International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Privacy Protection for E-Health Records Over Mobile Cloudlet

M.Bhargavi, P.Bharath Siva Varma

Abstract*: Preparing of therapeutic data for the foremost half incorporates operation, data storage and data sharing etc. Usual social services framework often wants the conveyance for restorative data to cloud which incorporates purchasers touchy information and cause correspondence. For intents and functions, restorative data sharing is basic and testing issue. Be that because it could, there has been protection worries as on the brink of home well-being information can be bestowed to those outsider servers, and to unapproved parties. To ensure the patient's authority over accessing their Personal Health Records (PHR), it is a promising strategy to cipher the PHR before reappropriating. However issues, as an example; danger of protection introduction, ability in key administration, adaptable access, and skillful client denial, have remained the foremost very important difficulties towards accomplishing fine-grained, typographically approved data gets to regulate. During this paper, we tend to propose a completely unique patient driven system and a set of parts for data gets regulate to PHR place away in semi confided in servers. To accomplish fine-grained and versatile data gets to regulate for PHR, we tend to influence Attribute based encryption coding (ABE) strategies to cipher each patient's PHR document. Distinctive in respect to past works in secure information redistributing, we tend to center on various data owner state of affairs, and gap the purchasers within the PHR frame-work into numerous securities areas that very lessens the key administration many sided nature for proprietors and purchasers transportable cloud let. A high-level of patient protection is ensured whereas by misusing multi-specialist ABE. Our commit to boot empowers dynamic modification of access strategies or record qualities, bolsters effective for the asking client/characteristic repudiation and break glass access below crisis things. Broad scientific and trial results as displayed that demonstrate the protection, ability, and productivity of our set up.

Keywords* : Attribute based encryption, Access control, Cloudcomputing, Medical data assistance, Personal health information.

I. INTRODUCTION

As of late, Personal health record (PHR) has risen as a patient driven model of well-being data trade. A PHR administration enables patient to make, oversee and control her own well-being data in one spot through web, which made capacity; recovery; and sharing of medicinal data progressively productive. Particularly; every patient guarantee the full control of her therapeutic records; and can impart her well-being data to a wide scope of clients; including social services suppliers, relatives or companion.Because of staggering expense of structure and keeping particular server farm, numerous PHR administrations are redistributed to given by outsider specialist organizations, for instance; Microsoft Healthvault1. As of late, models of putting away PHRS in distributed computing, and has been proposed. While this is often energizing to own advantageous PHRS administrations for everyone their square measure varied security and protection dangers that may hinder it's wide array. The principal concern is about whether patients might very management sharing of their touchy (PHI), significantly once they at place away on outsider server that individual might not fully trust. From one perspective; in spite of fact there exist medicinal services guidelines, for example, PHI which is as of late revised to fuse business partners, cloud suppliers are normally not secured elements. Then again, because of high estimation of touchy Personal health information (PHI), the outsider stockpiling servers frequently the objectives of different pernicious practices, which may prompt presentation of PHI. As popular episode, department of veterans affairs database containing delicate Phi of 26.5 million military veterans, including their standardized savings number and medical issues stolen by representative who took information home without approval. To guarantee tolerant driven protection command over their own PHRS, this is basic to have fine grained data gets to control instruments work with semi confided in servers. A possible and promising methodology is scramble the information before redistributing. Fundamentally, the PHR proprietor herself ought to choose how scramble documents and to permit which set of clients acquire access to each record. PHR document should be accessible to clients, who are given the relating unscrambling key, while stay secret to the remainder of clients. Besides the patient will dependably hold privilege to give, yet additionally renounce get to benefits when they feel this is essential. However, the objective of patient driven security regularly in struggle with versatility in PHR framework. The approved clients may either need to get to PHR for individual use or export purposes. Instances of previous are relative and companions, while last can be restorative specialists, drug specialists, and scientists, and so on. We allude to the two classes of clients as close to home export clients, individually.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
M.Bhargavi*, CSE department, S.R.K.R. Engineering College, Bhimavaram, India.
P.Bharath Siva Varma, CSE department, S.R.K.R. Engineering College, Bhimavaram, India.

The last has possibly extensive scale;should every proprietor herself be straight forwardly in charge of dealing with all the expert clients, she will effortlessly be overpowered by the key administration overhead. What's more, since those clients' entrance demands are commonly flighty, it is troublesome for a proprietor to decide a rundown of them. Then again, unique in relation to the single information proprietor situation considered in a large portion of the current works, in a PHR framework, there are various proprietors who may encode as per their specific manners, conceivably utilizing distinctive arrangements of cryptography keys. Giving every client a chance to acquire keys from each proprietor whose PHR she needs to peruse would restrain the availability since patients are not constantly on the web. An option is to utilize a focal expert (CA) to do the key administration for all PHR proprietors, yet this requires an excessive amount of trust on solitary specialist (i.e., cause the key escrow issue). In this paper, we try to think about the patient generic, secure sharing of PHRS put away on semi-confided in servers and spotlight on tending to confound, test, and key administration issues. To ensure the individual well-being data puts away on a semi confided in server, we receive Attribute based encryption (ABE) as the principle encryption crude. Utilizing ABE, get to strategies are communicated dependent on the traits of clients or information, which empowers a patient to specifically share her PHR among a lot of clients by encoding the document under a lot of characteristics without need to know a total rundown of clients. The complexities per encryption and key age and decoding are just straight with the quantity of characteristics included. In any case, to coordinate ABE into a huge scale PHR framework, significant issues, for example, key administration adaptability, dynamic strategy refreshes, and proficient on-request disavowal are non-paltry to explain, and remain to a great extent open modern.

II. PRIVACY PROTECTION & INTRUSION PROCEDURE IN CLOUD

Procedure relates to privacy protection cloud based healthcare systems procedure appear in figure 1.

The customer's physiological information are first gathered by wearable gadgets, for example, brilliant apparel [14]. At that point, those information are conveyed to cloudlet. The accompanying two imperative issues for social insurance information assurance is considered. The first issue is human services information security assurance and sharing information, as appeared in Fig. 1(a). The second issue is to create viable countermeasures to keep the medicinal services database from being barged in from outside, which is appeared in Fig. 1. We address the main issue on medicinal services information encryption and sharing as pursues.

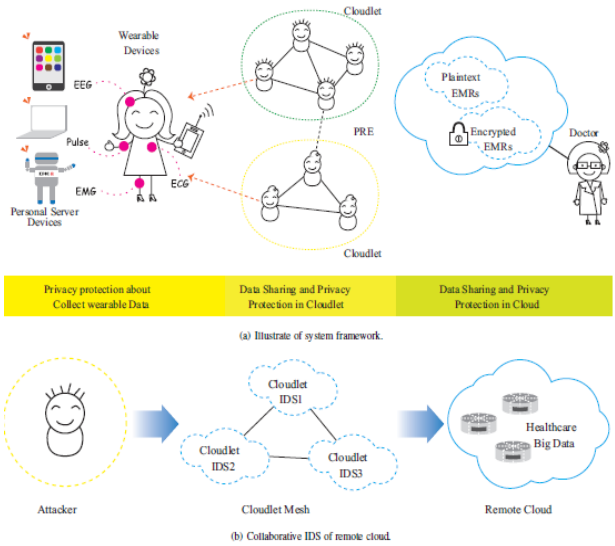

Fig.1. Privacy protection and intrusion detection procedure with respect to different patients data.

Client information encryption. We use the model exhibited in [13], and exploit NTRU [15] to secure the customer's physiological information from being spilled or mishandled. This plan is to ensure the client's protection when transmitting the information from the cell phone to the cloudlet. • Cloudlet based information sharing. Ordinarily, clients topographically near one another associate with the equivalent cloudlet. It's likely for them to share basic viewpoints, for instance, patients experience the ill effects of comparable sort of infection trade data of treatment and offer related information. For this reason, we utilize clients' closeness and notoriety as info information. After we acquire clients' trust levels, a specific edge is set for the examination. When coming to or surpassing the limit, it is viewed as that the trust between the clients is sufficient for information sharing. Something else, the information won't imparted to low confide in level.

Remote cloud information security insurance. Contrasted with client's day by day information in cloudlet, the information put away in remote contain bigger scale restorative information, e.g., EMR, which will be put away for a long haul. We utilize the techniques displayed in [16] [11] to isolate EMR into unequivocal identifier (EID), semi identifier (QID) and therapeutic data (MI). In the wake of grouping, appropriate security is given for the information containing clients' delicate data. • Collaborative IDS dependent on cloudlet work. There is a huge volume of restorative information put away in the remote cloud, it is basic to apply security system to ensure the database from pernicious interruptions. In this paper, we create explicit countermeasures to build up a barrier framework for the substantial restorative database in the remote distributed storage. In particular, community oriented IDS dependent on the cloudlet work structure is utilized to screen any visit to the database as an assurance outskirt. In the event that the recognition demonstrates a vindictive interruption ahead of time, the community oriented IDS will fire a caution and square the visit, and the other way around. The community oriented IDS, as a watchman of the cloud database, can ensure countless information and ensure the security of the database.

III. PROPOSED APPROACH FRAMEWORK

In our structure; there are numerous SDS, various proprietors, different AAs, and numerous clients. What's more, two ABE frameworks are included: for each PSD the YWRL's revocable KP-ABE conspire [9] is embraced; for every PUD, our proposed revocable MA-ABE plot is utilized. The system is delineated in Fig.2.

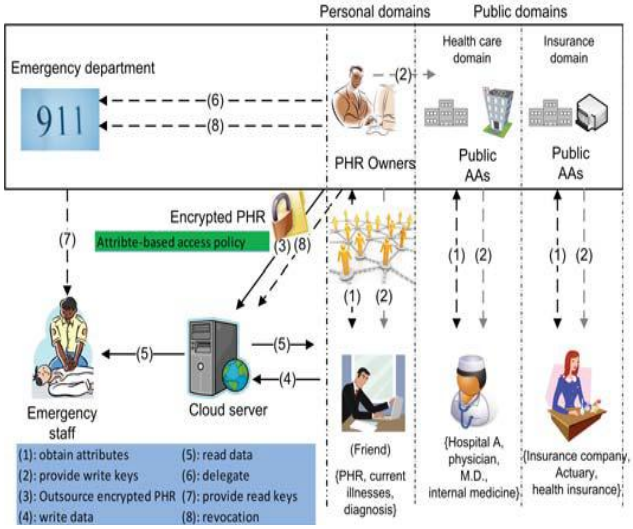

Fig.2. Patient centric procedure to secure patients data in proposed framework.

We term clients having perused and compose access information per users and givers singly, Framework setup and Key Distribution. The framework at the start characterizes typical universe of knowledge characteristics shared by every PSD; as an example, fundamental profile, restorative history, hypersensitivities, and medicines. A crisis quality is in addition characterised for break glass get to. every PHR proprietor's client application creates It's examination open/ace key. The open key are often distributed by means that of client's profile in on-line healthful services informal community (HSN) (which might be piece of the PHR administration; e.g. the Indigo framework). There square measure 2 alternative ways for spreading mystery keys. to start out with once 1st utilizing the PHR administration, a PHR man of affairs will verify entrance good thing about AN info per user in her PSD, and let her application produce what is additional, flow into relating key to the latter, in a very approach taking once solicitations in Googledoc. Second, a per user in PSD might get the mystery key by causing solicitation (showing that styles of documents she has to access) to PHR man of affairs by means that of HSN, and man of affairs can offer her set of mentioned info sorts. in sight of that the arrangement motor of application consequently determines an entrance structure and runs key info of KP-ABE to form the consumer mystery key that implants entrance structure.

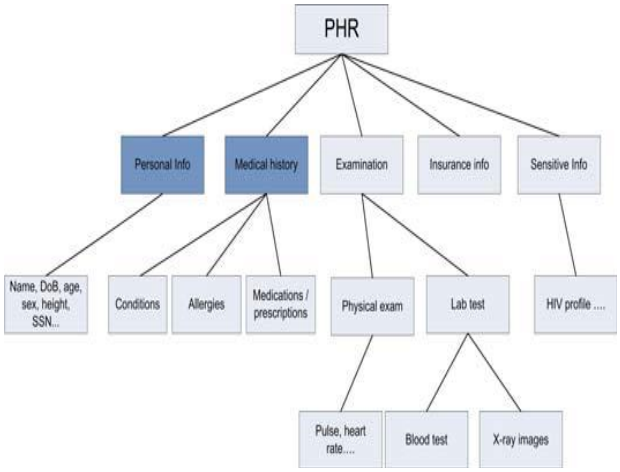

Fig.3. Hierarchy of representation of different attributes with respect to stored patients data.

Furthermore, the data qualities will be composed in a very numerous leveled manner for productive strategy age, see Fig. 3. At the purpose, once the shopper is allowed all the record varieties below a classification, her entrance profit are spoken to by that classed.

For the pudding (public domains) s, the framework characterizes job qualities, and a per user in a very pudding get's mystery key from AAS, that ties the shopper to her declared properties/jobs. as an example, a doctor in it'd get "emergency clinic A, doctor, M.D., interior medication" as her qualities from AAs. By and by, their exist numerous AAs every administering associate degree alternate set of job qualities. for instance, medical clinic staffs can have associate degree alternate AA from drug store execs. this can be mirrored by((1)) in Fig.3. ABE used to scramble that data conjointly the AAs circularize compose keys that grant donors in their pudding to stay in grips with bound patients PHR ((2)).

PHR encoding and access the proprietors transfer ABE encoded PHR records to server ((3)). Each proprietor's PHR record encoded each below an explicit fine grained what is a lot of, job based mostly access arrangement for the purchasers from pudding to gets to; and below selected set of knowledge properties that allow access from purchasers in PSD. because it were approved purchasers will unscramble the PHR documents; expulsion the server. For up effectiveness, the data traits can incorporate all the center of the road record varieties from leaf hub to the foundation. as an example in Fig:3, a "sensitivity" document's traits ar . the data perusers transfer PHR records from server, and that they will rewrite the records simply on the off probability that they need applicable attribute based mostly keys ((5)). the data supporters are allowed compose access to somebody's PHR, on the off probability that they gift legitimate compose keys ((4)). Client Revocation. Here we think about denial of an information peruser or her properties/get to benefits. There are a few conceivable cases: 1) renouncement of at least one job characteristics of an open area client; 2) repudiation of an open space client which is proportional to disavowing the majority of that client's traits. Basic procedure used to protect keys with respect to patients stored data shown in figure 5 with different steps to process different scenario's.

- Setup(1^κ) The same as Setup from [21], except that each AA_k $(k = \{1, ..., N-1\})$ defines an additional dummy attribute A_k^* with its corresponding public key and master key components, and each AA initializes a version number $ver = 1$. The AAs publish (ver, PK), while (ver, MK_k) is held by AA_k.
- KeyIssue($\mathbb{A}^u, MK, PK$) The same as KeyIssue from [21], except the key-policy $\mathbb{A}^u$ of each user must be ANDed with $A_1^*, ..., A_{N-1}^*$. The user receives (ver, SK_u), where ver is the current version number.
- Encrypt($M, \mathbb{A}^C_{PUD}, PK$) The same as Encryption from [21], except that A_k^* must be part of $\mathbb{A}^C_{AA_k}$ $(\forall k \in \{1, ..., N-1\})$. It outputs $CT = \langle ver, E_0 = M \cdot Y^s, E_1 = g_2^s, \{C_{k,i} = T_{k,i}^s\}_{i \in \mathbb{A}^C_{PUD}, k \in \{1,...,N\}} \rangle$. The encryptor stores the random number s used to compute CT.
- Decrypt(CT, PK, SK_u) The same as Decryption in [21], except it uses PK and SK_u with the same ver as in CT.
- MinimalSet($\mathbb{A}^u$) First, each AA_k runs algorithm $\gamma_k \leftarrow$ AMinimalSet($\mathbb{A}_k^u$) from [9]. Then $k_{min} \leftarrow \underset{k}{\text{argmin}}\{|\gamma_k|\}$, and output $\gamma_{k_{min}}$.
- ReKeyGen(γ, MK_k) Executed by AA_k. Given a set of attributes γ, for each $i \in \gamma$, run algorithm AUpdateAtt(i, MK_k) from [9] and output local re-key as $rk_k = (ver, \{rk_{k,i \to i'}\}_{i \in \mathcal{U}_k})$ where $\mathcal{U}_k$ is the attribute universe governed by AA_k. The global re-key is $rk = \{rk_k\}_{1 \le k \le N}$. Increase the system's ver by 1 (the other AAs will synchronize).
- ReEnc(CT, rk) Executed by the server. For each $1 \le k \le N, i \in \mathbb{A}^C_{PUD_k}$, run algorithm $C'_{k,i} \leftarrow$ AUpdateAtt4File($i, C_{k,i}, AHL_{k,i}$) from [9], which updates ciphertext component $C_{k,i}$ to its latest ver, where AHL is an attribute history list. Output $CT' = (ver + 1, \mathbb{A}^C_{PUD}, E_0, E_1, \{C'_{k,i}\}_{i \in \mathbb{A}^C_{PUD_k}, k \in \{1,...,N\}})$.
- KeyUpdate(SK_u, rk) User u gives part of SK_u to the server (except the dummy components). For each $1 \le k \le N, i \in \mathbb{A}^u_{PUD_k}$, run algorithm $D'_{k,i} \leftarrow$ AUpdateSK($i, D_{k,i}, AHL_{k,i}$) from [9]. Outputs $SK'_u = (ver + 1, D_u, \{D'_{k,i}\}_{k \in \{1,...,N\}, i \in \mathbb{A}^u_{PUD_k}})$.
- PolicyUpdate($\mathbb{A}^C_{PUD}, CT, s$). CT is parsed as: $\langle ver, \mathbb{A}^C_{PUD}, E_0, E_1, \{C_{k,i}\}_{i \in \mathbb{A}^C_{PUD}, k \in \{1,...,N\}} \rangle$. For each $i \in \{\bar{\mathbb{A}}^C_{PUD} - \mathbb{A}^C_{PUD}\}$, compute $C_{k,i} = T_{k,i}^s$. For each $i \in \{\mathbb{A}^C_{PUD} - \bar{\mathbb{A}}^C_{PUD}\}$, delete $C_{k,i}$. Output $\tilde{CT} = \langle ver, \bar{\mathbb{A}}^C_{PUD}, E_0, E_1, \{C_{k,i}\}_{i \in \bar{\mathbb{A}}^C_{PUD}, k \in \{1,...,N\}} \rangle$.

Fig.4. Step By Step Procedure For Different Data Steps In Data Sharing.

These activities area unit finished by the AA that the shopper contains a place with, wherever the real calculations will be appointed to the server to boost productivity ((8)). 3) Revocation of a personal area shopper's get to benefits; 4) resignation of a personal area client. These will be started through the PHR proprietor's client application comparably. Approach Updates. A PHR businessman will refresh her sharing approach for a current PHR archive by refreshing the characteristics (or access arrangement) within the figure content. The upheld tasks incorporate include/erase/alter, that ought to be potential by server in interest of shopper Break-glass. At, the point, once a crisis happens, the customary access arrangements could ne'er be pertinent. To wear down circumstances, break-glass get to is predicted to urge the unfortunate casualty PHR. In our system, each proprietors PHR entrance right is to boot assigned to a crisis division (ED (6)) to stay from mistreatment of break-glass selection, the crisis workers must contact impotence to substantiate her temperament, and crisis circumstance, and acquire impermanent browse keys ((7)).Once crisis is finished, a patient will deny the eminent get to by means that of impotence. An Example, Here we tend to show however our system functions utilizing a solid model. Assume PHR businessman Alice is that the patient connected with a emergency clinic A. once she makes the PHR record F1 (marked as "PHR; restorative history; sensitivity; crisis" in Fig: 4); she at first scrambles it as indicated by each F1's data marks (under YWRL KP-ABE); and job primarily based record get to approach P1 (under reversible MA-ABE). This approach will be chosen dependent upon steered settings by a framework, or Alice terribly own inclination. it'd appear as if P1:=((Profession=Physician)∧ (Specialty=Internal medicine)∧(Organization=Hospital A)). She to boot sent the break-glass key to it impotence. Moreover, Alice decides entrance privileges of shoppers in her PSD; that ought to be potential either on line or disconnected. For instance; she could affirm her companion Bobs solicitation to urge to documents with names {personal info} or {medical history}. Her client application can flow into the mystery key with entrance structure (individual information ∨ medical history) to Bob. At, the point, once Bob must get to a different document F2 with names "PHR — medicative history — prescriptions"; he will rewrite F2 because of the "therapeutic history" attribute. for one more shopper Charlie World Health Organization is that the doctor having some experience in inner medication in emergency clinic B in pudding, he gets his mystery key from totally different AAS, as an example, the yank Medical Association (MA), the yank Board of Medical Specialties (BMs), and therefore the yank Hospital Association (HA). Be that because it could, he cannot unscramble F1, on the grounds that his job qualities do not fulfill P1. At long last, a crisis area workers, Dorthy World Health Organization incidentally get the break-glass key from the impotence, will access F1 attributable to the crisis attribute in this key. The detachment of PSD/PUD and information/job characteristics mirrors this gift reality circumstance. In 1st place, in PSD, patient usually simply offers individual access of her touchy PHR to selected shoppers; as an example, family people and pricey companions, as hostile each one of the companions in informal organization. Distinctive PSD shoppers will be relegated various access advantages obsessed on their associations with the businessman. on these lines, patients will apply fine-control over entrance for each shopper in their PSD's. Second, by our multi-space and multi-expert system, each open shopper simply must contact AAS in its own pudding World Health Organization hand and glove creates the mystery key for the shopper, that lessens a remaining task at hand per AAs (since each AAs handles less range of qualities per key issuing). Likewise, multi-specialist ABE is flexible to cut price of up to N − two AAS during a pudding, that takes care of the key-escrow issue. Besides, in our structure shoppers job confirmation may be a ton easier. various associations will frame their own (sub) domains and become AA's to manage and guarantee distinctive arrangements of traits, that is like separation and customary.

IV. EXPERIMENTAL RESULTS

We evaluate scalability and efficiency of our solution regarding storage; communication and computation costs. We compare with previous schemes regarding cipher text size; user secret-key size; public key or information size; and revocation (re-keying) message size. Based on these parameters we calculate the performance of proposed approach with existing approaches regarding e-health data processing in cloud.

After performing above operations in uploaded file in e-health based cloud computing, the process to calculate time efficiency is given in Table 1 as follows:

Table-I: Comparative Analysis Of Key With Respect To Different Users.

Depth of Key	Time Efficiency
1	0.04986
2	0.05993
3	0.07011
4	0.08173
5	0.09861

Comparative evaluation for above mentioned table 1 as shown in figure5:

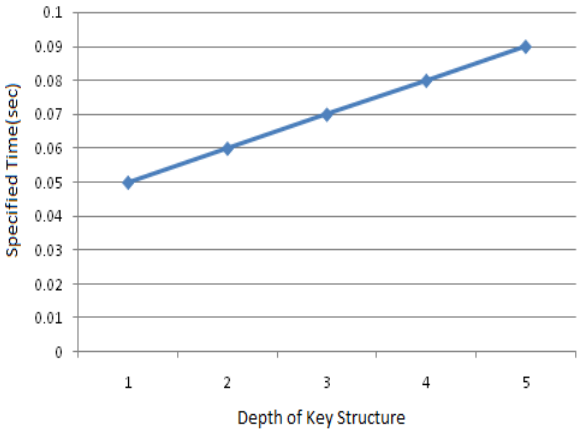

Fig.5. Key structure with respect to different attributes.

The scholar had performed data encryption and decryption of uploaded files in cloud computing based on attributes of uploaded file. The comparative analysis of proposed approach as follows:

Table-II: Time Efficiency Comparison Values For Different Attributes With Different Files.

S.No	Number of Attributes	Key Generation Time
1	10	0.9874
2	20	0.4012
3	30	0.5934
4	40	0.8124
5	50	0.9975

The process of encryption and decryption may perform in this approach is as based on attributes of the uploaded files with respect to time in number of files uploaded.

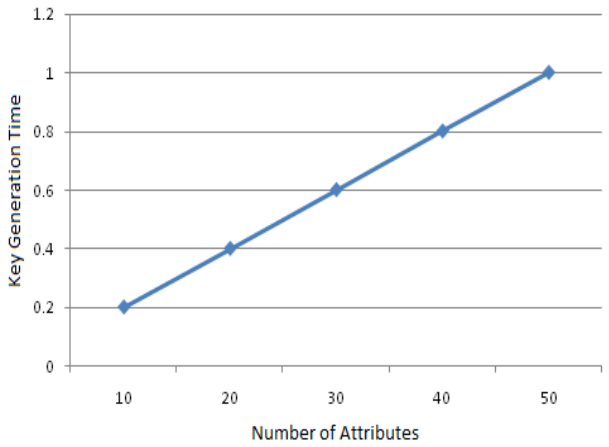

Fig.6. Attributes for key generation for each patient health data in outsourced cloud.

Based on results present in above discussion, we present the performance evaluation of proposed approach with respect to different attributes in key generation and other parameter sequences with different security notations.

V. CONCLUSION

We have projected a totally distinctive system for secure sharing of individual health records in distributed computing. Considering somewhat dependable cloud servers, we have a tendency to contend that to completely understand the patient-driven idea, patients will have unlimited authority for his or her own security through scrambling their PHR records to permit fine-grained gets to. The structure tends to exceptional difficulties brought by varied PHR proprietors and shoppers, in this we tend to significantly decrease the many-sided nature of key administration whereas upgrade the protection ensures contrasted and past works. we tend to use ABE to scramble the PHR data, thus patients can permit get to by on the brink of home shoppers, but else entirely completely different shoppers from open areas with varied professional jobs, capabilities, and affiliations. Moreover; we tend to enhance a current MA-ABE commit to influence effective and on-request shopper repudiation, and demonstrate its security. Through execution and duplicate, we tend to demonstrate that our answer is every variable and efficiency.

REFERENCES

1. Pieter Van Gorp∗, Marco Comuzzi∗, Andr´e Fialho† and Uzay Kaymak, "Addressing Health Information Privacy with a novel Cloud-Based PHR System Architecture", 2012 IEEE International Conference on Systems, Man, and Cybernetics October 14-17, 2012, COEX, Seoul, Korea
2. Min Chen, Yongfeng Qian, "Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing", UNDER REVIEW:IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. XX, NO. YY, MONTH 20XX.
3. D. Detmer, M. Bloomrosen, B. Raymond, and P. Tang. Integrated personal health records: Transformative tools for consumer-centric care. BMC Medical Informatics and Decision Making, 8(1):45, 2008.
4. G. Eysenbach. Medicine 2.0: Social networking, collaboration, participation, apomediation, and openness. J Med Internet Res, 10:e22, July 2008.
5. G. S. Ginsburg and J. J. McCarthy. Personalized medicine: revolutionizing drug discovery and patient care. Trends in Biotechnology, 19(12):491 – 496, 2001.

6. G. Hull, H. Lipford, and C. Latulipe. Contextual gaps: privacy issues on facebook. Ethics and Information Technology, 13:289–302, 2011.
7. D. Kaelber and E. C. Pan. The value of personal health record (PHR) systems. In AMIA Annu Symp Proc, pages 343–347, 2008.
8. D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates Viewpoint paper: A research agenda for personal health records (PHRs). JAMIA, 15(6):729–736, 2008.
9. J. S. Kahn, V. Aulakh, and A. Bosworth. What it takes: characteristics of the ideal personal health record. Health Aff, 28:369–376, Mar. 2009.
10. J. Kuczynski et al. Experimental and analytical tools for studying the human microbiome. Nature Reviews Genetics, 13(1):47–58, Dec. 2011.
11. S. Murphy. In need of a reality check. Nature Biotech, 27:422, May 2009.
12. C. Pagliari, D. Detmer, and P. Singleton. Potential of electronic personal health records. BMJ, 335(7615):330–333, 8 2007.
13. V. Rybynok, P. Kyriacou, J. Binnersley, and A. Woodcock. MyCare Card development: Portable GUI framework for the personal electronic health record device. IEEE Transactions on Information Technology in Biomedicine, 15(1):66–73, 2011.
14. D. F. Sittig. Personal health records on the internet: a snapshot of the pioneers at the end of the 20th century. Int. J. of Medical Informatics, 65(1):1 – 6, 2002.
15. A. Srinivasan. Keeping online personal records private: Security and privacy considerations for web-based PHR systems. Journal of AHIMA, 77:62–63, Mar. 2006.
16. Students of the Interdisciplinary Law and Technology Workshop. Privacy in the digital environment. Technical report, The Haifa Center of Law and Technology Publication Series n. 7, 2005.
17. P. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands. Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. JAMIA, 13:121–126, Mar. 2006.
18. P. Van Gorp and M. Comuzzi. MyPHRMachines: Lifelong Personal Health Records in the cloud. In Proc. 25th IEEE Int. Symposium on Computer-based Medical Systems, 2012. forthcoming.

AUTHORS PROFILE

M. Bhargavi completed B.Tech in Information Technology from Andhra University, India. She is currently pursuing M.Tech in Computer Science and Engineering from Jawaharlal Nehru Technological University Kakinada, India.

P. Bharath Siva Varma received his B.Tech in Information Technology from Andhra University,India and M.Tech in Computer Science and Engineering from Jawaharlal Nehru Technological University, kakinada, India. He also persuing Ph.D degree from Koneru Lakshmaiah University, Guntur, India. He is currently working as assistant professor in the department of computer science and engineering in SRKR engineering college.