Asian Journal of Information Technology 15 (1): 65-72, 2016
ISSN: 1682-3915

Attribute Base Access Control to Secure the Patient Health Record in Cloud

B. Seetharamulu and G.V. Uma
Department of Information Science and Technology, CEG Anna University, 600025 Chennai, India

Abstract: This study presents the development for healthcare authorities as well as healthcare services administration to install cloud computing platform. Personal Health Record (PHR) administration is a rising new model for health industry, this permits patients to make, oversee, control and share their health related data with different users and in addition to Health insurance companies. This study portrays the work on outlining and implementing patient-driven, patient's health information in a cloud platform in light of open-source Indivo X framework. In reality, a PHR administration is prone to be facilitated about outsourcing patients PHR information to cloud servers with a specific end goal to upgrade its interoperability. This study proposes a privacy preserving PHR framework utilizing Attribute Based Encryption (ABE) and provides the framework so that patients can encrypt their PHRs and store them on semi-trusted cloud servers such that servers don't have authentication to sensitive PHR information and the patients keep up full control over access to their PHR records, by doling out fine-grained, attribute-based access to some authorized data users while distinctive users can have entry to diverse parts of their PHR.

Key words: Personal health record, electronic medical record, access control, cipher text-policy attribute-based encryption, Indivo X

INTRODUCTION

It is by and large recognized that the utilization of data and its correspondence innovations in the wellbeing protection frameworks will improve mind conveyance extraordinarily. It may enhance subject's wellbeing and additionally including thriving besides social thought. In addition, it fabricates subjects bore for a collection and opportunity and diminishing rising social protection costs in the general public.

The late movement in social insurance have transport to a movement from the Electronic wellbeing Record (EHR) structures repressed by medicinal services giver to individual wellbeing Record (PHR) system controlled by patients themselves. PHR systems grant patients to make oversee and control their own particular PHRs through, the internet which conferred possible to effortlessly get to their wellbeing data on restorative administrations suppliers, assurance, protection experts, specialists, relatives and sidekicks. The wellbeing data on a PHR may be thought to be seen as complete and precise delineation of a singular's layout for a singular's helpful history of wellbeing status. On one hand, individuals can import their wellbeing data which may consolidate their restorative history, research centre and imaging results, record of the rapeutic issues and chronicled scenery from clinic EHR structure individuals may additionally exchange wellbeing estimations from their gadgets for example, remote electronic measuring scales or assembled latently from an advanced mobile phone. PHR systems can serve as a server farm point for patient's wellbeing administration by assisting patients with staying educated of their individual wellbeing information, relate precise history in the midst of clinical experiences, check for medicine cooperation's and take out superfluous duplication of lab tests and indicative studies. With PHR systems, patients can have section to a wide extent of wellbeing data resources and also enhancing their wellbeing mindfulness. At the same time, PHR structures help clinicians on better treatment choices by giving ceaseless data. PHR systems can likewise advantage the general area by giving wellbeing watching, episode watching, fortifying, interfacing with administrations and examination. PHR systems can give buyers the likelihood to have immense impact in guaranteeing and advancing the general's wellbeing. The distributed computing is a standout amongst the most difficult imaginative models which encourage simple, on-interest system access to a common pool of configurable preparing assets that safeguard to be immediately provisioned and discharged with unimportant administration exertion or administration supplier communication (Mell and Grance, 2009). As per a report from Gartner, there is a quickening of apportionment of distributed computing among

Corresponding Author: B. Seetharamulu, Department of Information Science and Technology, CEG Anna University, 600025 Chennai, India

undertakings. Gartner figure that the general cloud organization earnings would accomplish 148.8 billion USD by 2014, with tremendous part from the human services distributed computing business. National and commonplace medicinal services powers furthermore a social insurance administration supplier showed unimaginable intrigues and is presently making initial moves towards the introducing of distributed computing. Distributed computing can serve medicinal services suppliers to focus more on growing nature of conveyed social insurance rather to managing their IT. This is especially imperative for doctor's facilities, gathering care and specialist rehearses. Distributed computing streamlines data sharing among diverse social insurance associations incorporated into the consideration process. Moving the system and sensitive patient information data from specialist's offices to the cloud can act genuine security and insurance dangers. Some information in a PHR is seen as private and touchy. To shield patients from social mortification, inclination or uncalled for employment opportunity, data for example, fruitfulness, passionate and mental issue sexual practices or physical misuse et cetera shou access control system endeavor manhandle the use of cryptography to approve access control approaches. In such structures, there is no necessity for trusted servers to check customer certifications and each client can get the encoded data however just clients who have the right accreditations who have the right qualifications can decode the scrambled data (Goyal *et al*., 2006). In standard public key encryption systems or Identity Based Encryption (IBE) structures, scrambled data is cantered around for interpreting by a solitary known client who is portrayed by an automated confirmation or an identity. Consequently customary pubic key encryption arrangements or IBE arranges won't work for circumstances when the sender does not know the positive identity of the recipient. Case in point, if a patient needs to send his PHR data to various clients, the patient needs to know the mechanized underwriting or the character for each recipient and after that encode the same data conventionally using each recipient pubic key or character. Thusly, we require a crypto arrangement which offers a more suitable response for executing access game plans considering data recipient characteristics as opposed to the data's identity recipient. The patient demonstrates only the characteristics the recipient needs to have remembering the finished objective to get the opportunity to calm's data. To address these rising needs, (Sahai and Waters, 2005; Goyal *et al*., 2006) displayed the thought of trademark Based Encryption (ABE). What's more, ABE moreover has plot resistance property, i.e., if various clients intrigue, they should simply have the ability to just have the capacity to unscramble a figure content if no under one of the clients could decode, it isolated. Hence, data access is self-actualizing from the cryptography, obliging no trusted go in the middle.

ABE can be seen as a development of IBE in which client character is summed up to an arrangement of spellbinding traits instead of a singular string deciding the client personality. Relatively customary open key encryption and IBE, ABE IBE, ABE has vital point fulfils adaptable versatile one-to numerous encryption as opposed to coordinated, it is to envision as a promising device for tending to the issue of secure and fine grained data sharing and decentralized access control.

There are two sorts of ABE depending whereupon of private keys or figure messages that get to methodologies are joined with. In key-approach ABE (KP-ABE) system (Goyal *et al*., 2006; Ostrovsky *et al*., 2007), client's keys are issued by the trait power catches an entrance structure that figures out which kind of figure messages the key can decode, while figure writings are stamped by the sender with an arrangement of elucidating qualities. In the figure content arrangement ABE (CP-ABE), senders can encode a message with a clear get to strategy in obtainments of access structure over the attributes conveying what sort of collectors will be able to decode the figure content. Client has sets of properties and addition taking a gander at mystery trademark keys from the power. Such a client can decode figure content if his/her characteristic fulfils the entrance system related to the figure content. A depiction use of CP-ABE is secure framework with access approach.

Especially, there has been an extending energy for applying ABE to secure EHRs or PHRs (Ibraimi *et al*., 2009; Li *et al*., 2010; Narayan *et al*., 2010). Ibrahim *et al*. (2009) connected CPABE to approve persistent/ authoritative access control systems such that everyone can download the encoded data yet simply approved customers from the family, sidekicks or approved client capable area like specialists and medical attendants are allowed to unscramble it.

Mohan displayed the design and beginning model use of a Med Vault subsystem for EHR sharing which covers property based access control and specific wellbeing information disclosure. Mohan showed the arrangement and starting model use of a Med Vault subsystem for EHR sharing which covers property based access control and specific wellbeing information disclosure. Narayan *et al*. (2010) proposed a property based system for EHR structures where each patient's EHR reports are scrambled using a broadcast variety of CP-ABE that allows direct renouncement. On the other

hand, the figure content length increments with the numerals of unrevoked clients. Akinyele *et al.* (2011) give a layout and use of self-guaranteeing Electronic Medical Records (EMRs) using two fold system trait based encryption which can either be stored on cloud servers or phones so that EMR could be recovered from the net. Li proposed a patient-driven arrangement of secure sharing of PHRs in distributed computing. They focus on the distinctive data proprietor circumstance and allotment the client in the PHR structure into diverse security regions that essentially decreases the key organization multifaceted for proprietors and clients. A high level of patient security is guaranteed in the meantime by abusing multi-power ABE.

This study proposes a framework and actualizes a PHR cloud platform facilitated with the considered CP-ABE. The made PHR cloud stage engages patients to securely store and share their wellbeing records in a versatile way. The patient can store PHRs in an encoded structure and cryptographically approves the patient or definitive access techniques.

This study extemporize the upgrade PHR embracing so as to share arrangement of Indivo X wander (Narayan *et al.*, 2010) CP-ABE and a few premise about CP-ABE system are exhibited. The building outline of PHR cloud stage to be made, the execution experiences about PHR cloud stage.

Literature review

Access structure: Let us consider P = {P1, P2...Pn} be a set of parties. A collection A⊆2P is monotone if ∀B, C, we have that if B∈A and B⊆C then, C∈A. An access structure is a collection) A⊆2P\{ø}. A is said to be authorized sets and the sets that are not in the A are said to be unauthorized sets (Sahai and Waters, 2005; Goyal *et al.*, 2006). In this perspective, the function of the parties is taken with the attributes. Therefore, the access structure the sets in A are called the authorized sets of attributes. The monotone access structure is restricted. Four polynomial algorithms are in CP-ABE method as follows (Goyal, 2007).

Setup (1λ)→(params, msk): The setup algorithm called probabilistic polynomial-time algorithms which takes λ security parameter as input and outputs the public parameters params along with master key (msk) which is trusted Attribute Authority (AA).

Encrypt (params, m, A)→c: The public parameters params and message m along with access structure A which stated by the sender is an input to the PPT encryption algorithm. The cipher text c encrypted is a output.

KeyGen (params, msk, ω)→SKω: An interactive protocol between the AA and the user is the PPT key generation algorithm. The public parameters params are the common input to AA, ω is the set of attributes which is the user owns and the master key msk is the private input to AA. A decryption key SKω is received by users and associated by set of attributes.

Decrypt (params, c, SKω)→m or ⊥: The public parameters params are taken as input in the deterministic polynomial time algorithm, under the access structure A the cipher text c is encrypted and the secret key SKω of user is related to the set of attributes ω.ω∈A is the message m that is given and ⊥ if ω ⊥∈A is the error message. Security Model for CP-ABE Scheme: Similar to IBE method, the security model permits the opponent to enquiry for one private key that cannot be utilized to decrypt the challenge cipher text. In CP-ABE method, the private keys are recognized with attributes and the cipher texts are identified with access structures. It follows that the security model for CP-ABE method permits the opponent to enquire for any private key linked with the set of attributes αi that cannot be utilized to decrypt the challenge cipher text which is encrypted beneath an access structure A. For example: αi does not assure A. The proper security match for CP-ABE is illustrated as follows.

Setup: The challenger runs the Setup algorithm and produces the public parameters params to the adversary.

Phase 1: The adversary makes the repeated private keys associated to the sets of attributes γ1...γ q1.

Challenge: The adversary submits two equal length messages a0 and a1. In addition, the adversary gives a challenge access structure n0 such that none of the sets γ1...γq1. From phase 1 satisfy the access structure. The challenger flips a random coin b and encrypts nb under A. The adversary outputs a guess. The advantage of an adversary A in this game is defined as. This study note that, the method can easily be enhanced to manage chosen-cipher text attacks by permitting for decryption queries during phase 1 and phase.

MATERIALS AND METHODS

Architecture of PHR cloud platform: We recognize the guideline security requirements for PHR cloud stage as takes after. Confidentiality of wellbeing data archive and cross: By confidentiality, we mean the cloud supplier or an adversary won't have the ability to scrutinize patient's

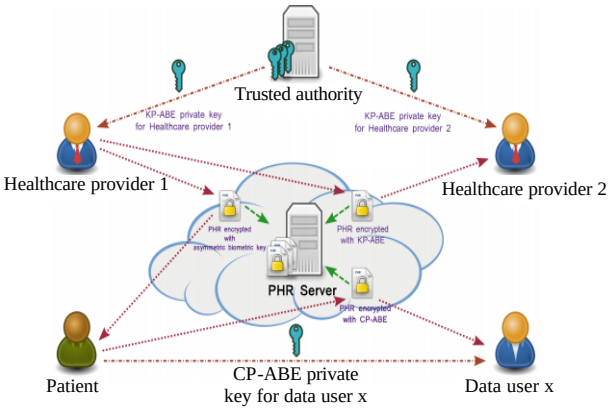

Fig. 1: System architecture and workflow

PHR data. Along these lines, the calm's PHR data must be mixed before, it is exchange to PHR cloud.

Integrity of wellbeing data: By integrity, we expect to shield the accuracy and consistency of data. In the PHR cloud stage, integrity suggests the way that PHR data has not been adjusted by unapproved use. Trustworthiness can be expert by cryptographic hash limit.

Authenticity of wellbeing data: By authenticity, we intend to ensure that the data are certifiable and to endorse that both sides included are who they state they are. In the PHR cloud organize, the PHR data are accumulated, secured and shared by a get-together other than the first social protection supplier. In light of current circumstances, the issue of affirming that the information was truly made by the attested source must be tended to.

Privacy security for patients: Data exposures are controlled taking after the data minimization standard to be particular, the revelation and support of individual data should be limited to what is particularly appropriate and vital to perform a predefined reason.

Patient-driven fine-grained access control: Patient should be aware of their security rights and prepared to focus furthermore, assign the passageway control methodology of their data. The patient encodes the PHR data according to figure content access approach such that simply the customers who satisfy the entrance methodology can unravel the secured data. Additionally, the passage approach should be versatile and supportive to make and supervise.

Revocation: When a customer's puzzle key or attributes are no more significant, this customer can't unscramble any PHR data.

There are five individuals in cloud stage: human administrations supplier, cloud organization supplier, quality force, proprietor (patient) and viewer.

The cloud organization suppliers are semi-trusted which infers that cloud organization suppliers would endeavor to find however, much PHR information as could sensibly be normal while taking after the tradition. The explanation behind existing is to engage patients to control the transport and use of their data. As a makeshift alleviation answer for this, PHR data ought to be encoded before exchanging to the cloud. The protection framework needs to ensure that tireless PHR data must be decoded by affirmed social occasions as showed by the course of action and consent. Figure 1 shows, the system auxiliary designing of the proposed cloud stage where the patient can securely manage his/her wellbeing records using the arrangement. In the going with, we clear up the affiliations that happen in the system.

Framework setup: AA runs setup calculation of waters' CPABE plan, it yields public parameters params in general parameters and the expert mystery key msk which is kept by AA secretly.

Generate PHR: PHR owner gets unique Electronic Restorative record (EMR) from human services supplier, then builds PHR information in light of EMR information and other information.

Encrypt: It's not suitable utilizing CP-ABE to encrypt the information for effectiveness reasons. Rather, PHR proprietor first creates an AES key indiscriminately as substance encryption key and encodes the PHR information utilizing the substance encryption key. PHR owner then sets access approach and encrypt the substance encryption key utilizing CP-ABE plan under the entrance strategy.

KeyGen: Client sends a solicitation for property private key alongside his accreditations to the AA. The AA director checks and imprints these solicitations as "sanction" or "denied". For the "sanction" demand, AA chairman signs the solicitation with his private key as qualified demand and sends, it to the AA server. At that point AA server checks marks for solicitations sanction by AA executive, runs the KeyGen calculation of AA plan and conveys the private key comparing to the arrangement of ascribes to the client. At present, the renouncement for AA. Plans is not extremely vigorous (Yin and Zhang, 2011), we embrace the thought of lapse to take care of this issue CP-ABE creates another access arrangement by adding termination ascribe to the first get to approach with coherent AND operation.

Implementation of PHR cloud platform: A secure PHR cloud floor using CPABE based on Indivo X (Mandl *et al*., 2007) is implemented. The data storehouse architecture and distribution mechanism of original PHA (Personal Health Application) and a new Indivo API calls are combined and a Python ABE library named payable is created and transformed. It is essential to choose an appropriate attribute set for scheming a PHR cloud floor. In earlier PHR systems proving ABE (Ibraimi *et al*., 2009; Li *et al*., 2010; Narayan *et al*., 2010; Akinyele *et al*., 2011; Zheng, 2011), they simply select user's workplace or job as attributes. To present more expressive behaviour, the (Name, Date of Birth (DOB), gender, marriage status, occupation, workplace, address, key expiration) are defined as the set of attributives. The key expiration is a set by AA to give key revocation and not an un-specified attribute. Two types of attributive: numerical type and non-numerical type are there, according to the water's CP-ABE scheme (Waters, 2011). The attr = value is specified as numerical type where the attribute is indicated as attribute and value is non-negative integer <264. Any string of digits, letters and underscores, beginning with a letter are non-numerical attributes. User's attribute privacy is preserved by name as non-numerical attribute, while the numerical form in attribute storage. In KeyGen algorithm the reason is that patient Occupation = Doctorand Occupation = Physician both has same meaning but, they are two different non-numerical attributes.

The PHR decryption is not possible in this case, when a patient encrypted a PHR with attribute Occupation = Doctor and thus the doctor gets his private key as associated with Occupation = Physician. To avoid decryption failures, the conversion of non-numerical to style attributes to numerical ones are avoided. For instance, numerical type age is converted to attribute DOB. The attributes gender, marriage and occupation as enumerated data types, like "0" represents female and "1" stands for male. The country, province, city, workplace/address are organized for the attributes workplace and address. A unique id is assigned for each concrete attribute and each table has a corresponding id for Foreign key reference (Alogrithm 1).

Alogrithm 1:

```
<? XML version = "1" Encodin"ISO-8859-1"?>
<Schema xmlns = "https://ww.w3.org/2001/
XMLSchema: ElementFormDefault = "Qualified"">
<Element name = "Abe document">
<Complex type>
<Sequence>
<Element name = "Name"          type= "String"
minOccurs = "1"                 maxOccurs = "1" />
<Element name = "Content"       type= "String"
minOccurs = "1"                 maxOccurs = "1" />
<Element name = "Keywords" type = "String" minOccurs = "0"
maxOccurs = "1" />
<Element name = "Policy"        type = "String"
                                        minOccurs = "0"
maxOccurs = "1" />
    </Sequence>
                                </Complex>
        </Element>
    </Schema>
```

The access strategy is embedded in cipher text and is specified by PHP that is expressed by the logical operations and comparison operators for numerical attribute expression. For instance, "Doctor OR 2 OF (Age<40, female OR male, child hospital)" could be a strategy. Python is used as a programming language in Indivo X. For accomplishing ABE functions the backend clients and servers the Python version pyabelib based on libfenc is built. The C library is used to finish the all computational task. Additionally, the python is used for making calls.

The patient's PHR are stored in XML plaintext in the original Indivo X Server. A new XSD (XML Schema Definition) to replace the original XSD to support CP-ABE scheme which depicted as follows.

The patients can identify the conventional PHR name, solid access strategy and keywords utilized for searching in the new XML. The encrypted PHR is the "content" element. To execute, the every step of encrypt and decrypt a client plugins is created by using PyQt framework. OAuth protocol (Akinyele *et al*., 2011) is followed in PHA for encrypting and sharing. Lets, patient to choose PHR and set encrypted PHR name, access policy and keywords, for encrypting PHA and then invokes the client plugins to complete encrypting operation. The security is provided by sharing mechanism in Indivo X. In improve sharing PHA, if the user is enabled once, it means that this user allows sharing his PHR with those who also enabled PHR sharing PHA. The

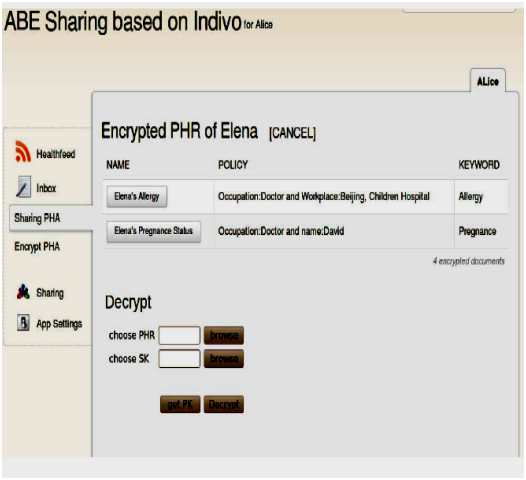

Fig. 2: User view and decrypt encrypted PHR

list of encrypted PHR is displayed to the user after authorization. The user can view, download and decrypt what he wants as in Fig. 2. The user's access policy is satisfied by private key then, it is embedded in the encrypted PHR and decrypted successfully.

RESULTS AND DISCUSSION

Evaluation of PHR cloud platform: As compared with Indivo X, our framework has little impact on the server side. We have included some new Indivo X style APIs taking after its security convention entirely, keeping in mind, the end goal to make Indivo X backend server bolster the new encrypt PHR storage configuration. The server side, the performance of the pyabelib is measured and then, it is compared with the libfenc. Params will be loaded to the client side from the cached files and to load params is also AA additionally needed along with msk from local files, it is important to consider the I/O expense of reading files. So, we state the total execution time for every encryption, decryption and KeyGen including the expense of reading files simultaneously, we evaluate the actual computation time in every step, omitting the cost. According to the Water CP-ABE method the non-numerical attribute associates to the single leaf node in the access structure where as the numerical form associates to the more leaf nodes in this way, we utilize the number of nodes rather the attribute numbers as X-axis, Y-axis is every step's period overhead. Using the using non numerical form randomly 100 attribute sets are created, if it is the ith attribute set, it has the i attributes similar as the leaf nodes. To verify that, each leaf node is visited during encryption AND gate approach is utilized. Then, same PHR plaintext is encrypted through, the

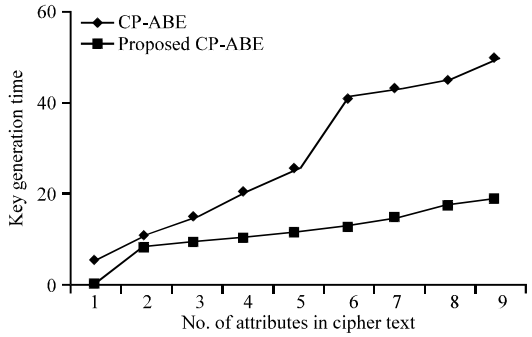

Fig. 3: Evaluation of pyabelib; key generation

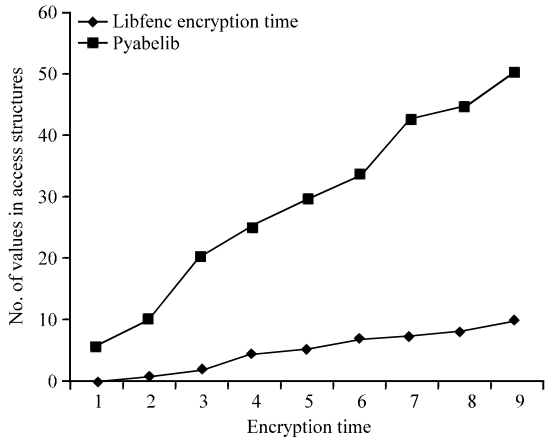

Fig. 4: Evaluation of pyabelib; encryption

pre-generated attribute sets ranging from 1-100. For example generated attribute set from {a1001}, {a1001, b1002}, {a1001, b1002, c1003}. Then, then attribute sets are converted as a1001", "a1001 and b1002", "a1001 and b1002 and c1003 to as the input for encryption. The 50 attribute sets are generated as same as above in KeyGen and these attributes sets are used to create SKω. To calculate the cost of the KeyGen procedure is executed for 10 times. To get the mean value the procedure is executed in 10 times. In decryption, the size of cipher text is fixed is set to 128 bit in the AES encryption key. To get the cipher text and SKω, the encryption and KeyGen steps are repeated as above. To ensure the accomplishment of decryption, the attribute set that are used in the KeyGen necessarily be utilized in the encryption. To get the mean value In, executed for 10 times. The server on Ubuntu 10.04 LTS, kernel 2.6.32-pae-32 bit, python 2.6.5, GCC 4.4.3, with 2 x Intel Xeon E5606 @2.13GHz CPU, 4 x 4GB of RAM are used to run these experiments.

The experimental evaluation output is shown in the Fig. 3-5, respectively. The cost of the libfenc is indicated with red line and the cost of the pyabelib indicated in the black line, definite, computational cost of the every step of CP-ABE scheme indicated by the blue line.

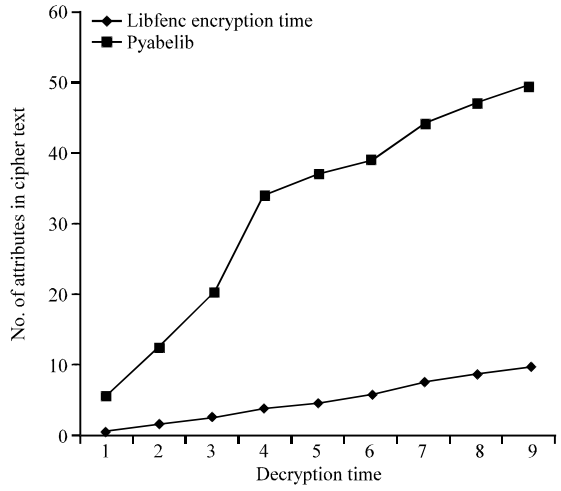

Fig. 5: Evaluation of pyabelib: decryption

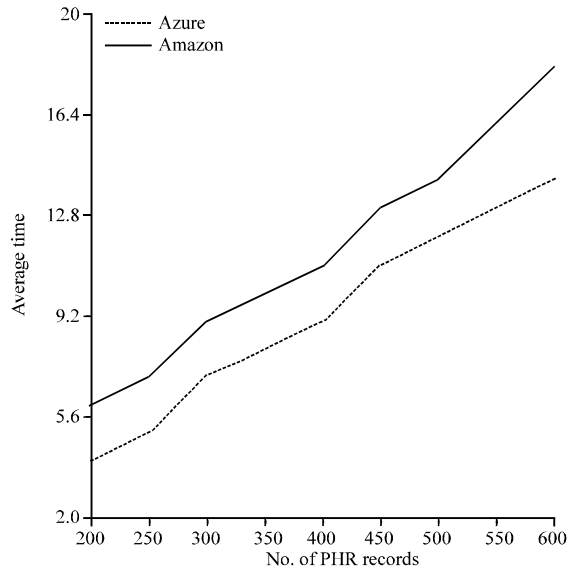

Fig. 6: Average time

The performance of pyabelib is reliable along with libfenc indicated by the red line which fully overlaps with the black line. The processing time eventually maximized linearly with the total number of leaf nodes present in addition to the cost of reading file is 0.5-0.7 sec.

As usual, time cost is adequate, therefore, it's practical for to merge CP-ABE with Indivo X. KeyGen is generally fewer than 1 sec below the 50 leaf nodes, the server. The server does not have much operating cost.

The time taken for revocation is as shown in Fig. 6. The measured the time drift on Amazon and Azure cloud is shown in Fig. 7.

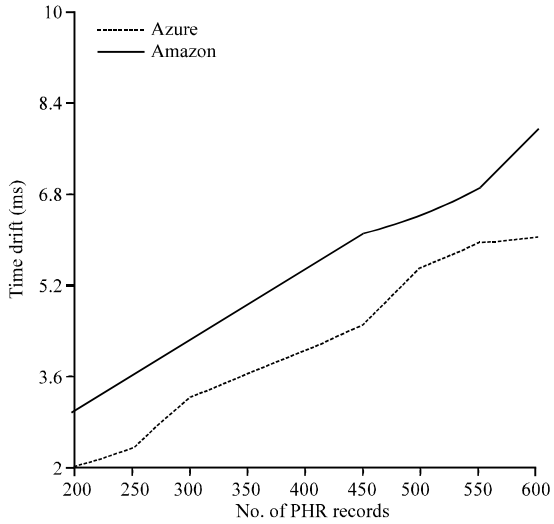

Fig. 7: Time drift calculation

CONCLUSION

Conventional access control instruments and in addition customary encryption procedures are not suitable to be utilized as a part of the general population PHR distributed computing situations which needs to give protection insurance and fine-grained access control. The CP-ABE plan has appeared to be more valuable in a medicinal services setting since, the entrance strategy is implemented by for all intents and purposes partner the entrance control strategy to the ensured information. This evacuates the requirement for including a trusted substance which needs to uphold access strategies. In this study, we propose a patient-driven, security safeguarding PHR sharing model in cloud, utilizing CPABE to give security insurance and fine-grained access control. At that point, we plan and execute a PHR cloud stage in light of Indivo X. PHR information are encoded utilizing CP-ABE plot and are put away in the cloud.

REFERENCES

Akinyele, J.A., M.W. Pagano, M.D. Green, C.U. Lehmann and Z.N. Peterson *et al*., 2011. Securing electronic medical records using attribute-based encryption on mobile devices. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, October 17-21, 2011, ACM, Chicago, IL, USA., pp: 75-86.

Goyal, V., 2007. Certificate Rrevocation Using Fine Grained Certificate Space Partitioning. In: Financial Cryptography and Data Security. Sven, D. and R. Dhamija (Eds.). Springer Berlin Heidelberg, Berlin, Germany, pp: 247-259.

Goyal, V., O. Pandey, A. Sahai and B. Waters, 2006. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security, October 30-November 3, 2006, ACM Press, Alexandria, VA, USA., pp: 89-98.

Ibraimi, L., M. Asim and M. Petkovic, 2009. Secure management of personal health records by applying attribute-based encryption. Proceesding of the 6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009, June 24-26, 2009, IEEE, 0slo, Norway, Europe, pp: 71-74.

Li, M., S. Yu, K. Ren and W. Lou, 2010. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks, September 7-9, 2010, Singapore, pp: 89-106.

Mandl, K.D., W.W. Simons, W.C. Crawford and J.M.I. Abbett, 2007. Personally controlled health record for health information exchange and communication. BMC. Med. Inf. DecisMak., 7: 1-10.

Mell, P. and T. Grance, 2011. The NIST Definition of Cloud Computing. NIST Special Publication, Maryland, USA., Pages: 50.

Narayan, S., M. Gagne and R.S. Naini, 2010. Privacy preserving EHR system using attribute-based infrastructure. Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, October 04-08, 2010, ACM, Chicago, IL, USA., pp: 47-52.

Ostrovsky, R., A. Sahai and B. Waters, 2007. Attribute-based encryption with non-monotonic access structures. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 28-31, 2007, ACM, New York, USA., pp: 195-203-10.1145/1315245.1315270.

Sahai, A. and B. Waters, 2005. Fuzzy identity based encryption. Adv. Cryptol. Eurocrypt, 3494: 457-473.

Waters, B., 2011. Ciphertext-policy attribute-based encryption: An expressive, efficient and provably secure realization. Proceeding of the 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011, Springer Berlin Heidelberg, Taormina, Italy, pp: 53-70.

Yin, C. and R. Zhang, 2011. Access control for the smart meters based on ABE. Proceeding of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011, October 10-12, 2011, IEEE, Beijing, China, pp: 79-82.

Zheng, Y., 2011. Privacy-preserving personal health record system using attribute-based encryption. MS Thesis, Worcester Polytechnic Institute, Massachusetts, USA.