# SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS IN LARGE NETWORKS USING ATTRIBUTES BASED ENCRYPTION

**G.Deepa,R.Kayalvizhi, P.Anitha**

**Assistantprofessor,departmentofcomputerscience**

**DhanalakshmiSrinivasancollegeofartsandscienceforwomen(autonomous)**

**Perambalur**

## Abstract

Outstanding Fitness Record is an electronic application used by patients to keep up and manage their prosperity information in a private, secure and mystery atmosphere. In appropriated figuring, cloud providers go probably as an outcast for the information exchange of individual prosperity records. Notwithstanding the way that this advancement supports successful organization and the sharing of patient's own special prosperity record, there are wide assurance worries, for instance, the presentation and transparency of fragile prosperity information by unapproved customers. To give security and insurance, it is essential to scramble the data preceding re-examining and just affirmed customers with significant attributes should be allowed to get to the data. Hiding the customers' information is furthermore critical while getting to data over the association. Moreover to reduce the key organization unpredictability of data owners, singular prosperity records are requested into various security spaces. To achieve fine-grained and versatile data access control for PHRs, to impact attribute based encryption techniques to encode each patient's PHR record. Not equivalent to past works in secure data re-examining, to base on the various data owner circumstance, and partition the customers in the PHR structure into various security zones that colossally diminishes the key organization unpredictability for owners and customers. A genuine degree of patient security is guaranteed at the same time by manhandling multiauthority ABE. Our agreement in like manner engages dynamic change of access methods or record credits, maintains valuable on-demand customer/property disavowal and break-glass access under emergency circumstances to cover the customer information, baffling approval through Attribute-Based Encryption method and fine-grained data access control through AES are gotten. This mix gives a genuine degree of assurance and security for the PHR record. This preparation enables the dynamic change of access approaches or best credits and on-demand customer repudiation. Expansive test and execution inspection show that the proposed contrive is capable to the extent security and pledge.

***Keywords:*** *Attribute Based Encryption (ABE), Personal Health record (PHR), anonymous authentication, Advanced Encryption Standard (AES).*

## 1. INTRODUCTION

Distributed computing is an arising innovation where all the IT assets are given as administrations through web. Significant Service models, for example, Software as a Service, Platform as a Service and Infrastructure as a Service that design cloud, all of which mean a Service Oriented Architecture [1]. Cloud administrations are been embraced generally because of its cost viability and adaptable assistance conveyance stage. Lately, Personal Health Records have created as the arising pattern in the medical care innovation. Cloud climate permits a patient to make, oversee, and control his/her own wellbeing data from anyplace through the web, which has made the capacity, recovery and sharing of the clinical data more effective. Particularly, every patient is guaranteed a full command over their clinical records. A patient can divide their subtleties between wide scope of clients, including medical care suppliers, relatives or companions dependent on their necessities or ability. While it is energizing to have helpful PHR administrations for everybody, there are numerous security and protection hazards in cloud climate. Because of the significant expense of building and keeping up specific server farms, numerous wellbeing record administrations are moved to or given by outsider specialist organizations, for instance, Google drive, iCloud and Dropbox [2]. For the most part, cryptography based encryption and decoding strategies are utilized for security [3].

RSA calculation can be utilized to encode the information before it is reevaluated in the cloud. Here to recuperate the information, a client should demand the critical chief to produce the public key given that the client should be an approved individual [4]. Past investigates on security uncover that, to guarantee security in cloud three insurance plans: Hash age calculation, Captcha calculation and AES calculation have been broadly utilized [5]. Presently, advanced mark is utilized for confirmation and AES encryption calculation for information classification [6]. The primary concern is about whether the patients could really control the sharing of their delicate individual wellbeing data (PHI), particularly when they are put away on an outsider worker which individuals may not completely trust. The PHR framework can restrict the entrance control of clients to the application. To accomplish this, the entrance strategies are made partner with the different arrangement of client trait. To develop this worry, information is scrambled under a bunch of qualities so different clients who have appropriate keys just can get to the information [7]. This possibility leads for an effective encryption and key administration. A protected multi proprietor plan can likewise be forced in the multi access network where the information can be shared safely in the untrusted cloud [8].

While it is energizing to have advantageous PHR administrations for everybody, there are numerous security and protection hazards which could hinder its wide appropriation. The primary concern is about whether the patients could really control the sharing of their delicate individual wellbeing data (PHI), particularly when they are put away on an outsider worker which individuals may not completely trust. From one viewpoint, despite the fact that there exist medical care guidelines, for example, HIPAA which is as of late changed to fuse business partners [4], cloud suppliers are typically not covered substances [5]. Then again, because of the high estimation of the touchy PHI, the outsider stockpiling workers are regularly the objectives of different vindictive practices which may prompt presentation of the PHI. As a renowned episode, a Department of Veterans Affairs information base containing touchy PHI of 26.5 million military veterans, including their federal retirement aide numbers and medical issues was taken by a representative who took the information home without approval [6]. To guarantee understanding driven security authority over their own PHRs, it is fundamental to have fine-grained information access control components that work with semi significant workers.

As quality Based Encryption has the exceptional component of forestalling client plot to a huge level to accomplish fine-grained admittance control, a Cipher text Attribute Based Encryption (CP-ABE) is utilized [9]. Property based encryption (ABE) is a kind of open key encryption in which the mystery key of a client and the ciphertext are needy upon ascribes [10]. For the most part search over scrambled archives is a troublesome, tedious cycle where machine coded hereditary advancement calculations can be utilized to lessen the overhead [11].Thus, these are a portion of the executions which secure the cloud related information and a few analysts are contributing towards cloud security, still use of encryption strategies on cloud needs certain upgrades.

The approved clients may either have to get to the PHR for individual use or expert purposes. Instances of the previous are relative and companions, while the last can be clinical specialists, drug specialists, and analysts, and so forth allude to the two classes of clients as close to home and expert clients, separately. The last has conceivably huge scope; should every proprietor herself be straightforwardly liable for dealing with all the expert clients, she will handily be overpowered by the key administration overhead. Likewise, since those clients' entrance demands are by and large surprising, it is hard for a proprietor to decide a rundown of them. Then again, not the same as the single information proprietor situation considered in the vast majority of the current works [8], [9], in a PHR framework, there are various proprietors who may scramble as indicated by their own specific manners, conceivably utilizing various arrangements of crypto-realistic keys. Letting every client get keys from each proprietor who's PHR she needs to peruse would restrict the availability since patients are not generally on the web. An option is to utilize a focal position (CA) to do the vital administration for all PHR proprietors, yet this requires a lot of trust on a solitary power.

In this project, attempt to contemplate the patient-driven, secure sharing of PHRs put away on half significant workers, and spotlight on tending to the muddled and testing key administration issues. To secure the individual wellbeing information put away on a semi confided in worker, to receive quality based encryption (ABE) as the primary encryption crude. Utilizing ABE, access strategies are communicated dependent on the qualities of clients or information, which empowers a patient to specifically divide her PHR between a groups of clients by encoding the document under a bunch of properties, without the need to know a total rundown of clients. The complexities per encryption, key age, and unscrambling are just direct with the quantity of qualities included. Be that as it may, to incorporate ABE into a huge scope PHR framework, significant issues, for example, key supervision adaptability, dynamic approach refreshes, and proficient on-request repudiation are nontrivial to address, and remain to a great extent open modern. To this end, to make the accompanying fundamental promises:

1. To propose a novel ABE-based structure for calm driven secure sharing of PHRs in disseminated figuring conditions, under the multiword settings. To address the key organization challenges, to nicely segment the customers in the structure into two kinds of spaces, to be explicit public and individual zones. In particular, the prevailing part proficient customers are supervised distributive by quality specialists in the past, while each owner only necessities to manage the keys of not many customers in her own space. In this way, our structure can concurrently deal with different kinds of PHR sharing applications' necessities, while causing unimportant key organization overhead for the two owners and customers in the system. Additionally, the structure executes create access control, handles dynamic methodology invigorates, and gives break-glass induction to PHRs a work in progress circumstances.

2. To give a serious assessment of the multifaceted nature and flexibility of our proposed secure PHR sharing course of action, with respect to various estimations in computation, correspondence, storing, and key organization. In like manner balance our arrangement with a couple past ones in multifaceted nature, versatility and security.

## EXISTING SYSTEM

A couple of security plans are under preparing for data sharing on untrusted laborers. Those techniques license data owners to store the mixed records in untrusted accumulating and pass on the contrasting disentangling keys solely with the affirmed customers. Thus it is acknowledged that unapproved customers can't get acquainted with the information reports set aside on the laborers. In these models AES is used as the fundamental encryption unrefined.

SriVarsha et al., future an encryption methodology which uses the substitution and change strategy. Here the key idea is planning the data reliant on properties which support access control and AES for ensuring about the records [10].

Randeep Kaur et al., researched cloud security reckoning and had an assessment on connection of symmetric counts dependent on different limits. Their test outcomes show that AES is faster and secure count [12]. AES has been realized commonly in various stages and it is pursued for some security applications.

Shaik Hussain et al., endeavored to repudiate the passageway assent of the customer using two strategies to be explicit ABE and Proxy Re Encryption (PRE) in p2p conveyed capacity. This makes the data secure on the cloud. Existing techniques are expensive in regards to time and viability when stand out from AES [13].

VikasVitthalLonare et al., have proposed a method Secure Hash Algorithm (SHA) for viable approval where the archive is mixed using AES to ensure scattered duty. The sender hashes the record and transported off the recipient. The recipient by then hashes the got record and a while later checks for the hashes arrange [14]. As SHA supporting in making a more expanded hash worth and it is more accident safe, it is used in all over.

Jasim et al., separated the show of encoded data base and contemplated that the introduction of scrambling gigantic data base using hilter kilter key figuring is lower when appeared differently in relation to symmetric-key computation [15]. Thus lopsided key counts can be used for scrambling short key worth.

All things considered, log archives record the passage nuances of the data customer. Since the log records are not mixed, the security isn't saved. As this reveals the customer puzzling nuances, there is no security for prosperity records. This prompts wrong check and data vulnerability.

Fundamentally SHA is used for approval as it jam data consistency and semantic assessments of components in the wake of hashing.

Disregarding the way that it is extensively used, it provides only a solitary guidance hash. So it can't maintain encryption and unscrambling of data over limit. Other than this count is all the more moderate computational estimation and has known security shortcomings.

In couple of systems like prosperity records the board a central position (CA) has been assigned to perform key organization of master customers. Regardless, that again requires an overabundance of trust on single position. Single authority may encounter the evil impacts of key over mixed data. Hereafter it is central purposes of using new encryption configuration called Attribute Based Encryption (ABE). In ABE, it is the characteristics of the customers or the data that picks the passage draws near, which enables a patient to explicitly split her PHR between a meetings of customers by motocross the record under a lot of properties, without the need to know an absolute summary of customers. Thusly, the amount of characteristics included chooses the complexities in encryption, key age and unscrambling. The Multi Authority Attribute Based Encryption plot is used to give different force based permission control instrument.

Similar number of researchers inspected various figurings and blends of different procedures on data security in cloud atmosphere, a sensible blend of computations for confirmation and endorsement may help in capable adaptable secure data storing.

## SECURITY IDEAL

In this project, to accept the laborer to be semitrusted, i.e., authentic yet curious as those in [28] and [15]. That infers the specialist will endeavor to find whatever amount of secret information in the set aside PHR records as could sensibly be normal, yet they will truly follow the show when everything is said in done. Of course, a couple of customers will moreover endeavor to get to the records past their preferences. For example, a medication store may have to get the cures of patients for exhibiting and boosting its advantages. To do thusly, they may interest with various customers, or even with the specialist. In like way, to expect each social event in our structure is preloaded with a public/private key pair, and substance affirmation should be conceivable by regular test response shows.

## OUR CONTRIBUTION

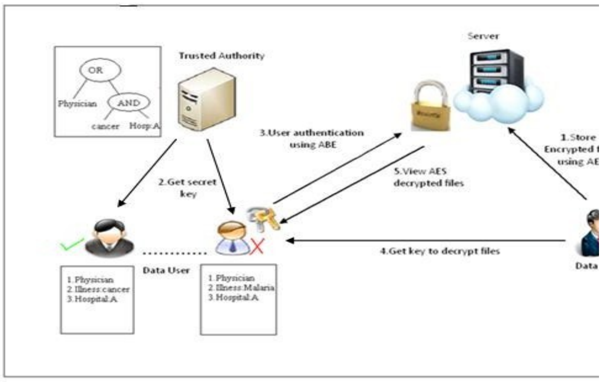

Fig.1 Architecture of user anonymous authentication system

Government assistance records are kept up in the spread atmosphere. To ensure the patient's control access over their own PHRs, one of the promising methods is encoding the PHRs before reexamining. To ensure the data security ABE plot is used.

As there is an open doors for intruders to smell the sign of endorsed customers, fragile data set aside in distant laborers may be mishandled. In various structures, a certain assumption essential is that each customer has some surprising distinctive information related with them which they can use to show what their personality is. Similar number of affirmation shows are fundamental, the correspondence can be conveniently seized and nuances can routinely be gotten too distantly without consideration regarding the owner. To hinder the malignant customers, baffling check can be upheld using the valuable cryptography structure. To achieve this, ABE technique is used to scramble customer approval nuances. As of our point by point study ABE was not now used for approval. Regardless, our test examination exhibited that ABE supports a successful obscure approval. Using ABE, access approaches are imparted subject to the characteristics of customers or data, which enables a patient to explicitly split their PHR between a lots of customers by encoding the record under a lot of properties, without the need of knowing all out overview of clients. The encryption and unscrambling cycle will be done using Advanced Encryption Standard. AES is used as the primary encryption rough. The encryption is done in decided number of rounds. This makes the data more secure.

Data owner: This is the tookstoring endorser who needs to move their data substance to the disseminated stockpiling system after encryption. The encoded substance can be granted to proposed recipients who have sufficient confirmations. The Patients can get to the records at whatever point and any spot required. The approval standard achieved to get to the prosperity record subject to the assent permitted. Here various data owner circumstance is proposed to manage the prosperity record in sensitive manner. A key organization perspective is proposed to attain the encryption over the attributes. Multifaceted nature is extended among owners and the end customers. The passage approval is denied from different customer as for clinical records for various purposes. Fig 2. Depicts the pattern of mixed data accumulating and recuperation.

## FUTURE WORK

The essential target of this framework is to give secure patient-driven PHR access and powerful key union. The key idea is to segment the structure into different security regions, for instance, public and private as demonstrated by the assorted customer's data access necessities. The character prosperity record includes customers who make access reliant on their master occupations, for instance, subject matter experts, chaperons and clinical examiners. Before long, a prosperity can be wanted to an independent region in the overall population, for instance, the clinical consideration, government or insurance zone. The different customers make gets to PHRs subject to get to rights alloted by the owner.

Relatively few past researchers have used SHA for confirmation, yet it can't ensure the security at raised level. In the PHR accessibility, the endorsement of prosperity record ensures huge degree of security. Resulting to moving the prosperity record into the specialist, the owner recuperates the key by means of the mailing station id to get to the principal data. The data are mixed and moved into the cloud specialist. Each data owner (e.g., understanding) is her own personal accepted power, who uses an ABE system to manage the secret keys and access advantages of customers in record. With the ultimate objective of individual territory access (PSD), each PHR report is set apart with its data attributes, while the key size is only honest with the amount of record classes a customer can get to. Since the amount of customers in a PSD is much of the time close to nothing, it diminishes the weight for the owner. Data owner needs to know the intrinsic data properties of PSD for scrambling the data. Considering the customer approval record access is upheld and sensitive property is covered using ABE Technique.

The owners move AES-mixed PHR archives to the specialist. Each owner's PHR record is mixed using AES in ABE system. The ABE, under a particular fine grained and employment based induction and under a picked set of data credits grants permission to customers in the PSD. In Key methodology Attribute Based Encryption (KP-ABE) the passage structure is connected with the key and the properties are connected with the code text which allows only the avowed customers to disentangle the code text. Thus the Key plan Attribute Based Encryption is grasped for singular space [16].This offers security to the delicate info set aside on the cloud. It moreover lessens an enormous section of the computational overhead to cloud laborers. Just affirmed customers can unscramble the PHR records.

The structure upholds break-glass access under emergency circumstances. The clinical staffs can have brief access when an emergency happens to the patient [17]. Around then the clinical staff requests and obtains the secret key from the emergency department(ED). The ED needs to affirm the clinical staff who requests for the key. This paper contains about the audit of Health record in the cloud specialist and proposed ABE count for approval. This idea urges to convey the examination report with new security method.

**ABE Algorithm**

Quality based encryption is a for the most part late technique that rethinks the possibility of public-key cryptography. In standard public-key cryptography, a message is encoded for a specific beneficiary using the recipient's public-key. Character based cryptography and explicitly character based encryption changed the ordinary cognizance of public-key cryptography by allowing the public-key to be an optional string, e.g., the email address of the beneficiary. ABE exceeds any and all expectations and portrays the character not atomic yet rather as a lot of properties, e.g., occupations, and messages can be encoded concerning subsets of characteristics or systems described over a lot of attributes (ciphertext-technique ABE - CP-ABE). The essential issue of interest is, that someone ought to just have the choice to unscramble a ciphertext if the individual holds a key for "organizing credits" (more underneath) where customer keys are continually given by some trusted in social event. This estimation incorporates 4 modules including key age.

agreement (I,U)- >(PK,MK) - The plan figuring takes security limit I as wellsprings of data and a universe portrayal U, which describes the course of action of allowed credits in the structure. It yields the public limits public key PK and the master secret key MK.

Encrypt(PK,M, S)- >CT - Encryption computation takes public limits PK, a Message M and a lot of characteristics S as data sources and yields a ciphertext CT related with the quality set.

KeyGen(MK,A)- >SK - The key age estimation conveys a private key SK by taking wellsprings of data expert secret key MK and a passageway structure A. Here the yield is connected with the attributes.

Decrypt(SK,CT)- >M - The interpreting count recognizes a private key SK which is connected with access structure An and ciphertext CT that is similarly associated with property set and gives a message M if S satisfies A.

**Algorithm 1: Setup phase**

Input: $P \in G1$ and $Q \in G2$, a set of attributes H

Output: Public Key PK(G1,G2, P, Q, $P\delta$, $\gamma$ ), f{H1……HN},

Master private Key MK($P\alpha$)

```
Choose at random : $\alpha$ and $\delta \in Z r$
$P\delta \leftarrow [\delta]P$
$P\alpha \leftarrow [\alpha]P$
$\gamma \leftarrow eopt(Q,P)\alpha$
for $i \leftarrow 1$ to #H do
    Generate a point $Hi \in G1$
end for
PK $\leftarrow$ (G1,G2, P, Q, $P\delta$ , $\gamma$ ), {H1……HN}
MK $\leftarrow$ ($P\alpha$)
return PK,MK
```

**Algorithm 2: Encryption phase**

Info: A message M, PK, an entrance structure S given as a u x t

Framework and $I \subset \{1, 2,\dots\dots,u\}$ as $I = \{i : \rho(i) \in H\}$

Data: MK and a bunch of client's ascribes H

Yield: A private key SK = {K, L, K1, … ..,KvH}

```
Choose at irregular $\in Fr$
$K \leftarrow P\alpha + [\ ] P\delta$
$L \leftarrow [\ ] Q$
for I = 1 to vH do
    $Ki \leftarrow [\ ]Hi$
end for
SK $\leftarrow$ {K, L,K1,… .,KvH}
return SK
```

**Algorithm 4: Decryption Phase**

Info: CT and its lattice S, SK and its arrangement of traits H

Yield: Plaintext M (if the characteristics in SK fulfill the ciphertext's approach)

```
$\hat{s} \leftarrow$ Reduce the grid S by eliminating the lines and sections inconsequential with the qualities in H
Find the determinant $\leftarrow Det(S) \in Fr$
Calculate the vector $\omega$ as the primary column of S1
for I = 1 to v do
    $C\,\omega i \leftarrow [\omega i]\, C$
```

Yield: Ciphertext CT = {S,C,Cd, (C1;D1), , (Cu,Du)}

```
Generate an irregular vector u = (s, y2, yt) $\in Z r$.
Calculate the segment vector $\lambda = Sut$
Generate another irregular vector x = (x1, ,xu) $\in Z r$.
$C = M \oplus H1\ (\gamma s)$
$K\rho(i)\omega i \leftarrow [\omega i]K\,\rho(i)$
End for

M = $C \oplus H1\ ((e\ (Cd,CiK)\ .\ e(L, \sum K\rho(i)\omega i\ ))1/\rho)$
Bring M back
iεH C ωi ) . ∏
iϵH e(Di,
Cd = [s] Q
For I = 1 to u do
    $Ci \leftarrow [\lambda i]\, P\delta - [xi]\, H\rho\ (I)$
    $Di \leftarrow [xi]\, Q$
end for
CT $\leftarrow$ {S,C,Cd, (C1,D1),… .., (Cu,Du)}
bring CT back
```

Algorithm 3: Key generation phase

## 4. RESULT AND DISCUSSION

Around 2500 KB of text intelligences were assembled and execution examination of ABE figuring was finished by unravelling the chronicles using different estimations as organized in Table.1. The examinations were done using a structure with Pentium-IV processor, 80GB RAM. Table 1 shows the time taken by different encryption computations for different size of data. The test outcomes reveal that Advanced Encryption Normal (AES) is quicker and generally proper for colossal data bases (Fig.3). Various counts can be masterminded as DES, 3-DES, RC4, in conclusion the Blowfish figuring.

Size is immediate with the amount of attributes in that customer's secret key. These show our arrangement is more adaptable than existing works.

Along these lines, the ABE plot is faster and more sensible for the time costs of key age, encryption, and interpreting measures are generally immediate with the plan of properties. From the system point, each data owner uses the ABE plot for game plan, key age, Encryption and Revocation and each PSD and PUD customer unscrambles the archive in less time. The Attribute Authority (AA) is used for game plan, Key Generation, User Revocation. On the off chance that there should be an event of 50 credits, they all take under 0.5s.Hence from the results, ABE is more versatile and capable to complete in Personal Health Domain as it decreases the multifaceted nature of key organization.

## CONCLUSION

Disregarding the way that it is shown that hashing based check estimations can give security as the key created by them can't be repeated, our tests exhibited that ABE is more secure. Researchers have found weakness in SHA1 and are presented to affect attack which is speculatively broken. Thusly it is seen as not, now secure. To proposed a novel arrangement of secure sharing of individual prosperity records in distributed computing. Contemplating to some degree reliable cloud laborers, to fight that to totally comprehend the patient-driven thought, patients will have full oversight of their own security through encoding their PHR records to allow fine-grained induction. The structure watches out for the fascinating challenges brought by various PHR owners and customers, in that tp uncommonly decrease the multifaceted idea of key organization while update the security guarantees differentiated and past works. To utilize ABE to encode the PHR data, so patients can allow access by near and dear customers, yet also various customers from public zones with different master occupations, capacities, and affiliations But ABE isn't conveyed to crash attack considering the way that the keys are made from different course of action of properties. To use ABE for data encryption and approval, a testing can be performed on the security of the data later on work. This work can be loosened up to encode media data and to settled check in appropriated atmosphere.

## REFERENCES

[1] Gurpreet Singh, Supriya. April 2013, "A Study of Encryption Algorithms for Information Security", *International Journal of Computer Application*, Vol.67,No.19,33-38.

[2] Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou and Robert H. Deng. February 2014, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", *IEEE Transactions on Parallel and Distributed Systems*, Vol.25, No.2.

[3] Rashmi Nigoti, ManojJhuria, Dr.Shailendra Singh. 2013, "A Survey of Cryptographic Algorithms for Cloud Computing", *International Journal of Emerging Technologies in Computational and AppliedSciences (IJETCAS),* 141-146.

[4] Pooja R. Vyawhare, Prof.Namrata D.

Ghuse. 2015, "User Anonymous Authentication Scheme for Decentralized Access Control in Clouds", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol.6, No.3, 2441-2447.

[5] SumitaLamba, Ajaykumar. February 2014, "An approach for ensuring security in cloud environment", *International Journal of Advances in Computer Science and Technology (IJACST),* Vol.3, No.2, 92-95..

[6] Dhaval Patel, M.B.Chaudhari. June 2014, "Data Security In Cloud Computing Using Digital Signature", *International Journal for Technological Research in Engineering,* Vol.1, Issue 10, 1177- 1180.

[7] Y.B.Gurav, ManjiriDeshmukh, "Scalable and Secure Sharing of Personal Health records in Cloud Computing using Attribute Based Encryption", International Journal of Science and Research (IJSR), Vol. 3 Issue 7, ISSN:2319-7064, July2014.

[8] Shucheng Yu, Cong Wang, Kui Ren and Wenjing Lou. 2010, "Attribute based data sharing with attribute revocation",*ASIACCS,10*.

[9] Y.Pavani, Rajasekar, D.Krishna. 2014, "Cloud Storage with data sharing and security for Multi access network by Using AES", *IJESC*,536-539.

B.SriVarsha, P.S.Suryateja. 2014, "Using Advanced Encryption Standard for Secure and Scalable Sharing of personal Health Records in Cloud", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 5(6), 7745-7747