International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

AN Effective PHR Based Secure Data Distribution using KC-ABE in Cloud Environment

Sangeetha.M, P.VijayaKarthik, Sivanesh Kumar. A

Abstract ***The objective of the research work is focused on cloud computing which is a developing design to give secure change among continuous applications. Secure information sharing is characterized as transmission of at least one documents profitably this procedure is utilized to share data's, characteristics, records among different clients and associations in secure mode and verifies from outsider clients. Usually it is finished by encryption and unscrambling process over private system. This kind of information sharing is finished by new innovation of key cipher text KC-ABE. It can give secure record transmission by having confined access innovation. This developing procedure has been checked in tolerant individual wellbeing record upkeep. These documents are recorded and recovered safely without access by unapproved clients. KC-ABE encryption framework is material to produce for adaptable and secure sharing of information's in distributed computing, which will reinforcement persistent wellbeing creating records in increasingly defensive manner. In KC-ABE strategy, the subtleties of patient are put away in KC-ABE server farm. In KC-ABE, Key backer just legitimize the entrance control and can't issue by the encryption. Along these lines the relating tolerant just reserve the options to get to this KC-ABE innovation. It gives more secure information sharing than other encryption framework. The fundamental utilization of this technique are High key age time and encryption time. It can accomplish less encryption time and key age time to improve productivity of KC-ABE.***

Keywords: KC-ABE, key issuer, Public key, cipher text, master key analysis.

I. INTRODUCTION

In the era of cloud computing, to shield information from spilling, clients need to encode their information before being shared. Access control is vital as it is the principal line of safeguard that avoids unapproved access to the mutual information. With the thriving of system innovation and versatile terminal, online information sharing has turned into another "pet, for example, Facebook, MySpace, and Badoo[1]. Similarly cloud is one of the most encouraging application stages to fathom the unstable growing of information sharing. In distributed computing, to shield information from spilling, clients need to scramble their information before being shared.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Sangeetha.M, Research Scholar Information Science and Engineering Sir M Visvesvaraya Institute of Technology, Bangalore India
P.VijayaKarthik, Professor Information Science and Engineering Sir M Visvesvaraya Institute of Technology, Bangalore India
Sivanesh Kumar. A, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai kas.sivanesh@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Access control is central that counteracts unapproved access to the mutual information. As of late, characteristic based encryption (ABE) has been pulled in considerably more considerations since it can keep information security and acknowledge fine-grained [2], one-to many, and non-intelligent access control. Cipher text-approach quality based encryption (CPABE) is one of doable plans which has substantially more adaptability and is more reasonable for general applications.

In distributed computing, authority acknowledges the client enlistment and makes a few parameters. Cloud service supplier (CSP) is the administrator of cloud servers and gives different administrations to customer. Information proprietor encodes and transfers the created cipher text to CSP [3, 4]. Client downloads and unscrambles the intrigued cipher text from CSP In existing system techniques are built using many encryption approaches like Attribute Based Encryption etc. If we maintain the data in cloud data Centre, it is so absolutely secured. Health and medical records are so complex. It needs more secure system to product from third parties. Otherwise it leads many illegal activities [5]. The existing system of using ABE in cloud computing is done by encrypt data using keys and attributes. Through internet anyone can download the details of patient. To avoid this drawback ABE technology is used to protect data by matching access user attributes with defined attributes [6]. If the scenario is matched only it will be accepted to access the data. That is, it is concluded that person is only the authorized user. Otherwise it will be rejected to access the data of health records.

Client downloads and unscrambles the intrigued cipher text from CSP. The common documents for the most part have progressive structure. That is, a gathering of documents are partitioned into various progression subgroups situated at various access levels. If the records in the equivalent various leveled structure could-based encoded by a coordinated access structure, the capacity cost of cipher text and time cost of encryption could be spared. distributed computing, a patient partitions his PHR [7] data M into two sections individual data m1 that may contain the patient's name, government disability number, phone number place of residence, and so forth. The medicinal record m2 which doesn't contain touchy individual data, for example, therapeutic test outcomes, treatment conventions, and activity notes. At that point the patient receives CPABE plan to encode the data m1 and m2 [8] by various access strategies dependent on the genuine need.

For instance, a going to doctor needs to get to both the patient's name and his therapeutic record so as to make an analysis, and medicinal specialist just needs to get to some restorative test results for scholastic reason in the related region, where a specialist must be a therapeutic scientist and the opposite isn't really valid. In order to overcome these drawbacks a new technology needs to improve the security level in cloud computing [9, 10]. In PHR system health records maintained in online. The health records included person's income, outcome timing experiment results, scanning data from wireless electronic devices. A new proposed system should be efficient and secure production for making use of patients. We can provide many new technologies by combining lot of cloud computing technologies.

II. KC-ABE Based Cloud modelling

Cloud computing and its modelling is completely comprised of PC assets and furthermore top level administrations. It is utilized to work fast without chance administration even in on request benefits. The primary piece of this distributed computing model is to safely move the any sort of documents. Usually distributed computing having three kinds of distributed computing models. SaaS is characterized as appropriation of numerous product applications. It is accessible consistently in on the web. There is no compelling reason to download. It resembles freeware administrations. Individuals can get to this administration by customer and server. It is relevant for office applications, Email applications, and games applications as shown in figure 1. Google and Microsoft organizations utilize this administrations through on the web. PaaS is a decent stage to grow more projects. Computer simulations are utilized related to handle estimations and lab concentrates to promote our comprehension of cloud material science. A wide range of models are utilized working at various goals, from the capacity to determine the definite synthetic and material science forms occurring in a solitary slope top cloud to an exceptionally parameterized representation of cloud in a territorial model or worldwide course model. Current comprehension of cloud procedures can be tried in the models by looking at yield from model runs initialized utilizing genuine information with field perceptions. Models can likewise be utilized to test the senility of the demonstrated framework to changes in the info parameters, and can assess the general significance of individual components. Most significant cloud material science studies have a huge demonstrating segment, with modelers engaged with arranging the estimation concentrates to be attempted to guarantee an incorporated methodology.

It is made mostly utilization of troubleshooting and altering procedure to the engineers. It is one of the fundamental reason for program engineers. It is helpful creating condition for creating organization apparatuses. GAE, Azure are instances of PaaS. IaaS is utilized as framework conveyance model. It goes about as goggle server, stockpiling system and OS. Distributed computing stage is utilized to get to the framework assets by the clients. In beginning time it is called as HaaS. It is unique in relation to past models. In KC-ABE model it comprises of cloud supplier information application, LAN, remote client, office specialist, emergency clinic and Internet. Through web cloud suppliers sent patient subtleties to the proper clients not instead of the others. Clinic additionally connected with web to get and keep up the patient wellbeing records. Through LAN office laborer and medical clinic has connected and shared the information to do the encryption and unscrambling process.

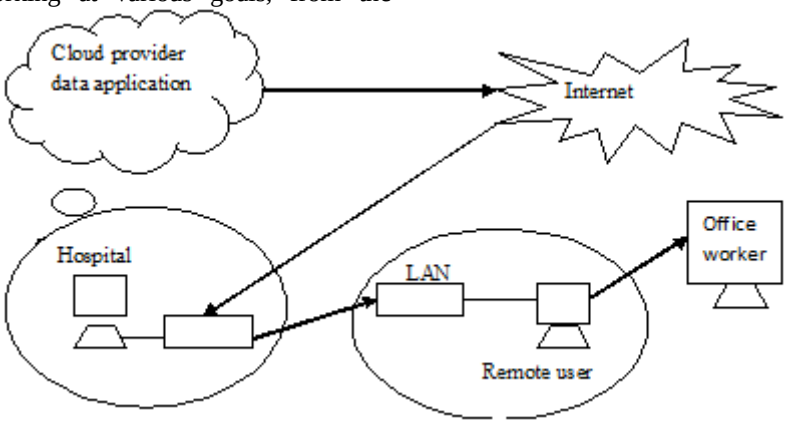

Fig 1. KC-ABE Cloud Modelling Approach

III. PHR Based Proposed Methodology

PHR is characterized as a lot of computer based instruments that enable individuals to access and arrange their long lasting wellbeing data and make suitable pieces of it accessible to the individuals who need it exactly. There isn't understanding or standard on what data a PHR ought to store. Some mutual data upheld by PHRs are issue records, techniques, significant sicknesses, supplier records, hypersensitivity information, home-checked information, family ancestry, social history and way of life, inoculations, meds and lab tests The KP-ABE & CP-ABE based encryption are imported here to get an new access control policy.

The proposed algorithm is named as KC-ABE where access structure tree has specified with a set of user attributes. This can solve the drawback of KP-ABE and reduce encryption time and key generation time. Cloud Simulation architecture has developed with layers. The components of each layer have a separate role to make communication by message passing. Using Cloud Simulation, we can generate private cloud data center using a virtual machine as shown in figure 2.

PHR stores delicate patient wellbeing data, thusly, access to PHR information must go along to security approaches characterized by the patient. In this work, we utilize the term solid to express the achievement of this security arrangements. Security is perceived as the most touchy part of a health record frameworks [10] and must be accomplished through a proper component. Security and protection of wellbeing information are one of the significant worries in e-wellbeing. Due that Cloud Server Provider for the most part is an outsider segment, wellbeing information ought to be safely put away to ensure the protection. Cloud servers are viewed as semi-trusted, on the grounds that they won't effectively attempt to get the data put away, yet they make for instance traffic examination, which may uncover information. Arrangements in the writing incorporate encryption of information before redistributing to cloud, access control, and gathering distinguishing pieces of proof to legitimate who is getting access.

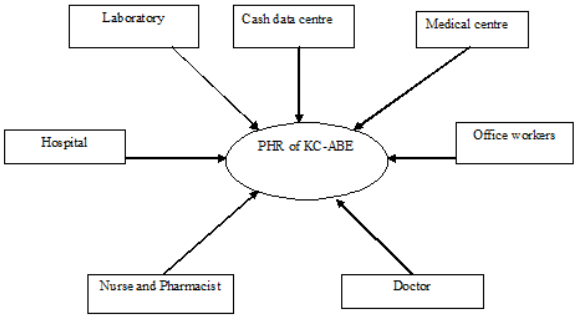

Fig 2. PHR Management System in distributed cloud

Our proposed model has been implemented with the help of CloudSim-3.0.3 simulation tool. It is simulation software designed with a virtual machine in which cloud data center has designed with required hardware, and it is applied real- time applications. The implementation and extension of cloud simulator are very easy technique [11]. In the principal stage looking through stage, we characterized an inquiry string and picked the database. As our survey question stays, we concentrated on looking through articles identified with PHR that spread three attributes (coordinated, dependable and cloud-based). For this reason, we characterized the pursuit string as "PHR AND (joining OR standard) AND security AND cloud". PHR is a word for looking through close to home wellbeing record system. Integration or standard alludes to term "coordinated". Data coordination is frequently base in the utilized of norms as shown in figure 3. To have solid data, protection must be characterized into medicinal services framework. Last term "cloud" establish the quest string for distributed computing. The database asset utilized was Google Scholar.

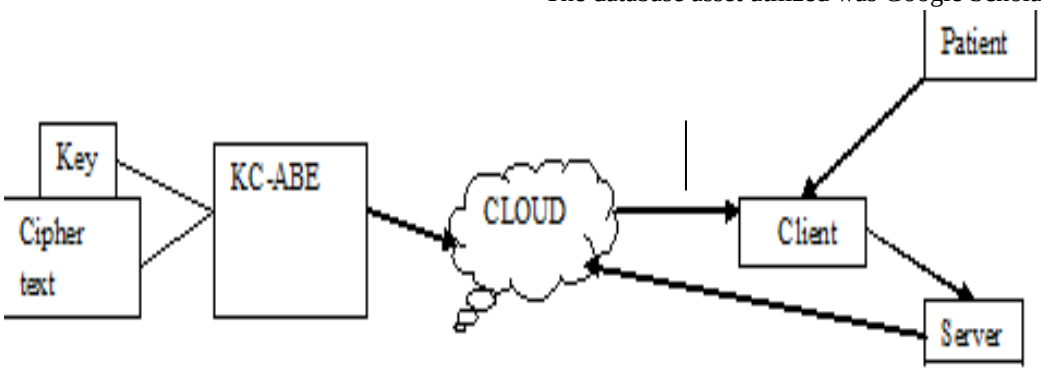

Fig 3. Flow Sequence of Patient Record in Cloud Centre

In above figure it is clarified how the subtleties are put away and kept up in cloud server farm. Customer has associated with both server and patient. Customer needs to get the subtleties of patients and after that it will be stacked safely in the server. Server has associated with cloud to keep up the information on demand. It will be gotten to with the assistance of key and figure content. On the off chance that the outsider keys are coordinated with the predefined keys of KC-ABE just it will be permitted to get to the patient subtleties. It implies that individual has proclaimed as approved individual to access and share the subtleties.

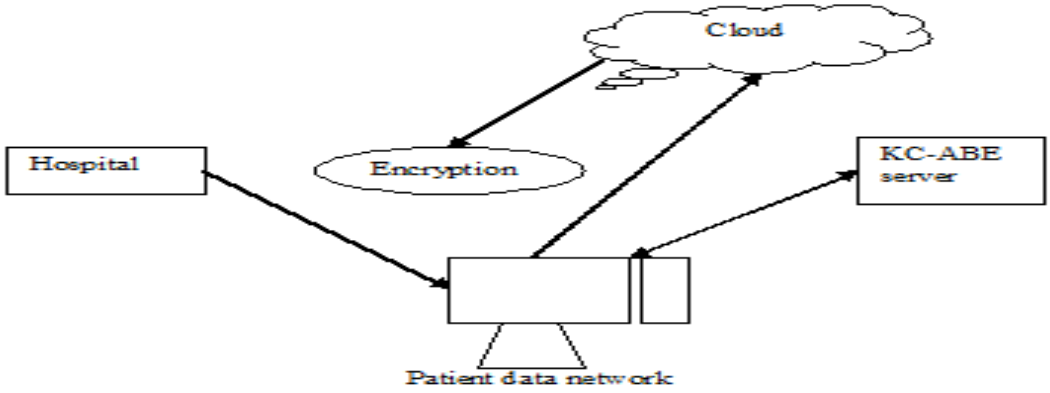

Fig 4. KC-ABE Data Set Retrieval

In above figure it is explained the flow process of data retrieval by KC-ABE. The details are maintained in KC-ABE server. It has connected with patient data network. If there any needs to come to get the details of patient it can be shared through patient data network. Before the retrieval process it should be encrypted by the encryption not by the key issuer. Whenever it needs by hospital it gets from patient network. This method provides more efficient data retrieval than other existing technology. It increases more efficiency and reduces key generation time and encryption time. This has to be done by following KC-ABE algorithm.

KC-ABE algorithm

1. Read both *PK* (public key) and *MSK* (Master secrete key)
2. *(PK, MSK)*
3. Source (SK) ←Key Generation (PK, MSK, S). The process responses

   PK, MSK and a established qualities of S and generates a secret key SK.
4. Patterned if linked and process to next key generation K_y
5. Squared if assessed (CT) ← Encrypt (PK, Bk, A).

   PK, Bk = {Bk1, . . . , Bkk } an ranked access tree
6. (Bki (i ∈ [1, k])) ← Decrypt (PK, CT, SK). The algorithm inputs PK, CT which comprises a combined access arrangement A, SK labelled by a set of qualities S. If the S competitions part of A, some gratified keys generate step 6
7. cki (i ∈ [1, k]) can be decrypted. If it contests the whole A, all the gratified keys can be decrypted. Then, the consistent files can generate step 7
8. mi (i ∈ [1, k]) will be decrypted with the gratified keys by the symmetric decryption algorithm
9. Finally the expected sequence of key can generate $\sum_{Ck}^{Bk} Mi[(Pk, Ct, Sk)]^{Pk}$

IV. KC-ABE Structure With Enhanced Encryption

To encourage the introduction in the underneath, we signify the above FH-KC-ABE plot as Basic FH-KC-ABE. We currently tell the best way to change the encryption procedure of Basic FH-KC-ABE plot so as to diminish computational intricacy. In figure content CT, some vehicle hubs are expelled from CT in the event that they don't convey any data about level hub, where the data means leaf hub, non-leaf hub, level hub, or transport hub in progressive access tree. That is, these vehicle hubs are expelled from CT on the off chance that they do not legitimately or in a roundabout way contain level hub. All the more decisively, we improve the part ˆC (x,y), j about transport hub in CT and KC-ABE as shown in table 1. Every other activity execute precisely as in Basic FH-KC-ABE. So as to make an obvious portrayal, we utilize a guide to further delineate the improved encryption process in the progression of ˆC (x, y), j of figure content and its results as shown in figure 5.

Table 1. Enhanced KC-ABE encryption

Element	KC-ABE	FH-KC-ABE	PHR	Results
Time taken for Encryption	99.02	89	97.03	90
Time taken for Decryption time	96.02	79.08	88.02	85
Scope value of PK	95.22	94.23	77.03	84
Scope value of MSK	93.33	98.33	66.6	78

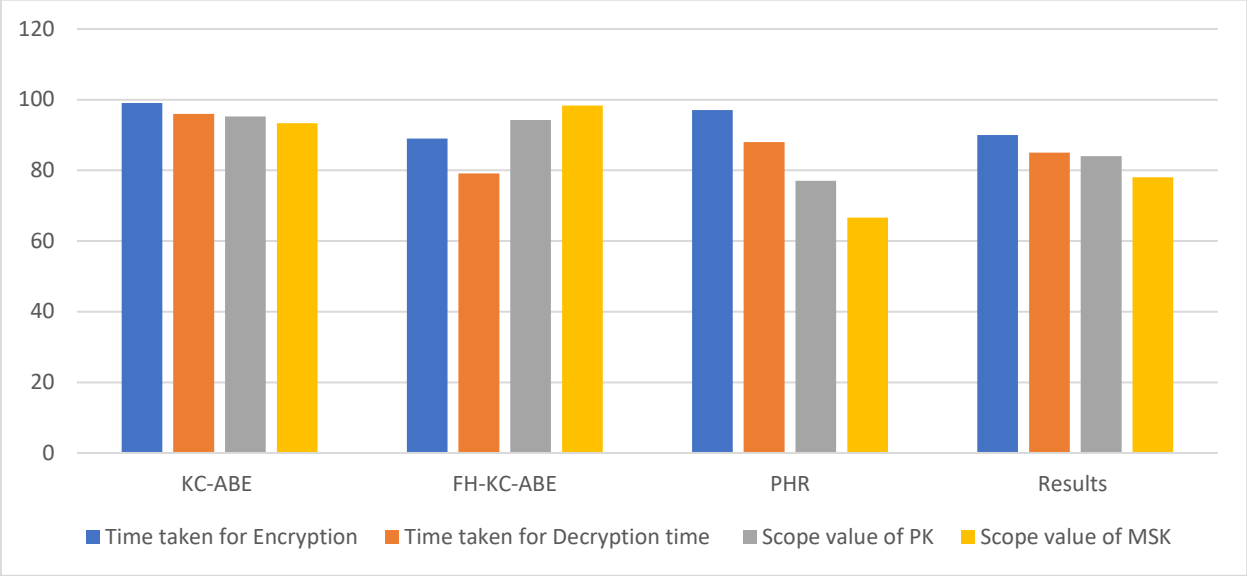

Figure 5. Metrics, value measures and scope of KC-ABE

V. CONCLUSION

Cloud security makes fundamental job to perform secure information sharing among more associations. Individual wellbeing record framework made with the assistance of distributed computing to create secure sharing. It has been put away with everyday patient data. It must be kept up with standards and guidelines over the web. Part of encryption strategies are proposed to verify share data of patient wellbeing records. KC-ABE is utilized to keep up and share the patient subtleties through coordinating key and traits. It is one stage proficiently upgraded by methods for key guarantor just access encryption process. Through this proposed framework it makes less key age time than other encryption methods. Along these lines KC-ABE has been demonstrated to apply the safe information sharing of patient wellbeing subtleties.

REFERENCES

1. M.Sangeetha, P.Vijaykarthick, "To proide a secured access control by using key-ciphertext attribute based encryption" IEEE International Conference on Intelligent Techniques in Control, Optimization & Signal Processing, Mar. 23 – 25, 2017, Srivilliputtur, INDIA.
2. Wagh Rohini H., Pimparkar Vrushali S, Pawar Pratiksha S, Avhad Sonali S, Prof. Kapadnis Jagdish Y, "Secure Sharing of Personal Health Records in Cloud computing using Smart card" Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-3 , 2016 ISSN : 2454.
3. Mr.Prasad P S1, Dr. G F Ali Ahammed, "Attribute-Based Encryption for Scalable and Secure Sharing of Personal Health Records in Cloud Computing",International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5038-5040
4. Chaudhari Swapnil H., Mandre B.R., "Secure Data Retrieval based on Attribute-based Encryption in Cloud," International Journal of Computer Applications (0975 – 8887) Volume 134 – No.13, January 2016.
5. J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244,Apr./Jun. 2016
6. Zhihua Xia 1,2,3, Liangao Zhang , "Attribute-Based Access Control Scheme with Efficient Revocation in Cloud Computing," IEEE transactions of Information Science & Technology, Nanjing, 210044, China, volume 12, july 2016.
7. Sanjay K. Madria, "Security and Risk Assessment in the Cloud ," Missouri University of Science and Technology published by IEEE transactions on computer society, vol 16, September 2016.
8. P.Datta,R.Dutta,and S.Mukhopadhyay, "Fully secure online/offline predicate and attribute-based encryption", in Information Security Practice andExperience,ser.Lecture Notes in Computer Science,j.Lope and Y.Wu, Eds.Springer International Publishing 2015, ol.9065,pp.331-345.
9. H. Wang, "Identity-Based Distributed Provable Data Possession in Multicloud Storage," IEEE Trans. Services Computing, vol. 8, no. 2, 2015, pp. 328–340.
10. V. Khadilkar et al., "Secure Data Processing over Hybrid Clouds," Bull. IEEE Computer Society Technical Committee Data Eng., vol. 35, no. 4, pp. 46–54, , 2015.
11. Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3, " A Survey on Attribute Based Encryption
12. Scheme in Cloud Computing",International Journal of Advanced Research in Computer and Communication Engineering" Vol. 2, Issue 11, November 2013
13. Ronald L.Krutz and Russell Dean Vines, "Cloud Security-A Comprehensive Guide to secure Cloud Computing," WILEY-INDIA Publications , Edition 2010.