# A Frame Work for Ensuring Security and Privacy of PHR'S

G Kumari, M Naveen Kumar, Dr. A Marysowjanya

1.**Research Scholar**, Department of Computer Science and Systems Engineering, Andhra University.

2. **Assistant Professor,** Department of Computer Science and Engineering, TKRCET.

3.**Assistant Professor**, Department of Computer Science and Systems Engineering, Andhra University.

*gubbala.kumari@gmail.com, navin.it27@gmail.com, sowmaa@yahoo.com*

**Abstract**: Creating procedures to safely store information crosswise over cloud is a quite interesting research topic of late. Distributed computing concentrates on amplifying the viability of the common assets and is advantageousfor putting away / recovery of enormous measure of information. Personal Health Records (PHRs) areconsidered to remain the long lasting property of patients and have to be displayable helpfully and safely to choose guardians. My PHR Machine is a patient driven framework that takes a new structural approach for PHR interoperability. Patients can upload their medical information and share through remote Virtual machine. We have made a study on methods to secure PHRs and discover open model of My PHR Machines for the utilization instance of a certifiable patient situation.

***Keywords*** *: Privacy, healthcare, Cloud,security, Virtual machines, PHR, Distributed Computing.*

*****

## 1. Introduction

Distributed computing open doors for supporting long haul record protection. My PHR Machines [1] is a patient claimed wellbeing record framework model in light of remote virtual machines facilitated in the cloud. It is especially encouraging for nations with an exceptionally heterogeneous engineering of frameworks crosswise over doctor's facilities and other care organizations. PHRs ought to be versatile since PHR frameworks offer usefulness to share, imagine and break down PHR information. My PHR Machines Secure deep rooted administration of patient restorative records since information is put away in the cloud and doesn't have to be conveyed by patients.

## 2. Background work

A patient probability of approaching a hospital nearby his/her locality is very high and goes through standard registration. The data is put away in their local database. At some instant of the time the patient needs to go to another medicinal service because reasons like inaccessibility of administration on siestas, requirement for specific wellbeing etc. The data put away in the local databases is just available to the workers of that center only and consequently stream of data gets restricted. Instead of putting away data on local database we can store this data outside i.e. cloud benefit supplier. In this study the issues of Security andUser Revocation are identified

The rest of the paper is as follows: Section 3 gives the structural representation of cloud based PHR stockpiling frameworks. Area 3 gives the structural representation of cloud based PHR stockpiling frameworks. Area 4 briefs about Proposed Techniques Securing PHR. Area 5 gives a wide outline of dialog of test results completed. Segment 6 finishes up the paper and layouts the future work. In this paper we made a successful attempt to address the above recognized issues of any PHR.

## 3. Cloud based PHR

### 3.1 Structural Representation:

The compositional representation of cloud based PHR stockpiling is spoken to in Fig 1. The entrance assumes an essential part in transferring of information, remote get to maintenance, begin/stop operation. PCAS get to is utilized to give and show data. The cloud assumes the liability of mounting the PHRs.

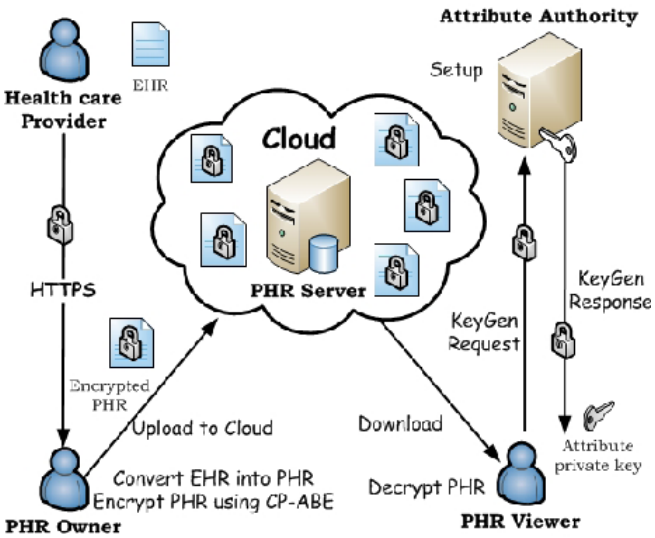


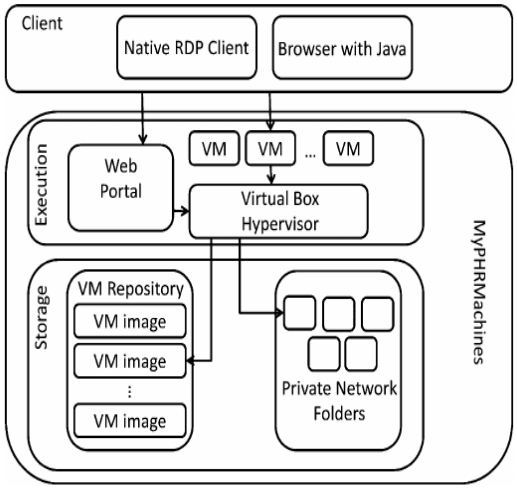

Fig. Structural example of Cloud based PHR

### 3.2 Compositional representation

The primary segment of My PHR Machine comprises of online interface which connects with Virtual Box Hypervisor. Virtual Machines are associated together with

 ISSN: 2321-8169
274 – 277

Virtual Box Hypervisor. The second part of My PHR Machine, stockpiling comprises of VM Repository which houses VM Data and Private Network organizers as showed in Figure 2.




**Work flow of PHR AND VM**

## 4. Proposed Approach

Existing strategies for securing PHR are Paper based PHRs, electronic gadget based PHRs and Web based PHRs [1]. PHR frameworks generally offer usefulness to see the PHR information and have no specialized measures to avert information misuse by the modules that are contributed by outside programming merchants. In our approach My PHR Machine can control the entire system by providing a privacy and security framework. Also PHRs are kept compact to make simple updations and proper recovery.

### 4.1Ensuring Security in PHR's using Blowfish algorithm:

Since PHR's security is always a concern for many patients/clients/organizations, in our proposed model we use Blowfish algorithm for encryption and decryption of data.

An encryption algorithm plays an important role in securing the data in storing or transferring it.

Blowfish is a symmetric block encryption algorithm designed in consideration with,

- **Fast:** It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.
- **Compact:** It can run in less than 5K of memory.
- **Simple:** It uses addition, XOR, lookup table with 32-bit operands.
- **Secure:** The key length is variable; it can be in the range of 32~448 bits: default 128 bits' key length.
- It is suitable for applications where the key does not change often, like communication link or an automatic file encryptor.
- Unpatented and royalty-free.

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

**Pseudo code.**

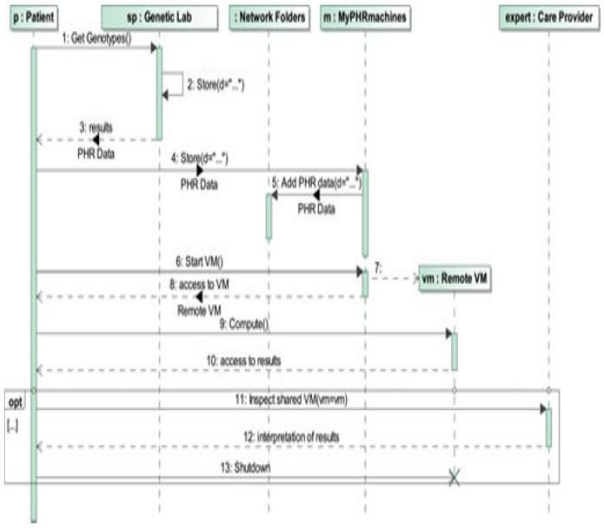
```
uint32_t P[18];
uint32_t S[4][256];

uint32_tf (uint32_t x) {
uint32_t h = S[0][x >>24] + S[1][x >>16&0xff];
return ( h ^ S[2][x >>8&0xff] ) + S[3][x &0xff];
}

voidencrypt (uint32_t& L, uint32_t& R) {
for (int i=0 ; i<16 ; i +=2) {
    L ^= P[i];
    R ^= f(L);
    R ^= P[i+1];
    L ^= f(R);
  }
  L ^= P[16];
  R ^= P[17];
  swap (L, R);
}

voiddecrypt (uint32_t& L, uint32_t& R) {
for (int i=16 ; i >0 ; i -=2) {
    L ^= P[i+1];
    R ^= f(L);
    R ^= P[i];
    L ^= f(R);
  }
  L ^= P[1];
  R ^= P[0];
  swap (L, R);
}
{
// ...
// initializing the P-array and S-boxes with values derived
from pi; omitted in the example
```

 ISSN: 2321-8169
274 – 277

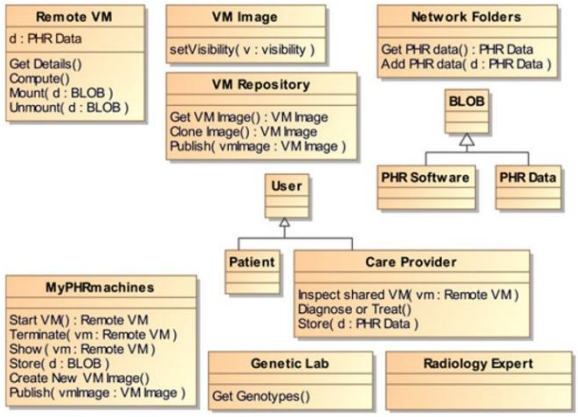
```
// ...
for (int i=0 ; i<18 ; ++i)
    P[i] ^= key[i % keylen];
uint32_t L =0, R =0;
for (int i=0 ; i<18 ; i+=2) {
    encrypt (L, R);
    P[i] = L; P[i+1] = R;
  }
for (int i=0 ; i<4 ; ++i)
for (int j=0 ; j<256; j+=2) {
      encrypt (L, R);
      S[i][j] = L; S[i][j+1] = R;
    }
}
```

### 4.2 Ensuring privacy in PHR's:

Below is the interaction model of our proposed framework




This is briefed in the UML chart specified below representing the Virtual machines, virtual machine repo's, client and user interface for interactivity and remote access to the central patient records.

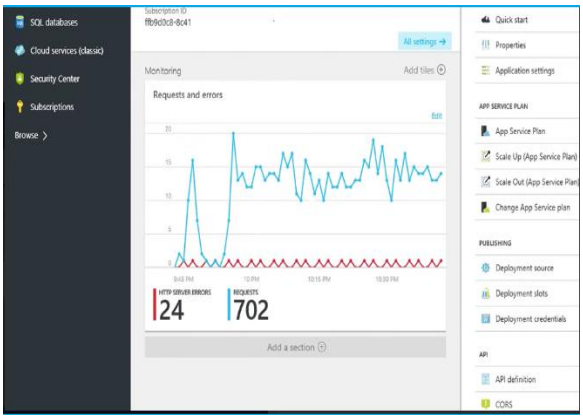



In our proposed model, client interacts with the virtual machines running in the cloud through an encrypted connection. Data in the virtual machines is stored in the form of blobs. Connect () function is used to initialize the communication from the client side, for which the vm running in the cloud replies with the set of parameters to be sent for validation and authentication. After successful validation and authentication, a secure channel is established between the client machine and vm. Required data operations are made through various data handling functions using CLI and the communication channel is terminated.

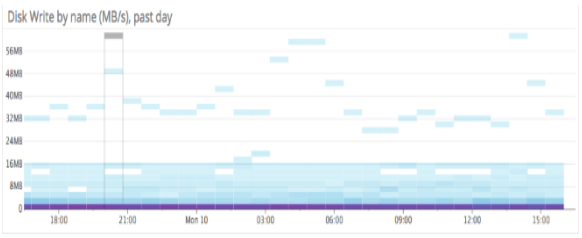
## 5. Results

My PHR Machines permits patients to fabricate PHRs which are strong crosswise over two specific measurements:

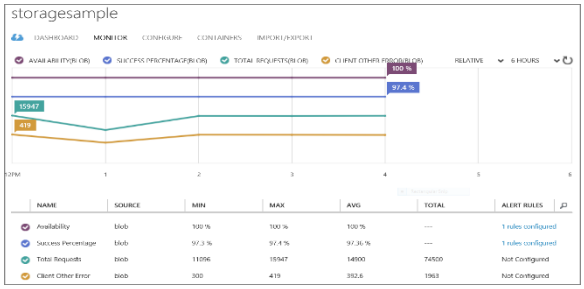
1. Space Dimension
2. Time Dimension




Snapshot of Virtual machine in cloud



Disk usage statistics of VM with PHR Data




Statistics of Virtual machine I/O request from PHR

## 6. Conclusion and Future work:

In this paper thorough research is carried on various computing models deployed in various virtual machines in cloud (Microsoft Azure). Results are also observed with various test cases. A secure framework pertaining to privacy preserve of patient has been proposed and demonstrated using cloud. A frame work for ensuring security using Blowfish algorithm and to provide privacy has been developed because PHR's have sensitive information and are stored on a cloud. Thisframework protects privacy thus building trust of patients to use the websites designed with this framework. To make it convenient for the patients to use this service, their account can be combine with their social networking accounts like Facebook.it can be made suitable for Android devices in the future.

## References

[1] Mamidala Naveen Kumar, Shaik Khaja Hafeezuddin, G Kumari, " Secure Communication Algorithm in Web-Services", International Journal of Science and Research (IJSR), https://www.ijsr.net/archive/v5i11/v5i11.php, Volume 5 Issue 11, November 2016, 97 – 101

[2] Jiawen Kang, Xumin Huang, Rong Yu, Yan Zhang, Stein Gjessing, "Hierarchical mobile cloud with social grouping for secure pervasive healthcare", E-health Networking Application & Services (HealthCom) 2015 17th International Conference on, pp. 609-614, 2015

[3] Assad Abbas, Samee U. Khan, "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds

[4] Cong Wang, Sherman S.M. Chow, Qian Wang, "Privacy-Preserving Public Auditing for Secure Cloud Storage."

[5] Cong Wang, Kui Ren, Wenjing Lou, Toward publicly auditable secure cloud data storage services

[6] en.wikipedia.org/wiki/Blowfish_(cipher)

## Authors Profile

**G Kumari**, working as a research scholar at department of computer science in Andhra University. She has 9 Years of teaching experience in various areas such as Big Data mining, Artificial Intelligence and Data Analytics including using various cloud technologies such as Microsoft Azure, AWS, Heroku, Data mining and Big data.

**M Naveen Kumar,** working as an Assistant Professor at TKRCET. He has 9 Years of extensive teaching experience in various domains such as Data mining, machine learning and Big Data analytics including various cloud models.

**Dr.A. M. Sowjanya** has done her B.Tech and M.Tech in Computer Science. Her Ph.D is in Incremental Clustering. She is currently working as an Assistant Professor in College of Engineering, Andhra University. Her research interests include Data mining and big data.