A REVIEW REPORT ON PERSONAL HEALTH RECORDS IN CLOUD USING ATTRIBUTE BASED ENCRYPTION

[1]Pokharkar Satish Tukaram, [2] Dr.Hare Ram shah.

[1]Phd Student, 2Assistant professor oriental University Indore
[1]Department of Computer science and Engineering,
[1]Oriental University, Indore, India.

Abstract : The across the board acknowledgment of cloud based administrations in the social insurance division has brought about financially savvy and helpful trade of Personal Health Records (PHRs) among a few taking an interest elements of the e-Health frameworks. In any case, putting away the secret wellbeing data to cloud servers is defenseless to disclosure or burglary and requires the advancement of procedures that guarantee the protection of the PHRs. Hence, we propose an approach called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR plan guarantees patient centric control on the PHRs and jelly the classification of the PHRs. The patients store the scrambled PHRs on the entrusted cloud servers and specifically award access to various kinds of clients on various bits of the PHRs. A semi-believed intermediary called Setup and Re-encryption Server (SRS) is acquainted with set up the general population/private key sets and to deliver the re-encryption keys. In addition, the philosophy is secure against insider dangers and furthermore upholds a forward and in reverse access control. Moreover, we officially dissect and confirm the working of SeSPHR philosophy through the High Level Petri Nets (HLPN). Execution assessment with respect to time utilization shows that the SeSPHR system can possibly be utilized for safely sharing the PHRs in the cloud**.**

***IndexTerms* - Access control, cloud computing, Personal Health Records, privacy.**

I. INTRODUCTION

Today, personal health record (PHR) has raised as a standard of heath report trade. A PHR model permits a client (tolerant) to make, oversee, and control health information at one focal spot through the innovation of web, which has in this way made putting away, recovery, and sharing of the data progressively productive. Here every patient is permitted to take the full control of medicinal records and can impart health data to an assortment of user, including medical report provider, relatives and friends .But while it is easier to have PHR services for everyone, but there can be many security and privacy risks which could slow down its acceptance. The main reason to worry about is whether the patients could control the sharing of their health information (PHI), specifically when they are stored on external servers where users may not fully assurance. On the other side, due to the susceptible health information (PHI), the external cloud storage servers are often at risk of various attacks which may lead to vulnerability of the PHI. To ensure users (patient) confidential control on their own PHRs, it is fundamental to have fine data access control model that works with non-trusted servers. A basic idea would be to encrypt the data before storing on cloud. Here basically, the PHR owner should be able to decide how to encrypt files and to allow or not which users to retrieve access to each file. A PHR record file must only be accessible to the users who are given the decryption key, while it remains confidential to the other users. Next would be that the patient shall always have the right to not only allow, but also be able to access authorization when they feel it is necessary. However, the patient-centric privacy is often in danger with amount of scalability in a PHR system. The certified users may either need to retrieve the PHR for own use or authoritative use. On the other side, different from the single data owner type which is often considered in most of the previous works, in a PHR system, there are numerous users who may encrypt according to their own possible ways, by using different sets of cryptographic keys. Here a concern would be, allowing each user acquire keys from every owner whose PHR wants to be read would limit the access since patients are not always online. So an alternative way would be to employ a central authority to do all the key management for all PHR owners, but this again requires too much trust on an authority

-

II. PRELIMINARIES

Au, Yuen, Liu, Susilo, Huang, Xiang, and Jiang, "A general framework for secure sharing of personal health records in cloud system," [1] Personal Health Record (PHR) has been developed as a promising solution that allows patient-doctors interactions in a very effective way. Cloud technology has been seen as the prominent candidate to store the sensitive medical record in PHR, but to date, the security protection provided is yet inadequate without impacting the practicality of the system. In this paper, provide an affirmative answer to this problem by proposing 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 record to specialists for research purposes, whenever they are required, while ensuring that the patients' information remain private. Our system also supports cross domain operations (e.g., with different countries regulations).

Hossain, Muhammad. "Cloud-assisted Industrial Internet of Things (IIoT) –Enabled framework for health monitoring" [12] The promising potential of the emerging Internet of Things (IoT) technologies for interconnected medical devices and sensors has played an important role in the next-generation healthcare industry for quality patient care. Because of the increasing number of elderly and disabled people, there is an urgent need for a real-time health monitoring infrastructure for analyzing patients' healthcare data to avoid preventable deaths. Healthcare Industrial IoT (Health IIoT) has significant potential for the realization of such monitoring. Health IIoT is a combination of communication technologies, interconnected apps, Things (devices and sensors), and people that would function together as one smart system to monitor, track, and store patients' healthcare information for ongoing care. This paper presents a Health IIoT-enabled monitoring framework, where ECG and other healthcare data are collected by mobile devices and sensors and securely sent to the cloud for seamless access by healthcare professionals. Signal enhancement, watermarking, and other related analytics will be used to avoid identity theft or clinical error by healthcare professionals. The suitability of this approach has been validated through both experimental evaluation, and simulation by deploying an IoT-driven ECG-based health monitoring service in the cloud.

Li, Yu ,Zheng, Ren, and Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," [3] Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often 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. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, 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-grained, cryptographically enforced data access control. In this paper, propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, use attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. This scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of proposed scheme.

Li "Electronic personal health records and the question of privacy" [4] Personal health records (PHRs), centralized places for consumers to electronically store, manage, and share their personal health information, offer new opportunities to help consumers manage their own health and health care. However, ensuring the privacy and confidentiality of health information contained within PHRs is challenging. This paper analyzes the major properties of existing PHR systems and identifies specific privacy and security issues with each type of PHR. It proposes a consumer-controlled privacy protection approach that includes high-minded privacy principles such as independent consent management, independent privacy and security audits, and regulatory compliance requirements. It further presents a consumer-controlled system architecture that embodies these principles in the web-based PHR system.

Chen, Liu, Chen, Chen, Bau, and Lin, “Secure Dynamic access control scheme of PHR in cloud computing.” [5] With the development of information technology and medical technology, medical information has been developed from traditional paper records into electronic medical records, which have now been widely applied. The new-style medical information exchange system “personal health records (PHR)” is gradually developed. PHR is a kind of health records maintained and recorded by individuals. An ideal personal health record could integrate personal medical information from different sources and provide complete and correct personal health and medical summary through the Internet or portable media under the requirements of security and privacy. A lot of personal health records are being utilized. The patient-centered PHR information exchange system allows the public autonomously maintain and manage personal health records. Such management is convenient for storing, accessing, and sharing personal medical records. With the emergence of Cloud computing, PHR service has been transferred to storing data into Cloud servers that the resources could be flexibly utilized and the operation cost can be reduced. Nevertheless, patients would face privacy problem when storing PHR data into Cloud. Besides, it requires a secure protection scheme to encrypt the medical records of each patient for storing PHR into Cloud server. In the encryption process, it would be a challenge to achieve accurately accessing to medical records and corresponding to flexibility and efficiency. A new PHR access control scheme under Cloud computing environments is proposed in this study. With Lagrange interpolation polynomial to establish a secure and effective PHR information access scheme, it allows to accurately access to PHR with security and is suitable for enormous multi-users. Moreover, this scheme also dynamically supports multi-users in Cloud computing environments with personal privacy and offers legal authorities to access to PHR. From security and effectiveness analyses, the proposed PHR access scheme in Cloud computing environments is proven flexible and secure and could effectively correspond to real-time appending and deleting user access authorization and appending and revising PHR records.

Xiao and Xiao, “Security and privacy in cloud computing.” [6] Recent advances have given rise to the popularity and success of cloud computing. However, when outsourcing the data and business application to a third party causes the security and privacy issues to become a critical concern. Throughout the study 9at hand, the authors obtain a common goal to provide a comprehensive review of the existing security and privacy issues in cloud environments. We have identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Beginning with these attributes, we present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario. Future research directions are previously determined for each attribute.

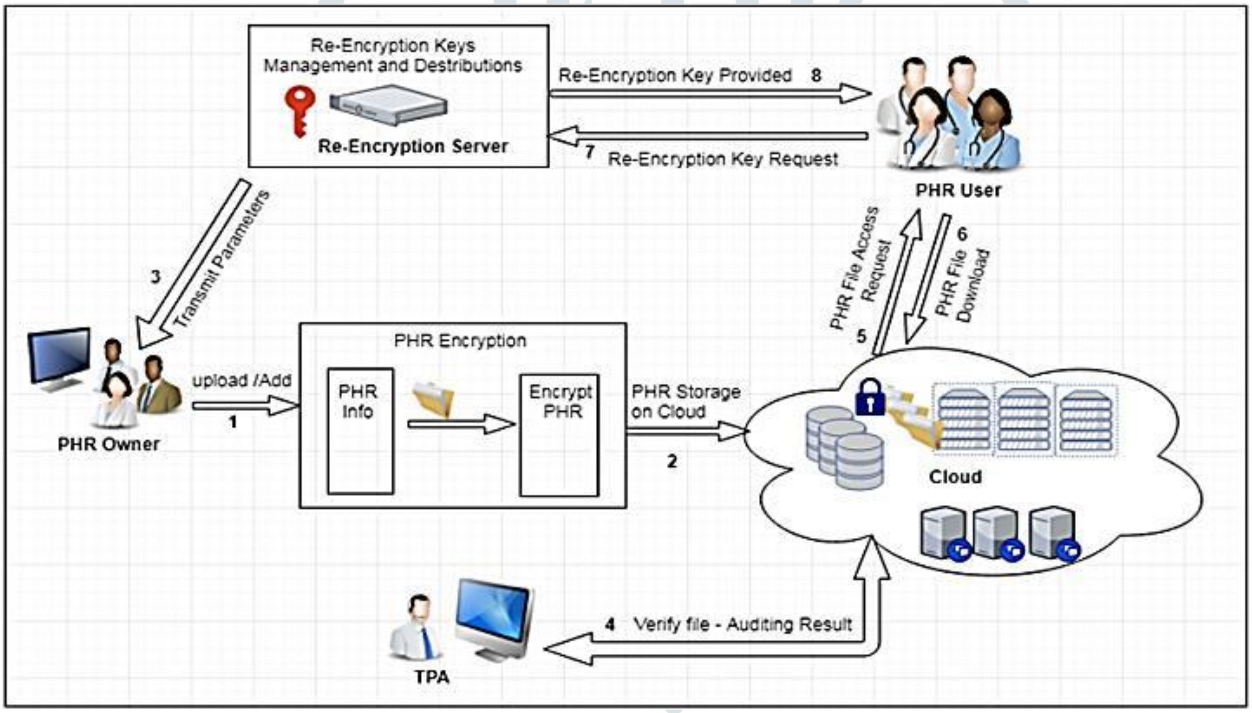
In general, the owner is defined as the creator of the information. Establishing information ownership is necessary for protection against unauthorized access or misuse of patient's medical information. Ownership of healthcare information can be protected through a combination of encryption and watermarking techniques that results in secured healthcare information that cannot be transmitted, accessed, or released without the mutual acceptance of all entities involved in the ownership/creation of the healthcare information. Patients can allow or deny the sharing of their information with other healthcare practitioners [8]. To implement patient data sharing in a healthcare system, patient may grant rights to users based on a role or attributes held by the respective user to share specific healthcare data with that user. Authenticity in general refers to the truthfulness of origins, attributions, commitments, and intentions. It ensures that the entity requesting access is authentic. In healthcare systems, the information provided by the healthcare providers and the identities of the entities using such information must be verified via the Authentication Act [9]. The authentication of information can pose special problems, like man-in-the middle attacks, and is often mitigated with a combination of usernames and passwords. Most cryptographic protocols include some form of endpoint authentication specifically to prevent man-in-the-middle attacks. In a healthcare system, both healthcare information offered by providers and identities of consumers should be verified at every access.

Confidentiality is the act of ensuring that patient’s health data is kept completely undisclosed to unauthorized entities. Delegating data control to the cloud, leads to an increase in the risk of data compromises, as the data becomes accessible to an augmented number of parties. Due to the increased number of parties, devices and applications involved, there is an increase in data compromise threats. To make the patient/doctor relationship work effectively, it is necessary for the patient to trust the healthcare system to protect the confidentiality of his data. If the patient feels that the information, he gives to his doctor is not protected, and that his privacy is threatened, he can be more selective about the information he will provide to his doctor in the future. The threat of data compromise can harm the patient/doctor relationship and hamper the proper medical diagnosis and treatment [10]. For example, an employer may refuse a job if the patient's medical data are disclosed. Confidentiality can be achieved by access control and using encryption techniques.

.

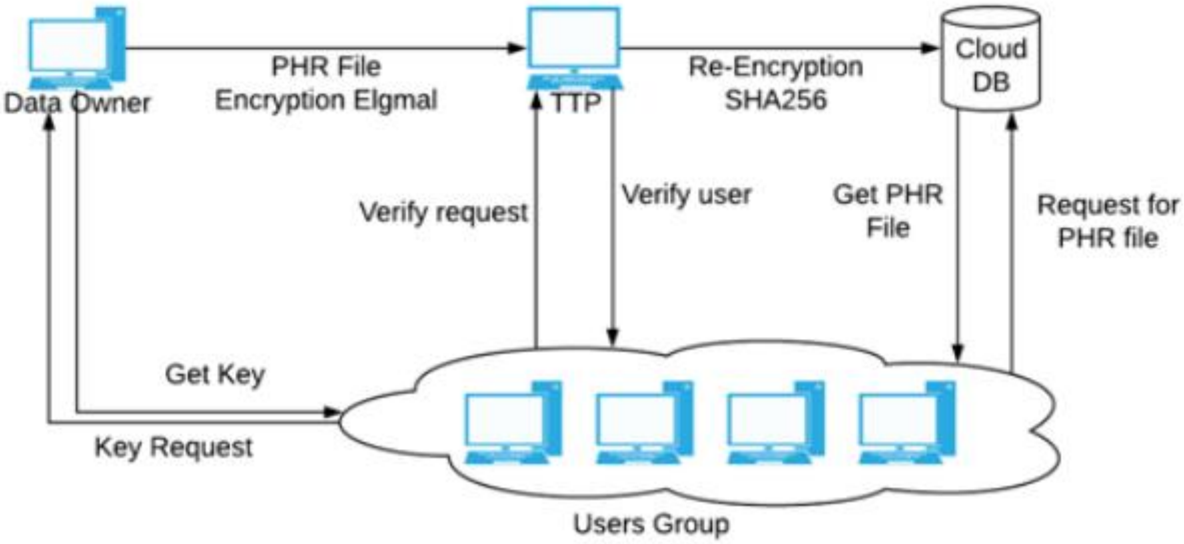
III. PROPOSED METHODOLGY DURING THE TENURE OF THE WORK

In the proposed research work to design and implement a system that can provide the security to Personnel Health Records (PHR) files using encryption as well as proxy re-encryption services, in cloud environment and provide the security from insider attacks like collusion attack, bruited force attack as well as SQL injection attack.



In this architecture they will give some security and privacy mechanism such as, confidentiality, data integrity and fine-grained access control. The privacy and security are most affected issue in the cloud environment. In this architecture used clouds with some advantages like as a huge storage capacity and high scalability. The used attribute encryption based (ABE) algorithm for the fine-grained access control. The attribute-based encryption algorithm first encrypt data before storing on the cloud server. In ABE there are two variants based on placing attributes and access attribute policy.

- The system first uploads the own PHR file on cloud using Elgamal encryption scheme.
- These files first received by TTP and generate the proxy re-encryption using SHA-256 algorithm and store the file into the cloud server.
- Data owner can share the file to individual user as well as whole group using RBAC algorithm.
- When end user’s give request to CSP, then authentication has done by TTP.
- In the proposed work we have written web service for owner that can 24*7 available for private key distribution.
- When data owner revokes any user system automatically expired the existing keys and generate new keys.



This paper is based on the works in cryptograph-icily enforced access control for the data stored in cloud and attribute-based encryption. To apply fine-grained access control, the conventional public key encryption (PKE) based techniques either include high key management overhead, or require encrypting copies of a file using different set of user's keys. To enhance the scalability of the solutions mentioned above, encryption schemes like ABE can be used. Here in Goya paper on ABE information is encrypted under a group of attributes so that multiple users who have proper keys can decrypt it. Thus, it makes encryption and key management more efficient. Fine-grained Data Access Control using ABE: The numerous schemes use ABE to understand fine-grained access control for outsourced data. Specially, there has been an increase in interest in applying ABE based encryption schemes to protect electronic healthcare records (EHRs).Lately, Narayan recommended an attribute-based framework for an electronic healthcare records systems, where each users(patient) EHR files are encrypted using a variant of CPABE that allows direct revocation. But however, the cipher text range grows sequentially with the numerous of unrevoked users. Here in another scheme of ABE that allows relegation of access rights is used for encrypted EHRs. Ibraimi applied cipher text policy ABE to maintain the sharing of PHRs, and popularized the theory of social/professional domains. Here in, Akinyele investigated using ABE to generate self-assured EMRs, which can each of two can be stored on cloud servers or mobile devices so that EMR could be gained when the health provider is offline. But however, there are various familiar drawbacks of the above works.

Here, they will usually consider the use of a one separate trusted authority (TA) in the structure. It may create a load bottleneck, and it also may undergo the key escrow issue since the TA can acquire all the encrypted files, which may lead to privacy disclosure. Also in addition, it is not practically acceptable to give all attribute administrative functions to one TA, along with certifying all users‟ attributes or roles and generating secret keys. Different organizations usually form their own domains and become authorities to define and approve different sets of attributes belonging to their concern (i.e., divide and rule). Let's say for e.g., an experienced professional association would be responsible for certifying professional medical specialties, elsewhere a regional health provider would authorize the job ranks of its staffs. But there still lacks an efficient and on-call user revocation structure for ABE with the backing for productive policy updates, which are crucial elements of secure PHR sharing.

Here we are developing a web-based application which will help users to login/authentication, upload and download medical records. The system will connect to one console application SRS, to generate the keys. The SRS also takes cares of permission per files and all data is kept in MySQL database. The internal communication between SRS and web-application is based on HTTP protocol. Proxy Re-encryption based approach is used for the SRS to generate the re-encryption keys for secure sharing of PHRs among the users. The PHRs are encrypted by the patients or PHR owners and only the authorized users having the keys issued by the SRS can decrypt the PHRs. Moreover, the users are granted access to the specific portions of PHRs as deemed important by the PHR owner.

SEED based XOR technique is used for encryption of files.

The simple XOR cipher is a type of additive cipher, an encryption algorithm that operates according to the principles:

$A \oplus 0 = A,$

$A \oplus A = 0,$

$(A \oplus B) \oplus C = A \oplus (B \oplus C),$

$(B \oplus A) \oplus A = B \oplus 0 = B,$

For example, the string "Wiki" (01010111 01101001 01101011 01101001 in 8-bit ASCII) can be encrypted with the repeating key 11110011 as follows:

```
          01010111 01101001 01101011 01101001
          11110011 11110011 11110011 11110011
=         -------------------------------------------------
          10100100 10011010 10011000 10011010
```

And conversely, for decryption:

```
          10100100 10011010 10011000 10011010
          11110011 11110011 11110011 11110011
=         -------------------------------------------------
          01010111 01101001 01101011 01101001
```

The XOR operator is extremely common as a component in more complex ciphers. By itself, using a constant repeating key, a simple XOR cipher can trivially be broken using frequency analysis. If the content of any message can be guessed or otherwise known then the key can be revealed. Its primary merit is that it is simple to implement, and that the XOR operation is computationally inexpensive. A simple repeating XOR (i.e. using the same key for XOR operation on the whole data) cipher is therefore sometimes used for hiding information in cases where no particular security is required. The XOR cipher is often used in computer malware to make reverse engineering more difficult.

IV. The PHR Partitioning

The PHR is logically partitioned into the following four portions:

- Personal Information;
- Medical information;
- Insurance related information;
- Prescription information

However, it is noteworthy that the above said partitioning is not inflexible the PHR into lesser or more number of partitions. The PHRs can be conveniently partitioned and can be represented in formats, for example XML. Moreover, the PHR owner may place more than one partition into same level of access control. Any particular user might not be granted a full access on the health records and some of the PHR partitions may be restricted to the user. For example, a pharmacist may be given access to prescription and insurance related information whereas personal and medical information may be restricted for a pharmacist. Likewise, family/friend may be given full access to the PHR. A researcher might only need the access to the medical records while de-identifying the personal details of the patients. The access rights over different PHR partitions are determined by the PHR owner and are delivered to the SRS at the time of data uploading to the cloud.

4.1 Key Generation

As expressed before in Section 3 that the obligation of the SRS is to produce the private/open key sets for the clients having a place with the arrangement of approved clients. Be that as it may, the key age time for the frameworks with huge quantities of clients may influence the general execution of the framework. In this manner, we evaluated the presentation of the SeSPHR as far as the time devoured for the key age venture for various number of client. The time utilization for producing keys for 10, 100, 500, 1000, 5000, and 10,000 clients in introduced in Fig. 3. As opposed to the general pattern of expanded key age time when the quantity of clients builds, it very well may be found in Fig. 3 that with the expanded number of clients, the comparing increment in the key age time isn't uniform. For instance, the time utilization to produce keys for 10 clients is 0.6 second while for 100 clients, the key age time increments to 0.97 second. In like manner, the key age time for 10,000 clients is watched 2.16 seconds, which is additionally entirely sensible thinking about the high number of clients. The key age time for recently joining individuals is likewise insignificant in light of the fact that such individuals join once in a while and creating keys for a solitary client is for sure a proficient procedure.

4.2 Encryption and Decryption

The time utilization of the SeSPHR strategy to scramble and decode the information documents of differing sizes is likewise assessed. The record sizes utilized for the experimentation are 50 KB, 100 KB, 200 KB, 500 KB, 800 KB, 1024 KB, 1500 KB, also, 2048 KB. The time utilization for both the encryption and unscrambling tasks for the documents of aforementioned sizes is appeared in Fig. 4 and Fig. 5, separately. From Fig. 4 we can see that with the expansion in PHR record size, the encryption time likewise increments. For instance, the encryption time for the document of size 50 KB is 0.13 second though the encryption time for the 2 MB record is 1.289 sec-onds. Despite what might be expected, the time required for decoding of the PHR documents was impressively not exactly the encryption time. A normal decline of 24.38% in.

V. RESULTS AND DISCUSSION

The performance of the system to securely share the PHRs among different types of users was evaluated by developing a client application in Java. Due to the fixed size of the prime number, the encryption and decryption process was carried out in the chunks of 64 bytes. The experiments were conducted on the computer having Intel® Core i5-2600 CPU @ 2.00 GHz with 4 GB memory. The time consumption for generating keys for 10, 100, 500, 1000, 5000, and 10,000 users in presented

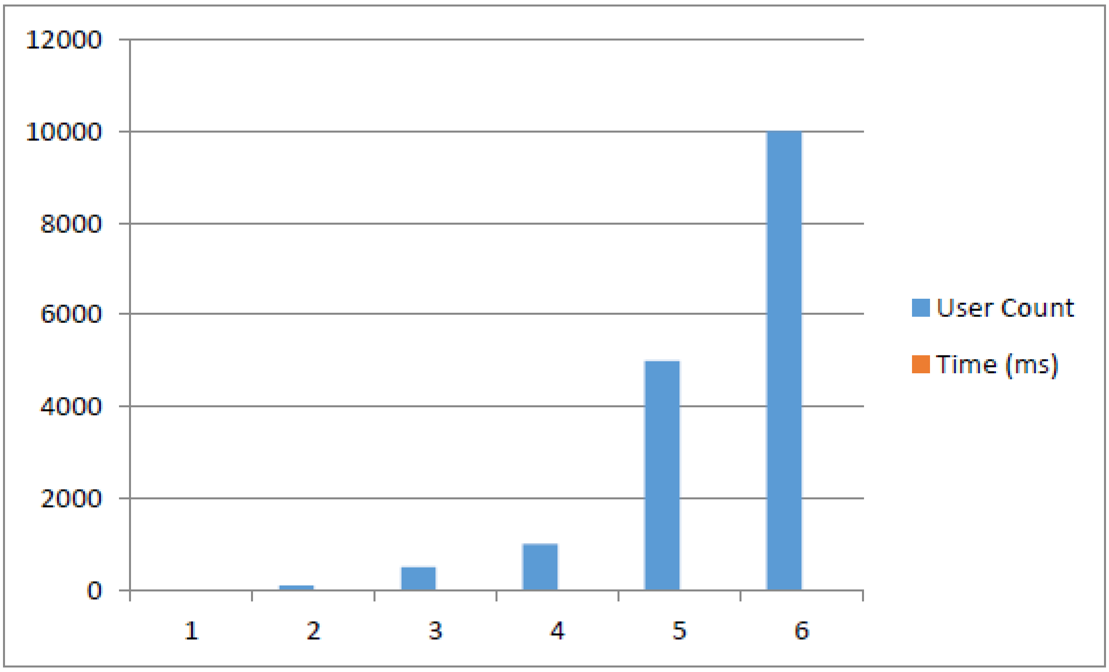


Fig.3: Time consumption for generating keys

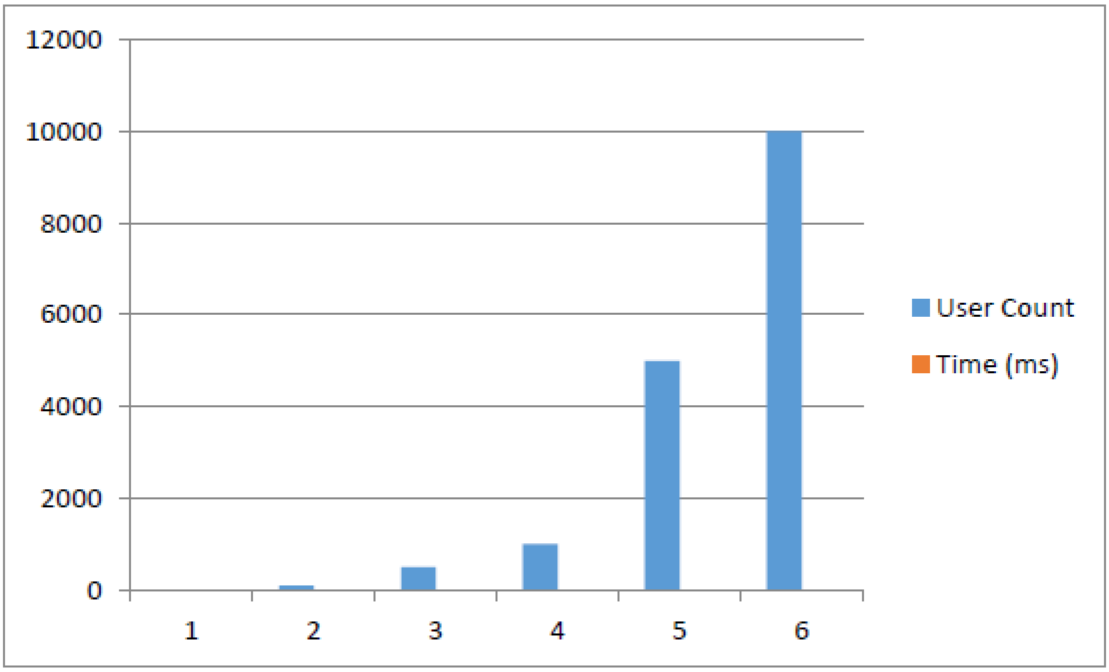


Fig.4: The time consumption for Encryption and Decryption

VI.ACKNOWLEDGMENT

We proposed an approach to safely store and transmission of the PHRs to the approved elements in the cloud. The philosophy saves the privacy of the PHRs and implements a patient-driven access control to various segments of the PHRs dependent on the entrance master vided by the patients. We actualized a fine-grained access control strategy so that even the substantial framework clients can't get to those parts of the PHR for which they are not approved. The PHR proprietors store the encoded information on the cloud and just the approved clients having substantial re-encryption keys issued by a semi-believed intermediary can decode the PHRs. The job of the semi-believed intermediary is to produce and store the bar lic/private key sets for the clients in the framework. Notwithstanding safeguarding the classification and guaranteeing dad tientcentric access power over the PHRs, the philosophy likewise manages the forward and in reverse access control for withdrawing and the recently joining clients, separately. In addition, we officially examined and confirmed the working of SeSPHR technique through the HLPN, SMT-Lib, and the Z3 solver. The presentation assessment was done on the based on time devoured to produce keys, encryption and unscrambling activities, and turnaround time. The test results display the feasibility of the SeSPHR philosophy to safely share the PHRs in the cloud condition..

REFERENCES

[1] 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, vol. 90, pp, 46-62, 2017

[2] 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, vols. 4344, pp. 99-109, 2015.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.

[4] J. Li, “Electronic personal health records and the question of privacy,” Computers, 2013, DOI: 10.1109/MC.2013.225.

[5] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, “Secure Dynamic access control scheme of PHR in cloud computing,” Journal of Medical Systems, vol. 36, no. 6, pp. 4005– 4020, 2012.

[6] Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 1–17, Jul. 2012.

[7] R. Wu, G.-J. Ahn, and H. Hu, “Secure sharing of electronic health records in clouds,” In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing (Collaborate Com), 2012, pp. 711-718

[8] A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, “Incremental proxy re-encryption scheme for mobile cloud computing environment,” The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.

[9] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, “A research agenda for personal health records (PHRs),” Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.

[10] 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, pp. 1-9

[11] A. Abbas and S. U. Khan, “A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds,” IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.

[12] M. Shamim Hossain, Ghulam Muhammad, et al. "Cloud-assisted Industrial Internet of Things (IIoT) –Enabledframework for health monitoring." 2016 evier B.V.

[13] Ming Li, Shucheng Yu, and Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption”, IEEE Transactions On Parallel And Distributed Systems 2012.

[14] IEEE 2012 paper on “Improving the interoperability of healthcare information system through HL7 CDA and CCD standards”.

[15] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, ―Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes,‖ 2009.

[16] “Privacy-preserving personal health record system using attribute-based encryption,” Master’s thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.

[17] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted personal health records in cloud computing,” in ICDCS ’11,Jun. 2011.

[18] S. Narayan, M. Gagn´e, and R. Safavi-Naini, “Privacy preserving phr system using attribute-based infrastructure,” ser. CCSW ’10, 2010, pp. 47–52.

[19] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control inmulti-owner settings,” in SecureComm’10, Sept. 2010, pp. 89–106.

[20] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in IEEE INFOCOM’10, 2010

[21] C. Dong, G. Russello, and N. Dulay, “Shared and searchable encrypted data for untrusted servers,” in Journal of Computer Security, 2010