International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Secure Data Sharing of Sensitive Medical Record (Phr) In the Cloud

L. Ramesh, R. A. Roseline

Abstract: ***Present day human services areas need to make a domain which lessens tedious endeavors and other expensive tasks to acquire a Patient complete medicinal transcription and consistently incorporates this multifariousness accumulation of therapeutic information to convey it to the social insurance specialists. Sensitive medical record (PHRs) came to be generally embraced to empower social insurance suppliers and patients to make, oversee and get to human services data from wherever, and whenever. Cloud administrations give the essential foundation at lower cost and better quality. Distributed computing when utilized in Healthcare segment diminishes the expense of putting away, handling and refreshing with improved proficiency and quality. In any case, the security of information in the cloud isn't acceptable today. The electronic wellbeing record comprises of pictures of the patient's record which is exceptionally private. Human services information has stringent security prerequisites for secrecy, accessibility to approved clients, and detect ability of connection. The focal point of the present examination is explore on the above mentioned problem necessities and suggest an answer for human services cloud suppliers this study will assist in ensuring persistent' information they have and of those mentioned high significance. The attention will be on explicit distributed computing medicinal services confidential matter and how cloud homomorphic encryption with part key and key designation can help in gathering social insurance administrative necessities. The recommended system depends on proposed calculation, RSA calculation, and Secret sharing calculation, Data imparting calculation to key assignment to guarantee information privacy, validation, respectability, and accessibility in a staggered progressive request. This will empower the social insurance supplier to accept/discard several entrance conditions in several requests, particularly in therapeutic investigation condition.***

Keywords: PHR,ABE,QR-Code,QR-KP ABE.

I. INTRODUCTION

Distributed computing give away another paradigmatic for upgrading the conveyance of medicinal services, expanding the patronage adaptability of restorative associations, empowering them to work with more prominent proficiency, cost-adequacy, and readiness. Utilization of cloud administrations has taken off crosswise over incalculable enterprises. Reception of distributed computing in human services has occurred somewhat more probably, as suppliers sorting the profit by cloud contributions and the amount of their activities they can bear to shift to the cloudspace.

Manuscript published on 30 August 2019.
*Correspondence Author(s)
L.Ramesh, Research Scholar, Government Arts College, Coimbatore, India, Tamil Nadu, India.
R.A.Roseline, Associate Professor & Head, Government Arts College, Coimbatore, India, Tamil Nadu, India.

Sensitive Medical Records (PHRs), investigation and portray frameworks are a couple of territories where medicinal services suppliers have discovered accomplishment with cloud organizations. Distributed computing is characterized as an innovation which plays the web and focal remote computer to keep up information and different apps. Distributed computing enables endeavors and buyers to utilize applications without establishment and access their records at any PC with web get to. This innovation takes into consideration effective figuring by incorporated information stockpiling, preparing and data transmission. Distributed computing has been envisioned as the forefront information advancement plan for endeavors, because of its extensive summary of exceptional central focuses in the IT history: on interest self-organization, shared framework get to, zone self-ruling resource pooling, snappy resource flexibility, and transference of risk and utilize based evaluating. As a risky development with critical implications, appropriated processing changes the nature and the technique for how adventures use information advancement. The basic piece of this viewpoint changing is that data are being concentrated or re-appropriated to the cloud. From the client point of view, securing data remotely to the cloud in a versatile on-demand way brings drawing in favorable circumstances, for instance, easing of the weight in case of general data access with territory opportunity, storing the officials, and evading of capital use on gear, programming parts and staff support, etc., Thus Cloud assurances to offer organization to customers without reference to the establishment on which these fogs are encouraged.

II. LITERATURE REVIEW

2.1 Present day Cryptography

Present day Encryption calculations, (for example, All symmetric Algorithms) still assume the primary job in information security of distributed computing. The assessment has been performed for those encryption calculations as indicated by irregularity examine by utilizing NIST measurable examine in distributed computing condition[6]. From reenactment results, the creators reasoned that no solid signs of factual shortcomings for the 8 present day encryption calculations when connected in distributed computing conditions.

A half breed encryption procedure (utilizes RSA, 3-DES and Random Number generator calculation) is proposed to upgrade the security of cloud database [7]. This strategy gives the adaptability in range and grouping to the client's decision.

This is on the grounds that a client can apply the majority of the three encryption strategies or exclude any in any request. Regardless of whether the client does not choose any encryption system, the arbitrary number calculation will in any case be actualized as a matter of course, therefore giving in any event a solitary level security. The selected grouping will likewise be put away in the database so the decoding can be conceivable. The negative impact of this plan is that it makes surface on the question execution because of the staggered idea of encryption and unscrambling. Likewise the calculation time increments as the size of information increments.

Elliptic Curve Cryptography was proposed to investigate information security (privacy and validation of information) between mists [8]. Elliptical curve cryptography(ECC) is an open key encryption method dependent on elliptic bend hypothesis that can be utilized to make quicker, littler, and increasingly effective cryptographic keys. ECC creates keys through the properties of the elliptic bend condition rather than the customary technique for age as the result of extremely huge prime numbers. The innovation can be utilized related to most open key encryption techniques, for example, RSA, and Diffie-Hellman.

2.2 Homomorphic cryptography

The FHE is certifiably not another thought as it has been, for a long time, saw as a dream that could never work out as expected. R. L. Rivest, L. M. Adleman, and M. L. Dertouzos. [9] proposed that completely homomorphic encryption might be conceivable in 1978, soon later the innovation of the RSA cryptosystem [10], however were not able locate a safe plan for its acknowledgment. It was changed since 2009, with an achievement revelation by Craig Gentry [11, 12], who was then an alumni understudy at Stanford University. (He is presently at IBM Research.) Since at that point, further refinements and all the more innovative thoughts in future at a quick move [13].

Earlier attempting to clarify how homomorphic encryption functions, we ought to clarify the word homomorphic [14]. The Greek roots decipher as same shape or same structure, and the hidden thought is that of a change that has a similar impact on two distinct arrangements of items. The idea originates from the elusive universe of conceptual variable based math, yet we can offer an all the more unattractive model, where the 2 arrangements of articles are the positive genuine numbers from one viewpoint and their different logarithms. At that point increase of genuine numbers and expansion of logarithms are homomorphic tasks. For any positive genuine numbers x, y and z, on the off chance that x•y = z, at that point log(x) + log(y) = log (z).Such homomorphism offers two elective courses to a similar goal. On the off chance that we are granted x and y, we can increase them legitimately, at that point include, lastly return the antilog of the outcome. In likewise we end up with z. Homomorphic cryptography offers a comparative dual of pathways.

In encoded calculation, the client determines scrambled contributions to a program, and the server PCs on scrambled contributions to deliver a scrambled outcome. This scrambled outcome is transmit back to the client who decodes it to get the real outcome. The Fully homomorphic encryption (FHE) conspire, implies that there are no impediments on what controls can be excecuted [15] . The FHE plot permits a specialist that does not have the mystery unscrambling key to process some aftereffect of the information (even encoded), notwithstanding when the capacity of the information are exceptionally perplexing.

III. EXISTING METHODS:

3.1 Hierarchical Attribute-Base Encryption (HABE)

Wang et al [10] have been proposed Hierarchical Identity Base Encryption (HIBE) and CP-ABE. It gives satisfied access control, full assignment and superior. The HABE plan comprises of many characteristic specialists and numerous clients. ABE utilizes isolated typical structure approach. A similar characteristic might be administrated by various space bosses as per explicit arrangements, which is most muddled to actualize by and by. ABE [10] model comprises of a Root Master (RM) and different areas. One area comprises of figure of space experts and units of clients identified with end clients It is chiefly material to the earth of ventures sharing information in cloud. The above mention plan has dispute with numerous qualities assignments and functional usage is exceptionally troublesome in light of the fact that equivalent characteristic might be managed by various area experts.

3.2 Hierarchical Attribute Set Based Encryption

(HASBE) HASBE plan is proposed and executed by Zhiguo Wang et al [10].The above mention plan stretched out the ASBE plan to deal with the progressive skeleton of the framework. In the above mention model believed expert is in charge of overseeing top level space specialists. Every client in this framework is relegated a key structure. This plan give adaptable, adaptable and fine grained access control in distributed computing. Proficient client denial should be possible in this plan because of trait allocated numerous qualities.

3.3 Multi-Authority Attribute Base Encryption

M-ABE model comprises of numerous characteristic specialists and numerous clients. Properties key age calculation will run the specialist and solution will send to the client. In a multi-expert ABE plot, numerous quality specialists screen various arrangements of traits and issue relating decoding keys to clients and encoded can necessitate that a client get keys for suitable characteristics from every specialist before unscrambling a content. Pursue [11] represent a multiauthority ABE plot sustain that a wide range of experts working all the while, each dealing with out mystery keys for an alternate arrangement of properties PHR [9] is a rising Patient driven model of wellbeing data trade. For secure sharing of PHR information, a system is utilized. The above model proprietors allude to Patient who have full command over their personal PHR information. They can make, Bring up-to-date, oversee and erase it.

Retrieval Number: J92830881019/19©BEIESP
DOI: 10.35940/ijitee.J9283.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Because of the staggering expense of information stockpiling and dealing with the information, PHR data are re-appropriate to cloud storage. The cloud storage is semi-trust, so before re-appropriate to the outsider, ought to encode the information.

A. Accessible Encryption

Accessible encryption is an expansive idea that manages look in encoded information .The objective is to redistribute scrambled information and have the option to restrictively recover or question information without decoding every one of the information. There are 2 ways in which to contend with the accessible encoding. The principal approach is to utilize symmetric encryption [17, 18], though the second 2nd methodology for is to utilize hilter encoding.

B. Attribute (Primarily) Based Encoding

In the Attribute Primarily Based Encoding ABE, the traits and strategies related with the message and the customer choose which customer can unscramble a figure content. A focal specialist will make mystery keys for the clients dependent on traits/approaches for every client. Clients in the framework have properties; clients gets a key ("or key group") from a specialist for their arrangement of characteristics. Figure content contains a strategy (a Boolean predicate over the trait space). In the event that a client's characteristic set fulfills the strategy, he can utilize his key group to unscramble the figure content. Different clients can't pool their traits together.

The principle part of our structure is to give secured understanding fundamental PHR access and helpful key administration together. Here the objective is to separate the PHR framework into various security concern (to be specific, open areas (PUDs) and individual spaces (PSDs)) as indicated by the different clients' information get to prerequisites. In the two sorts of security concerns, we use ABE to see cryptographically fortify, understanding fundamental PHR get to. Uncommonly, in a PUD multi-expert ABE is utilized. Every datum proprietor is his very own tenable specialist PSD, he utilizes a KP-ABE framework to keep up the mystery keys and get to power of clients in his PSD.

In distributed computing, there are diverse existing systems that give security, information classification and access control. Here clients need to impart their delicate data to others dependent on the recipient's capacity to deal with an approach in dispersed frameworks. One of the encryption plans is Attribute Based Encryption (ABE) which is another procedure where such strategies are named and cryptographically authorized in the encryption calculation within. Henceforth, the current ABE plans are of two kinds. They are Key-Policy ABE (KP-ABE) plan and Cipher content Policy ABE (CP-ABE) conspires. Encryption systems for individual wellbeing records in distributed computing writing audit as pursues.

IV .ATTRIBUTE-BASED ENCRYPTION:

Attribute (Primarily) Based Encoding (ABE) could be a speculation of personality based encoding technique that fuses credits as contributions to its cryptanalytic natives. Info is encoded utilizing a load of qualities with the goal that totally different shoppers who increase legitimate keys will unscramble. Attribute (Primarily) Based Encoding (ABE) offers fine-grained access management further more as counteracts against agreement. Here to execute fine grained access management, the standard open key encoding primarily based methods and either expertise high key administration overhead, or need encrypted duplicates of a document utilizing distinctive arrangement of clients keys. To boost the flexibility of the above arrangements, encoding methods, for example, Attribute (Primarily) based encoding (ABE) will utilized. The basic target for these models is to grant security and access management. The fundamental angles are to grant ability, versatility and fine grained access management. In proportional style model, this framework will be accomplished simply once client and server are in a confided in space. On these lines, the new access management conspire that's "Attribute (primarily) Based Encryption (ABE) ‟ setup was bestowed that comprise of key strategy quality based encoding (KP-ABE). As contrasted and ancient model, KP-ABE gave fine grained access management. Anyway it fizzles relating to ability and flexible once specialists at varied levels are considered. In ABE conspire each the client mystery key and also the figure content are connected with a lot of properties. ABE is executed for one-to various encoding in which figure writings aren't extremely disorganized to 1 specific client, it would be for more than one number of clients.

4.1 QR-ATTRIBUTE BASED ENCRYPTION (ABE)

In the planned framework, the individual information of the Patient are going to be place away during form of info on cloud which is able to be place away in an encoded arrangement on the cloud for security functions. Attribute (Primarily) Based Encryption (ABE) are going to be utilized for the procedure of encoding. This encoded info are going to be saved cash on verified cloud. A QR code are going to be made utilizing properties like patient name and Patient ID. To get rid of the information from the cloud the client are going to be needed to visualize the QR code to induce to the information. When confirmation the decoded information are going to be shown to the verified client. The PHR will be are going to be gotten to by utilizing a flexible application. The selection of permitting access privileges of this PHR can give for the patient. The patients, specialists can have a privilege for adjustment of the data whereas drug specialists can simply have acceptable to succeed the supported prescription.

Individual Health Record: Personal Health Record (PHR) could be developing patient-driven architecture of welfare data trade, which is often re-appropriated to be put away at an outsider, for example, cloud suppliers. A PHR act of administering enables a Patient to make, oversee, and control her own wellbeing information in one spot through the web, which has made the capacity, recovery, and sharing of the medicinal data progressively proficient. Particularly, every patient is guaranteed the full determined of his/her restorative records and can transfer communication his/her wellbeing information with a wide scope of clients, including medicinal services suppliers, relatives or companions.

QR-Code: The 4-square QR code comprises of coding area and utilitarian locales. The coding area is portrayed by certain features, which speak to the information, adaptation, position, etc. The practical districts are the blend of limitation diagram, rectifying chart, separator and some looking for diagrams, which would not be utilized for information encoding. The district of 4 modules wide around the QR code picture is named as clear, which has the equivalent intelligent file with light-shaded modules. The most amazing locales are 3 diagram squares utilized for picture chasing. The three
diagram squares situate at the upper left corner, left lower corner and the upper right corner of the QR code picture, separately.

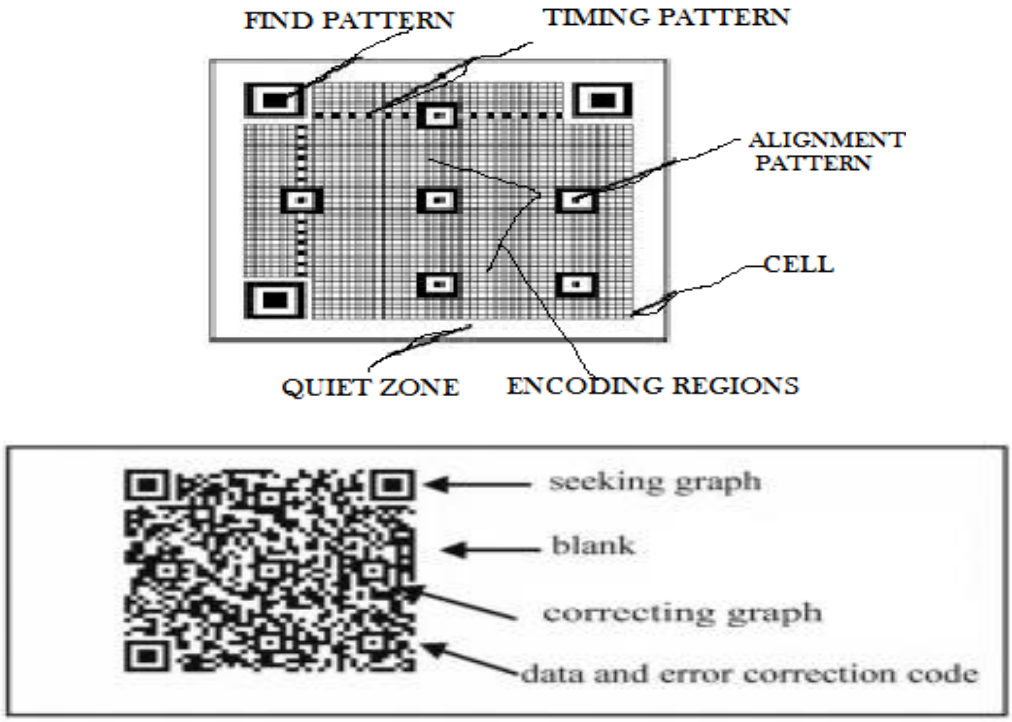

Fig 1 Structure of QR code

The searching for diagram is formed of 3 lined concentrically squares, together with 7x7 dull hued models, 5x5 light-weight hued modules and 3x3 dim hued modules. The breadth extent of the modules is 1: 1: 3: 1: 1. Since the link of those modules shows up only sometimes in pragmatic procedure of picture chasing, we use them to characterize the situation of the looking for charts and get the picture data. The separators arranged between the looking for chart squares and cryptography space. They're one-module breadth and light-shaded. The limitation chart comprises of dim hued and light shaded module orchestrated on the other hand which adjust to a line and a segment. They will specific the thickness of attributes, form and choose the basic organize angle of models. The rectifying chart is made out of 3 line concentric squares, as well. They're dim shaded, light-hued and dim hued modules organized from outside to inside separately. The particulars of the units following 5x5, 3x3, a dull hued module within the middle. Simple Version-one of QR code picture absence of confinement diagram, the others have their separate limitation charts. These confinement diagrams of QR code picture orchestrated by symmetry in a corner to corner position and might be utilized to address the facilitate estimation of current locale in scanner tag picture acknowledgment.

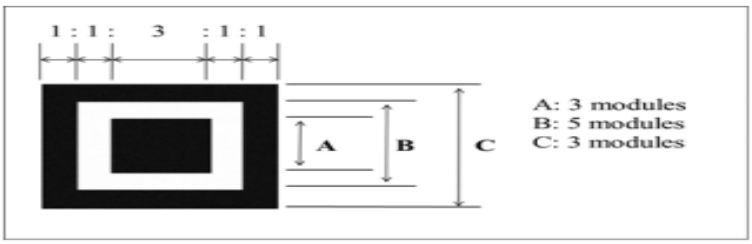

Fig 2 Phases of QR Code blocks

Numerous analysts have managed QR code picture during a decades ago, however the process speed of it is consistently an issue hard to increment. We proposed a novel discovery strategy for QR code in the paper as indicated by the qualities of QR code shape. Figure demonstrates the progression of QR code picture preparing.

The primary procedures incorporate picture chasing, restriction modification and picture acknowledgment.

The activities of proposed therapeutic record sharing framework consolidate KP-ABE and Multi-Authority ABE and conventional cryptography, enabling Patient to transfer his/her medicinal records. These tasks can be arranged into following modules: In this area we examine principle module plan idea for sharing of restorative records utilizing, Property based encryption – (KP-ABE and Multi Authority-ABE is called QR-KPABE).

Modules of the framework are:

1. Framework Setup and Secret Key Generation
2. Encryption of Medical Records by using QR
3. View Medical Records (Decryption)
4. Repudiation of Public space User/qualities

The framework initially characterizes a typical universe of information qualities shared by each PSD, for example, "individual data", "average history", "sensitivities", and "solutions" "crisis" , "companion", "relative" , "crisis". A crisis trait is additionally characterized for break-glass get to. Every datum proprietor's customer application produces its comparing open/ace keys utilizing Key-Policy quality Based Encryption. The open keys can be distributed with assistance of framework given by specialist organization. Information Owner determine the entrance strategy of information peruser in her own area, and produces mystery key utilizing Key-Policy property Based Encryption. Individual area client acquires mystery key from the information proprietor through secure email by sending a solicitation for the keys. or then again information proprietor send the mystery key to individual space client by means of secure email. An utilization of Attribute-Based Encryption (ABE) procedures to achieve versatile and fine grained

Procedure for Proposed work

Personal Domain:

information access control for individual wellbeing records to encode every patient's PHR document. In this paper we focus on the different information proprietor circumstance, which is unmistakable from past works in secure information re-appropriating. It partitions the clients in the PHR framework into a few security areas which diminishes the key administration multifaceted nature for proprietors and clients. At the same time, quiet classification is kept up and ensured by abusing Multiauthority ABE. In crisis situation, proposed plot (QR-KPABE) gives dynamic difference in access strategies or record properties supports break glass access and efficient on-request client/quality repudiation. Broad expository and trial results are given which demonstrates the Security, Scalability, and Efficiency of our plan.

QR Code Working flow of the Medical data encode Encryption and Decryption

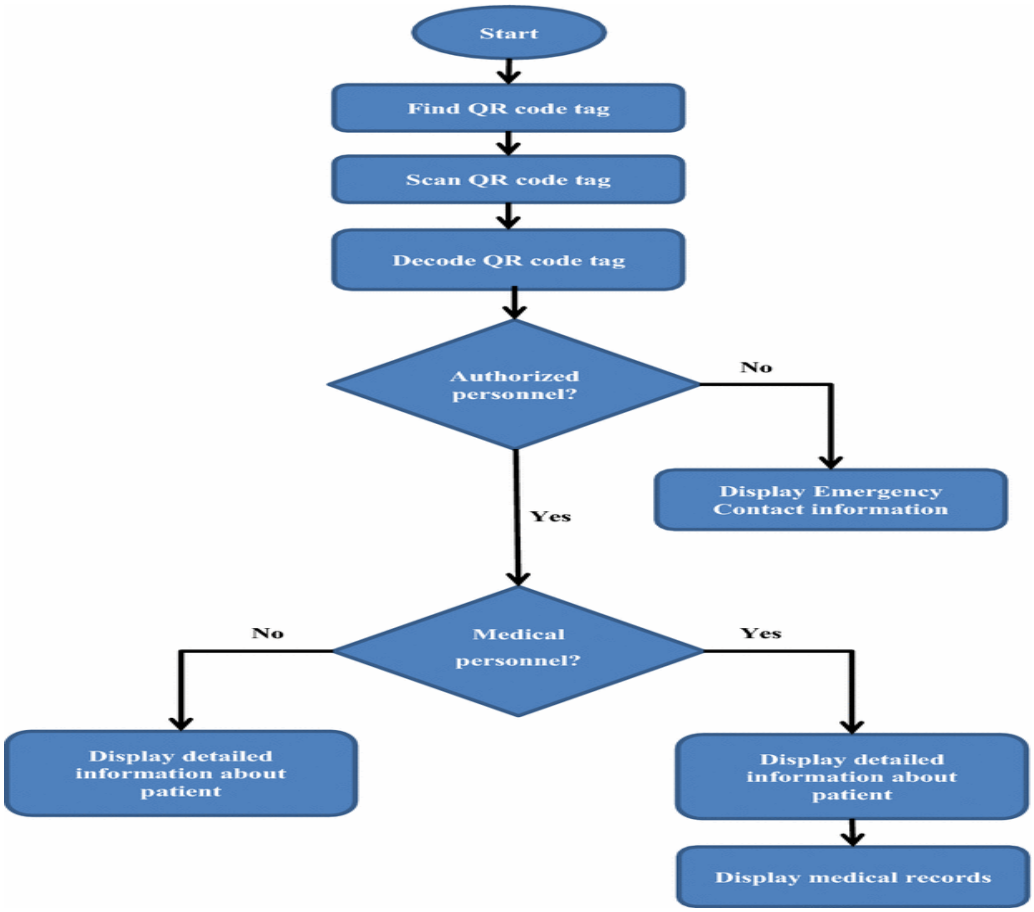

Fig 3 Shows QR Code Working flow of the Medical Data

This tables demonstrate the correlation of existing and proposed strategy precision and timespan based we determined the qualities, every hub and information stockpiling quick, transfer and download based the Accuracy and Time period determined.

Table 1: Accuracy and Time period of existing and proposed method

S.NO	ALGORITHM	ACCURACY	TIME PERIOD
1	ABE	89.4	2.8
2	KP-ABE	94.2	1.7
3	QR-KPABE	97.6	1.4

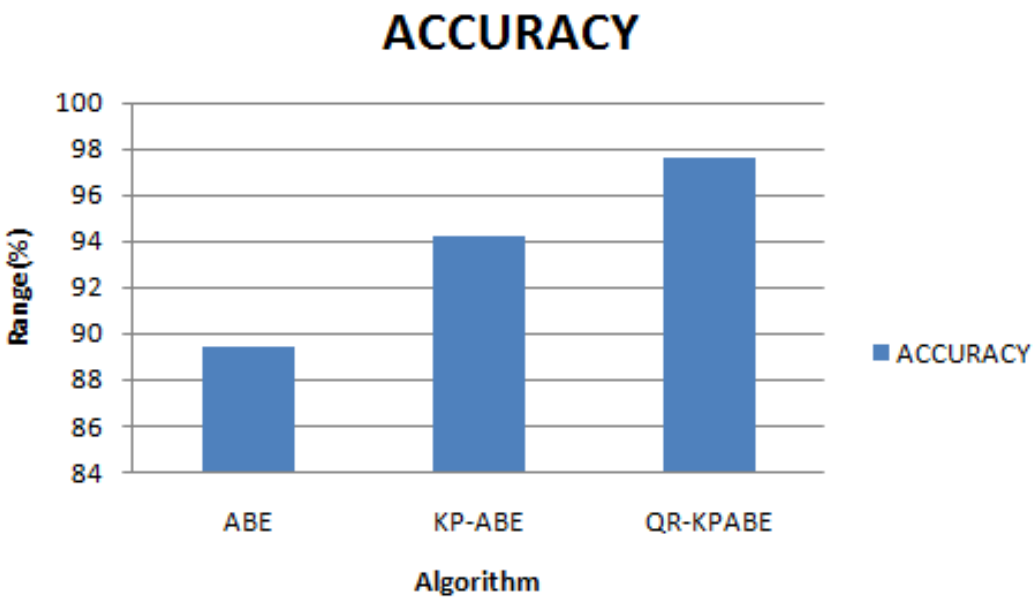

Fig.4. Accuracy Comparison for existing methods (ABE, and KPABE) and proposed method (QR-KPABE).

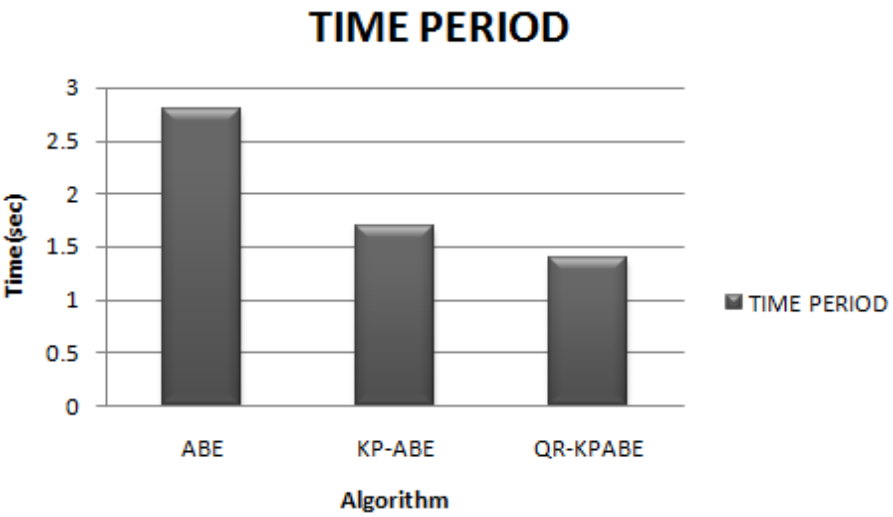

Fig .5. Time period comparison for existing methods (ABE, and KPABE) and proposed method (QR-KPABE)

Minimizing Data Storage and Data delivery Costs

Data Storage and data delivery costs are evaluated using the previous scheme in terms of password text size, user's secret key size, public key / information size, and size of message

revocation. The worst case analysis is used for this purpose. In this case each user has the potential to access a part of each owner's data.

Table 2: Storage of existing and proposed method

S.No	ALGORITHM	STORAGE
1	ABE	350 mb
2	KP-ABE	200 mb
3	QR-KPABE	150 mb

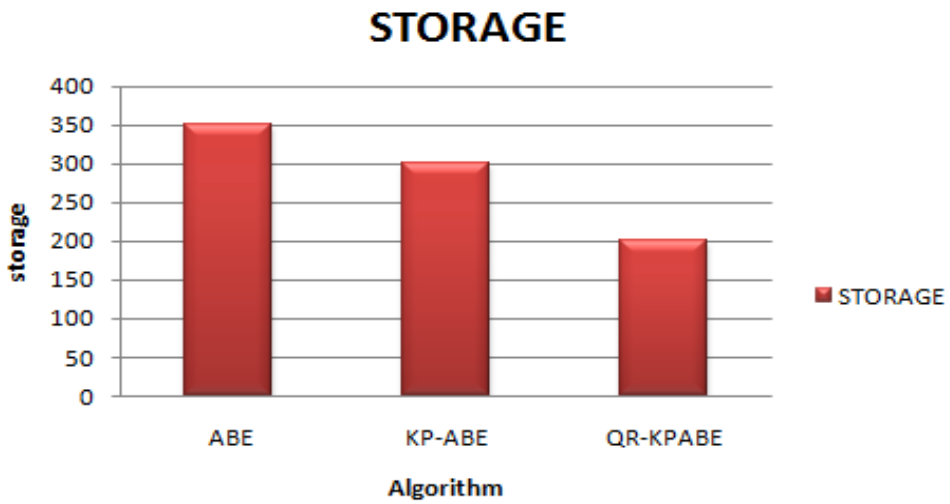

Fig.6. Storage Comparison for existing method (ABE, and KPABE) and proposed method (QR-KPABE).

Computation Cost

Computation cost charges from the suggest plan are examined utilizing hardware in the cloud condition. In the suggest plan, every datum proprietor utilizes the ABE conspire for setting, key age and repudiation, utilizing both and improved MA-ABE for encryption. To execute a work process the board framework, PUD and PSD utilizing ABBE. The plan is utilized for unscrambling of PSD clients while PUD clients receive the upgraded MA-ABE plot for decoding. Every AA utilizes an upgraded MA-ABE for setting, lock making and lifting. From this examination it is realized that the computational expense of this plan is lower than different plans. Additionally server figuring expenses are lower than different plans.

V. CONCLUSION

This study conferred a style of detail and detail on the implementation of a unique framework plan sharing safe personal medical records in cloud computing. Given that some cloud servers can be trusted, we tend to argue that to fully understand patient-centric thinking; patients must have complete management of their own privacy through encrypting their history files to allow smooth access. This framework addresses the typical challenges brought by many homeowners and users; in this case we tend to reduce the complexity of key management while ensuring privacy. We tend to use different types of ABE to write history files, so patients will allow access not only by private users, but also many users from the public domain with very different skills roles, qualifications and affiliates have proposed a new framework of safe sharing of personal health records in cloud computing.Considering some reliable cloud servers, we argue that in order to fully realize the patient-centered concept, patients must have complete control of their own privacy through their PHR file encryption to allow fine-grained access. This framework addresses the unique challenges brought by many PHR owners and users, in this case we greatly reduce the complexity of key management while increasing privacy guarantees compared to previous works. We use ABE to encrypt PHR data, so patients can allow access not only by private users, but also various users from the public domain with different professional roles, qualifications and affiliations.

In addition, we are improving the existing MA-ABE scheme to handle the removal of efficient and on-demand users, and to prove its security. Through implementation and simulation, we show that our solutions are scalable and efficient.

ACKNOWLEDGEMENT

I gratitude my humble indebtedness and sense of obligation to my research supervisor Dr.R.A.Roseline, for her invaluable assistance for the completion of this paper.

REFERENCES

1. Samir Bahsani, Tarik Nahhal," Encryption as a Service for Data Healthcare Cloud Security **",** IEEE, 2016.
2. Mr.K.A.Muthukumar,Dr.M.Nandhini, "Modified Secret Sharing Algorithm for Secured Medical Data Sharing in Cloud Environment", IEEE, 2016.
3. Fahad Saeed Alamri, Ki Dong Lee, "Secure Sharing of Health Data OverCloud", IEEE, 2015.
4. Alex Page, Ovunc Kocabas, Scott Ames, "Cloud-based Secure Health Monitoring: Optimizing Fully Homomorphic Encryption for Streaming Algorithms", IEEE, 2014.
5. Huda Elmogazy, Omaima Bamasak," Towards Healthcare Data Security in Cloud Computing", IEEE, 2013.
6. S. El-etriby, E. M. Mohamed, H. S. Abdul-kader, "Modern Encryption Techniques for Cloud Computing", ICCIT. 2012.
7. A. Kaur, M. Bhardwaj, "Hybrid Encryption for Cloud Database Security", UESAT, Vol-2, Issue- 3, pp737 - 741, May-Jun 2012. (http://www.ijesat.org)
8. V. Gampala, S. Inuganti, S. Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", USCE, Vol. 2, Issue 3, ISSN: 2231-2307, July 2012.
9. R. L. Rivest, L. M. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Sec.Comp. pp. 169-180, 1978.
10. R. 1. Rivest, A. Shamir, and 1. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Common. ACM, 21(2):pp.120-126, 1978.
11. C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University,2009,www.crypto.stanford.edulcraig.
12. C. Gentry, "Fully homomorphic encryption using ideal lattices", In M. Mitzenmacher, editor, SIOC, pp.169- 178.ACM, 2009.
13. M. Tebaa, S. EI hajji, Abdellatif EI ghazi,"Homomorphic Encryption Applied to the Cloud Computing Security" ,World Congress on Engineering (WCE) Vol. 1, July 2012.
14. B. Hayes, "Alice and Bob in Cipherspace", American Scientist, Vol. 100, pp. 362-367, Sep-Oct 2012, www.americanscientist.org
15. C. Gentry, "Computing Arbitrary Functions of Encrypted Data", ACM, Vol. 53 Issue 3, pp. 97-105, March 2010

AUTHOR PROFILE

Ramesh L is a Research scholar, PG and Research Department of Computer Applications. He did his M.Phil in Computer Science with specialization in the area of information security at Bharathiar University. He has published about 5 papers in international journals. His research interests include Networks, Information security, Cloud computing and IoT. He has presented papers in international conferences at Malaysia. He has been an active member of the society of digital information and wireless communications, internet society, Indian Academician and Researcher Association, International society for research and development, International Association of Engineers, International Economics Development Research Center, International Computer science and Engineering society and the institute of Research Engineers and Doctors.

Dr. R.A. Roseline is Associate Professor and Head, PG and Research Department of Computer Applications. She did her PhD in Computer Science in the area of Wireless Sensor Networks at Bharathiar University . She received M. Phil in Computer Science from Periyar University specialising in Mobile Adhoc Networks. She has published about 20 papers in international journals. She has completed a UGC Minor Project in Pollution monitoring using Sensor networks with a funding of 1.7 lacs. Her research interests include Sensor Networks, Cloud computing, Data mining and IoT. She had presented papers in international conferences at Australia and Malaysia .