Determining Security and Efficiency of PHR using Different Algorithms with Attribute Based Encryption in Cloud Computing

Mr. Markad Shrikant Kacharu[1] Prof. Rahul B. Mapari[2]
[1,2]Maharashtra Institute of Technology, Aurangabad

Abstract— A PHR is nothing but the personal health record related to the patient and patient itself is responsible for maintaining his own personal health record. A Personal Health Record service allows a patient to create, manage, and control his personal health data from one place through the web, in this patient is the PHR owner and he has full rights towords his PHR such as storing ,retrieving ,deleting ,sharing ,provide read write access to the selected users. now here is our intension is to provide security to the PHR and also determining the efficiency of different algorithms in terms of execution speed , performance and most important storage requirements. In the previous work on this topic demonstrates that we required a huge cost for maintaining specialized data centers so instead of creating data centers we are outsourced our PHR data after encryption process. In this framework we have to consider two domains first is private domain and later is public domain. Private domain consist of the people who are very close to the patient such as friend ,family members ,caregiver etc.depending on the relation with the patient ,PHR owner decides the sharing policy . another domain is the public domain which consist of the people from different category such as doctor, insurance company, medical store etc. when PHR owner outsourcing his own PHR file at that time owner of that PHR decides to whom it is shared with. For this operation we are providing separate unique ID's to each and every category that are included in the framework. Another important flaws of existing work is single trusted agent,with this number of problems created ,as there are number of PHR owner and PHR users and when PHR is shared at that time user demand for secret key so as there are number of users so bottleneck is generated to the single trusted agent and we avoid this by using AA(Attribute Authority) by dividing the key distribution task to more than one attribute authority. Before outsourcing PHR on cloud first we have to make encryption process by using fine grained attribute based encryption . In this framework we are also providing different facilities to the PHR Owner such as Break Glass ,user revocation etc. for scalability and flexibility.

Key words: Security and Efficiency, PHR Algorithms, Encryption

I. INTRODUCTION

A personal health record, or PHR, is a health record where health data and information related to the care of a patient is maintained by the patient[2][3]. This stands in contrast to the more widely used electronic medical record, which is operated by institutions (such as hospitals) and contains data entered by clinicians or billing data to support insurance claims[3][4]. The intention of a PHR is to provide a complete and accurate summary of an individual's medical history which is accessible online. The health data on a PHR might include patient-reported outcome data, lab results, data from devices such as wireless electronic weighing scales or collected passively from a smartphone. The term "PHR" has been applied to both paper-based and computerized systems; current usage usually implies an electronic application used to collect and store health data. In recent years, several formal definitions of the term have been proposed by various organizations. It is important to note that PHRs are not the same as electronic health records (EHRs). The latter are software systems designed for use by health care providers. Like the data recorded in paper-based medical records, the data in EHRs are legally mandated notes on the care provided by clinicians to patients. There is no legal mandate that compels a consumer or patient to store her personal health information in a PHR[27][28]. PHRs can contain a diverse range of data, including but not limited to allergies and adverse drug, reactions chronic diseases ,family history, illnesses and hospitalizations imaging reports (e.g. X-ray), laboratory test results medications and dosing prescription record surgeries and other procedures vaccinations etc[5][6].

There are some procedure to enter the PHR data ,on way is to PHR owner write in his way and the another alternative is to upload the PHR file web[16][17][18].The terms electronic health records, personal health records, and patient portals are not always used correctly. The generally agreed upon definition of these terms relates mainly to the ownership of the data. Once data is in a PHR it usually owned and controlled by the patient. Most EHRs, however, are the property of the provider, although the content can be co-created by both the provider and patient[5][6]. A patient has a legal right in most states to request their healthcare data and under recent USA legislation those providers using a certified EHR will be required to provide an electronic copy as well. Electronic health records and electronic medical records contain clinical data created by and for health professionals in the course of providing care. The data is about the patient but the data resides in a health care provider's system. The patient portal is typically defined as a view into the electronic medical records. In addition, ancillary functions that support a health care provider's interaction with a patient are also found in those systems e.g. prescription refill requests, appointment requests, electronic case management, etc. Finally, PHRs are data that resides with the patient, in a system of the patient's choosing. This data may have been exported directly from an EMR, but the point is it now resides in a location of the patient's choosing. Access to that information is controlled entirely by the patient.

II. LITERATURE SURVEY

In the existing work a number of works used ABE to handle PHR efficiently on cloud [13], [14], [9], [15]. For security purpose attribute based encryption is used in the personal health record.Recently, Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast of CP-ABE [16] that allows changing privileges.But one problem is that the

length of encrypted file grows simultaneously for unrevoked users . In [17], a variant of ABE that allows transfer of access rights is proposed for encrypted EHRs. Ibraimi et al. [18] applied ciphertext policy ABE (CP-ABE) [19] to manage the sharing of PHRs, and introduced the concept of social/professional domains. In [20], Akinyele et al. investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cellphones so that EMR could be accessed when the health provider is offline.

The main problem of existing work is single key distribution authority. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys. In fact, different organizations usually form their own (sub)domains and become suitable authorities to define and certify different sets of attributes belonging to their (sub)domains (i.e., divide and rule). For example, a professional association would be responsible for certifying medical specialties, while a regional health provider would certify the job ranks of its staffs. Second, there still lacks an efficient and on-demand user revocation mechanism for ABE with the support for dynamic policy updates/changes, which are essential parts of secure PHR sharing. Finally, most of the existing works do not differentiate between the personal and public domains (PUDs), which have different attribute definitions, key management requirements, and scalability issues. Our idea of conceptually dividing the system into two types of domains is similar with that in [18]; however, a key difference is in [18] a single TA is still assumed to govern the whole professional domain.

III. FRAMEWORK AND ITS OVERVIEW

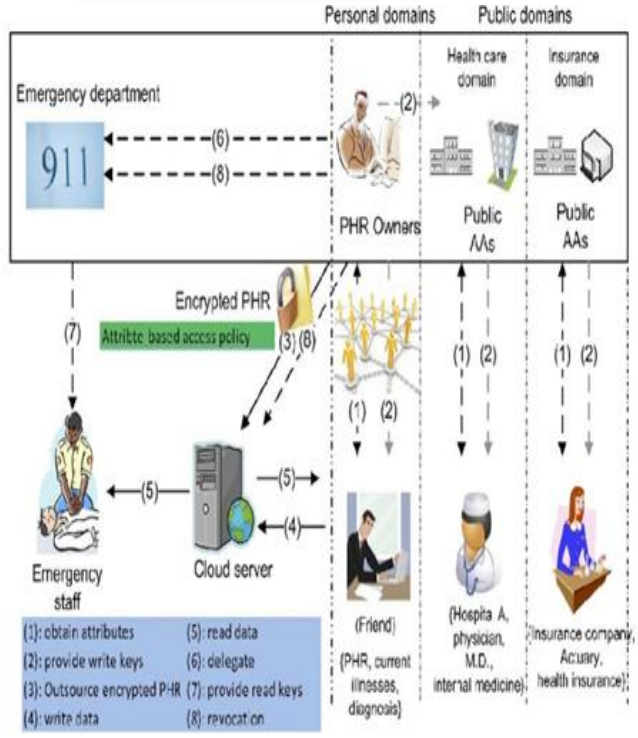

Fig. 1. Architecture of the system

The Proposed framework is basically divided into following entities and modules[1].

A. PHR Owner

PHR owner is responsible for creating his own PHR.To use the PHR system every PHR owner has to fill up the registration form,after his registration username and password is allocated to the respective PHR owner in order to create the PHR file.PHR owner decides to whom his PHR is share with.

B. User

The User is a person who may be doctor, medical, or from insurance company means simply the user is decided by PHR owner(only shared PHR is accessible to the respective person).for this project there is at most three users for each PHR doctor, medical and insurance company.

C. Doctor

There is separate login for each doctors to access the PHR records ,when PHR owner is sharing PHR with doctor if that doctor is agreed to provide treatment to the patient then he/she can demand for secret key that can be provided by attribute agent.

D. Insurance Company

It helps to keep track the records of the patient against the medical claim, because of this facility company will easily know all the details that are related to the each and every patient who want medical claim against different disease.

E. Cloud Server

In proposed framework, the server play role in interaction between user and system. We can stored all the patient PHR data on the server or there is another alternative to stored this data on the cloud.

F. Emergency Department

This is the emergency department that can be used in the break glass system.in this temporary access is provided to the hospital when they can be contacted with the emergency department.

G. Policy Update

A PHR owner can update her sharing policy for an existing PHR document by updating the attributes (or access policy) in the ciphertext. The supported operations include add/delete/modify, which can be done by the server on behalf of the user.

H. Break Glass

When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department (ED, (6)). To prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys (7). After the emergency is over, the patient can revoke the emergent access via the ED.

IV. RESULT ANALYSIS

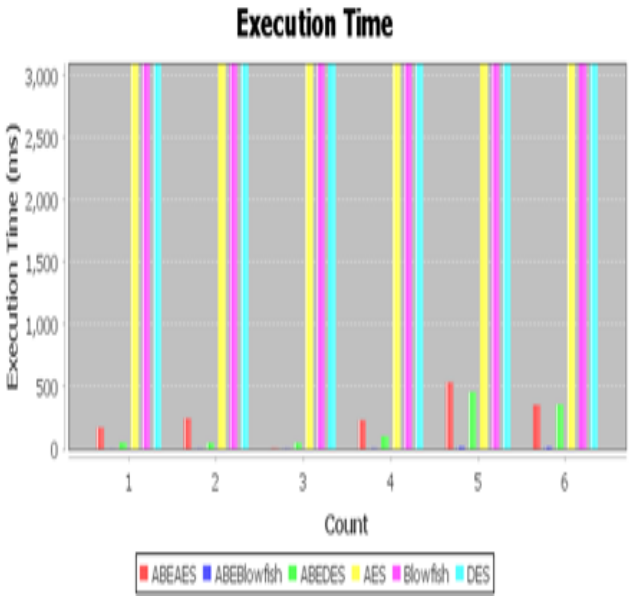

Fig. 2. comparison of execution time.

In this we provide six input and determine the time required to execute each PHR file.

Execute time=start time-end time

Algo	AES	DES	BLOWFISH	ABE AES	ABE DES	ABE BLOWFISH
Data Set	Output of different data sets					
1	37152	37222	36944	175	5	2
2	10042	10093	9684	248	51	3
3	8339	8390	7967	5	32	4
4	9181	9333	8679	233	104	6
5	16807	17069	15309	537	460	19
6	35740	36052	34820	355	360	17

Table 1: Representation of execution time in miliseconds.

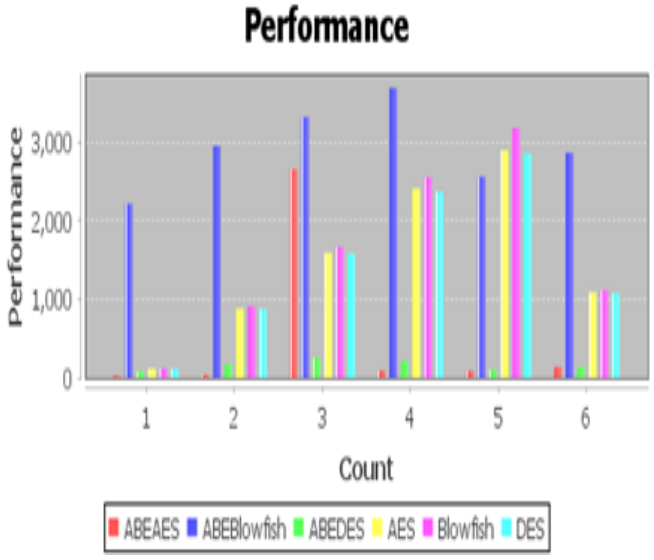

Fig. 3. Performance Graph.

The exact values for the performance graph can be shown in the following table and those algorithm provide better result can be indicated as the different colour. For calculation of performance we can use the same set of dataset that are used to calculate the execution time.

Performance=total length of file / total time of execution

Algo	AES	DES	BLOWFISH	ABE AES	ABE DES	ABE BLOWFISH
Data Set	Output of different data sets					
1	119	119	119	25	83	2215
2	882	877	914	35	173	2953
3	1593	1584	1668	2658	255	3322
4	2412	2373	2552	95	212	3691
5	2899	2854	3183	90	105	2554
6	1088	1079	1117	137	135	2866

Table 2: Performance graph values.

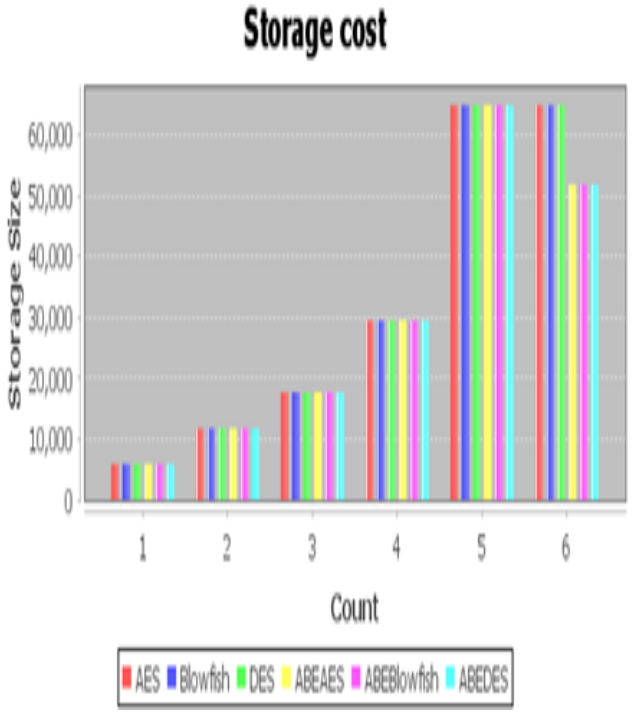

Fig. 4. Storage Cost Graph.

Storage cost can be considered in terms of memory storage requirement. When any PHR file can be encrypted by using any algorithm indicates the total memory used to stored that file.following table shows representation of storage cost graph in terms of values.

Storage cost=total length of file in bytes

Algo	AES	DES	BLOWFISH	ABE AES	ABE DES	ABE BLOWFISH
Data Set	Output of different data sets					
1	5912	5912	5908	5912	5912	5908
2	11820	11820	11816	11820	11820	11816
3	17728	17728	17720	17728	17728	17720
4	29548	29536	29536	29548	29536	29536
5	64984	64984	64976	64984	64984	64976
6	51904	51896	51884	64984	64984	64976

Table 3: Storage Cost Values in Bytes.

V. CONCLUSION

In this way we have to effectively implement the novel framework for fine-grained access control to personal health record with flexible revocation capability. After encrypting PHR file we have to analyse some algorithm in terms of execution time, performance, storage cost and finally conclude that among all algorithm attribute based encryption using blowfish algorithm provides better results as compare to other algorithms. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management when the number of owners and users in the system is large. We utilize multi-authority attribute-based encryption to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from different public domain.

REFERENCES

[1] Ming Li, shucheng Yu, Yao zheng "scalable and secure sharing of PHR in cloud computing using attribute based encryption Vol.24 Jan 2013
[2] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.
[3] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safe-guarded," http://articles.latimes.com/2006/jun/26/health/ he-privacy26, 2006.
[4] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.
[5] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.
[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM '10, 2010.
[7] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.
[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.
[9] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.
[10] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryp-tion with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.
[11] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009.
[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.
[13] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010.
[14] X. Liang, R. Lu, X. Lin, and X.S. Shen, "Patient Self-Controllable Access Policy on Phi in Ehealthcare Systems," Proc. Advances in Health Informatics Conf. (AHIC 10), 2010.
[15] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.
[16] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.
[17] J.A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin, "Self-Protecting Electronic Medical Records Using Attribute-Based Encryption," Cryptology ePrint Archive, Report 2010/565, http://eprint.iacr.org/, 2010.
[18] M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009.
[19] X. Liang, R. Lu, X. Lin, and X.S. Shen, "Ciphertext Policy Attribute Based Encryption with Efficient Revocation," technical report, Univ. of Waterloo, 2010.
[20] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
[21] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,"Proc. ACM Symp.

Information, Computer and Comm. Security (ASIACCS), Mar. 2011.
[22] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Comm. (TrustCom), 2011.
[23] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," EUROCRYPT: Proc. 30th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp 568-588-2011
[24] "Indivo." http://indivohealth.org/, 2012.
[25] S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-Encryption: Management of Access Control Evolution on Outsourced Data," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), pp. 123-134, 2007.

