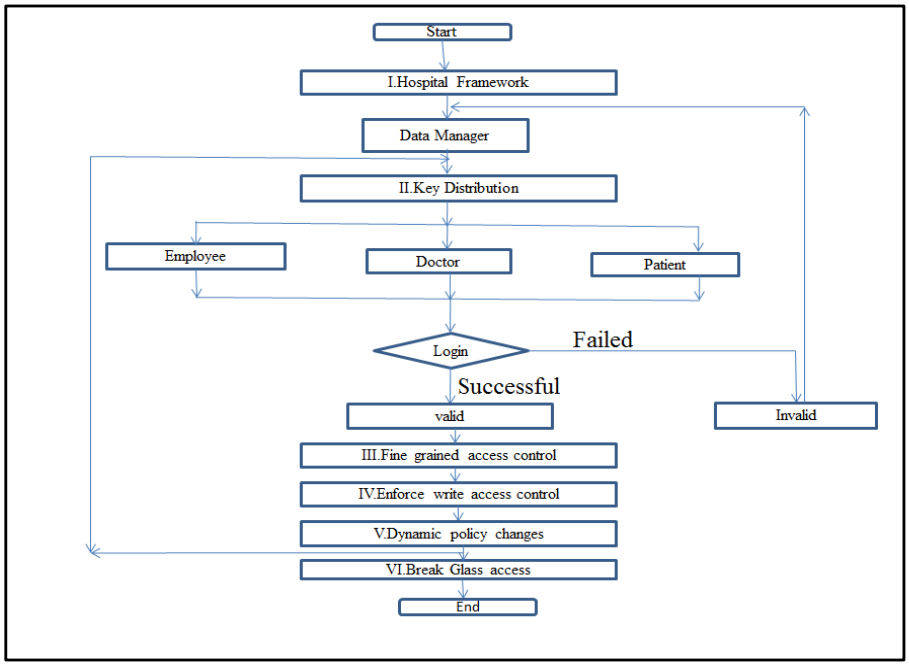

Fig.1. Flow chart

In normal case patient's record are on paper that are kept in file and that files are searched by patient id. All are in readable format so somebody can access file and read information. If a patient having diseases like AIDS or Cancer then this information is called as sensitive information because banks or employers could refuse a loan or a job if the data about the health of a person is available. If health data is leaked outside the system deliberately or accidentally, the responsible health professionals or IT providers would have to face several legal penalties for violating privacy laws.

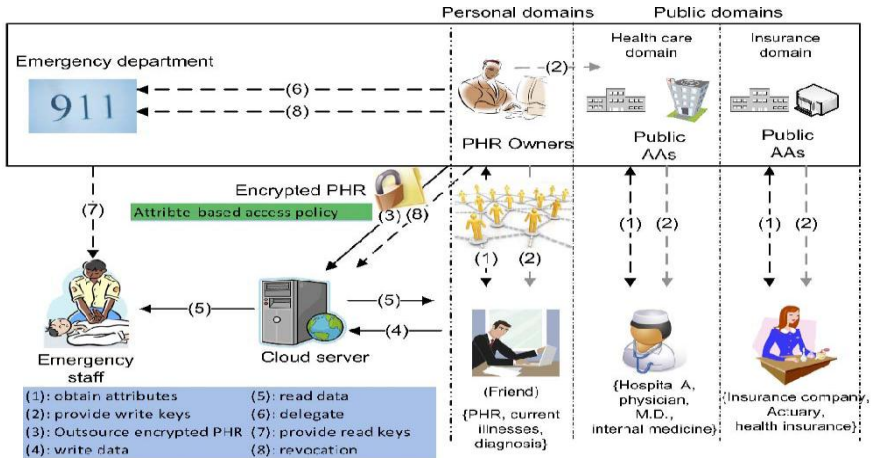

Fig.2. The proposed framework for patient-centric, secure and scalable PHR sharing on semi trusted storage under multi owner settings [5].

Examples:

a) (30<Z1<60)^(Z2="*")^(Z3Є{Names of state }) ^ (Z4="cancer")^(Z5="Hospital A")[6].
b) P1 : ''(profession=physician)^ (specialty=internal medicine)^ (organization =hospital A)''
c) "(Physician AND M.D.) OR (nurse AND any nursing license)" [5].

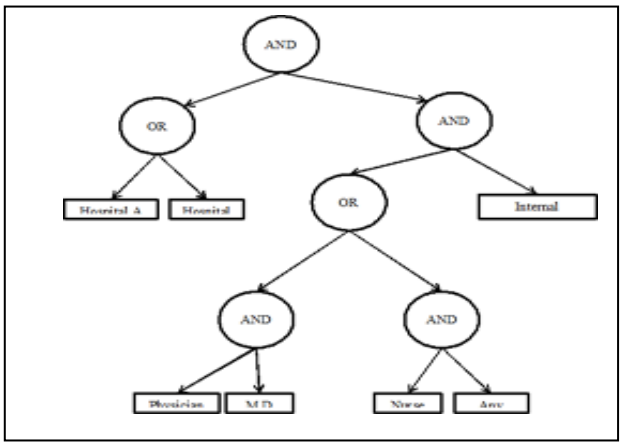

Fig.3 Example policy realizable under proposed framework using MAABE, following the enhanced key generation and encryption rules [5]

Table I shows an example,there are three Attribute Authorities (AA). American Medical Association (AMA),American board of medical specialties (ABMS) and American Hospital Association (AHA) they all are working to decide roll based attributes for public domain user as per there qualification and affiliation for access control.

TABLE II. SAMPLE SECRET KEYS AND KEY-POLICIES FOR THREE PUBLIC USERS IN THE HEALTH CARE DOMAIN [5]

Attribute authority	**AMA**				**ABMS**		**AHA**	
Attribute type	***A1:Proffesion***		***A2:License status***		***A3:Medical speciality***		***A4:Organisation***	
A^{u1}:user1	Physician	*	M.D.	*	Internal Medicine	*	Hospital A	*
A^{u2} :user1	Nurse	*	Nurse license	*	Geronto logy	*	Hospital B	*
A^{u3} :user1	Pharmacist	*	Pharm License	*	General	*	Hospital C	*
Key Policy	1-out of n1^1-out of-n2				1-out-of-n3		1-out-of-n4	

IV. ALGORITHMS USED

CP-ABE :

- Setup. A randomized algorithm Setup(k) takes in as input a security parameter and provides a set of public parameters (PK) and the master key values (MK).
- Encryption. The algorithm Enc(M, T , PK) is a randomized algorithm that takes as input the message to be encrypted (M), the access structure T which needs to be stashed and the public parameters (PK) to output the cipher text CT. We can say that the encryption algorithm embeds the access structure in the cipher text such that only those users with attributes satisfying T will be able to decrypt and retrieve the message M.

- Key-Generation. The KeyGen(MK, PK, A) algorithm takes as input the master key values (MK), the public parameters (PK) and the attribute set of the user (A), and outputs for the user a set of decryption keys SK which corms the users possession of all the attributes in A and no other external attribute.
- Decryption. The decryption algorithm Dec(CT, SK, PK) takes as input the cipher text CT, the user secret keys SK and the public parameters PK, and it outputs the encrypted message (M) if and only if the attributes A embedded in SK satisfy the access structure T which was used while encrypting the cipher text CT. i.e If T (A) = 1 then message M is output else, it will not show message is in original form.

V. MODULES

To describe working of PHR there are different modules [5]

A. Hospital framework.

B. Key management.

C. Fine-grained access control

D. Enforce write access control

E. Dynamic policy change

F. Break-glass access

A. Hospital framework

Here created a hospital framework in the web application, for the personal health records. In the framework there are entities like Master, Patient, Hospital employee, and some needed person. The Master can only able to observe overall records and other is not. The main goal of this framework is to provide secure patient-centric PHR access and efficient key management at the same time.

B. Key management

The key idea is to divide the system into multiple security domains (namely, public domains and personal domains) 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. The system first defines a common universe of data attributes shared by every PSD, such as "basic profile," "medical history," "allergies," and "prescriptions." An emergency attribute is also defined for break-glass access. Each PHR owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an On line healthcare social-network (HSN).

C. Fine Grained Access Control

Fine grained access control means, to accessing the record by only the authorized user, not others. The Personal health records having more number of user records, this access control used to shown the details to the particular users, only key match users can be able to view the profiles. The key-policy ABE to secure outsourced data in the cloud where a single data owner can encrypt her data and share with multiple authorized users, by distributing keys to them that contain attribute-based access privileges.

D. Enforce write access control

If there are no restrictions on write access, anyone may write to someone's PHR using only public keys, which is undesirable. By granting write access, we mean a data contributor should obtain proper authorization from the organization. For example, a doctor should be permitted to write only during her office hours; on the other hand, the doctor must not be able to write to patients that are not treated by him or her.

E. Dynamic policy change

In this module, for doing dynamic changes in the policies, for example, add, modify, and delete the records. This only done by the authorized users and doing for their personal details only. If a patient does not want doctors to view her PHR after she finishes a visit to a hospital, she can simply delete the cipher text components corresponding to attribute "doctor" in her PHR files. Adding and modification of attributes or access policies can be done by proxy re encryption techniques.

F. Break-glass access

This only happens at the emergency time period, in that time records couldn't be accessing. This situation is get handled, using break glass access method, in this method; the particular staff accesses the patient details at emergency time. The details accessed after that, the user details can again encrypted and stored into the database. The PHR data, medical staffs need to have temporary access when an emergency happens to a patient, who may become unconscious and is unable to change her access policies beforehand. The medical staffs will need some temporary authorization (e.g., emergency key) to decrypt those data. Under our framework, this can be naturally achieved by letting each patient delegate her emergency key to an emergency department. Specifically, in the beginning, each owner defines an "emergency" attribute and builds it into the PSD part of the cipher text of each PHR document that he or she allows break-glass access Key-policy "emergency," and delegates it to the ED who keeps it in a database of patient directory. Upon emergency, medical staffs authenticates themself to the ED, requests and obtains the corresponding patient's skEM, and then decrypts the PHR documents using skEM. After the patient recovers from the emergency, she can revoke the break-glass access by computing a rekey: rkEM, submit it to the ED and the server to update her skEM and CT to their newest versions, respectively.

VI. CLIENT INTERFACE

Fig.4 is a web page designed for client interaction through which client or user can interact with others. It is having different modules, first doctor and patient has to register through patient and doctors registration.

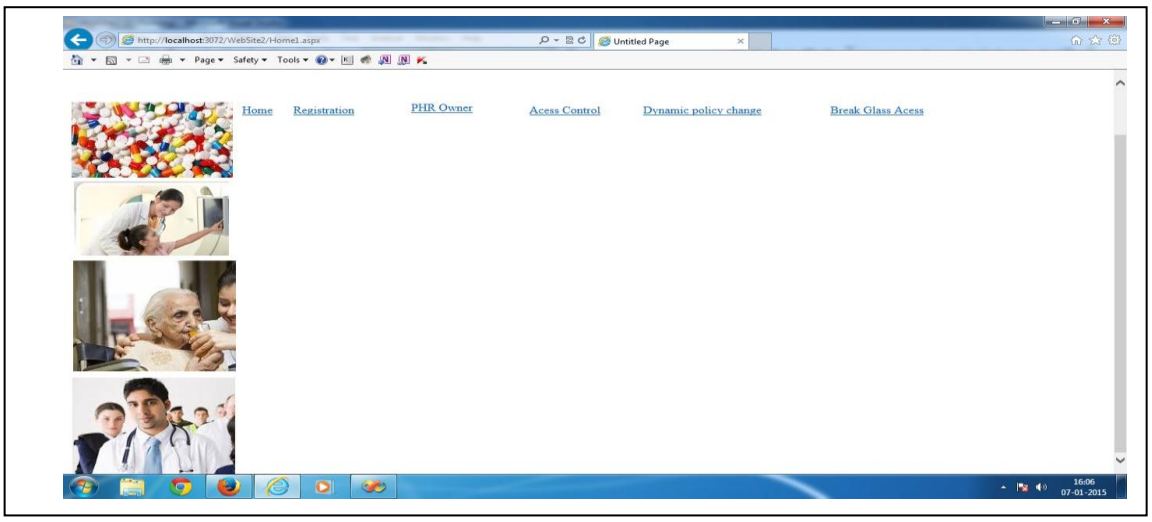

Fig.4. screen1

After registration ,through access control doctor and patient login are there doctor can login through doctor login and write down report regarding patient health that information is get uploaded.n fig. 5 it isshown that information is in encrypted form.

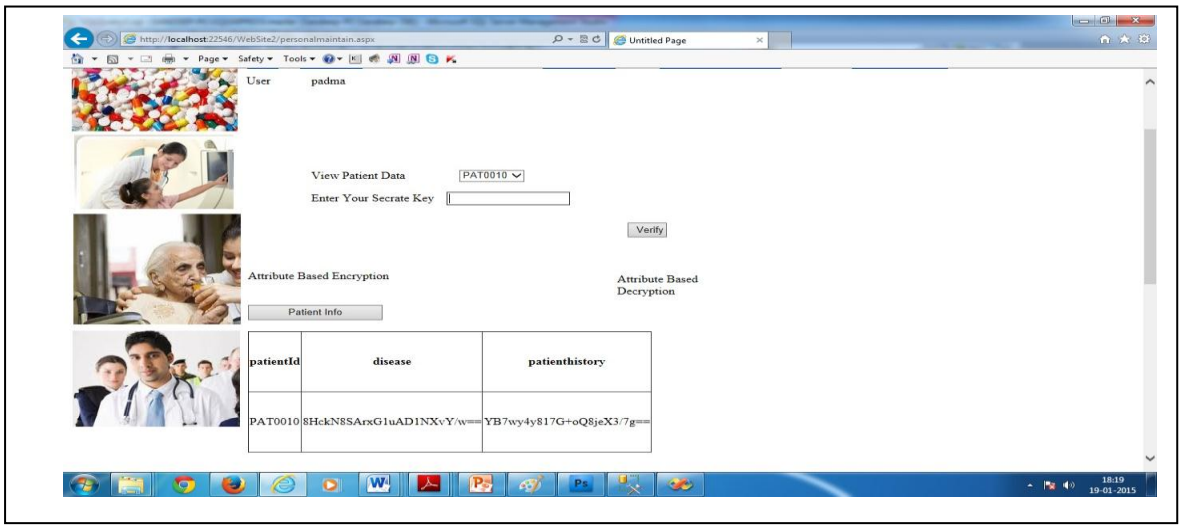

Fig.5. screen 2

When user apply proper secret key that information is get converted into its original form that is shown in fig. 6, Fig.7 and Fig.8.

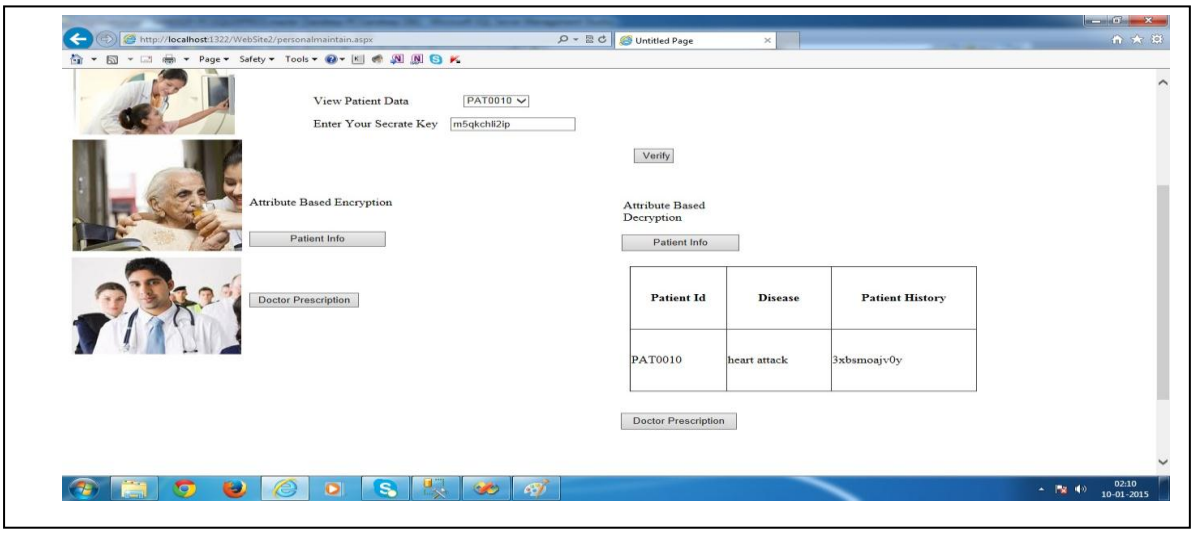

Fig.6. screen 3

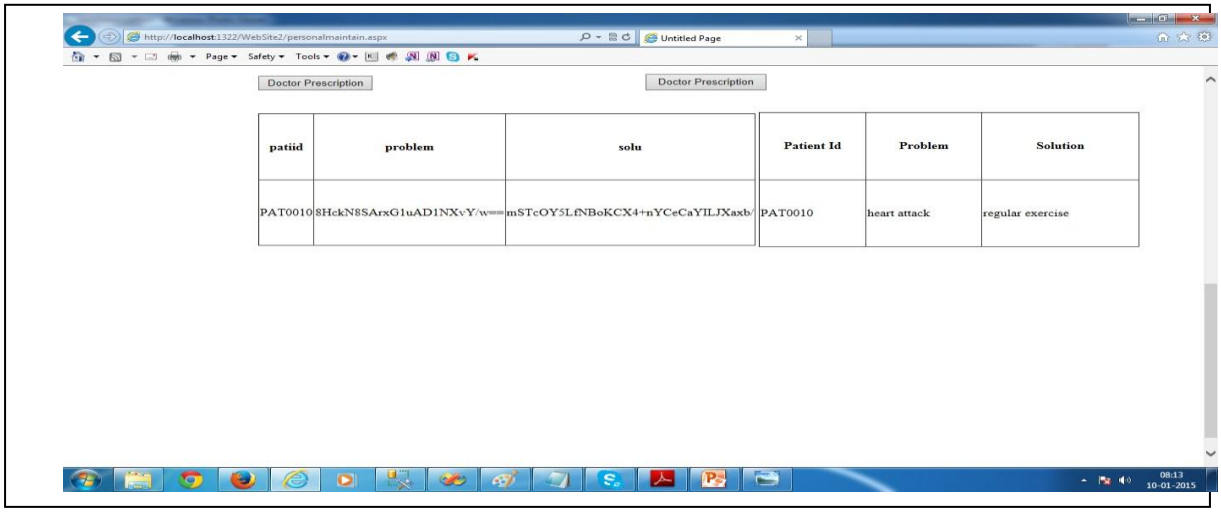

Fig.7. screen 4

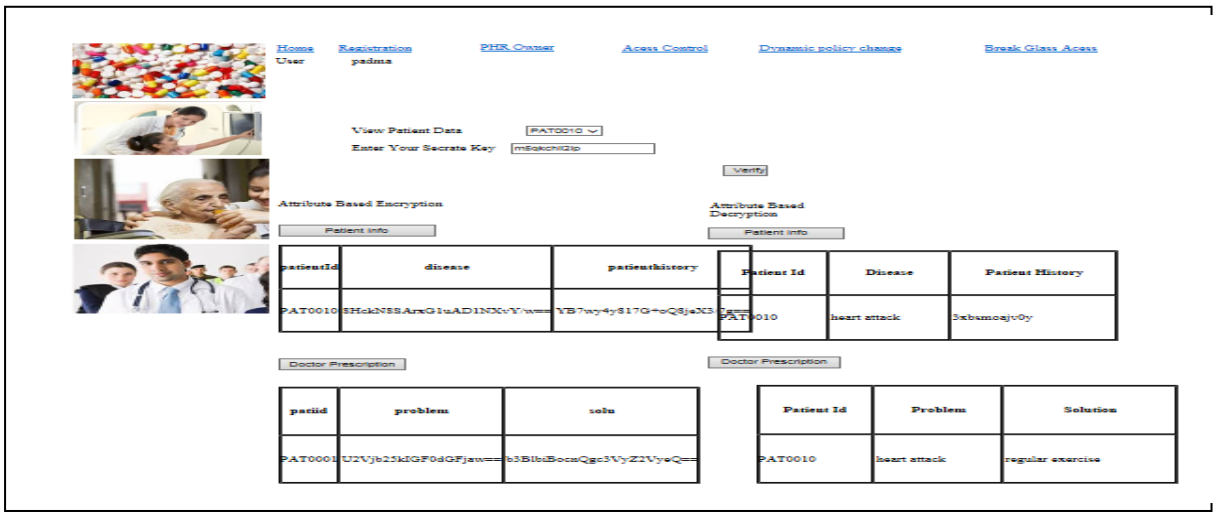

Fig.8. Screen 5

VII. TECHNOLOGY USED FOR FRONTEND AND BACKEND

This work is carried out on windows XP platform and for frontend C# .NET used and for backend Microsoft SQL Server 2012 is used.

ACKNOWNLEDGMENT

Most of the contents of this paper taken from "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption" this paper explains each and every concept so,my great thanks for Ming Li, Shucheng Yu, Yao Zheng, Kui Ren,Wenjing Lou.Many thanks goes to Sahai and Waters because they had given idea of this concept in 2005.Thanks to Atul Kahate, because he's book cryptography and network security cleared many doubts regarding basic concepts of cryptography.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", *Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.*

[2] A Wiley Tech Brief, Jon C. Graff, "Cryptography and E-Commerce Guide", *Wiley Computer publishing, ISBN-0471-40574-4.*

[3] Darrel Hankerson, Alfred Menezes, Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer Professional Computing, , *ISBN 0-387-95273-X.* S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.

[4] Changji Wang Yang Liu, "A Secure and Efficient Key-Policy Attribute Based Key Encryption Scheme", *IEEE 978-0-7695-3887-7/09/$26.00 ©2009, PP1601 -1604.*

[5] 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, VOL. 24, NO. 1. JANUARY 2013, pp. 131-143.*

[6] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing", *Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.pp 1-12.*

[7] H. Lo, A.R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud", Proc .*First ACM Int'l Health Informatics Symp.(IHI '10), pp. 220-229, 2010.*

[8] John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-policy attribute-based encryption".In *IEEE Symposium on Security and Privacy, pages 321-334, 2007*

[9] Benoît Libert and Damien Vergnaud, "Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption",*IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 57, NO. 3, MARCH 2011 pp.1786-1802.*

[10] 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", *Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (Secure Comm '10), pp. 89-106, Sept. 2010.*

[11] https://www.healthvault.com/in/en

[12] https://www.certicom.com/

