Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.514 – 521

RESEARCH ARTICLE

Secure Sharing of Medical Records Using Cryptographic Methods in Cloud

M.P. Radhini[1], P.Ananthaprabha[2], P.Parthasarathi[3]

[1]P.G. Student, Department of CSE, Sri Krishna College of Technology, Coimbatore

[2,3]Assistant Professor Department of CSE, Sri Krishna College of Technology, Coimbatore

Email: [1] radinimp4@gmail.com,[2] ap.prabha@gmail.com, [3] sarathi.p@gmail.com

Abstract—Cloud based data is safer than paper and client-server records. Now, medical practices just have to be willing to look to the cloud for the future of healthcare IT. There are lots of security issues related with the storage of sensitive personal health information in the cloud, which will make lots of security challenges to the PMR privacy and confidentiality. Cryptography is an essential tool that helps to assure our data accuracy. The Cryptographic techniques can be employed to protect the data in cloud environment. The technique used for security is multiple authority attribute based encryption technique which focuses on the multiple data owner scenario and divide the users in the PMR system into multiple security domains which leads to key management complexity for owners and users. In the proposed distributed attribute based encryption scheme PMR can be accessed from any hospital using a single key thereby reducing the complexity of key management.

KEYWORDS: Personal medical records; cloud computing; key management; attribute based encryption; Personal health record

I. INTRODUCTION

Cloud computing is an efficient technique by which the user can access any data from anywhere and anytime through internet. Thus it's providing the new world of computing technology to the world. The personal health records are thus also using this cloud computing technology for the efficient storage and retrieval system. But there is still a comparison is going on with the electronic health record and personal health record.

Electronic health record is the electronic version of the medical record of the care and treatment the patient receives. It is maintained and managed by the health care organizations. But our PMR is the collection of important information that the patient maintain about their health or the health of someone they are caring for. It may be short and simple or very detailed.[1]The traditional PMR was in the form of paper documents, electronic files maintained by their computer, but now the PMR is created by using the tools available in the internet. So which make the facility to use the health information across any distances, and to share with the selective users with special read and write access.

But while using third party service providers there are many security and privacy risks for PMR. The main concern is whether the medical record owner actually gets full control of his or her data or not, especially when it is stored in third party servers which is not fully trusted.

The normal public key encryption methods and another traditional encryption schemes are making lots key management problem for the sharing of the personal health record and also all those methods provide very less scalability to the system. The main goal of our framework is to provide secure patient-centric PMR access and efficient key management at the same time.

PMR architectures are based on fundamental assumptions that:

- The complete record is held in a central repository.
- Patients preserve authority over complete access to their own records.

Therefore, we propose the PMR to achieve the following:

- Integration of patient's health information.
- Patient's right to complete access of his/her PMR.
- Provision for accurate access settings to various parts of the PMR for different users.

Security Concerns

The major issue in adopting cloud is the security. The data stored in the cloud get increased every day and hence we need some mechanisms to ensure that our data is stored in secured manner without any unauthorized access. The main goal of this framework is to provide secure patient-centric PMR access even from different hospitals and efficient key management at the same time.

The remainder of this paper is organized as follows: Section II overviews the related work. Section III describes the cryptographic cloud storage. Section IV describes the system model and design goals. Section V explains the implementation details. Finally, we conclude the paper in Section VI.

II. RELATED WORK

In [2] Stefan Katzenbeisser et al. introduced a distributed attribute based encryption technique because ciphertext policy attribute-Based Encryption allows to encrypt data under an access policy, specified as a logical combination of attributes. Such cipher-texts can be decrypted by anyone with a set of attributes that fits the policy. But in distributed attribute-based encryption (DABE), where an arbitrary number of parties can be present to maintain attributes and their corresponding secret keys. This is in bare difference to the classic ciphertext policy attribute based encryption schemes, where all keys are distributed by one central trusted party. We provide the construction of a DABE scheme; the construction is very efficient for encryption and decryption.

In [3] Matthew Pirretti et al. proposed a Secure attribute based systems in which attributes define and classify the data to which they are assigned. However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. In which a novel secure information management architecture is introduced based on emerging attribute-based encryption primitives. A policy system that meets the needs of complex policies is defined and illustrated. Based on the needs of those policies, therefore proposed a cryptographic optimizations that vastly improve enforcement efficiency.

In [4] Milan Petkovic et al. proposed a secure management of personal health records by applying attribute-based encryption, which enables secure storage and controlled sharing of patient's health records. A variant of a ciphertext-policy attribute-based encryption scheme is used to enforce patient/organizational access control policies such that everyone can download the encrypted data but only authorized users from the social domain (e.g. family, friends, or fellow patients) or authorized users from the professional domain (e.g. doctors or nurses) are allowed to decrypt it.

In [5] Shucheng Yu et al. introduces a attribute based data sharing with attribute revocation which focus on an important issue of attribute revocation which is cumbersome for CP-ABE schemes. In particular, it resolves this challenging issue by considering more practical scenarios in which semi-trustable on-line proxy servers are available. This solution enables the authority to revoke user attributes with minimal effort. This is achieved by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enable the power to delegate most of arduous tasks to proxy servers. Formal analysis shows that it is provably secure against chosen cipher-text attacks.

In [6] Allison Lewko et al. developed a new proof methods for attribute-based encryption for achieving a full security through selective techniques in which a new methodology for utilizing the prior techniques to prove selective security for functional encryption systems as a direct ingredient in devising proofs of full security is introduced. This deepens the relationship between the selective and full security models and provides a path for transferring the best qualities of selectively secure systems to fully secure systems. In particular, we present a Ciphertext-Policy Attribute-Based Encryption scheme that is proven fully secure while matching the efficiency of the state of the art selectively secure systems.

The main goal of this framework is to provide secure patient-centric PMR access even from different hospitals and efficient key management at the same time.

III. CRYPTOGRAPHIC CLOUD STORAGE

The data may get disclosed or modified by an unauthorized access. It is essential that special care must be taken to protect our sensitive data. A secure storage[7] must be achieved in cloud computing. So we adopt cryptographic techniques for the secure storage. The data is encrypted by the data owner before the data is uploaded to the cloud. the major feature of a cryptographic storage is that the security properties that are described below are accomplished.

Fig.1 represents cryptographic cloud storage. The owner of the data applies the cryptographic methods to the sensitive data to protect the information from unauthorized access. The owner uploads the encrypted data to the cloud environment. The authorized user can decrypt the data and download the required file.

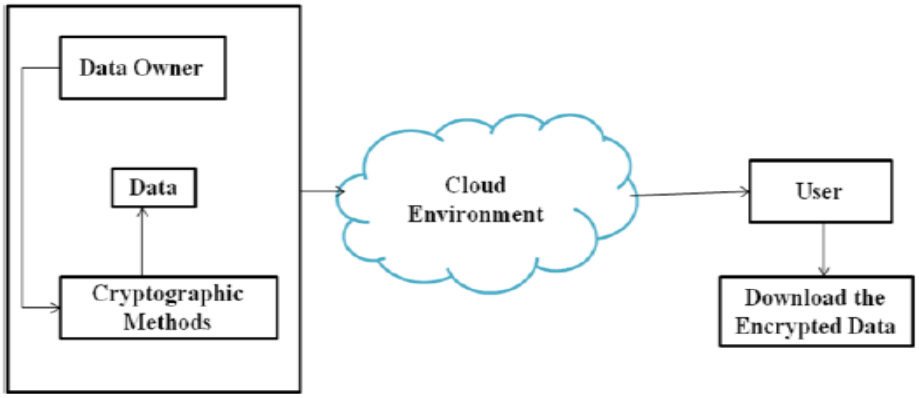


Fig.1

Strength of Cryptographic Cloud Storage

Confidentiality **:** Cryptographic Cloud Storage [8] provides Confidentiality as the main characteristics. The information were encrypted with the advanced cryptographic techniques and thus the secrecy is maintained.

Integrity: Cloud Storage provides Integrity to the data and thus it prevents any unauthorized people to modify the data.

TABLE I
Comparisons of various ABE techniques

TYPES OF ABE	ADVANTAGES	DISADVANTAGES
KP-ABE	In key policy ABE cipher texts are associated with sets of descriptive attributes and users key are associated with policies.	No full access control of the data, descriptive attributes are used to encrypt the data.
CP-ABE	Used for efficiently handling more expressive types of encrypted access control.	Cipher text length grows linearly with the number of unrevoked users.
MA-ABE	Arbitrary TA's, each governs a distinguished subset of the user's attributes and the secret key. User can get part of the key from each TA.	It is not clear how to realize efficient user revocation.

IV. SYSTEM MODEL AND DESIGN GOALS

For actual encryption/decryption of data we will be using Advance encryption Standard i.e. AES. Till date no known attacks are identified against AES. The various algorithms which belong to DES standard are prone to attacks and also require huge computation. This scheme uses the advanced encryption standard for encrypting the attributes of all the patient details. Attribute Based Encrytption is used to separate the patient records into each and every attribute and all this attributes are encrypted with the help of (AES) algorithm. The patient records are maintained without any leakage of data by combining using Distributed Attribute Based Encryption(DABE)technique and Advanced Encryption Standard(AES)algorithm together.

A. Admin Support System and Patient Care System

This module is used to control all the process. Administration is a dynamic work in every field. The initial meaning of administration is the running of a business or system. In every step of business or system, it needs administration. To run faster in the technological scenario a business need to be administered.

In our project administrative support services in various administrative levels rightly starts from:

- Admin management
- Hospital management
- Pharmacy management

Patient Care System is a computer-based "patient record system" which facilitates an electronic patient encounter, helping and automate the entire clinical workflow. This allows capture of medical data in a standard format, making its collection, comparison and use

across the health care spectrum quick and efficient. In our Healthcare organization it requires a comprehensive information management to ensure that vital patient information is always available to caregivers. A well-designed patient care system simplifies the workflow, reduces the risk of medical errors and improves the patient care experience for caregivers and patients alike.

Fig.2 represents the patient care framework establishes and generates the clinical tools needed to manage the delivery of patient care. Combined with hospital management solution, the patient care framework covers functional areas such as diagnosis, review details, inpatient & outpatient management, doctors appointments, prescriptions, operation theatre management. The system provides an extensive MIS reports and that data can be used for research and analysis.

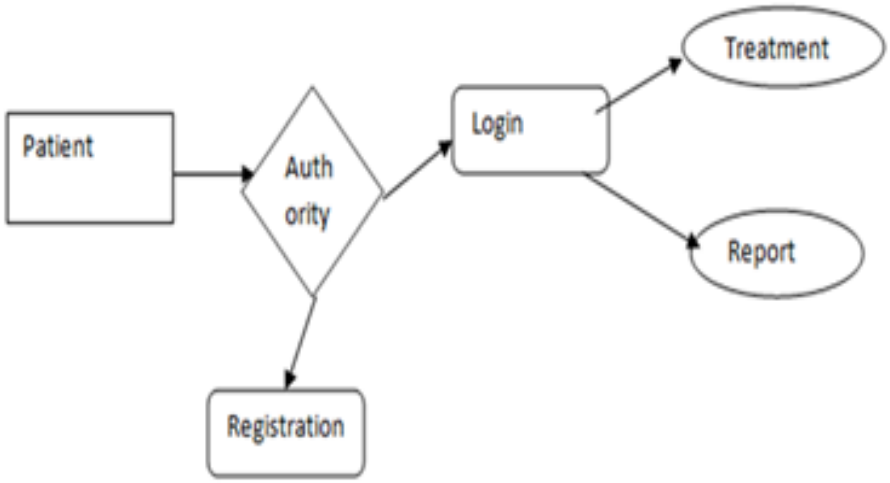


Fig.2

INPUT: Get patient personal data, patient required data.

OUTPUT: It will give the patient required page and data.

B. Data Privacy System

In this ABE module, distributed attribute-authorities monitor different sets of attributes and issues corresponding decryption keys to users and for encryptions it requires keys for appropriate attributes from each authority before decrypting a message.Fig.3 represents the Attribute-Based Encryption (ABE) scheme allows user's private key to be expressed in terms of any access formula over attributes. The existing ABE schemes were limited to expressing only monotonic access structures. It provides a proof of security for our scheme based on the data privacy system.

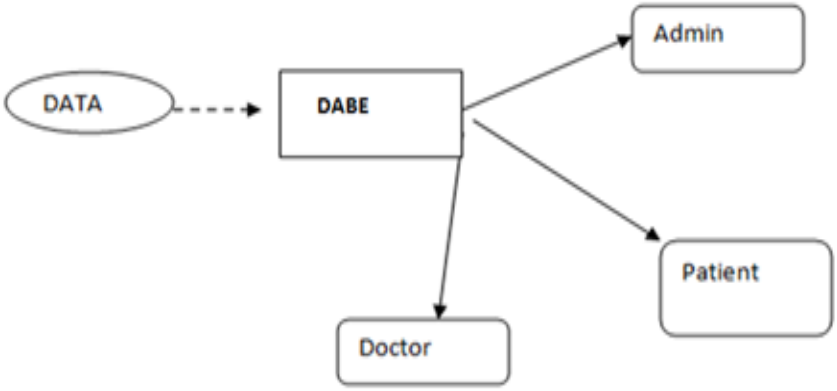


Fig.3

INPUT: Get all the admin and patient values.

OUTPUT: It will convert original data into chipper text using attribute based encryption.

C. Data Provider System

In this module providers may be an individual or an institution that provides preventive, curative, promotional or rehabilitative health care services in a systematic way to individuals, families or communities. This data service provider maintains large amount of patient database and maintains all record in order to transfer and deliver content to those paying the subscription fee. Fig.4 describes the data service provider, comprehensively handles the client needs from concept to installation through support. This process normally involves studying the client's current infrastructure, evaluating the client's needs, specifying the mix of manufacturers records and details required to meet client goals at the client's site.

Computer-based patient record (CPR) systems form the infrastructure for the timely and accurate collection of exchange of data, information, and knowledge in healthcare organizations, and thus a more efficient use of scarce resources.

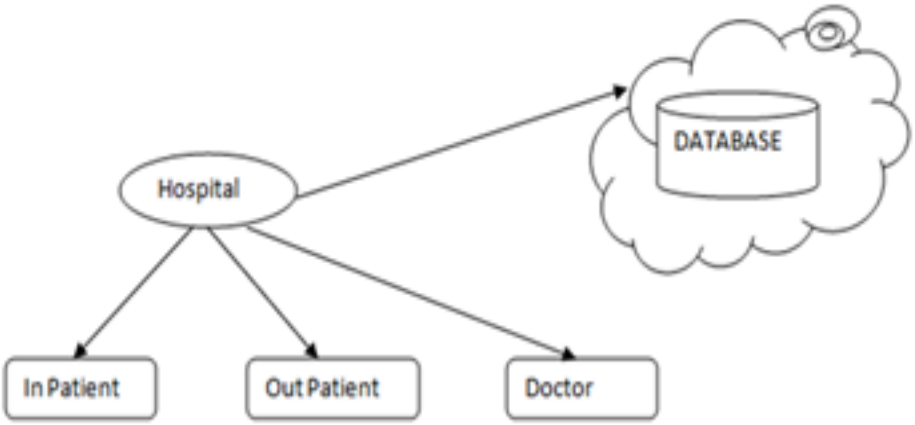


Fig.4

INPUT: Get the patient data, doctor data, and patient treatment.

OUTPUT: It will provide patient page, doctor page and research people page.

D. Health Information Exchange

In this Health Information Exchange (HIE) refers to the process of reliable and interoperable electronic health-related information sharing conducted in a manner that protects the confidentiality, privacy, and security of the information. The development of widespread HIEs is quickly becoming a reality.

1) Personal Report

Fig.5 represents the personal data that are retrieved from the database by the family members or friends. Personal data is information that relates to individuals. It does not include information relating to the deceased or to groups or communities of people information. Personal information is about the patient details. It includes names, addresses and dates of birth, as well as information relating to the services which individuals receive from the Council.

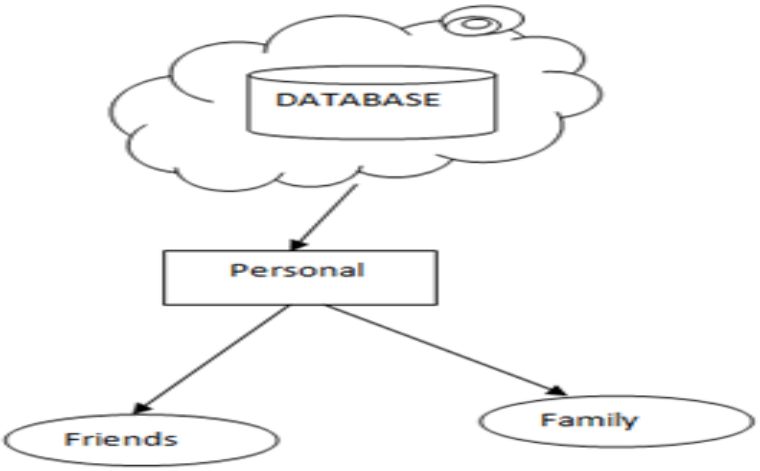


Fig. 5

INPUT: Get the data from patient's friends and family request.

OUTPUT: I will provide the user required data from cloud database.

2) Professional Report

Fig.6 represents the professional data that are retrieved from the database by the research members or the doctors. The professional report is a claim by the Department of Health that patient data shared with private firms for medical research would be anonymized has been challenged by privacy campaigners. It is used to further research and another treatment. All the research people access the patient professional reports. It is only for doctors and also research peoples.

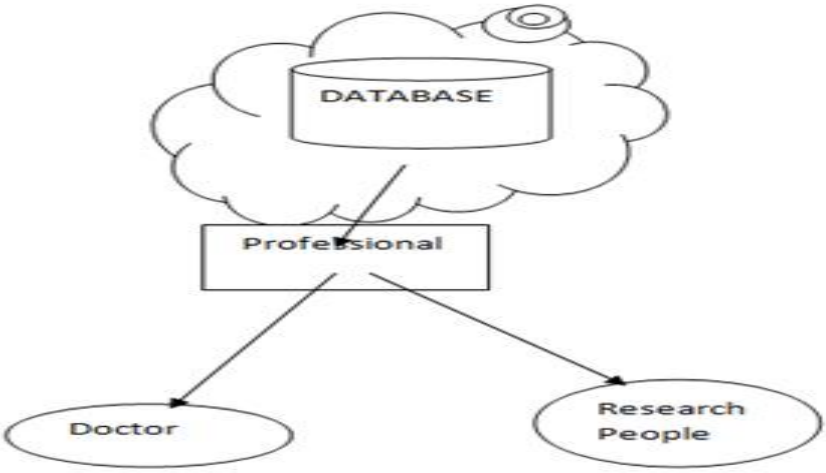


Fig.6

INPUT: Get the data from doctor and research people request.

OUTPUT: I will provide the user required data from cloud database.

Some benefits of storing Personal Medical Records in cloud is given below:

- Helps to keep track of our health concerns like sugar level, cholesterol level etc.
- Insurance company may need PHR as they make payment for the Hospitals.
- Helps to know the drug allergies in case of emergency
- Helpful in case of periodic checkups for the patient
- x-ray or some other laboratory tests can also viewed.
- Helps to share the health related information with our care providers.

C. DATA FLOW DIAGRAM

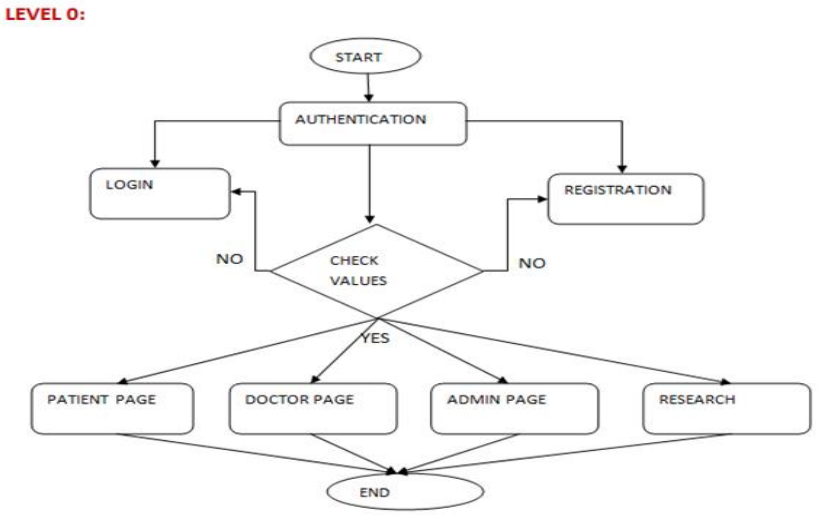


Fig.7

In our first level of DFD(Fig.7) is representing the connection establishment of system and monitoring. System will get the input, port and name from the user. Each node will connect to the cloud system. This node will collect all the patient details from system.

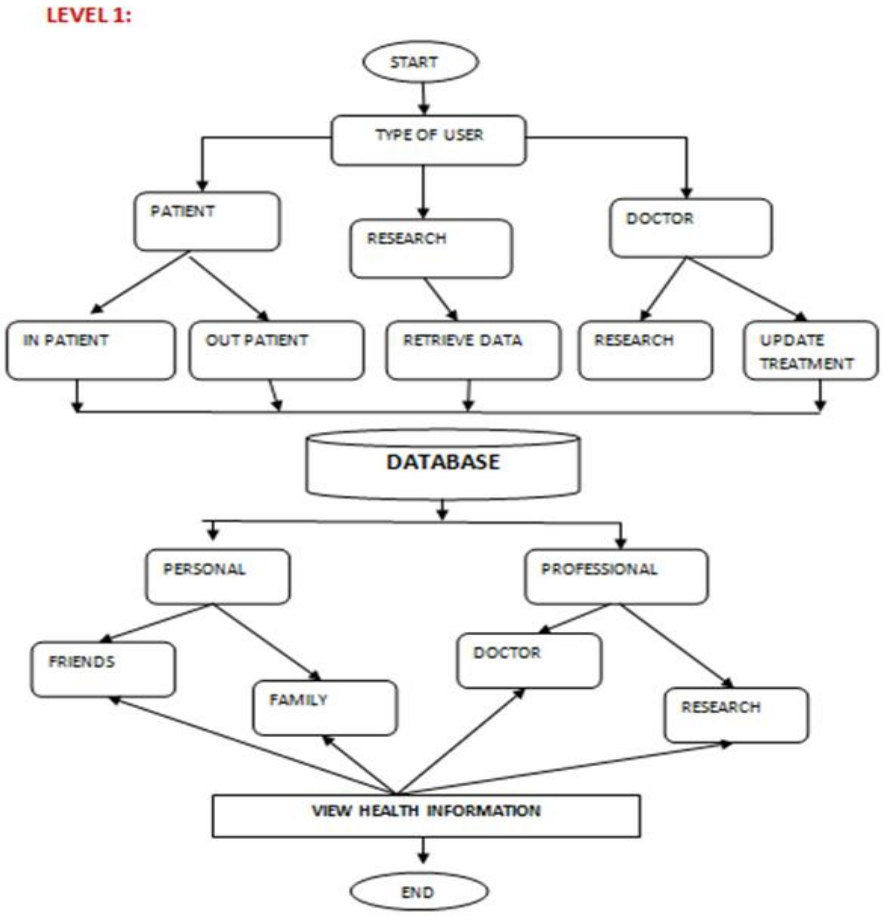
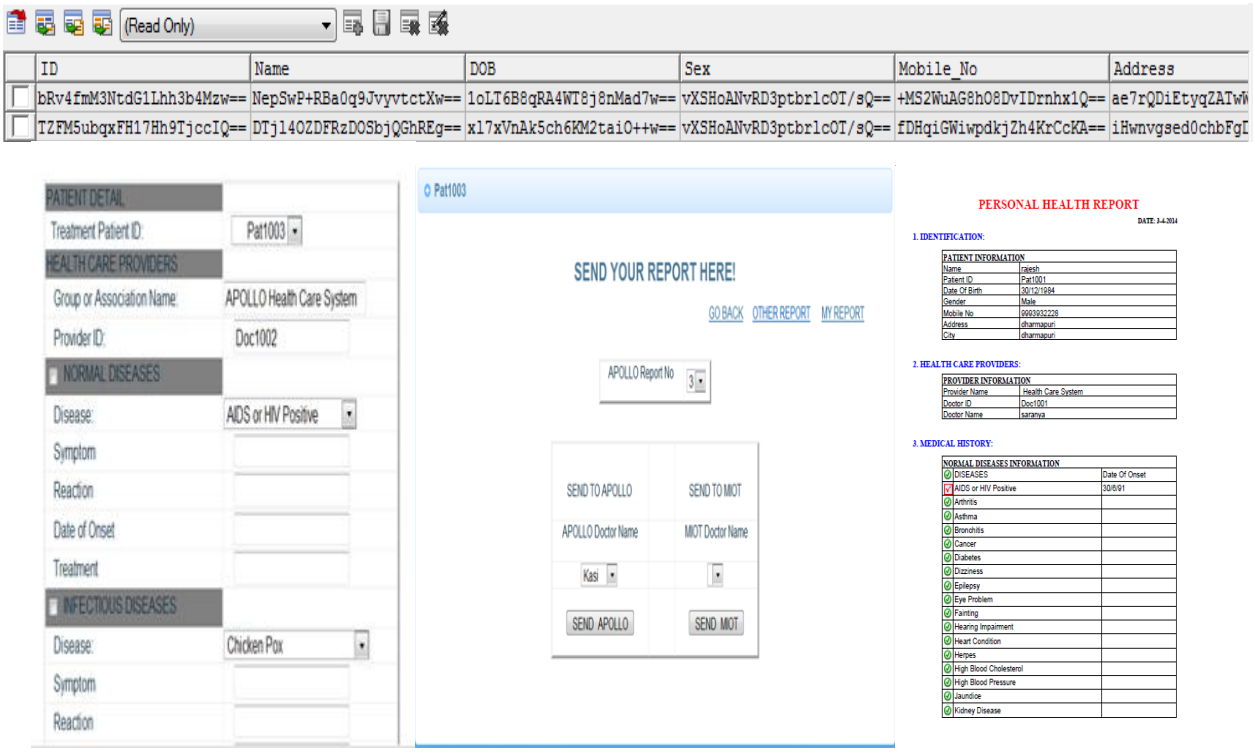


Fig.8

In our second level DFD diagram(Fig.8) is represent the flow of process. System will connect to cloud database. Then it will collect all the information from each patient system. After this Cloud give the two processes. It is professional and personal.

V. IMPLEMENTATION DETAILS

This scheme uses the advanced encryption standard for encrypting the attributes of all the patient details. Attribute Based Encryption is used to separate the patient records into each and every attribute and all this attributes are encrypted with the help of (AES) al gorithm. The patient records are maintained without any leakage of data by combining using Distributed Attribute Based Encryption(DABE)technique and Advanced Encryption Standard(AES)algorithm together. Distributed Attribute Based Encryption technique is used in the case of fast and secure sharing of patient's report between the hospitals mostly during the case of emergencies.



VI. CONCLUSION

The personal health records are now considered as the emerging trend in the personal health information exchange field. So cloud computing storage and sharing service is highly utilized by the users. We can provide good security to our data's using encryption technique in cloud the data security is the main privacy issue. Hence, the attribute based encryptions and its variations such as distributed attribute based encryptions are applied for key management and for maximizing the security purpose. The PHR will use more secure encryption primitives in the future for reducing the key management problems and complexity and for providing more secure storage and sharing features to the data stored in the clouds.

REFERENCES

[1] M. Li, S. Yu,Y. Zheng, ,K. Ren, &W. 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(1), pp. 131-143, 2013.

[2] S. Müller, S. Katzenbeisser, & C. Eckert, *On multi-authority ciphertext-policy attribute-based encryption* Bulletin of the Korean Mathematical Society,46(4),pp. 803-819,2009.

[3] M. Pirretti, P.Traynor, P. McDaniel, & B. Waters *Secure attribute-based systems*, Journal of Computer Security, 18(5), pp. 799-837, 2010.

[4] S. Yu, C. Wang, K. Ren, & W. Lou, *Attribute based data sharing with attribute revocation*, In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261-270, 2010.

[5] S. Ruj, A. Nayak, & I. Stojmenovic, *Dacc: Distributed access control in clouds*, In Trust, Security and Privacy in Computing and Communications (TrustCom),IEEE 10th International Conference on pp. 91-98, 2011.

[6] S. Kamara, &K. Lauter, *Cryptographic cloud storage*, In Financial Cryptography and Data Security, Springer Berlin Heidelberg ,pp. 136-149, 2010.

[7]] L. Ibraimi, M. Asim, & M. Petkovic, *Secure management of personal health records by applying attribute-based encryption*, In Wearable Micro and Nano Technologies for Personalized Health (pHealth), IEEE,pp. 71-74, 2009.

[8] A. Bessani,M. Correia,B. Quaresma, F. André, & P. Sousa, *DepSky: dependable and secure storage in a cloud-of-clouds*, ACM Transactions on Storage (TOS), vol.9(4), pp. 12, 2013.

[9] A. Lewko, & B. Waters, *New proof methods for attribute-based encryption: Achieving full security through selective techniques*, In Advances in Cryptology–CRYPTO ,Springer Berlin Heidelberg, pp. 180-198, 2012.

[10] J.Bethencourt, A. Sahai, and B. Waters, *Ciphertext-Policy Attribute-Based Encryption*, Proc. IEEE Symp. Security and Privacy

(SP '07), pp. 321-334, 2007.

[11] M.Chase and S. S. Chow, *Improving privacy and security in multi-authority attribute-based encryption*, in *CCS '09*, pp.121–130,2009.

