CLOUD ASSISTED PRIVACY PRESERVING AND DATA INTEGRITY FOR MOBILE HEALTH MONITORING

K.M.Jadhav[1], S.R.Idate[2]

[1]PG Student,Department Of Information Technology, Bharti Vidyapeeth Deemed University College Of Engineering, Pune, India

[2]Assoc.Prof., Department Of Information Technology, Bharti vidyapeeth Deemed University College Of Engineering, Pune, India

Abstract

In cloud computing system ,data is stimulated to a distantly placed cloud server. Cloud provisions the information authentically and go back to the proprietor whenever wanted. But there is no assurance that information store in the cloud is protected and not changed by cloud . In order to defeat the danger of honesty of data, the user must be able to use the help of Third party Auditor(TPA).TPA has understanding in inspection honesty of the information, that clouds users does not have, and that is difficult for the owner to check .The data in the cloud should be exact ,reliable ,available and elevated excellence.[1]This paper is to address this important problem related to the data integrity and design a cloud assisted privacy preserving mobile-health monitoring system to protect the privacy of the involved parties and their data. for that purpose we have used the algorithms:1)Tate pairing 2)Token generation 3)AES(Advanced Encryption Standards)-SHA1 and MD5.

***Keywords—** Data integrity,TPA,Tate pairing, Cryptography*

--***--

1. INTRODUCTION

Cloud storage is service ,where data is remotely maintained and back up. The service is available to user over a network ,which usually the internet. It allows the user to store files online ,so that the user can access them from any location via the internet. The provider company makes them available to the user online by keeping the uploaded files on an external server. This gives companies using cloud storage service ease and convenience, but can potentially be costly. Users should also be aware that backing up their data is still required when using cloud storage service ,because recovering data from cloud storage is much slower than local backup. Some of the cloud storage advantages are decrease expenditure, afford more flexibility. In spite of these advantages ,"cloud" require in some of the issues like information honesty ,information loss, illegal right of entry, isolation etc.

fortunately, even though cloud-assisted mHealth monitoring could offer a huge chance to get better the excellence of healthcare services and potentially reduce healthcare costs .There is uncertain chunk in creation this technology a truth.[2] exclusive of correctly addressing the information organization in an mHealth system ,customers isolation may be harshly breach during the collection ,storage ,diagnosis, communications and computing .A current learning shows that 75% Americans judge the isolation of their health information important or very important[3].

2. RELATED WORK

1 .Gorp, P.V.; Comuzzi, M.; Fialho, A.; Kaymak, U.Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on2012

In this paper, we show that both requirements can be satisfied fully when adopting a novel cloud-based PHR system architecture. [4]

2. Smith, R.; Jie Xu; Hima, S.; Johnson, We present a prototype which takes health records from a commercial data provider, anonymises them in an innovative way and makes them available within a secure cloud-based Virtual Research Environment (VRE)[5]

T.; Fabian, B.Business Informatics (CBI),. we present a novel secure architecture for sharing electronic health records in a cloud environment.[6]

Lingfeng Chen; Hoang, D.B.This paper addresses security and privacy challenges in healthcare cloud by deploying a novel framework with CPRBAC (Cloud-based Privacy-aware Role Based Access Control) model for controllability, traceability of data and authorized access to system resources[7]

3. EXISISTING SYSTEM

They have proposed mobile health monitoring system which provides a good opportunity for adversaries to obtain a large set of medical information. In that clients input there related health data such as a systolic blood pressure(BP),whether they missed daily medications or have an abnormal diet and the energy consumption of physical activity to the decision support system, which will then return a recommendation on how the clients can improve their condition[2]

3.1 Limitations of Existing System

- Exisisting system does not store medical data on cloud side[2].
- Exisisting system does not focus on Data integrity issue.

4. PROPOSED SYSTEM

In proposed health monitoring system, If the patient wants to consult about his BP problem or Diabetes problem such as increase or decrease in the sugar level. For the medical advice regarding above problem ,He can log in To The mobile health monitoring Application, To use this Application his mobile must have android base and he has to install This particular mobile health monitoring application. There is another application ,in which the provider can store the general information regarding the health related problem such as BP, Diabetes and Hypertension. In this Mobile Health Monitoring System, provider have suggested, how to take care when above described problems are arised. All data of these application are stored on cloud. some times what happens if there is no strong security system used then data can be altered, changed or hacked by the hackers. Thus there is no fear to provider or user regarding data security ,because In this applications data is secured strongly by using following algorithms.Namely:1)Tate pairing 2)Token Generation 3)AES (Advanced Encryption standards)

4.1 System Architecture

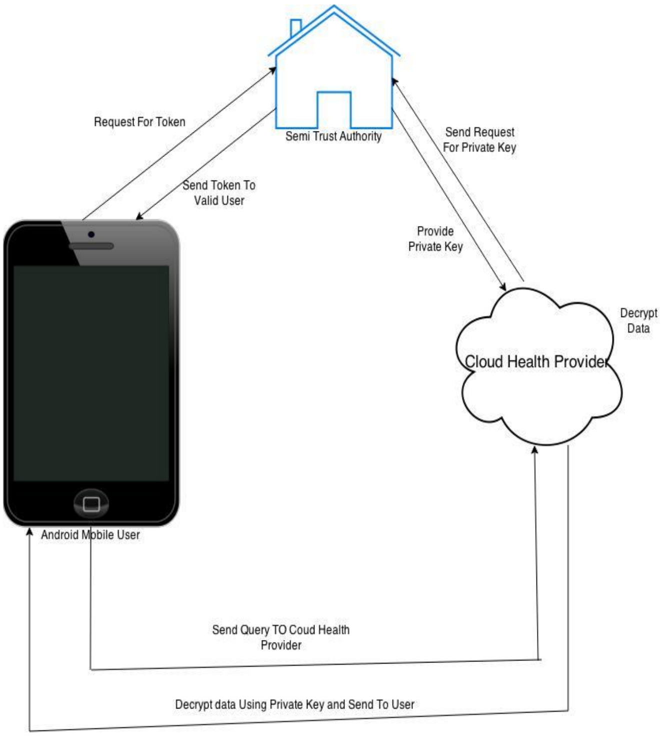


Fig 1 System Architecture

We now highlight our design of the proposed cloud assisted privacy preserving and data integrity for Mobile Health Monitoring System. Above fig 1.consist of 3 parties i.e 1)Android Mobile User 2)Cloud Health Provider and Semi Trust Authority. Semi Trust Authority generate public and private key for each and every user who does the registration to Mobile Health Application. when any android mobile user first do the registration to Mobile Health Application and After that he will send Request for token to the Semi Trust Authority .when Semi Trust Authority receives request he will first check whether it is valid user or not and if it is valid then he will send token to requested user. when user receives token ,he will encrypt data by using that token and send query for ex. systolic Bp:100 e.t.c.to cloud Health Provider. When Cloud Health Provider Receives query from user, cloud health provider requires the users private key to decrypt users data .so ,he will send request to the semi Trust Authority for users private key After receiving request ,Semi Trust Authority sends users private key to cloud Health Provider and then Cloud Health Provider decrypts data by using AES algorithm send Query Result to requested user.

In our proposed cloud assisted privacy preserving and data integrity for Mobile Health Monitoring System, actually consist four modules which are as follows:

a) Cloud server
b) M-Health Provider
c)Trusted Authority
d) Client

a) Cloud Server:
1) Acts as offline storage
2) All data are saved in encrypted format
3) Even passwords of users too

b) MHealth Provider
1) Stores Data on cloud in encrypted format
2) can view user detail
3) Add medical data detail (BP,Systolic,e.t.c)
4) View or add comments or Description

c) Trusted Authority
1) Activates user account
2)Generate token for user
3)Trusted Authority can't view token as it is generated and to client .

Token = jz6v|ERHZiowFuiPL8SiB9==

d) Client
1) Registers with mHealth
2) Trusted authority must activate the user
3) can view their details
4) Raise Query
5) view Query results
6) Using token he can view query results
7) Query automatically send to Trusted authority.
8) Query = "blood pressure 50,missed medication:3"

4.2 Mathematical Function Definition for the System

M = Message
Min1 = Minimum value.
Max1 = Maximum value.
M = { , , ... }

Where,
M = Message as per the High BP range and Low BP range.
for example,
Min1 -> specifies the low value
Range of Min1 = 60 -70 means it represents the low BP.

Min2-> Specifies the another Low value,
Range of Min2-> - 80-90 it represents normal BP.

Max1->Specifies the High value.
Range of Max1 ->100-120 it represents the normal BP.

Max2->130-160 it represents the high Bp.

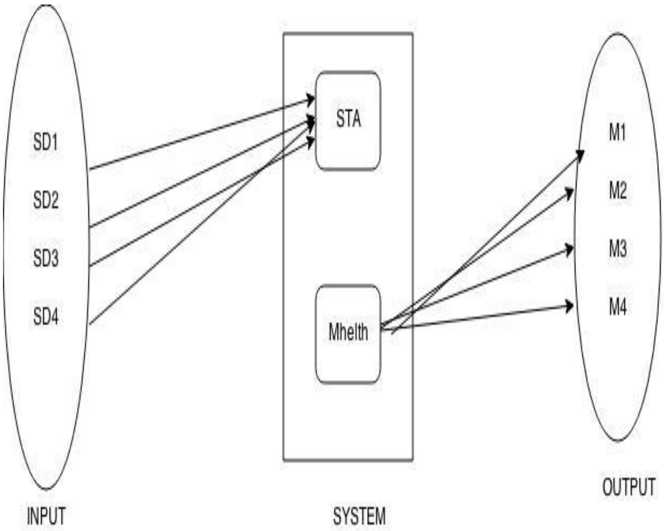


Fig 2 Mathematical Function Definition For The System

4.3 Algorithmic Strategy

1) AES Algorithm

a) Encryption

```
Input:  String to be encrypted
Output: Encrypted value

Begin
Get the instance of Cipher class i.e java.crypto.cipher.
Step 1: Generate the dynamic Key
Step 2:Using Base 64 encoder encode the bytes of given String and get the encrypted value.
Return encrypted value.
End
```

b) Decryption

```
Input:  String to be decrypted
Output: decrypt value
Begin
Get the instance of Cipher class i.e java.crypto.cipher.
Step 1: Generate the dynamic Key
Step 2:Using Base 64 decoder to decode the bytes of given String and get the decrypted value.
Return decrypted value.
End
```

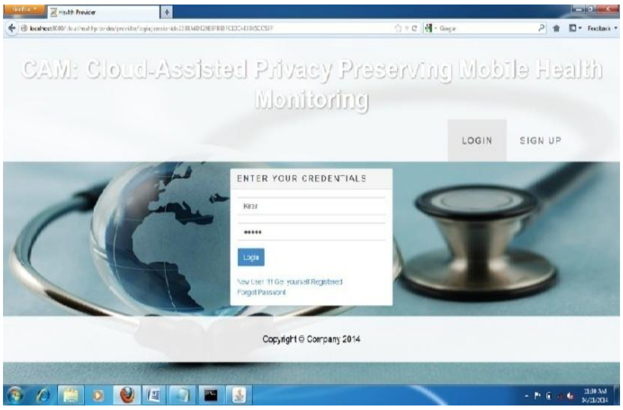
2) Tate Pairing

```
Input: Generate the public key and private key
Output: public key value and private key value
Begin
Point Key = new point(x,y)
pairing e = new Tate pairing curve,grouporder,coFactor);
point p = new point(x2,y2);
point Ppub = new point(x3,y3);
BFMasterPublicKeyparam = new BFMasterPublicKey(e,p,Ppub);
private key = new  BFUserPrivateKey(key param);
Return Public key and Private key

End
```

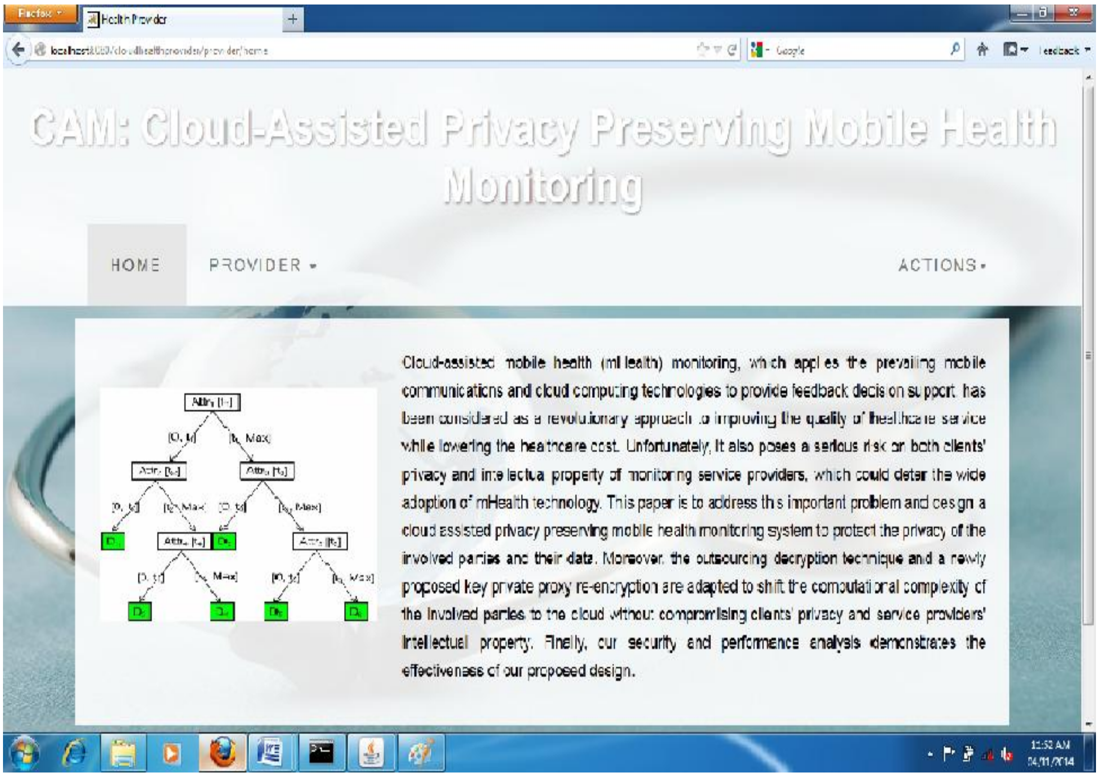
4.4 Experimental Results

1) Health Provider



STEPS:
TO START TOMCAT

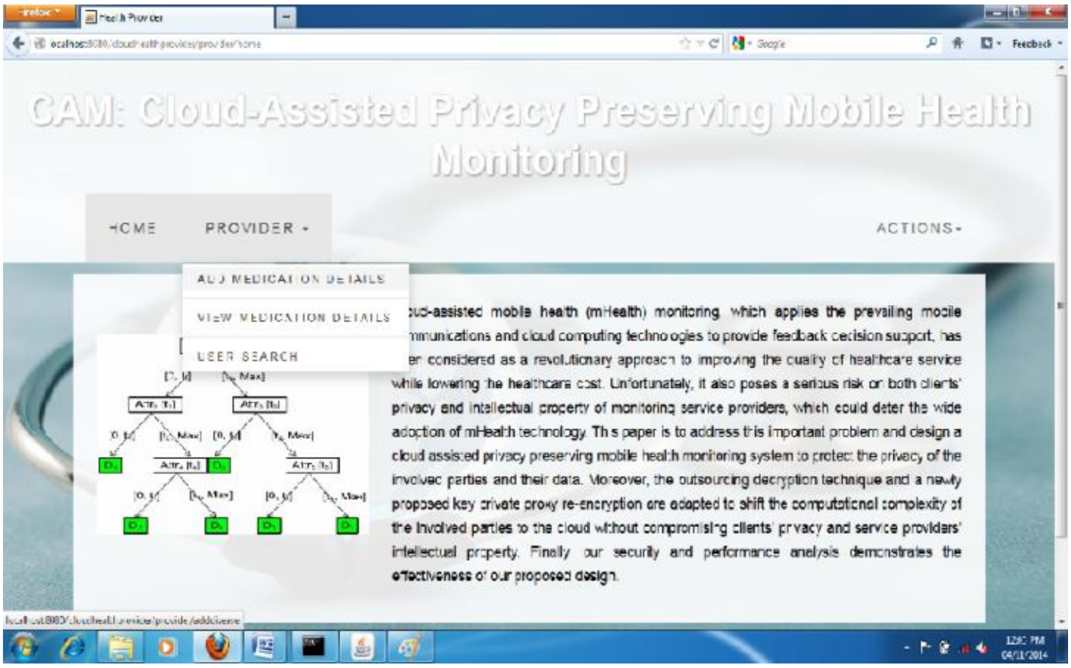
- Go to command line- Type cd C:\CloudHealth\apache-tomcat-7.0.54\bin
- write : startup.bat
- 3 Go to Firefox : http://localhost:8080/cloudhealthprovider
- 4 click on signup and create new account
- 5 sign in to application with user name and password.
- 6 After sign in following window will be displaye**d**



CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring

Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, It also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. This paper is to address this important problem and design a cloud assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy re-encryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' Intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

- In Above window There are three buttons
  a) Home
  b) Provider
  c) Action
- After clicking provider button following window will be displayed:

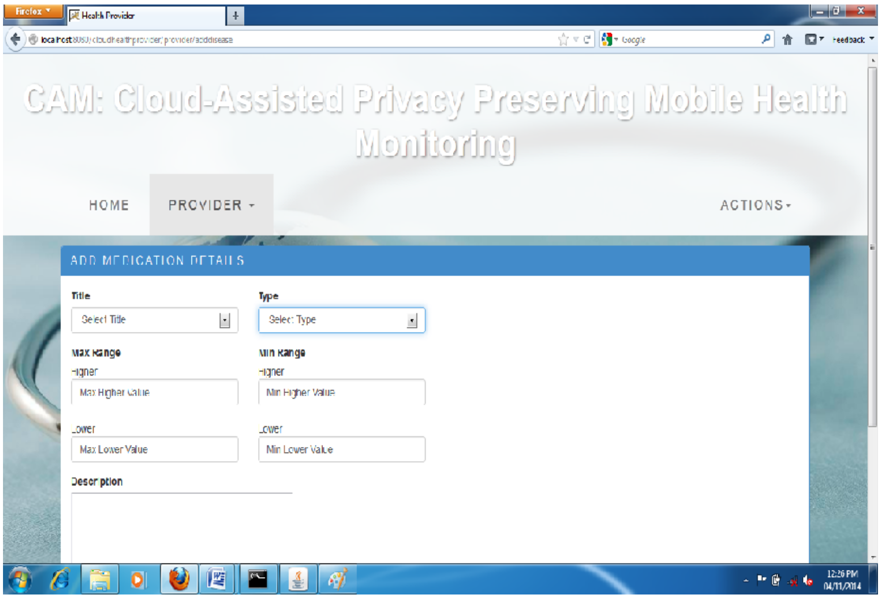


CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring

...ud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile ...mmunications and cloud computing technologies to provide feedback decision support, has ...en considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. This paper is to address this important problem and design a cloud assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy re-encryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

- In above window, After clicking provider option ,The three sub options of provider will open these are:
  a) Add medication details
  b) View medication details
  c) user search

a) In add medication detail provider can add medication details of diseases which are displayed in following window:



b) In view medication details, provider can view the details of medications which he had added.

c) when user click on Action option then will get three sub options which are:

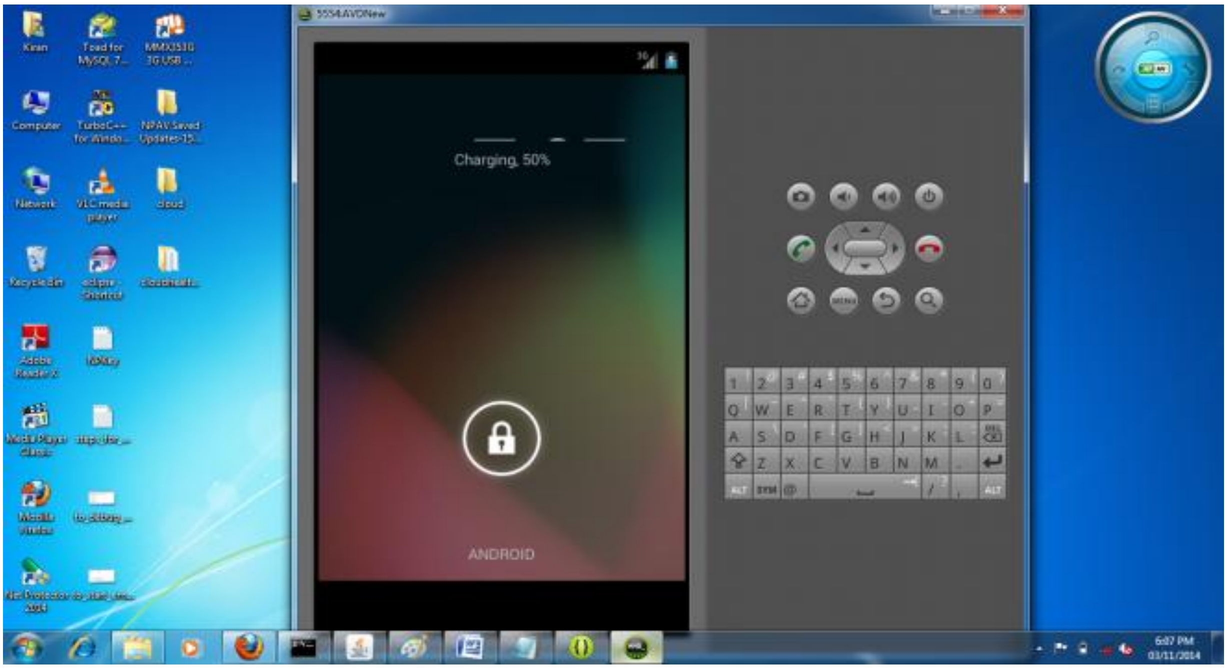
1)Update Profile
2)Change Password
3)Logout

1) If provider wants to update his profile then he has to click on update profile button.
2) If provider wants to change password then he has to click on change password button.
3) If provider wants to Logout from application then he has to click on logout button.

2) For Android User

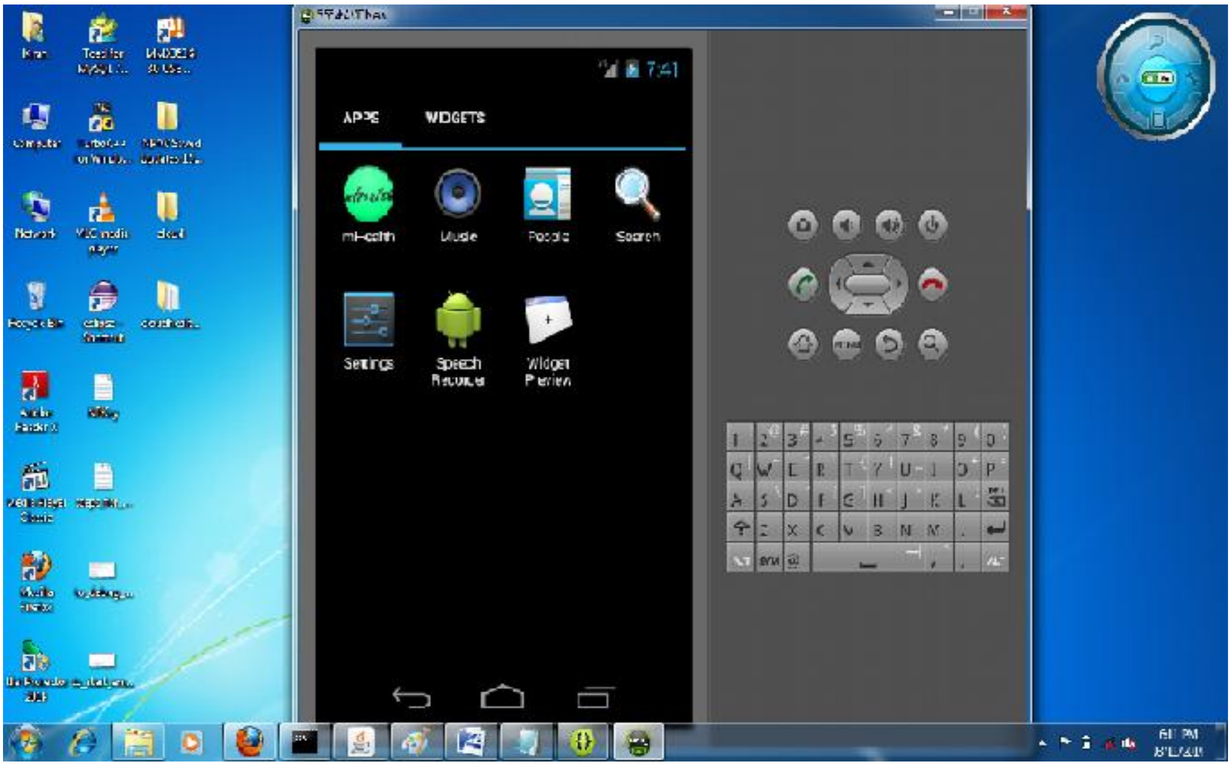
STEPS:

- C:\CloudHealth\adt-bundle-windows-x86_64-20140702\eclipse . start eclipse.
- After starting the eclipse following window will open

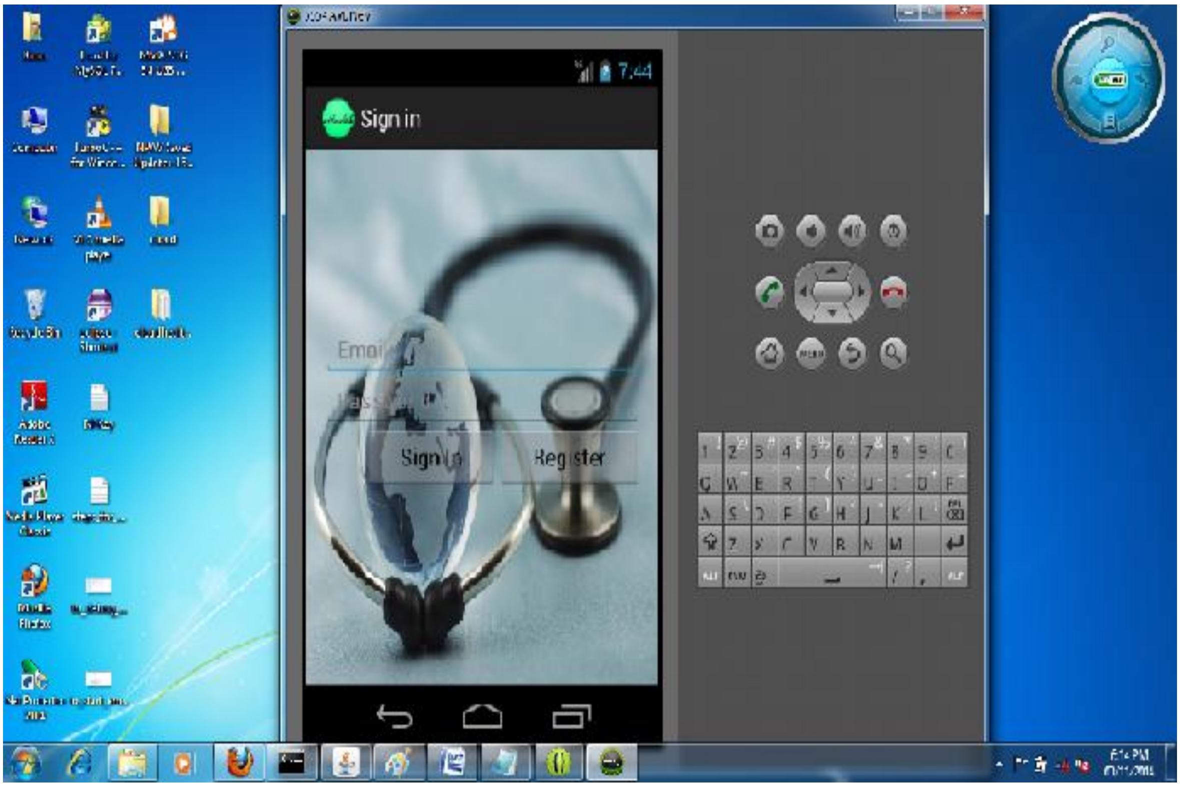


.

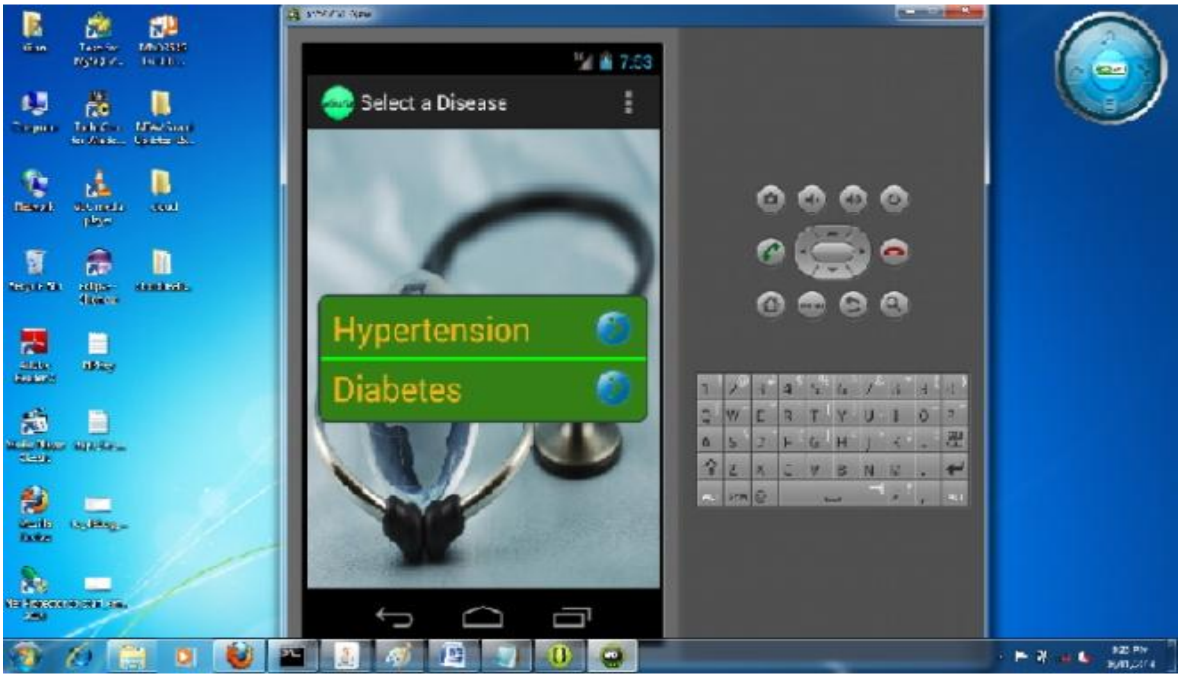
- After dragging the android mobile lock displaced in above window then following window will open. This window is consisting of different options. as well as different applications. from these applications one has to select mobile health application i.e m_Health.



- After clicking mobile health application the next window will open. In that window there are two options one is sign in and another is register. if the user is already having his account then he has to sign in only, otherwise he has to open new account by clicking on register option. and has to submit it, then he will get his username and password.



- After signing in to the android mobile health application following window will open.



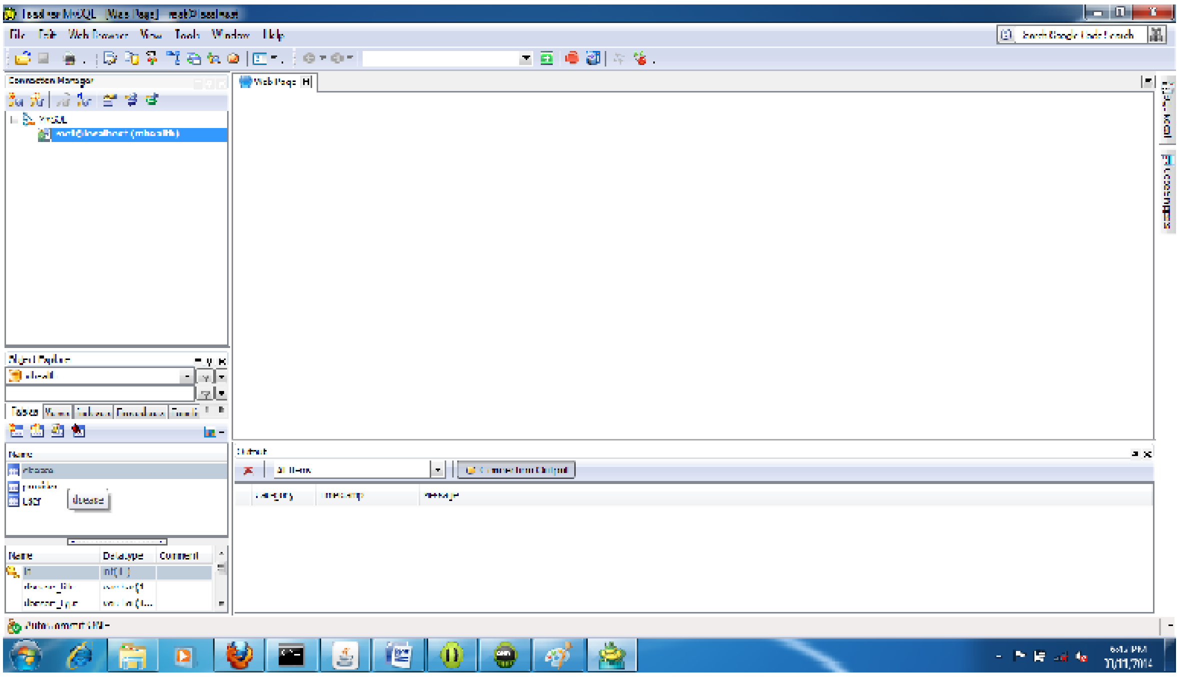
In This window There are two options of two types of diseases These are:
i) Hypertension
ii)Diabetes

According to the need of user he has to select any one application from above mention window and to click the same.
For example, If the user is blood pressure patient, and if he knows that his BP is at high level, then he has to enter his information about BP reading in the Hypertension form. after submitting it ,he will get immediately the required message displaced on the mobile screen and then according to the suggestions of that message he has to act to control his BP level to normal side.

4.5 To View Databse

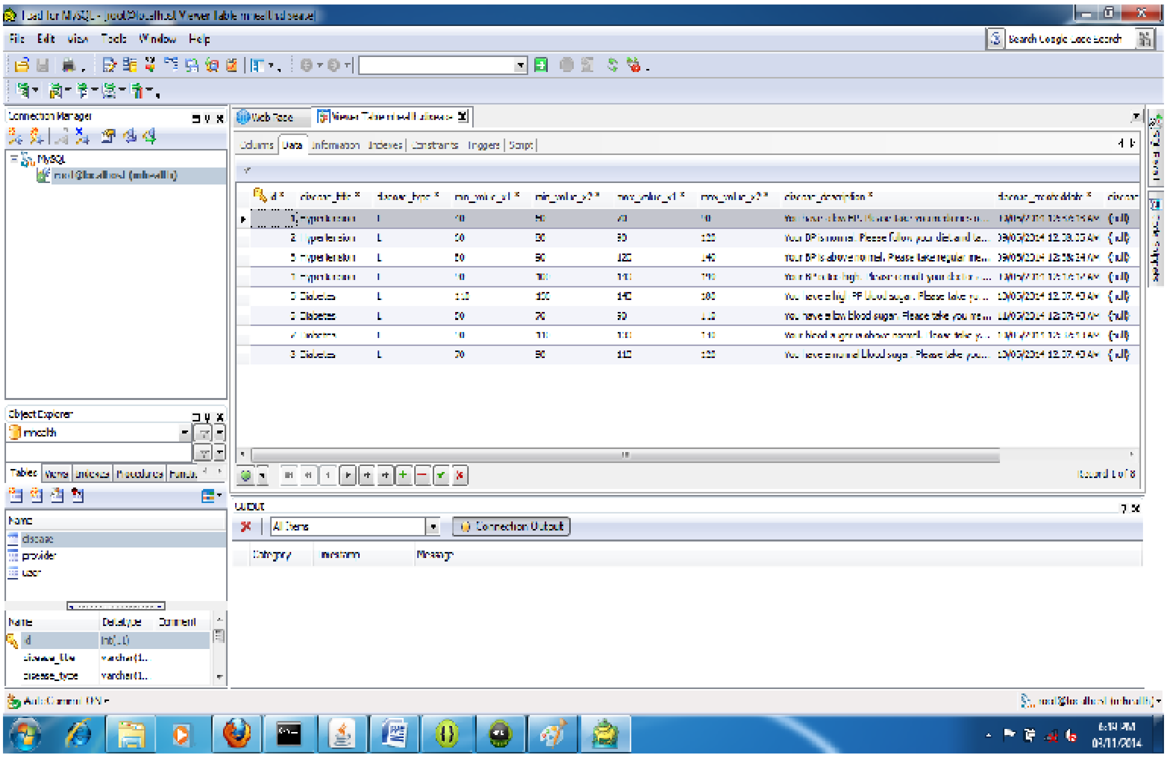
- **STEPS:**

1. Start toad



In Above Database Healthcare provider, user and disease data is stored. The data stored in database is in encrypted format. This data is encrypted by using Tate pairing algorithm and AES Algorithm. so there is no need to fear about the data is stolen or hacked by anybody. following screen is displaying the user and provider data in encrypted format. This all Healthcare provider and user data will be finally stored in cloud side with encrypted format. As per the requirement of user or provider same data stored on cloud side will be decrypted as an when required by the user or provider.

- **USER DATA**

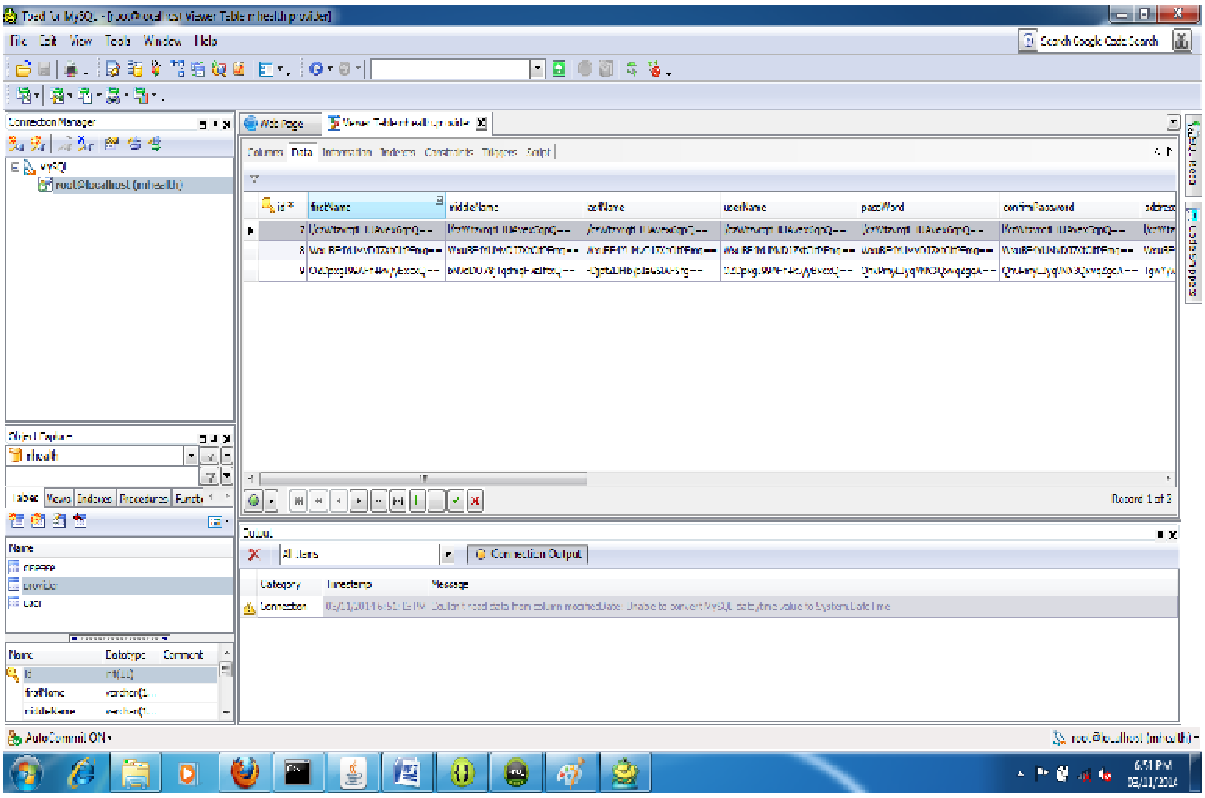


id	disease_title	disease_type	min_value_x1	min_value_x2	max_value_x1	max_value_x2	disease_description	disease_createddate	disea
1	Hypertension	1	70	50	70	40	You have a low BP. Please take your medicines o...	10/05/2014 12:36:13 AM	(null)
2	Hypertension	1	50	90	90	120	Your BP is normal. Please follow your diet and ta...	09/05/2014 12:38:33 AM	(null)
3	Hypertension	1	50	90	120	140	Your BP is above normal. Please take regular me...	09/05/2014 12:38:34 AM	(null)
4	Hypertension	1	90	100	140	190	Your BP is too high. Please consult your doctor ...	10/05/2014 12:36:17 AM	(null)
5	Diabetes	1	110	100	140	180	You have a high PP blood sugar. Please take yo...	10/05/2014 12:37:43 AM	(null)
6	Diabetes	1	50	70	50	110	You have a low blood sugar. Please take your me...	10/05/2014 12:37:43 AM	(null)
7	Diabetes	1	70	110	110	140	Your blood sugar is above normal. Please take y...	10/05/2014 12:37:43 AM	(null)
8	Diabetes	1	70	90	110	120	You have a normal blood sugar. Please take you...	10/05/2014 12:37:43 AM	(null)

Record 1 of 8

Category	Timestamp	Message

- **PROVIDER DATA**



id	firstName	middleName	lastName	userName	passWord	confirmPassword	address
7	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
9	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Record 1 of 3

Category	Timestamp	Message
Connection	03/11/2014 6:51:15 PM	Couldn't read data from column createdDate. Unable to convert MySQL date/time value to System.DateTime

5. CONCLUSION

We have come to the conclusion that, the above designed application will help to the healthcare provider and to the patient to solve there problems of medication.Thus this paper has addressed this important problem related to the data integrity and design a cloud assisted privacy preserving mobile-health monitoring system to protect the privacy of the involved parties and their data. for that purpose we have used the algorithm:1)Tate pairing 2)Token generation 3)AES(Advanced Encryption Standards)-SHA1 and MD5 algorithms

REFERENCES

[1]. Saranya eswaran and Dr,sunitha Abburu,"Identifying Data Integrity in the Cloud storage" in IJCSI,Vol.9,Issue 2,No 1,March 2012.
[2]. CAM:Cloud-Assisted Privacy Preserving Mobile Health Monitoring Huang Lin,Jun Shao,Chi Zhang,and Yuguang Fang,Fellow,IEEE.VOL. 8,NO.6,JUNE 2013.
[3]. L.Ponemon Institute,Americans' Opinions on Healthcare Privaacy,2010[Online].Available:http://tinyurl.com/4atsdlj.
[4]. Gorp, P.V.; Comuzzi, M.; Fialho, A.; Kaymak, U.Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on2012
[5]. Smith, R.; Jie Xu; Hima, S.; Johnson, O.Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on2013
[6]. Ermakova, T.; Fabian, B.Business Informatics (CBI), 2013 IEEE 15th Conference on2013
[7]. High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on2011.