Privacy Preserving Health Record System in Cloud Computing using Attribute based Encryption

Kushal P.Kulkarni
Department of Computer Engineering,
PVPIT/JSPM, Bavdhan, Pune,
Maharashtra, India

A.M.Dixit
Department of Computer Engineering,
PVPIT/JSPM, Bavdhan, Pune,
Maharashtra, India

ABSTRACT

Cloud computing is a modern as well as advanced computing technology, which provides flexible, on-demand, and low-cost usage of computing resources, but the information is outsourced to some cloud server providers, and various privacy concerns emerge from it. Different techniques based on the attribute-based encryption have been proposed to secure the cloud storage. Sharing of personal health record is an emerging patient centric model of health data exchange which is often outsourced by the third party such as cloud server. The confidentiality of the personal record is major problem when patient use commercial cloud server to store their health records, it can be viewed anyone is the Attribute-Based Encryption (ABE) has emerged as a promising platform providing end-to-end data security and privacy in cloud storage system. It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data. We also leverage Windows Communication Foundation (WCF) Technique that allows secure communication or exchange of data in real time. Personal Health Record (PHR) contains the details of the patient health which is monitored and handled by the patients and they can add, delete, and modify their own record.

General Terms

Cloud computing, Attribute based Encryption, Security, XML, SOAP, WSDL.

Keywords

Cloud computing, PHR system, Web Services, WCF, and Base-64.

1. INTRODUCTION

Cloud Computing is new emerging technology in business domain as well as in the health care sector or organization. Large number of healthcare institutes started migrating the electronic health information records to the cloud platform. Cloud can be concerned as a platform that stores gigantic or huge amount of health data and also acts as a structured management of health data across multiple service providers. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode. It is based on the internetwork and has the format of various services provided for the consumer [3]. Cloud computing system provides the service for the user and has the character of high security, scalability and reliability. The resource in the cloud system is transparent for the application and the user do not know the place of the resource. The users can access your applications and data from anywhere. Cloud computing model uses the third party service provider that manages the hardware and software resources with reduction of maintenance cost. Components of CC are organized into five categories, as shown in fig 1,

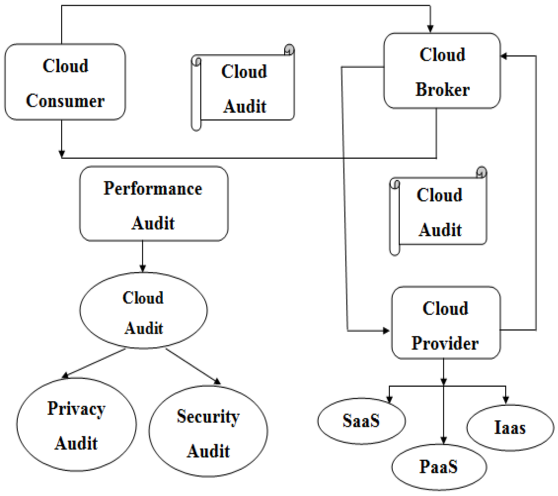


Fig 1: Cloud computing architecture

Cloud Consumer: It can be a person or organization who wants to use service from Cloud Providers.

Cloud Provider: It can be a person, organization or institute that provides the services to the users.

Cloud Auditor: It is a party who has to verify whether cloud provider is providing the services to user according to the service level agreement and user's requirement or not.

Cloud Broker: It is the intermediate between cloud provider and the user.

Cloud Carrier: It is a transport media by which services are routed towards the appropriate user.

Attribute-based Encryption (ABE) is an encryption technique that can achieve the fine grained access control with encryption in the manner that a user can only read the parts of data that they are allowed to read, or the data can only be read by a user with certain attributes. Therefore ABE is suitable for PHR system in the cloud in which many users can retrieve the same PHR while every user can only decrypt the parts that they are allowed to read. Data is encrypted using a set of attributes so that multiple clients who possess proper authorization can decrypt the data. Attribute-Based Encryption (ABE) not only provides fine-grained access control but also take action against collusion. Attribute Based Encryption (ABE) [7], [8] had been proposed for data encryption and decryption. ABE is an extension of IBE scheme in that multiple public known attributes as the public key.

The rest of the paper is organized as follows. Section II discusses architectural view of Proposed PHR System. Section III gives overview of design methodology i.e. modules. Section IV gives brief idea about the Web Services and Windows Communication Foundation [WCF] services. Section V mentioned algorithmic strategy implementation details and experimental results. Section VI concludes the discussion and highlights the open research issues and areas.

2. ARCHITECTURAL VIEW OF PROPSED PHR SYSTEM

Due to the high cost of maintaining and building specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft Health Vault. It is exciting to have convenient PHR services for everybody but, there are many security and privacy risks. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. In Existing system a PHR system model, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner whose PHR she wants to read would limit the accessibility since patients are not always online [1]. An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority. One of the disadvantage of existing system is there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. The proposed system is providing the fine-grained access control to the system by using the different attribute based encryption schemes. In this system, the users are classified into two security domains called Personal Security Domain and Public Security Domain as shown in fig 2. The users like family members, friends are included in the personal security domain (Private users) and the users from the health care sectors and insurance environment are considering as the data users from the public security domain (Public users). For both the two different set of user domain the variations of attribute based encryption is used. For the personal security domain the Key-policy attribute based encryption scheme is used. For the public security domain the Multiple-Authority attribute scheme is proposed.

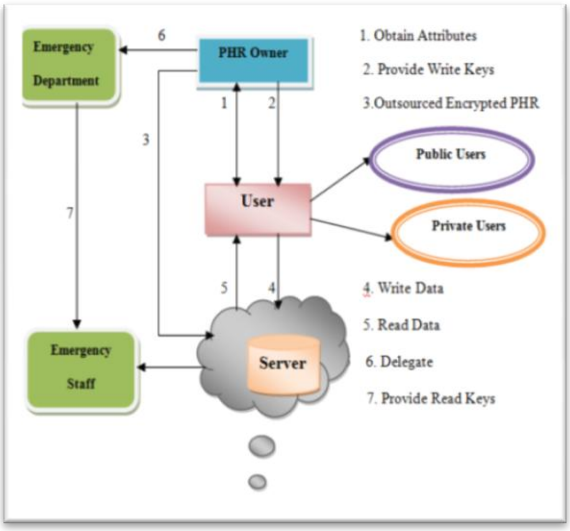


Fig 2: Proposed PHR System

In PSD, the owner used key-policy Attributed based encryption technique and generates secret key for their PSD clients and in PUD the multi-authority attribute based encryption scheme is preferred. Secret Key for PUD users are generated by multiple authorities depending on their both specialization and profession.

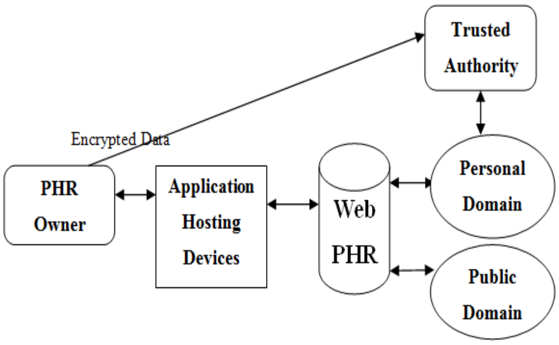


Fig 3: Architectural view of PHR

The scenario gives the idea about the need for a system which fulfills the following security requirements:

• Protect health records from network attacker. So, data is to be encrypted before it is sent to the web PHR. [6]

• Health records protected from third parties who store PHRs. The third party manages web PHRs which are not accessible to the plain data.

• The access policy concerned with the encrypted data, such that only those users having a secret key associated with set of attributes which satisfies the policy might be capable of decrypting it.

• Users from the professional domain and users from the social domain both need to be properly authenticated and authorized to access the data.

3. METHODOLOGY

The operations of proposed medical health data sharing system combine KP-ABE and Multi-authority ABE and traditional cryptography, allowing patients to share their health records. These operations can be divides into following modules:

- PHR owner Module
- Cloud Server Module
- Attribute based Access Policy Module
- Data Confidentiality Module

The main goal is to provide efficient key management and secure patient-centric PHR access at the same time. According to the various users' data access requirements we split the system into multiple security domains (i.e., personal security domains (PSDs) and public security domains (PUDs)).In PHR owner module every data owner (e.g., patient) is a trusted authority of her own PSD, who uses a key generation scheme to manage the secret keys of users in their personal domain (PSD). For PSD, data attributes are defined which refer to the intrinsic characteristics of the PHR data, such as the category of a PHR file. For the purpose of PSD access, each PHR file is labeled with its data attributes. Since the number of users in a PSD is often small, it reduces the burden for the owner. When encrypting the data for PSD, all that the owner needs to know about the intrinsic data properties. A PHR service permits a patient to create, manage, update, access and control their personal health data record in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient.

Cloud server module acts as a third party server which stores encrypted sensitive data of owner, the server will try to find out as much private information in the stored PHR files as possible, but they will honestly follow the protocol in general. The server is to be semi trusted, honest On the other hand; some users will also try to access the files beyond their privileges. For example, a chemist may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collide with other clients, or even with the server.

In our proposed framework, there are multiple domains, multiple owners, multiple authorities, and multiple users and additionally, two ABE [1] systems are involved named as read and write access as data readers and contributors, respectively. The health data privacy preserving in the cloud has multiple requirements to be fulfilled. The requirements include integrity, confidentiality, authenticity, security, reliability, accountability, audit, non-repudiation, anonymity, and unlink ability.

Data confidentiality module deals with Attribute Based Encryption. In this encrypted PHR files are uploading to the server by the owners. Every owner's PHR file is encrypted under a certain role-based and fine grained access policy for users from the public domain to access and under a chosen group of data attributes that allows access from users in the personal domain. The PHR files can be decrypt by the authorized users, excluding the server.

4. WEB SERVICES & WCF

4.1Web Services

Web Services are self contained, self describing, standards-based, language-agnostic software entity that accepts specially formatted requests from other software entities on remote machines via vendor and transport neutral communication protocols producing application specific responses. These services can be published, found and used on the web. Web services communicate using open protocol [9]. The extensible Markup Language (XML) is a W3C recommendation for creating special-purpose markup languages that enable the structuring, description and interchange of data. Building blocks of XML are, Elements concerned with pairing of a start tag and an end tag. Attributes consists of a name-value pair that is part of a starting tag of an Element. Processing Instructions are special directives to the application that will process the XML document. Comments deals with messages helping a human reader understand the source code. Character Data consists of characters in a specific encoding, Entities and Whitespace. Web services having two types of uses such as reusable application component and connect existing software.

Simple Object Access Protocol (SOAP) is an industry accepted W3C specification for XML distributed computing infrastructure. SOAP is an XML based protocol for accessing the web services. The root element of a SOAP message is the Envelope element. It contains an optional Header element and the required Body. Elements called Faults can be used to describe exceptional situations. It can contain optional attachments in MIME encoding for exchanging binary data. The SOAP Message Transmission involves three main roles as shown in fig.5 The SOAP Sender creates and sends a SOAP Message to an ultimate SOAP Receiver. One or more optional SOAP Intermediaries can be positioned to intercept messages between the sender and the receiver. They can perform filtering, logging, catching etc. The SOAP sender's intended destination is called the Ultimate SOAP Receiver. Transmission of SOAP message is shown in the fig as,

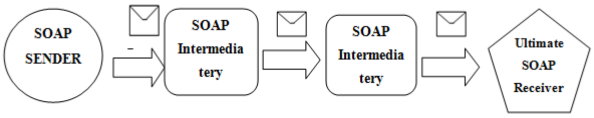


Fig 4: Transmission of SOAP Message

Web Services Description Language (WSDL) is an XML format for describing all the information needed to invoke and communicate with a Web Service. A WSDL Document is a set of definitions with a single root element. Services can be defined using the XML elements. A WSDL Document can contain zero or more portType .A portType element contains a single name attribute. Naming convention "nameOfWebService PortType" A portType contains one or more operation elements, with a name attribute can contain input, output and fault elements. A WSDL document can contain zero or more message elements. Each message element can be used as an input, output or fault message within an operation.

Resource Description Framework (RDF) is a framework for describing resources on the web .It is written in XML.RDF is a W3C recommendation.

Really Simple Syndication (RSS) allows to syndicate the site contents.RSS defines an easy way to share & view headlines & content. RSS files can be automatically updated It is also written in XML.

4.2 Windows Communication Foundation (WCF)

Windows Communication Foundation (WCF) is a framework for building service-oriented applications. Using WCF, you can send data as asynchronous messages from one service endpoint to another. A service endpoint can be part of a continuously available service hosted by IIS, or it can be a service hosted in an application. An endpoint can be a client of a service that requests data from a service endpoint. The messages can be as simple as a single character or word sent as XML, or as complex as a stream of binary data. WCF is a replacement for all earlier web service technologies from Microsoft. Difference between Web services and WCF is Web Services can be accessed only over HTTP & it works in stateless environment [4], where WCF is flexible because its services can be hosted in different types of applications. Common scenarios for hosting WCF services are Internet Information Service (IIS) Server, Self-hosting, Managed Windows Service. WCF is used in secure service to process business transactions. WCF also used in a chat scenario that allows two people communicate or exchange data in real time. WCF supplies current data to others, such as a traffic report or other monitoring service. Web Services Use XmlSerializer But WCF uses DataContractSerializer which is better in Performance as Compared to XmlSerializer. XmlSerializer serializes only public fields or properties of .NET types can be translated into XML whereas DataContractSerializer Explicitly shows which fields or properties are serialized into XML. The DataContractSerializer can translate the Hash Table into XML.

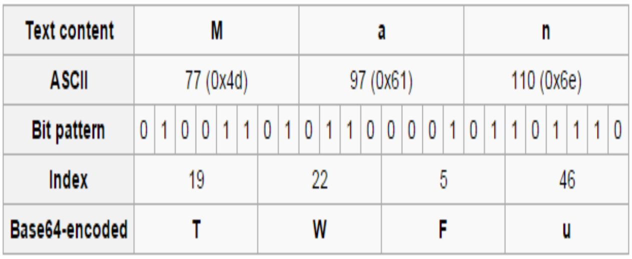
4.2.1Features of WCF:

- Service Orientation
- Interoperability
- Multiple Message Patterns
- Service Metadata
- Data Contracts
- Security
- Multiple Transports and Encodings
- Reliable and Queued Messages
- Durable Messages
- Transactions

5. IMLEMENTATION DETAILS & EXPERIMENTAL RESULTS

Base-64 Algorithm

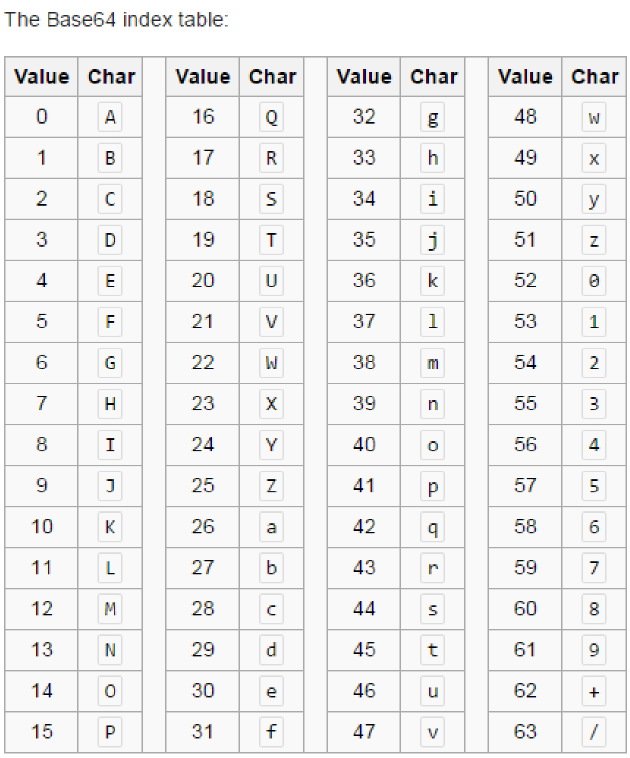
Base 64 is a group of similar binary –to-text Encoding scheme that represents binary data in an ASCII string format by translating it into a radix-64 representation. The term Base64 originates from a specific MIME content transfer encoding. Base64 encoding schemes are commonly used when there is a need to encode binary data that needs to be stored and transferred over media that is designed to deal with textual data. This is to ensure that the data remains intact without modification during transport. Base64 is commonly used in a number of applications, including email via MIME, and storing complex data in XML. Consider one word "Man".



<table>
<tr><td>Text content</td><td colspan="8">M</td><td colspan="8">a</td><td colspan="8">n</td></tr>
<tr><td>ASCII</td><td colspan="8">77 (0x4d)</td><td colspan="8">97 (0x61)</td><td colspan="8">110 (0x6e)</td></tr>
<tr><td>Bit pattern</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td></tr>
<tr><td>Index</td><td colspan="6">19</td><td colspan="6">22</td><td colspan="6">5</td><td colspan="6">46</td></tr>
<tr><td>Base64-encoded</td><td colspan="6">T</td><td colspan="6">W</td><td colspan="6">F</td><td colspan="6">u</td></tr>
</table>

Fig 5:Encoded Value[11]

In the above quote encoded value of man is TFWU Encoded in ASCII, the characters M, a, and n are stored as the bytes 77, 97,110 which are the 8-bit binary values 01001101, 01100001, and 01101110. These three values are joined together into a 24-bit string, producing 010011010110000101101110. Groups of 6 bits (6 bits have a maximum of $2^6 = 64$ different binary values) are converted into individual numbers from left to right (in this case, there are four numbers in a 24-bit string), which are then converted into their corresponding Base64 character values [11].



The Base64 index table:

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Fig 6:Base 64 index table[11]

Secrete Key Generation

/*Generate new SKey*/

SELECT @NewSKey = SUBSTRING (CONVERT (varchar (255), NEWID ()), 0, 9)

Ex: 4C02DE56

In this system inbuilt keyword NewID is used which is available in sqlserver. It returns the combination of alphanumeric key which is non-repeatable. There is no `O' included in this but zero is included to avoid confusion to user. It is not case sensitive. The key is always updated for every login for each user. The same key is sent as sms as well as in e-mail.

5.1 Implementation steps

5.1.1 Setup algorithm (MK, PK) Setup:

It is run by the trusted authority or the security administrator. The setup algorithm takes as input a security parameter k and Outputs a master secret key MK and a master public key PK.

5.1.2User Registration:

In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users such as public domains (PUD), personal domains (PSD), and attribute authority (AA), MultiAuhority ABE (MA-ABE), Key policy (KP-ABE).

5.1.3 Key Generation (SK) Key Gen (MK,):

It is run by the trusted authority, and takes as input a set of attributes and MK. The algorithm outputs a user secret key SK associated with the attribute set. [6]

5.1.4 Encryption (CT) Encrypt (m, PK, P):

It is run by the encryptor. The input of the algorithm is a message m, a master public key PK and an access control policy P, the output of the algorithm is a cipher text CT encrypted under the access control policy P.

5.1.5 Decryption algorithm (m) Decrypt (CT, SK):

It is run by the decryptor. The input of the algorithm is a cipher text CT to be decrypted and a user secret key SK. The output of the algorithm is a message m, if the attribute set of the secret key satisfies the access policy P under which the message was encrypted, or an error message if the attribute set of the secret key does not satisfies the access policy P under which the message was encrypted.

5.2 Developing WCF

To develop a service in WCF will write the following code;

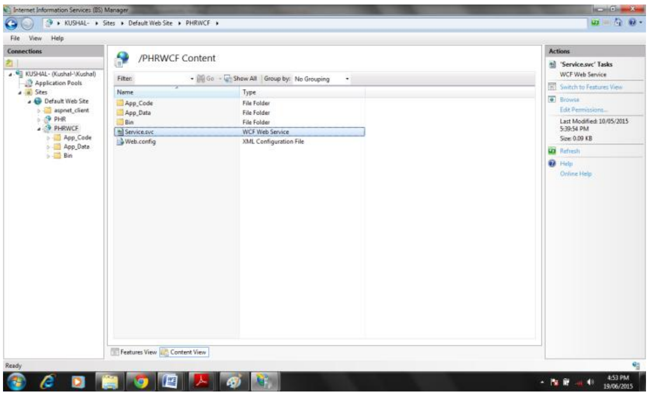
```
<pre lang=”C#”>
[ServiceContract] public interface ITest
{
 [OperationContract]
string ShowMessage (string strMsg);
}
public class Service: ITest
 {
public string ShowMessage (string strMsg)
 {
return strMsg;
}
}
</pre>
```

The ServiceContractAttribute specifies that a interface defines a WCF service contract, OperationContract Attribute indicates which of the methods of the interface defines the operations of the service contract. A class that implements the service contract is referred to as a service type in WCF.

5.3 Hosting WCF

WCF Service can be hosted within IIS consisting following steps;

- Compile the service type into a class library .
- Copy the service file with an extension .SVC into a virtual directory and assembly into bin sub directory of the virtual directory.
- Copy the web.config file into the virtual directory.

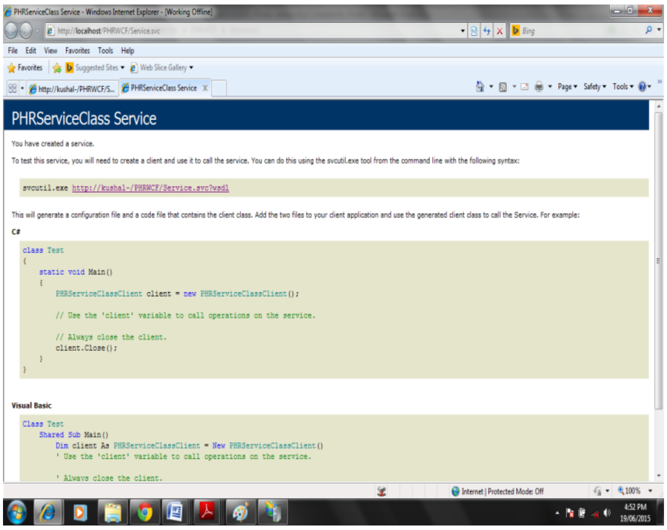


/PHRWCF Content

Name	Type
App_Code	File Folder
App_Data	File Folder
Bin	File Folder
Service.svc	WCF Web Service
Web.config	XML Configuration File

'Service.svc' Tasks
WCF Web Service
Last Modified: 10/05/2015 5:39:54 PM
Size: 0.09 KB

Fig 7: Service File i.e. service.scv


PHRServiceClass Service - Windows Internet Explorer - [Working Offline]
http://localhost/PHRWCF/Service.svc
Bing
File
Edit
View
Favorites
Tools
Help
Favorites
Suggested Sites
Web Slice Gallery
http://kushal-/PHRWCF/S...
PHRServiceClass Service
Page
Safety
Tools
Internet | Protected Mode: Off
100%
4:52 PM
19/06/2015

PHRServiceClass Service

You have created a service.

To test this service, you will need to create a client and use it to call the service. You can do this using the svcutil.exe tool from the command line with the following syntax:

```
svcutil.exe http://kushal-/PHRWCF/Service.svc?wsdl
```

This will generate a configuration file and a code file that contains the client class. Add the two files to your client application and use the generated client class to call the Service. For example:

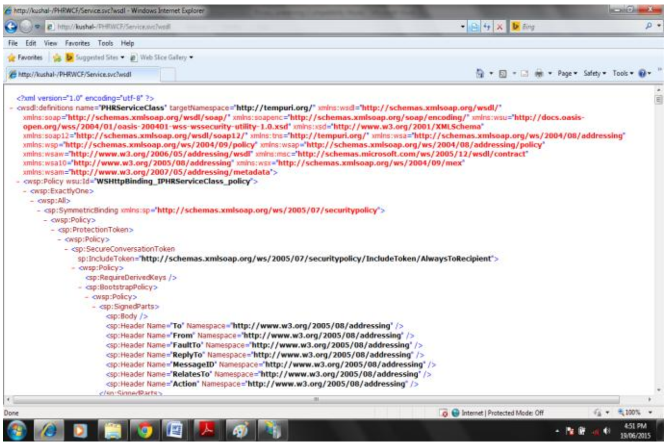
C#

```
class Test
{
    static void Main()
    {
        PHRServiceClassClient client = new PHRServiceClassClient();

        // Use the 'client' variable to call operations on the service.

        // Always close the client.
        client.Close();
    }
}
```

Visual Basic

```
Class Test
    Shared Sub Main()
        Dim client As PHRServiceClassClient = New PHRServiceClassClient()
        ' Use the 'client' variable to call operations on the service.

        ' Always close the client.
```

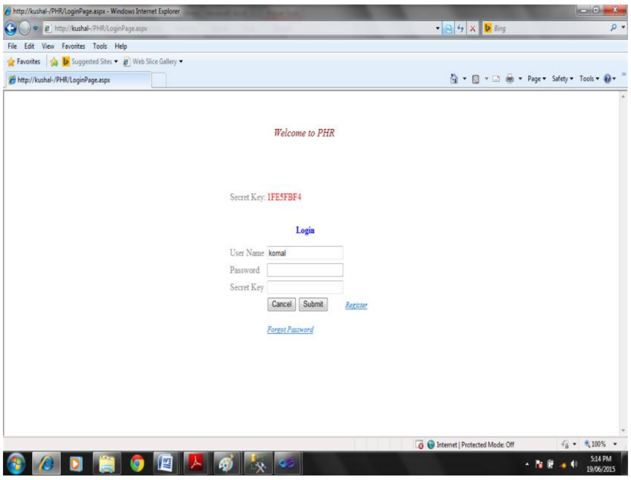
Fig 8: Hosting of WCF


http://kushal-/PHRWCF/Service.svc?wsdl - Windows Internet Explorer
http://kushal-/PHRWCF/Service.svc?wsdl
Bing
File
Edit
View
Favorites
Tools
Help
Favorites
Suggested Sites
Web Slice Gallery
http://kushal-/PHRWCF/Service.svc?wsdl
Page
Safety
Tools
Done
Internet | Protected Mode: Off
100%
4:51 PM
19/06/2015

```
  <?xml version="1.0" encoding="utf-8" ?>
- <wsdl:definitions name="PHRServiceClass" targetNamespace="http://tempuri.org/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:wsu="http://docs.oasis-
    open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:tns="http://tempuri.org/" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
    xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
    xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" xmlns:msc="http://schemas.microsoft.com/ws/2005/12/wsdl/contract"
    xmlns:wsa10="http://www.w3.org/2005/08/addressing" xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex"
    xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata">
  - <wsp:Policy wsu:Id="WSHttpBinding_IPHRServiceClass_policy">
    - <wsp:ExactlyOne>
      - <wsp:All>
        - <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          - <wsp:Policy>
            - <sp:ProtectionToken>
              - <wsp:Policy>
                - <sp:SecureConversationToken
                    sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient">
                  - <wsp:Policy>
                      <sp:RequireDerivedKeys />
                    - <sp:BootstrapPolicy>
                      - <wsp:Policy>
                        - <sp:SignedParts>
                            <sp:Body />
                            <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing" />
                            <sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing" />
                            <sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing" />
                            <sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing" />
                            <sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing" />
                            <sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing" />
                            <sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing" />
                          </sp:SignedParts>
```

Fig 9: Successful Hosting of WCF

In this system first user have to login themselves with their role as a doctor or owner (i.e. patient) or lab assistant or health insurance agent, if user is existing then he or she can logged in successfully with secrete key but, if new user want to login then they have to register and then logged in with key.


http://kushal-/PHR/LoginPage.aspx - Windows Internet Explorer
http://kushal-/PHR/LoginPage.aspx
Bing
File
Edit
View
Favorites
Tools
Help
Favorites
Suggested Sites
Web Slice Gallery
http://kushal-/PHR/LoginPage.aspx
Page
Safety
Tools
Internet | Protected Mode: Off
100%
5:14 PM
19/06/2015

Welcome to PHR

Secret Key: 1FE5FBF4

Login

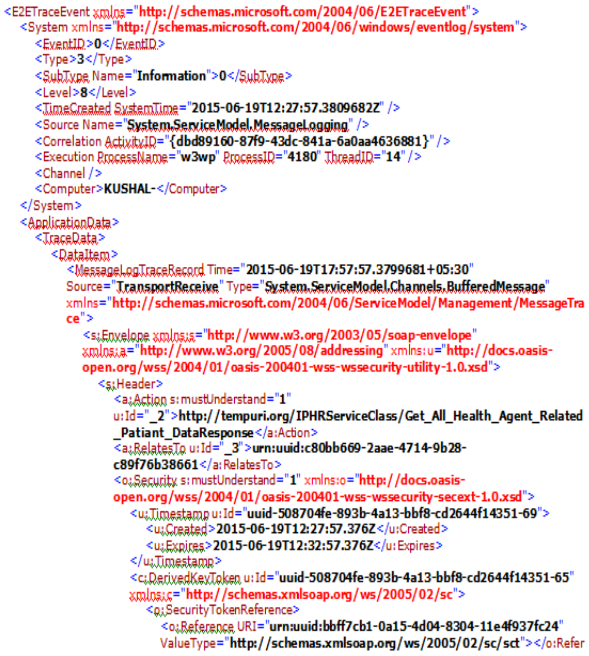
User Name: komal
Password:
Secret Key:

Cancel | Submit | Register

Forgot Password

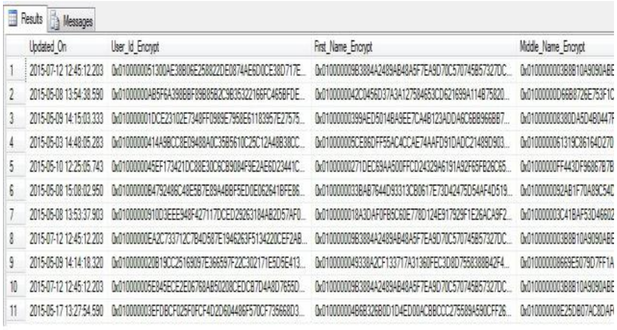
Fig 10: Key generation

After Logged in successfully Doctor can see the all patients' health information, Patient or owner can see their own profile and health data not others. They can update their information Lab assistant can upload patients reports and health insurance agent can see the details of patient's policy name, policy date ,premium amount & date, maturity date, claimed date and claimed against disease and balance amount. Encryption of All attributes is done with the help of web services SOAP and WSDL. Attribute based Encryption is shown in the message log XML format as



```
<E2ETraceEvent xmlns="http://schemas.microsoft.com/2004/06/E2ETraceEvent">
  <System xmlns="http://schemas.microsoft.com/2004/06/windows/eventlog/system">
    <EventID>0</EventID>
    <Type>3</Type>
    <SubType Name="Information">0</SubType>
    <Level>8</Level>
    <TimeCreated SystemTime="2015-06-19T12:27:57.3809682Z" />
    <Source Name="System.ServiceModel.MessageLogging" />
    <Correlation ActivityID="{dbd89160-87f9-43dc-841a-6a0aa4636881}" />
    <Execution ProcessName="w3wp" ProcessID="4180" ThreadID="14" />
    <Channel />
    <Computer>KUSHAL-</Computer>
  </System>
  <ApplicationData>
    <TraceData>
      <DataItem>
        <MessageLogTraceRecord Time="2015-06-19T17:57:57.3799681+05:30"
        Source="TransportReceive" Type="System.ServiceModel.Channels.BufferedMessage"
        xmlns="http://schemas.microsoft.com/2004/06/ServiceModel/Management/MessageTra
        ce">
          <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
          xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
          open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
            <s:Header>
              <a:Action s:mustUnderstand="1"
              u:Id="_2">http://tempuri.org/IPHRServiceClass/Get_All_Health_Agent_Related
              _Patiant_DataResponse</a:Action>
              <a:RelatesTo u:Id="_3">urn:uuid:c80bb669-2aae-4714-9b28-
              c89f76b38661</a:RelatesTo>
              <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-
              open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                <u:Timestamp u:Id="uuid-508704fe-893b-4a13-bbf8-cd2644f14351-69">
                  <u:Created>2015-06-19T12:27:57.376Z</u:Created>
                  <u:Expires>2015-06-19T12:32:57.376Z</u:Expires>
                </u:Timestamp>
                <c:DerivedKeyToken u:Id="uuid-508704fe-893b-4a13-bbf8-cd2644f14351-65"
                xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
                  <o:SecurityTokenReference>
                    <o:Reference URI="urn:uuid:bbff7cb1-0a15-4d04-8304-11e4f937fc24"
                    ValueType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct"></o:Refer
```

Fig 11: Web Message Log



	Updated_On	User_Id_Encrypt	First_Name_Encrypt	Middle_Name_Encrypt
1	2015-07-12 12:45:12.203	0x0100000051300AE38B06E258822DE0874AE6D0CE38D717E...	0x010000009B3884A2489AB48A5F7EA9D70C570745B57327DC...	0x010000003B8B10A9090ABE
2	2015-05-08 13:54:38.590	0x01000000AB5F6A398BBF89B85B2C9B35322166FC465BFDE...	0x0100000042C0456D37A3A127584653CD621699A114B75820...	0x01000000D66B8726E753F1C
3	2015-05-09 14:15:03.333	0x010000001DCE23102E7348FF0989E7958E61183957E27575...	0x01000000399AED5014BA9EE7CA4B123ADDA6C6BB966BB7...	0x010000008380DA5D4B0447F
4	2015-05-03 14:48:05.283	0x01000000414A9BCC8E09488A0C35B5610C25C12A48B38CC...	0x010000005CE86DFF55AC4CCAE74AAFD91DADC21489D903...	0x0100000061319C86164D270
5	2015-05-10 12:25:05.743	0x0100000045EF173421DC88E30C6CB9084F9E2AE6D23441C...	0x01000000271DEC69AA500FFCD24329A6191A92F65FB26C65...	0x01000000FF443DF96867B7B
6	2015-05-08 15:08:02.950	0x01000000B4792486C48E5B7E89A4BBF5ED0E062641BFE86...	0x0100000033BAB7644D93313CB0617E73D42475D54AF4D519...	0x0100000092AB1F70A89C54D
7	2015-05-08 13:53:37.903	0x01000000910D3EEE948F427117DCED29263184AB2D57AF0...	0x0100000018A3DAF0FB5C60E778D124E917929F1E26ACA9F2...	0x010000003C41BAF53D46602
8	2015-07-12 12:45:12.203	0x01000000EA2C733712C7B4D587E1946263F5134220CEF2AB...	0x010000009B3884A2489AB48A5F7EA9D70C570745B57327DC...	0x010000003B8B10A9090ABE
9	2015-05-09 14:14:18.320	0x0100000020B19CC25169097E366597F22C302171E5D5E413...	0x0100000049338A2CF133717A31360FEC3D8D7558388B42F4...	0x010000008669E5079D7FF1A
10	2015-07-12 12:45:12.203	0x010000005E845ECE2E06768AB50208CEDCB7D4A8D7655D...	0x010000009B3884A2489AB48A5F7EA9D70C570745B57327DC...	0x010000003B8B10A9090ABE
11	2015-05-17 13:27:54.590	0x010000003EFDBCF025F0FCF4D2D604486F570CF735668D3...	0x010000004B6B326B0D1D4ED00ACBBCCC275589A590CFF26...	0x010000008E25DB07AC8DAF

Fig 12: Secured Encrypted Database

6. CONCLUSION

This paper, proposed a novel patient centric framework of secure sharing of personal health records in cloud computing with considering trusted authority as cloud servers. Data owner i.e. patients shall have complete control of their own privacy through encrypting their PHR data files to allow fine-grained access. Patients can easily insert, delete, modify, and access their personal health record. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous patients can allow access not only by personal domain users, but also various users from public domains with various professional roles, qualifications, and affiliations. We utilize ABE to encrypt the PHR data, with the help of Web services as SOAP, WSDL and XML also use WCF service so that we enhance data confidentiality and proving its security.

7. REFERENCES

[1] 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 encryption," IEEE Transactions on Parallel and Distributed Systems, January 2013, pp. 131-143.

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

[3] Linke Guo, Chi Zhang, Jinyuan Sun, and Yuguang Fang, "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks" IEEE mobile computing, vol. 13, no. 9, September 2014

[4] Kushal Kulkarni, A.M.Dixit, "Privacy Preserving System Using Attribute Based Encryption for e-health Cloud", IJSR Volume 3 issue 12 December 2014.

[4] Implementing a Basic WCF Service – Code Project at www.codeproject.com.

[5] Luan Ibraimi, Muhammad Asim, Milan Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption". Technical report, Univ. of Twente, 2009.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-Policy Attribute- Based Encryption," Proceedings of the 28th IEEE Symposium on Security and Privacy (Oakland), 2007.

[7] Z. Zhou and D. Huang, "An optimal key distribution scheme for multicast group communication," in IEEE Conference on Computer Communications (Infocom), 2010.

[8] Web Service Tutorials-W3CSchools from www.w3schools.com

[9] Web Services Tutorial – www.tutorialspoint.com

[10] CAM: Cloud assisted privacy preserving mobile health monitoring by Huang Lin, Jun Shao, Chi zang, Yuguang Fang, Fellow IEEE.

[11] Base 64- Wikipedia free encyclopedia https://en.wikipedia.org/wiki/Base64

[12] Jyoti Deshmukh, A.M.Dixit, "Message Privacy with Load Balancing Using Attribute Based Encryption", IJCA (0975 -8887) Volume 103, No. 10, October 2014.