Secure Mechanism for Sharing Patients Medical Information using Cloud

Ms. Snehal Salunke
Department of Computer,Engineering
Amrutvahini College of Engineering
Sangamner, India

Dr. B. L. Gunjal
HOD, Information technology
Amrutvahini College of Engineering
Sangamner, India

Abstract: *The broad acknowledgment of cloud based services in the healthcare sector has brought about practical and helpful trade of Personal Health Records (PHRs) among a few taking part elements of the e-Health systems. Nevertheless, putting away the secret health data to cloud servers is susceptible to revelation or theft and requires the improvement of approaches that guarantee the protection of the PHRs. There may be privacy problems if disclosed to 3rd party servers and uncertified users. The protection mechanism is to safeguard the private info from property right access. Users within the planned system square measure outlined in Access management List Module wherever, differing types of access granted to numerous users. The forward and backward access management is additionally enforced within the planned theme. The methodology use El-Gamal coding and proxy re-encryption to make sure the PHR confidentiality. Experimental results and performance ends up in the planned system establish that the planned theme is economical in terms of security and privacy. Setup and re-Encryption Server (SRS) semi- trustworthy server is employed for putting in user's public and personal key pairs.*

Keywords*—Personal Health Records, Setup and re-encryption Server, Access management List, re-encryption*

I. INTRODUCTION

Nowadays, in Medical system lack of access to their complete health info. So a private Health Record or PHR may be a health record system wherever health info info associated with the patient is maintained by the patient or somebody on behalf of patients. A PHR service permits a patient to form, manage, modify and management their personal health knowledge in one place through the net. The aim of PHR is to produce absolute and correct outline of patient's medical record that is accessible on-line from anyplace. The private Health Record (PHR) are often used to access, manage and coordinate patient's womb-to-tomb health. Information makes acceptable components of it on the market to those that can like knowledge at any time just in case of emergency. PHR is Associate in Nursing integrated, inclusive read together with info folks generates themselves like, info from doctors like treatments and take a look at results, and data from their pharmacies and insurance agents. PHRs will contain separate vary of knowledge together with however not restricted to allergies, diseases, Family medical record, ill health and hospitalization reports, imaging reports, laboratory take a look at results, medications and dosing, prescription records, surgeries, vaccinations, observations of daily living. As a results of high price of framing and providing trained knowledge centers, several PHR services square measure used to or provided by third-party service suppliers. One in every of the foremost important problems for PHRs is however the technology may disclose the privacy of patient's protected health info(PHI). Network interruptions have become additional common, therefore assortment of medical info on-line will cause concern of the revelation of health info to amerciable people. To create certain patient basic privacy management over their own PHRs, it's necessary to own compressed knowledge access management mechanisms that job with semi-established servers. To run-over the challenges we've developed a web-based personal health record system (PHR) that may be utilized by patients to accumulate and administer their health info to produce the guarantee to our health info, we have a tendency to used the El-Gamal coding algorithmic program. By victimization this algorithmic program we will encode the patient health info before storing into third party server. Cloud supplier or third party persons cannot access the info, though they need provision to look at the PHR knowledge, it solely seems within the type of encoded knowledge, Whereas decrypting the knowledge we want decrypt key, solely certified persons having the decrypt key will simply access PHR knowledge. Personal health records primarily, the PHR owner ought to decide a way to cipher PHR files and to permit that set of users to get access to every file. A PHR file ought to solely be on the market to the users World Health Organization have the corresponding secret writing key, whereas it'll stay confidential to the remainder of users. What is more, the patient shall continually absorb the proper to not solely grant, however conjointly revoke access privileges after they feel it's necessary. However, the ambition of patient-basic privacy is commonly in battle with ability in an exceedingly PHR system. The certified users might either got to access the PHR for private handling or skilled functions. Cloud computing plays Associate in Nursing crucial role here. Cloud ADP system provides the service for the user and has the character of high security, quantifiability and reliable ness. However, Sharing of non-public Health records have expose a good threat to user's privacy and security. The isolation of PHRs are often at hazard in many ways that, as an example break-ins, accident, leakage. Furthermore there also are threats by valid insiders to the info. as an example, the PHRs either in cloud storage or in transit from the patient to the cloud or from cloud to the other user could also be prone to uncertified access owing to the malicious behavior of external entities. But

they'll be coding from in such how that neither the cloud server suppliers nor the uncertified users ought to be able to access the PHRs once the PHRs square measure hold on on the third-party cloud storage. With the 'right-to-know' access, solely the organizations or people ought to be able to connect with the PHRs. The mechanism for granting the access to PHRs ought to be monitored by the patients itself. Thus the motivation behind this work is to assure the confidentiality of the PHRs hold on on the cloud servers. Our major contributions are summarized below:

- To propose a system that share patient's Health Records over the cloud confidentially and firmly.
- To overcome the dynamic access management issues.
- To resist internal and external attacks.
- To improve patient safety and quality care, however conjointly scale back time and resources.

II. PROBLEM DEFINATION

To solve the problem of data exchange between medical units, We propose system which helps to improve patient safety and quality care, but also reduce time and resources.

III. LITERATURE SURVEY

[1] Assad Abbas, Samee U. Khan, Senior Member, has come up with "A Review on the State of- the-Art Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014. This paper aimed to encompass the state-of-the-art privacy preserving approaches employed in the e-Health clouds. Also, the privacy preserving approaches are categorized into cryptographic and non-cryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted.

[2] M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, has come across "A general framework for secure sharing of personal health records in cloud system", Journal of Computer and System Sciences, 2017. In this paper, Author provided an affirmative answer to this problem by presenting a general framework for secure sharing of PHRs. This system enables patients to securely store and share their PHR in the cloud server (for example, to their carers), and furthermore the treating doctors can refer the patients' medical information to specialists for research analysis, whenever they are required, while ensuring that the patients' information remain private. This system also supports cross domain operations (e.g., with different countries
regulations).

[3] David Daglish and Norm Archer, "Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues", IEEE 2009. This paper gives design and architectural problems of PHR systems, and focused on privacy and security issues which must be addressed carefully if PHRs are to become generally acceptable to consumers.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing", in Proceedings of the IEEE INFOCOM, March 2010. This paper addressed important open problems, permitting the data owner to delegate many of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents. It achieved this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. This scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that this scheme is highly efficient and provably secure under existing security models.

IV. SYSTEM ARCHITECTURE AND OVERVIEW

Proposed System presents a methodology that permits patients to administer the sharing of their own PHRs in the cloud. The proposed methodology employs the encryption and decryption to ensure the PHR confidentiality. The methodology allows the PHR owners to selectively grant access to users over the portions of PHRs based on the access level specified in the ACL for different groups of users. To generate the re-encryption keys for different groups of users thereby eliminating the key management overhead at the PHR owners end. Formal analysis and verification of the proposed methodology is performed to validate its working according to the specifications. To solve the problem of data exchange between medical units, We propose system which helps to improve patient safety and quality care, but also reduce time and resources.

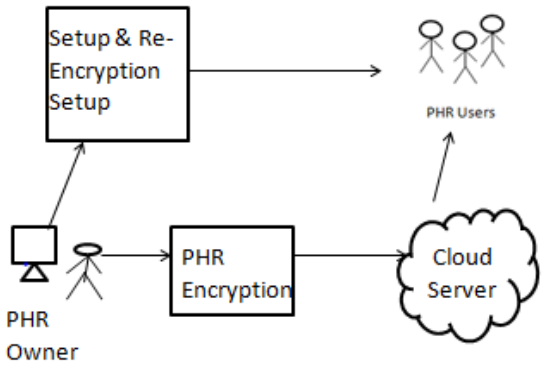

Fig. 1. Proposed System

A. Architecture

The patients transfer the encrypted PHRs by on an individual basis encrypting the partitions of PHRs, for example: (i) personal data, (ii) Medical data, (iii) insurance connected data, and (iv) prescription data. Moreover, the consumer application for the PHR additionally generates the re-encryption parameters that area unit afterwards transmitted to the SRS. If a user desires to access any portion of the PHR, the user downloads the PHR from the cloud when authentication. it's necessary to state that also at now, the user cannot decipher the PHRs, as a result of the user must get the corresponding secret writing parameters from the SRS.

B. Algorithms

El-Gamal encoding system is associate public-key cryptosystem that relies on the Diffie–Hellman key exchange. It uses uneven key encoding for human action between the 2 parties and encrypting the message. The system provides a further layer of security by unsymmetrically encrypting the keys antecedently used for radial message encoding. El-Gamal encoding consists of 3 components: the key generator, the encoding formula, and also the secret writing formula. it's most fitted for economical user revocation. thus its a public-key cryptanalytic system with associate formula that's each straightforward and economical and may give straightforward shopper revocation with an occasional price and overhead.

There are three main steps of the El-Gamal encryption algorithm as follows:

Initialization: Given a large prime p and generator g of the multiplicative group $Zp*$. Select a random secret key a and compute $b = g\text{^a } mod\ p$. Moreover, (p, b, g) represents the generated public key.

Encryption: The message m is encrypted by the sender by obtaining the receiver's public key (p, b, g) as follows:

$$\gamma = g\text{^a } mod\ p \qquad (1)$$

and,

$$\delta = m * (g\ \text{^a})\text{^}\ k \qquad (2)$$

The encrypted message $(m) = (\gamma, \delta)$ is sent to the receiver.

Decryption: The encrypted message (m) after it is received by the receiver is decrypted by means of the private key x and the decryption factor as follows:

$$d = (\gamma\ \text{^}(p-1-\text{a})\ )\ mod\ p \qquad (3)$$

The encrypted message m is recovered as:

$$((m)) = (d) * \delta\ mod\ p \qquad (4)$$

C. Working of Proposed Methodology

The proposed methodology consists of the 4 steps as follows:

(a) setup,
(b) key generation,

(c) encryption, and
(d) decryption.

(a) setup:

Two groups A1 and A2 with the prime order q this methodology works. The bilinear mapping of A1 and A2 is A1 × A1 → A2 . A parameter g is a random generator such that $g \in$ A1 . The variable Z is another random generator such that $Z = (g, g) \in$ A2 .

(b) key generation:

The public/private key pairs are generated by the Setup re-encryption system as follows for the set of authorized users.

The Private key: $SKi =$,

The Public key: $PKi = g\text{^} xi$ (5)

where x$i \in Z*$q .

(c) encryption:

In the case patient is going to upload his personal health records on the cloud. The application generates random numbers equal to PHR partitions placed in the different access level groups by the users of the system. Therefore, in our case $r1$, $r2$, $r3$, $r4$ four random variables r1, r2, r3, r4 $\in Zq *$ are generated. The i-th partition of the PHR used to encrypt variable ri. Each partition is encrypted separately by the application. The XML format allows the application to perform encryption/decryption on logical portions of the PHR. The encryption of the aforesaid partitions of the PHR is performed as follows

$Cper = Z\text{^}r1.\ PHRper$ (6)

$Cins = Z\text{^}r2.\ PHRins$ (7)

Cmed$= Z\text{^}r3.\ PHR$med (8)

$C = Z\text{^}r4.\ PHR$pres (9)

where $PHRpres$ refers only to the prescription information partition of the PHR. Here, C represents the complete encrypted file that contains all the partitions in the encrypted form.

In addition to the above stated encryptions, the client also calculates the following parameters.

$Rper\_P = g\text{^}r1xp$ (10)

$Rins\_P = g\text{^}r2xp$ (11)

$Rmed\_P = g\text{^}r3xp$ (12)

$Rpres\_P = g\text{^}r4xp$ (13)

where xp is the private key of the patient that is uploading the PHR. The parameter R is used to produce the re-encryption key for the partition indicated in the subscript of each R. The completion of the encryption phase is followed by the upload of complete encrypted file C to the public cloud. The parameters $Rper\_P$, $Rins\_P$, $Rmed\_P$, and $Rpres\_P$ are transmitted to the SRS along with the file identification for which these parameters are generated.

(d) decryption:

Suppose a user U desires to access the encrypted PHR (C) uploaded by the patient P. The user U downloads the C directly from the cloud. Afterwards the user U requests the SRS to compute and send the corresponding R parameters that are used for decryption. The SRS checks the ACL for the requesting user and determines whether the access to the partition for which the user has requested R, is granted by the PHR owner or not. According to the access permissions specified in the ACL, the SRS will generate the corresponding parameters and will send those to the requesting user.

Therefore, we assume that user U has access to all of the partitions. The SRS calculates the re-encryption key and R and transmits it to the user U. The re-encryption keys and R are calculated below:

$RKP \rightarrow U = g\text{^}xU/xP$ (14)

where $RKP \rightarrow U$ is the re-encryption key from patient P to user U, xU and xP are the private keys of U and P, respectively.

V. EXPERIMENTAL DETAILS

RESULTS:

Data User: Doctors, nursing staff, pharmacies, clinical laboratory personnel, insurance providers, and the service providers is the data users in Health network. Each data user has a set of attributes, such as affiliation, department and type of health care staff, and is authorized to search on encrypted EHRs based on his set of attributes.

Data Owner: Data Owner Module contains patients health information, which is controlled by the patients themselves. The PHRs permit patients to manage the information, such as demographics, diagnosis, treatments, monitoring, and self-care.

Public Cloud: The public cloud has almost unlimited storage and computing power to undertake the PHR remote storage task and respond on data retrieval requests. Lightweight test algorithm is designed in our proposed system to improve performance.

Key Generation Center(KGC): KGC generates public parameters for the entire system and distributes secret keys to data users. A data users set of attributes is embedded in his secret key to realize access control.

Fig.2. PHR Owner Login

Fig.3. PHR Owner Registration

The performance of the proposed methodology was evaluated regarding generation, encryption, decryption, and turnaround time.

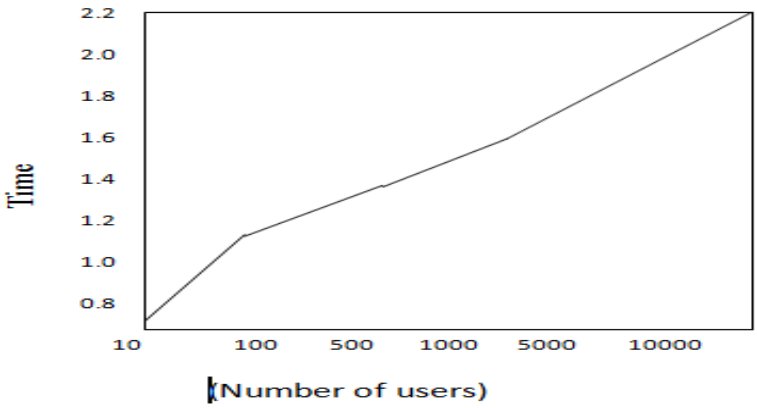

Fig. 4. Time consumption for Key generation

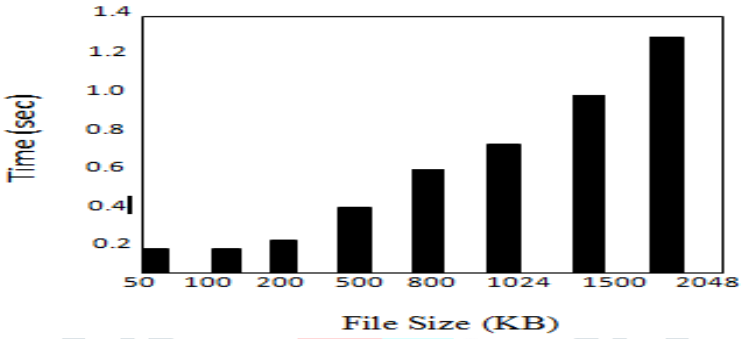

Fig .5. Time Consumption for Encryption

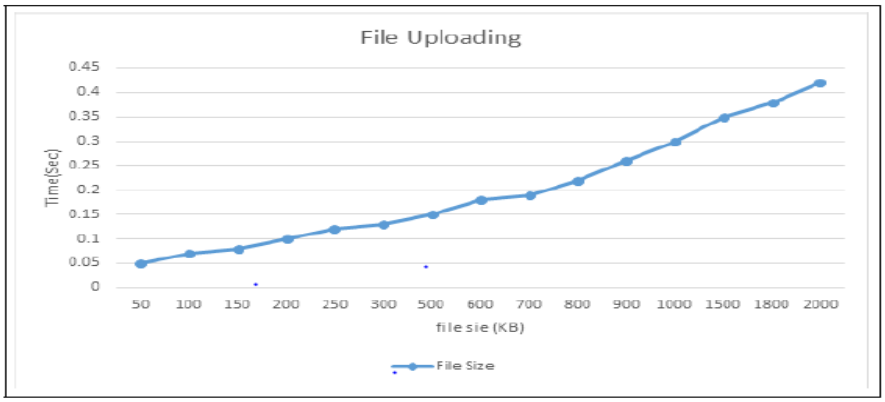

Fig. 6. Time consumption for file uploading

In proposed system, data is stored on cloud. Before uploading files on cloud, files encrypted and then stores on cloud. While storing files on cloud, it will take some time to write files on cloud. In experiment, file size considered in kb, as file size increase required time to uploading increases exponentially. The time consumption of the methodology to encrypt and decrypt the data files of varying sizes is also evaluated. The file sizes used for the experimentation are 50 KB, 100 KB, 200 KB, 500 KB, 800 KB, 1024 KB, 1500 KB, and 2048 KB. We analyze that with the increase in size of PHR file, encryption time also increases. On the other hand time required for decryption of PHR files is considerably less than the encryption time. The existing scheme differs from the proposed as the scheme uses proxy re-encryption technique to re-encrypt the PHRs after the revocation of the users. Therefore, the proposed scheme provide the turnaround time slightly smaller than the existing scheme.

B. System Requirements:

1) Software Requirement:

• Operating System: Windows 7 and above.

• IDE: Netbeans

• Programming Language : Java

• Database: MySQL 5.5

• Toolkit: JDK 1.8

2) Hardware Requirement:

• Processor : Intel

• CPU Speed : 1.1 GHz or Higher

• RAM : 2 GB or Higher

• Hard Disk : 256 GB or Higher

VI. CONCLUSIONS

We planned a procedure to soundly store and transmission of the PHRs to the authorized components within the cloud. The strategy preserves the protection of the PHRs and authorizes a patient-driven access management to varied segments of the PHRs on the access provided by the patients. We tend to dead a fine-grained access management technique so that even the valid system shoppers can't get to those segments of the PHR for which they're not approved. The PHR homeowners store the encrypted info on the cloud and simply the approved users having valid re-encryption keys issued by a semi-trusted authority will decode the PHRs. the duty of the semi-trusted authority is to provide and store the public/private key sets for the shoppers within the system. The performance analysis was done on the supported time needed to come up with keys, encryption and secret writing tasks, and work time. The trial results show the reasonability of the proposed system to secure share the PHRs within the cloud setting.

ACKNOWLEDGEMENT

I would like to thank my project guide Dr. B. L. Gunjal and project coordinatior prof. S. K. Sonkar, Department of Computer Engineering,AVCOE, Sangamner for the valuable advice, support and the interest shown in this project by timely suggestions in this work.

REFERENCES

[1] Mazhar Ali, Assad Abbas, Muhammad Usman Shahid Khan and Samee U. Khan "SeSPHR: A methodology for secure sharing of personal health records in the cloud",IEEE Transactions on Cloud Computing, 2018, 2854790.

[2] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in Edge-of-Things", Future Generation Computer Systems, 2018.

[3] M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system", Journal of Computer and System Sciences, 2017.

[4] K. Gai, M. Qiu, and X. Sun, "A survey on FinTech", Journal of Network and Computer Applications, 2017.

[5] A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach, Future Generation Computer Systems, 2015.

[6] Kabilan N, "Scalable and secure sharing of Health record maintenance using advanced encryption standard", SR Research paper 2014, vol. 1, no. 4 may.

[7] Assad Abbas, Samee U. Khan, Senior Member, "A Review on the State-of-the-art Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014.

[8] Leng, C., Yu, H., Wang, J., & Huang, J. "Securing Personal Health Records in the Cloud by Enforcing Sticky Policies," TELKOMNIKA Indonesian Journal of Electrical Engineering, 11 (4), 2200-2208, 2013.

[9] J. Li, "Electronic personal health records and the question of privacy", Computers, 2013.

[10] Ming Li Member, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. "Scalable and secure sharing of Personal Health records in cloud computing using Attribute Based Encryption" IEEE transaction on parallel and distributed systems 2012 Vol 3.

[11] Chen, Y. Y., Lu, J. C., & Jan, J. K. "A secure EHR system based on hybrid clouds," Journal of medical systems, 36 (5), 3375-3384, 2012

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine grained data access control in cloud computing", in Proceedings of the IEEE
INFOCOM, March 2010.

[13] David Daglish and Norm Archer, "Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues", IEEE 2009.