An Integrated System for Personal Health Record in Cloud Computing Using Attribute-Based-Encryption

Mrs. A.KOUSAR NIKHATH[1], R.VASAVI [2], BOGA MAMATHA[3]
Assistant Professor[1,2], M.Tech[3], Software Engineering[3]
Department of Computer Science and Technology
VNRVJIET, Hyderabad-90, India
Email: kousarnikhath@vnrvjiet.in[1], vasavi_r@vnrvjiet.in[2], mamthaboga16@gmail.com[3]

Abstract- Cloud Computing offers unique opportunities for supporting long-term record preservation. We present MyPHRMachines, a cloud-based PHR system that answers our research question. Personal health record (PHR) as “a set of computer-based tools that allow people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it”. Personal Health Records (PHRs) is based on cloud virtual machine in web oriented application in which the lifelong health data of patients, who should be able to show them conveniently and securely to selected disables in a institution. MyPHRMachines is a cloud-based PHR system taking a radically new architectural solution to health record portability. After uploading their medical data to MyPHRMachines, patients can access them again from remote virtual machines that contain the right software to visualize and analyze them without any need for conversion. Patients can share their remote virtual machine session with selected caregivers[1].

Keywords: PHR Access Systems, PHR(Personal Health Records), Cloud Computing, ABE(Attribute-based-Encyption

1. INRODCUTION

A personal health record is a record where health related data and information is maintained by patient itself. This contrast to electronic medical record, which is maintained by institutions (like hospitals) and contain data entered by clinics, to support insurance claims. The aim of PHR is to provide accurate and complete medical history of individual which is accessible online[1]. PHR includes health data like diagnosis, treatments, doctors notes, patients notes, observation reports etc. The Personal health record is not a new term, it applies to both paper-based and computerized systems, but currently it applies to an electronic application used to retrieve and store the health data.[3]

It is important to know that PHR’s are not same as EHR’s. This software system is designed for the use of health care providers, the data in paper based medical records, from PHR is legally mandated notes on the care provided by clinics to patients but there is no legal mandate that compels a patient to store their personal health information in PHR. Patient can enter data directly by typing into fields or by uploading or by transmitting data from a file or another website.

Not all PHR’s have the same capability , individual PHR can support one or all of these methods. PHR allows patients to access the wide range of health knowledge. The entire medical records of an individual is stored at one place instead of paper based files in doctor’s offices or care institutions.

PHR’s has potential to analyze an individual health profile and identify health threats and improve opportunities based on analysis of interaction, current best medical practices, breaks in medical plans and identify medical errors. It can track patient illness in conjunction with health care providers. PHR makes communication facility easy and continuous for clinicians to care for their patients. Eliminating communication barriers and allowing documentation flow between patients and clinicians in a timely fashion can save time consumed by face-to-face meetings and telephone communication . Improved communication makes the process easy for patients and care givers to ask questions, make appointments, to report a problems, to request refills and referrals. In case of emergency PHR can provide critical information to proper diagnosis or treatment fast[1].

2 ARCHITECTURE OF PHR SYSTEMS

The PHR Access system model clearly distinguishes PHR data from the software to work with these data. We can demonstrate how this provide novel opportunities of the PHR software service without compromising the patient privacy in the market . PHR access systems allows patients to build PHRs by the *space* and *time* dimensions.

Space: Patients travelling or relocating across different countries during their lifetime will always be able to reproduce their original health record and the software required to visualize those. This is currently not possible because of high functional and architectural heterogeneity of health care information systems across different countries/states.

Time: As technology evolves, the software application can becomes obsolete.

In the server-side, PHR systems prevents attribute based problems by virtualization in the execution environment. The software creates the contemporary hardware and software and it is maintained by big vendors. In the client-side, PHR access systems rely on contemporary web technologies. Hence client software maintenance is decoupled from the number and complexity of PHR software services. PHR systems offers functionalities like share, visualize, and analyze PHR data[4]. PHR access systems also enables its users to share software with the health-related data, keeping data and software clearly separated in the system architecture. The separate data and functionality allows access to different stakeholders[8]. PHR access systems allows patients to reveal selected health information to other stakeholders and it guarantees that once shared to stakeholder, health information can be stored properly. Firstly, the software specialists deploying third party PHR services that never get access to patient data. Secondly, even those who have been given access to patients remote VM sessions cannot use or store the data/software. Currently available PHR systems do offer selective attribute mechanisms, but can cause fundamental privacy threats in this context[1,4]. Figure 1 shows the architectural view of PHR systems

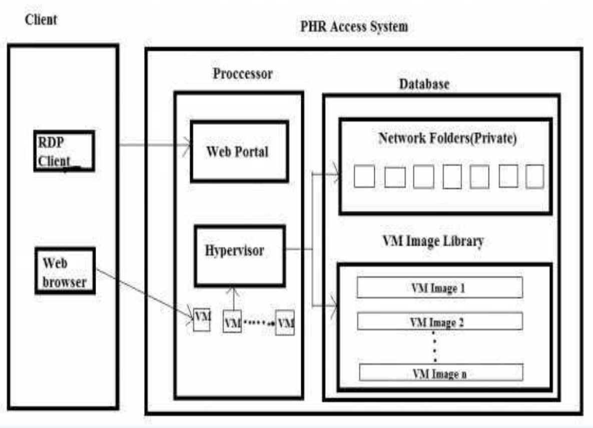
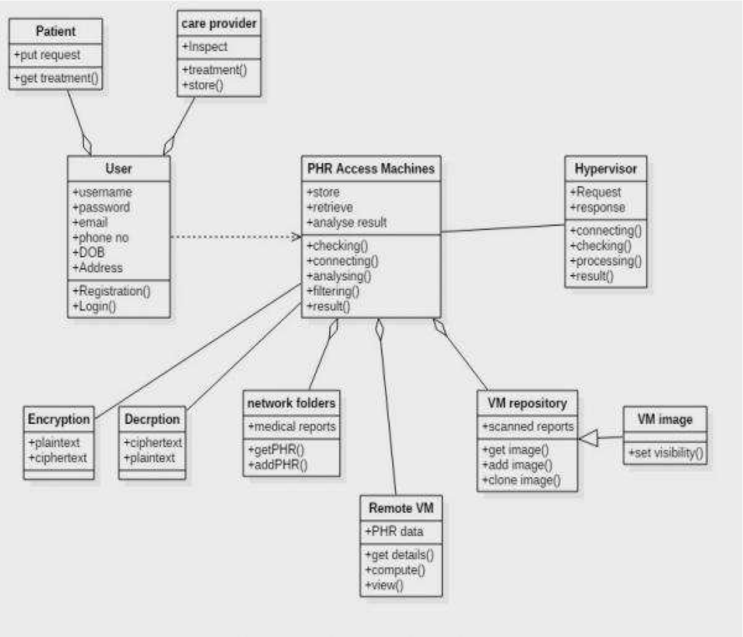


Figure 1. Architecture of PHR systems

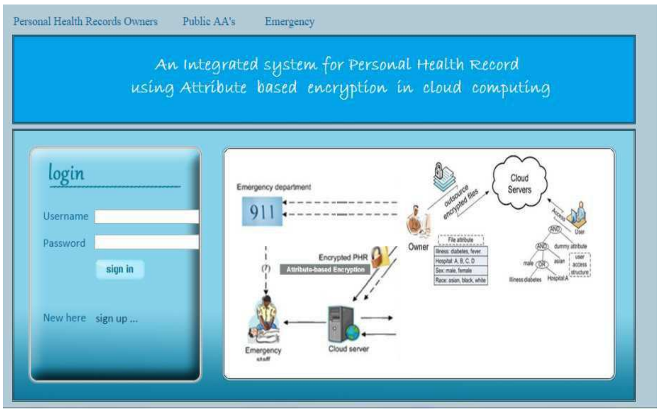
3. MODELLING OF PHR SYSTEMS

Every user(Patient) must type in, scan, or download salient portions of his/her medical records(like treatments, medication, doctors notes, patients notes etc). This type PHR owner is portable user[1]. He/she can move it among health care setting, employers and insurers. Care providers may or may not have the means in the PHR when they make treatment decisions.[1] Figure 2. Shows the structure of PHR system.



.

Figure 2. PHR Access system model



Personal Health Records Owners Public AA's Emergency

An Integrated system for Personal Health Record
using Attribute based encryption in cloud computing

login

Username

Password

sign in

New here sign up ...

Figure 3. Homepage of PHR Access systems

4. ACHIVEING PRIVACY AND SECURITY

Personal health record contains all the health data and information of a patient. So patient seek for the privacy, this privacy is provided by only a patient can have access to this personal health record by username and password. When comes to security issue there will be provided a secret key to access the patient record since the data stored is encrypted. We provide this encryption by the RSA algorithm.

4.1 Why RSA?

There are many cryptographic algorithms available in the market for encrypting the data. The strength of encryption algorithm relies on the computer systems that used for key generation. Algorithms like AES, RSA, MD5[9,10]. AES is better secured algorithm when compared to RSA but to encode a message, the receiver has to have the key, so there is a problem with key exchange. This problem can be solved bt RSA. Figure5 shows RSA processing.

4.2 RSA(Cryptography)

RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. It uses Variable size keys and Variable size blocks of data. Two prime numbers are used for generating the public key and private key, which are used for encryption and decryption.[12,13]. RSA uses three steps:

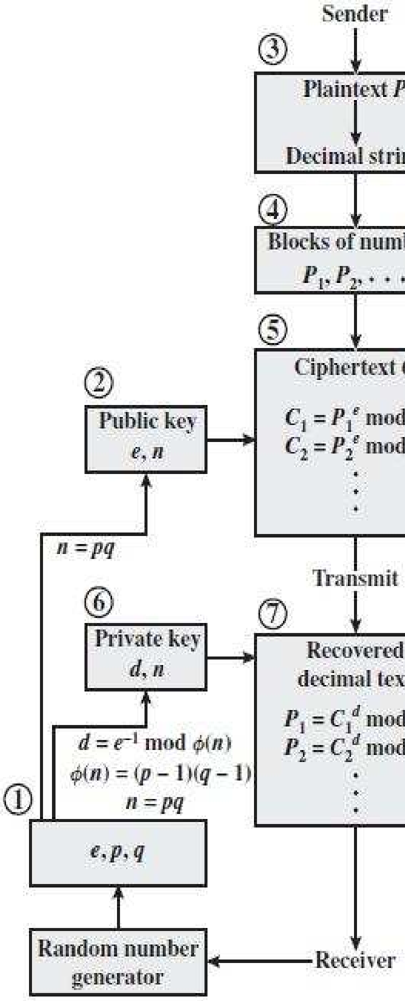


Figure 4. RSA processing Multiple blocks [10]

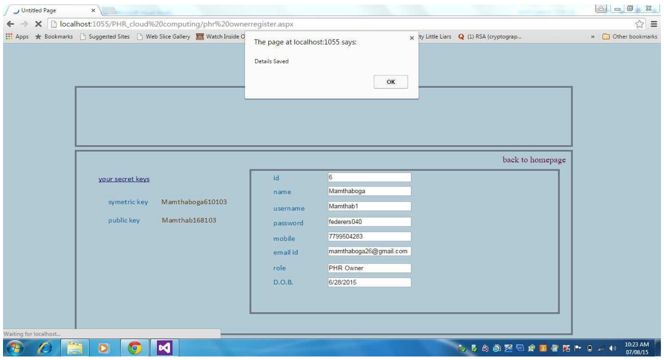
1) key generation

- Choose two distinct large random prime numbers p & q such that p ≠ q.
- Compute n= p × q.
- Calculate: phi (n) = (p-1) (q-1).
- Choose an integer e such that 1<e<phi(n)
- Compute d to satisfy the congruence relation d × e = 1 mod phi (n); d is kept as private key exponent.
- The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

2) Encryption
- Plaintext: P < n
- Ciphertext: C= Pe mod n.

3) Decryption
- Ciphertext: C
- Plaintext: P=Cd mod n.

5. IMPLEMENTING PHR ACCESS SYSTEMS



The page at localhost:1055 says:

Details Saved

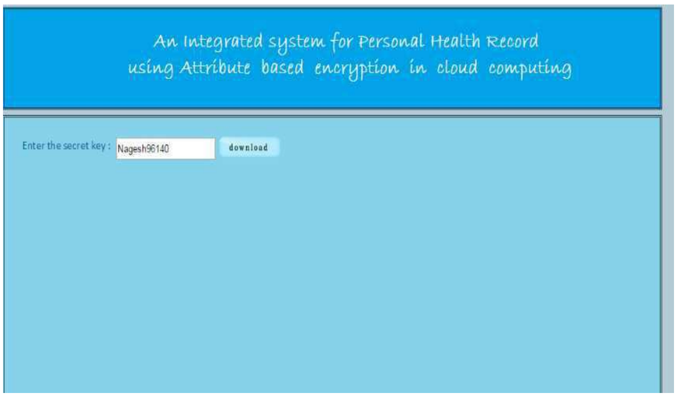
your secret keys

symetric key Mamthaboga610103

public key Mamthab168103

id 6
name Mamthaboga
username Mamthab1
password federers040
mobile 7799504283
email id mamthaboga26@gmail.com
role PHR Owner
D.O.B. 6/28/2015

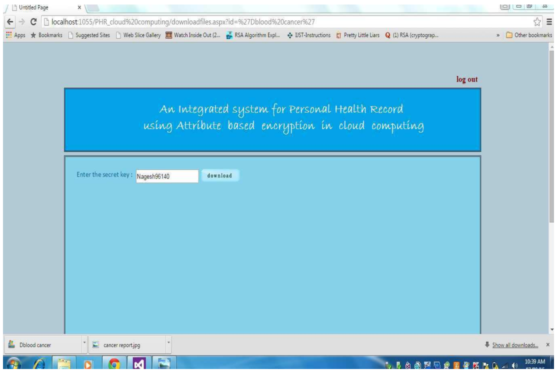
Figure 5. Keys generated after registered



An Integrated system for Personal Health Record using Attribute based encryption in cloud computing

Enter the secret key : Nagesh96140

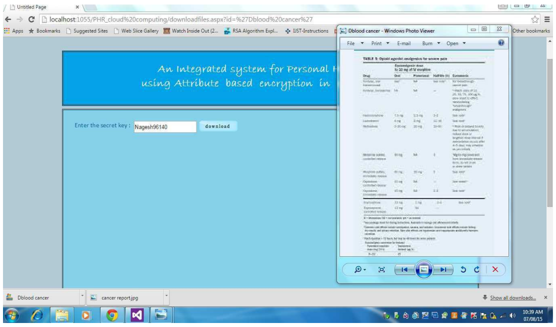
Figure 6 To download the file should enter key



An Integrated system for Personal Health Record using Attribute based encryption in cloud computing

Enter the secret key : Nagesh96140

Figure 7. file downloaded



Untitled Page

localhost:1055/PHR_cloud%20computing/downloadfiles.aspx?id=%27Dblood%20cancer%27

An Integrated system for Personal H
using Attribute based encryption in

Enter the secret key : Nagesh96140 download

Dblood cancer - Windows Photo Viewer

Figure 8. File view

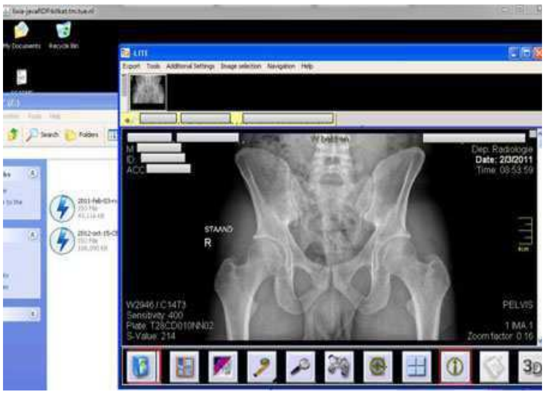
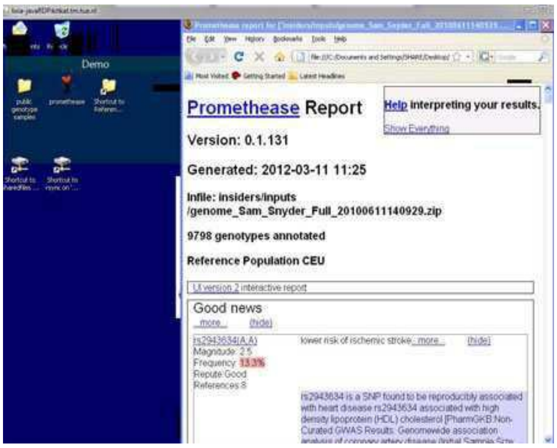


Figure 9. Radiology scan report



Promethease Report

Help interpreting your results.

Show Everything

Version: 0.1.131

Generated: 2012-03-11 11:25

Infile: insiders/inputs
/genome_Sam_Snyder_Full_20100611140929.zip

9798 genotypes annotated

Reference Population CEU

UI version 2 interactive report

Good news

rs2943634(A;A) lower risk of ischemic stroke
Magnitude: 2.5
Frequency: 13.3%
Repute: Good
References: 8

rs2943634 is a SNP found to be reproducibly associated with heart disease rs2943634 associated with high density lipoprotein (HDL) cholesterol [PharmGKB Non-Curated GWAS Results: Genomewide association

Figure 10. Genetic Data report

6. LIMITATIONS

Most people do not keep record of their healthcare data, so they find it difficult to make use of web-based PHRs. So the sites selected for evaluation offered limited functionalities to the public. Less adoption of web-based PHRs can be a direct result of limitations in these applications. The development of PHR should be guided by ample of patient-oriented research in future[1]. We can differentiate the limitation of our work from the one related to the functionality of PHR Access system which is currently implemented and the ones related to the research method adopted for its evaluation. We can overcome this issue by a careful and accurate design of the interface of PHR access system used by patients to upload, share, and organize their PHR data, which should be intuitive and secure the technical details[3,4].

7. FUTURE ENHANCEMENTS

PHRs are the lifelong data which resides with the patient itself. This data may be exported directly from an EMR, but the point is that it resides in a location of the patient's chosen systems. Access to that information is controlled entirely by the patient. A new concept is being discussed is that UHR or "universal health record", which can be a patient centered and controlled body of information that could be shared in a granular way to particular health care providers[4]. This project would enlist open source contributions and enhancements from developers, with particular emphasis on supporting patient expectations of privacy and responsible for patients control of private health information (PHI). It is expected that effective implementation of one or more "open source" approach to the UHR would benefit both providers and patients, including cost-effective solutions to currently difficult problems including entry/verification/update of personal health data[6], enable the responsibility of patient-controlled granular release of PHI, and support the interoperability and effective collaboration of patients and physicians across disparate EHR/PHR platforms[12].

8. CONCLUSION

PHR access system provide a novel lifelong health secured data. Leveraging virtualization techniques, PHR access systems allows patients to build lifelong PHRs. As technology evolves patients will always be able to use original and secured software to view and analyze health data, even when that software becomes obsolete and possibly no longer supported by the stakeholder that produced the data.

Acknowledgement

I would like to acknowledge the support of the VNRVJIET for providing this opportunity and also greatful to the CSE department HOD Dr.B.Raveendra Babu garu, and also our M.Tech coordinator R.Vasavi. I am also grateful to my guide Mrs.A.Kousar Nikhath who encouraged me to pursue this topic and spent extra time helping me to achieve a clearer structure.

REFERENCES

[1] Lifelong personal health data and application software via virtual machine in the cloud(2014) by Peter Van Gorp and Marco Commuzi.

[2] William Stallings, “Cryptography and network Security: Principles and Practice”, Pearson Education or Prentice Hall, 5th Edition.

[3] AHIMA e-HIM Personal Health Record Work Group, “Defining the personal health record,” J. AHIMA, vol. 76, no. 6, pp. 24–25, Jun. 2005

[4] Health Informatics—Electronic Health Record—Definition, Scope and Context, International Standards Organization, ISO/TR 20514:2005, Jan. 2005

[5] Wetterstrand. (2012, Jan.). DNA sequencing costs—Data from the NHGRI large-scale genome sequencing program. [Online]. Available:http://www.genome.gov/sequencingcosts/

[6] Van Gorp and P. Grefen, “Supporting the internet-based evaluation of research software with cloud infrastructure,” Software. Syst. Model, vol. 11, no. 1, pp. 11–28, 2012.

[7] Wang, X. Liu, and W. Li, “Implementing a personal health record cloud platform ciphertext-policy attribute-based encryption,” in Proc. 4th IEEE Int. Conf. Intell. Network. Collaborat. Syst, Sep. 2012, pp. 8–14

[8] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based en-cryption,”IEEE Trans. Parall. Distrib. Syst., vol. 24, no. 1, pp. 131–143,Jan. 2013

[9] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm’s", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.

[10] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118, 1121, 2011.

[11] N. Archer, U. Fevrier-Thomas, C. Lokker, K. A. McKibbon, and S. E. Straus, “Personal health records: A scoping review,” J. Amer. Med. Inform. Assoc., vol. 18, pp. 515–522, Jul. 2011.

[12] A. S. McAlearney, D. J. Chisolm, S. Schweikhart, M. A. Medow, and K. Kelleher, “The story behind the story: Physician skepticism about relying on clinical information technologies to reduce medical errors,” Int. J. Med. Inf., vol. 76, no. 11–12, pp. 836–842, 2007.

Authors Profile

My guide, Mrs. A.Kousar Nikhath is working as Asst. professor at VNRVJIET. She is received B.Tech and M.Tech degree in Computer Science and Engineering and currently pursuing Ph.D at KLUniversity. Her main research interest includes Text mining, Data mining, Artificial Intelligence and Network. Modeling and Simulation

My coordinator, R.Vasavi is working as Asst. professor at VNRVJIET. She is received B.Tech, M.Tech in Computer Science and Engineering. Her main research interest are Software Engineering, BigData Analysis and Operating Systems

B.Mamatha pursuing M.Tech Software Engineering in VNRVJIET. I have received B.Tech degree in Computer Science and Engineering. My area of interest are Cloud Computing and Big Data.