International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

PERSONAL HEALTH MANAGEMENT IN CLOUD USING BLOWFISH ALGORITHM

Ms.S.Dhivyabharathi[1], D. Prem kumar[2], R.Rakesh[3], S.Sahaya Salima[4]
[1,2,3,4]*Department of CSE, Kathir College of Engineering*

Abstract: Personal health management are a modern health technology with the ability to engage patients more fully in their healthcare. Personal health management including hospitals and ambulatory care settings, insurers and health plans.Each patient is promised the full control of her medical records and can hare her health data with an including healthcare providers, family members or friends. The main theme of the PHR is to empower patient to control to their own medical decisions. The PHR is a tool that you can use to collect, track and share past and current information about your health of someone in your care. A PHR is information about your health compiled and maintained by you. The difference is in how you use your PHR to prove the quality of your health care. Take an active role in monitoring your health and healthcare by creating your own PHR.
Keywords*:* Personal Health Record (PHR), Cloud based data management, Electronic Health Record (EHR), Provider.

I. INTRODUCTION

Many Personal Health Record services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing Personal Health Record in cloud computing have been proposed in. Building and maintaining specialized data centres for personal health record system require high cost. Important to know about a Personal Health Record is you should always have access to your complete health. Information in your PHR should be accurate, reliable and complete. You should have control over how your health information is accessed, used and disclosed. A PHR may be separate from and does not normally replace the legal medical record of any provider. The intention of a PHR is to provide a complete prescription.

II. LITERATURE SURVEY

Distributed m-healthcare systems support for efficient patient treatment of high quality. But it brings about series of challenges in personal health information confidentiality and patient's identity privacy **.**we have used AES algorithm to encrypt patient's health information. It makes many existing data access control and anonymous authentication schemes inefficient in distributed m-healthcare systems .To solve this problem, novel authorized accessible privacy model (AAPM) is established. The users health data are processed by the private cloud and stored in the public cloud thus guaranteeing efficient & timely retrieval of data .This system builds privacy into mobile healthcare system with the help of the private cloud. The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time .This make accesses to PHRs based on access rights assigned by the owner.it done by Attribute-Based Encryption .Advantage of ABE algorithm is Data confidentiality, Access Control .Main drawback of ABE is complexity in key management. Electronic Health Record (EHR) system is necessary for high-quality patient treatment .The proposed system enable secure sharing of sensitive patient data during cooperation and preserve patient data privacy. Realizes access control, if no entities other than the authorized entities can access the patient data.it is proceeded using **i**dentity Based Encryption(IBE).Advantages is Enables data sharing across healthcare providers.Disadvantages Decrypt any data without uthorization.Cloud computing is used broadly in several services that maintain Personal Health Record (PHR).It is a patient health-centric model for data exchange in cloud**.** Considers the multi owner scenario and divides the user in PHR

system into multiple security domains that greatly reduces the key management issues**.** Algorithm used Multi-Authority Attribute Based Encryption Advantages Quickly find out the information about the patient heath record.Disadvantages No trusted central authority.

III. PROPOSED SYSTEM

The proposed system aims at maintain a patient record and report to access this in world wide. Also we maintain hostel details i.e. License verification, insurance claim process etc. It is a promising method to encrypt the personal health record before outsourcing. The main advantage of personal health system is to use collect entire data it is centralized and it is maintained by cloud provider. 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. Issues 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- rained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to Personal Health Record stored in semi-trusted servers. Extensive analytical and experimental results are presented which shows scalability, security, Efficiency**.**

IV. ARCHITECTURAL DESIGN

4.1Admin Process

The admin process of our project includes Patient details registration, Hospital details registration. Other registrations are Insurance company registration and emergency hospital registration. These details are then stored into the cloud database

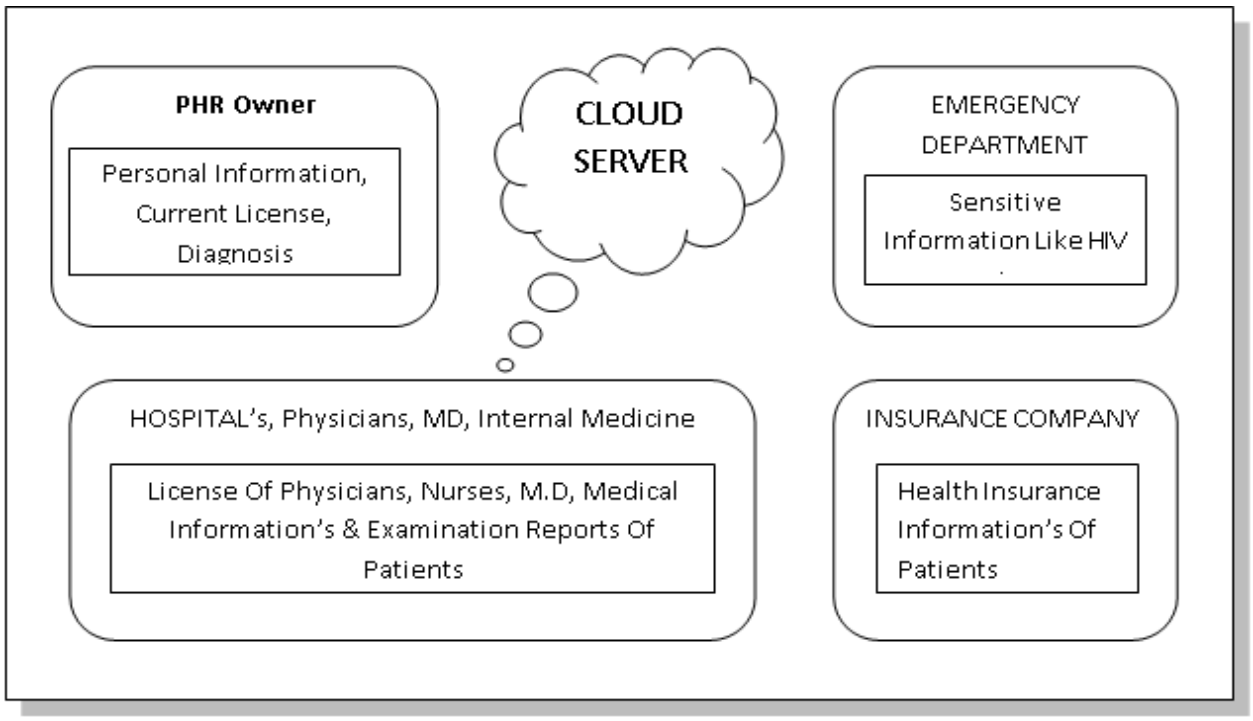


Fig 1: Architecture Diagram

4.2 Hospital Maintenance

In this module each and every hospital details, license Information's are maintained by Personal health record owner. These details are maintained and stored to cloud database in encrypted format.

4.3 License & Passport Verification

Every hospital and doctors having their own license. Our PHR owner verify the license details and passport verification for identifying an authorized doctor. If the license will be in expired, the PHR owner notifies that particular hospital or doctor for license renewal

4.4 Insurance Process

This module provides the insurance to patients. First it checks whether the patient got treatment or not by verifying the patient id. After verification, the insurance will be provided to the patients. Also the patient can apply the insurance by themselves.

4.5 Emergency Process

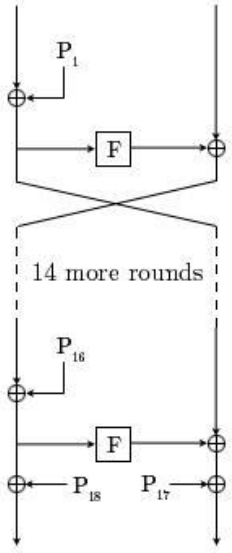
Due to any emergency process, it contains some emergency hospital details. So any one emergency mean, it's directly communicated to emergency hospital for their treatments.

V. UML DIAGRAM FOR PERSONAL HEALTH RECORD

Fig 2:Uml Diagram

VI. ALGORITHM

Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms such AES, DES and 3 DES etc. Blowfish is a symmetric block encryption algorithm designed in consideration with it encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte. It can run in less than 5K of memory. It uses addition, XOR, lookup table with 32-bit operands .The key length is variable ,it can be in the range of 32~448 bits: default 128 bits key length .It is suitable for applications where the key does not change often, like communication link or an automatic file encryption.



6.1 Description of Algorithm

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time.it will follows the feistel network and this algorithm is divided into two parts.

A. Key-Expansion

It will converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Blowfish uses large number of sub keys. These keys are generate earlier to any data encryption or decryption.

The p-array consists of 18, 32-bit sub keys:

P1,P2,……,P18

Four 32-bit S-Boxes consists of 256 entries each:

S1,0, S1,1,…….S1,255

S2, 0, S2, 1. S2,255

S3, 0, S3, 1, S3, 255

S4, 0, S4, ……..1,S4,255

B. Data Encryption

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

C. Blowfish Encryption

Divide x into two 32-bit halves: xL, xR

For i = 1to 16:

xL = XL XOR Pi

xR = F(XL) XOR xR

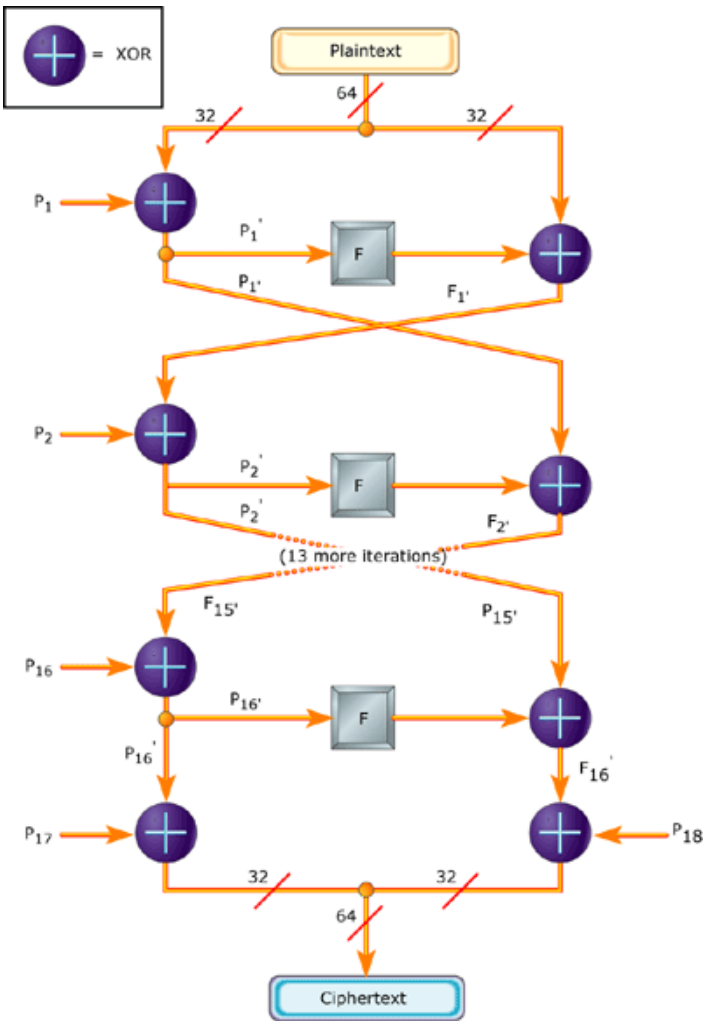
Swap XL and xR

Swap XL and xR (Undo the last swap.)

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR



VII. ADVANTAGE OF PHR

- Scalability
- Security
- Efficiency.

VIII. FUTURE WORK

In our personal health management system that is to self-monitoring and it followed by the normal level of security. In Future ESnhancement it will have high level Privacy Requirement in the Distributed Health Care Cloud Computing System.

IX. CONCLUSION

The main goals of the Personal Health Record (PHR)system is to empower patients to access to their own medical decisions.in our framework is to self-monitor and control personal health. Also the PHRs are useful at home care, or private care facility where Patient constant monitoring and control are needed.

REFERENCE

1. J. Zhou, Z. Cao, X. Dong, X. Lin, "TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems," *IEEE INFOCOM*, 2015.

2. J. Hur, D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
3. M. Chase, S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," 16th ACM Conf. Compute. Common. Security, 2009, pp. 121–130.
4. J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute- based encryption," IEEE Symp. Security Privacy, 2007, pp. 321–334.
5. N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," 31st Int. Conf. Distribute. Compute. Syst., 2011, pp. 393–402.
6. F. Cao and Z. Cao, "A secure identity-based multi-proxy signature scheme," Compute. Electr. Eng., vol. 35, pp. 86–95, 2009.
7. R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel distribute. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

