Medicare

Saurabh Gharte[1] Simarpreet Bagga[2] Virendra Deore[3] Rohit Suryawanshi[4] Prof. Geetanjali Mohole[5]

[1,2,3,4,5]Jawahar Education Society's, Institute of Technology, Management & Research, Gowardhan, Nashik

Abstract— Towards the motivation of digital india we need to get more and more digital. Smart phone is one of the evidence towards digital india. According to fact of a digital india we are developing an application which can transforms the social life of mediacl industry into digital. Mostly what happend nowadays when anyone has to go to doctor he need to wait for very long time at clinic or hospital so to avoide such a problem our application will provide online appointment management module. We are also providing feature which will update patient or user of our application by providing different different news updates related to health camp because we always unaware of those healthcamps so we will provide that updates to users through our application. Also we are also provide report management system by using these user can manage his reports through his mobile phone also user can view and send reports to doctor online no need to carry it by hand user can maintain it digitally. Also we are using AES algorithm which can provides security to user data.

Key words: M Health (Mobile Health), Privacy, AES algorithm, Encryption, Decryption, Private Key

I. Introduction

As today's era is moving towards being cashless with a great speed, the youth want everything very easily. Not only the youth but the people of all generation are finding it very easy to be cashless and more and more people are getting attracted or joined towards this technology of being "cashless".

Anywhere you go, you get this technology available. You either go for shopping or buying movie tickets or to a café or a restaurant, even for buying household things at roadside vendor.

So we thought of using this technology and adding more to it for our final year project. Nobody likes to sit for our long waiting hours just to get checked by the doctor and that to doctor checks you in 5 minutes or so. To avoid this and to save time of our patients we are creating a app called "Medicare".

In our application we have major 2 sections i.e. Doctor and patient section. In the doctor section the doctor has the authority to add or accept the patient or to reject or delete the patient request and also have a communication with the patient where he/she can send reports to the patient. In the patient section the patient the view the profile of the doctor, can send the previous history or previous reports to the doctor so that the doctor can very well understand his patient. If required or if the doctor suggests the patient to take appointment and personally visit the doctor the patient can book an appointment itself from the application wherein the time going and sitting at the doctor's clinic or hospital will be reduced and the patient's time will be saved.

One more very useful and important advantage of our system is that the patient can maintain the reports using the cloud. He does not have to carry them every time and can access them very easily.

There are some applications which provides online healthcare system but those application cannot provide HIPPA law. HIPPA law can provides a law according to it Administrator cannot provides any kind of information of patient to anyone wheather it is important reason or not. So we are applying HIPPA law for our application.

In this paper we had developed a system known as "Medicare".

Firstly we focused on the real time problems related to the medical industry by finding that problem we tried to solve that problem by usFirstly we focused on the real time problems related to the medical industry by finding that problem we tried to solve that problem by using our application.

Mainly we are focusing on the problem realated to communication gap between patient and doctor . for that we are using system by which user can request to doctor for communication through application doctor will decide does he have to accept request of patient or not by accepting it patient and doctor can communicate each other by application.

Second Important thing is report management system by which patient can maintain all his reports through application maintain that reports patient don't need to carry that reports physically, patient can carry it digitally in his mobile phone .

Next important part is feedback module in which user will give feedback to doctor.

Patient can easily switch between doctors by easily clicking on switch doctor option.

II. System Model

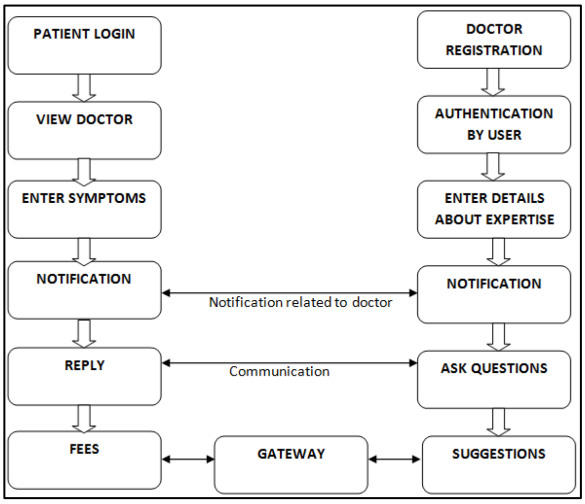

Fig. 1: System Model

We would first like to elaborate our paper "Medicare". Medicare consists of 7 different modules. The modules are as follows.

1) Registration Module
2) Login Module
   a) Client Login
   b) Doctor Login
3) OTP generation/forget password
4) Notification Module
5) Dieses registration Module.
6) Image Upload/Download Module
7) Cloud Server

The Registration Module will be used for the registration of the patient. The doctor's registration will have all the details of the doctor and the user's registration will include his name, phone number, password, all details which are necessory etc. The login module will have 2 sections i.e. the client (patient) and the doctor login. The login section will have only 2 fields i.e. the username field and the password field. After that module comes the next module i.e. the OTP generation and the forget password module. In this module the authentication of the patient and the doctor will be done. The authentication of the client will be done by the OTP generation which will be sent to the client on his mobile number. administrator will be responcible for authentication of doctor. The admin will personally check the details of the doctors, their degree, their qualification, their clinic or their respective hospitals. Forget password module also included in it. If the user forgets his password easily recover it with the help of admin. Next module is the notification module. Next is the dieses registration module. All the dieses will be already registered in the application along with the preferred doctor who can cure the dieses. The patient/user has to enter the dieses and he will get the list of doctors who can help him curing his dieses. another module in our application is image upload/download module in which patient or doctor can easily upload and download images . and patient or doctor can easily transfer images to each other by using secure FTP protocol.

GUI

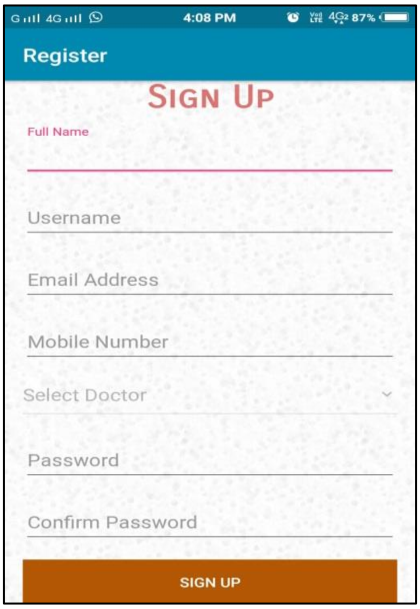

Fig. 2: Regostration window

In this registration window user will enter all the details for signing up. He has to fill all the details mentioned in above image.

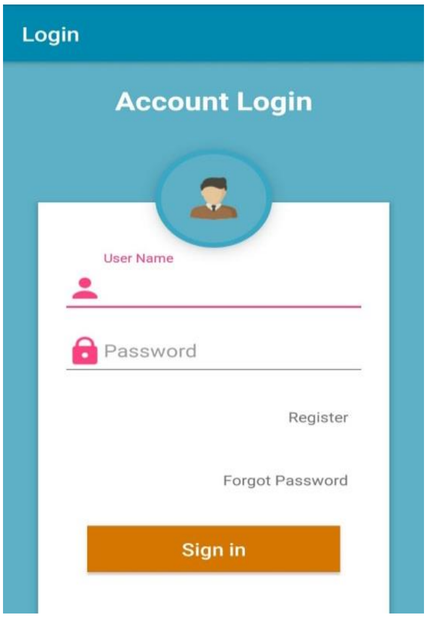

Fig. 3: Login window

Login window is used by patiend or doctor for signing up into application.

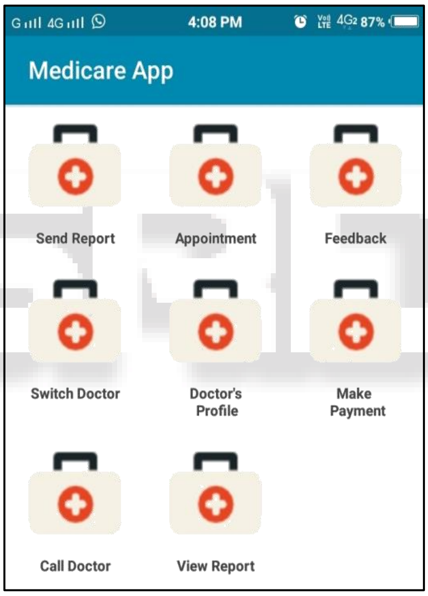

Fig. 4:

This application will consist of all features shown in image.

- Send Report:- User will send report to doctor through send report feature or he can chat with doctor through it.
- Appointment :- user will take appointment towards doctor by clicking on take appointment. Time has been predefined by clicking on it user will be assigned with date and time.
- Feedback:- Feedback will be given by user.
- Switch Doctor:- Doctor will be switched by patient meand user will switch one doctor to another.
- Doctors profile:- User will be able to see profile of current doctor.
- Make payment:- User will pay to doctor through this feature.
- Call doctor:- user will directly call to doctor through this feature.
- View reports:- Report management will provide through this feature.

III. Algorithms Used

A. AES (Advanced Encryption Standard)

AES stands for Advanced Encryption Standard. This algorithm is a symmetric encryption algorithm. The two scientistJoan Daemen and Vincent Rijmen developed this algorithm. This algorithm was designed to be effective on both hardware and software and block length of 128 bits is supported and also key length of 128, 192, and 256 bits is supported.

The AES algorithm consists of 2 parts i.e. Encryption and decryption. Encryption can convert the pain text into cipher text. This cipher text is the text which is in unreadable format. And decryption is the reverse process of encryption. It converts cipher text into plain text.

1) Encryption

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

2) Decryption

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

B. Mathematical Model

C. Homomorphic Encryption HEnc (.)

This gives 2 encrypted messages:
HEnc(m1+m2)= HEnc(M1)*HEnc(M2)
*: Corresponds to operation in Cipher Text
M1: Message 1
M2: Message 2
It can encrypt the message under Range [r1, r2]
Receiver can decrypt the message with the privacy key corresponding to the range [r1, r2]
Encryption
Anonenc (id,pp,m)
pp : System Parameter
M:message
id :identity
Input: M 2 M
Output: C= (C1, C2, C3)
With r= H3(mj j s)
C1= gr
C2=s_H2(e(H,(id),y)r)
Where,
S: random element from m

Decryption
Algorithm performed by decryptor:
(c,Skid)
Input: cSkid
Compute
c2_ H2 (e (Skid: (1)) =s c3 _ H4(s) =m

1) Success Case

1) Successful login.
2) Successful Communication between patient and doctor.

2) Failure Case

1) Login Failed.
2) Patient not in the range of Wi-Fi.

D. FTP Algorithm

FTP Protocol is used to transfer the computer files between client and server on a computer network

The reports made by doctors or the previous history of reports can be send to patient or doctor by using FTP protocol.

IV. Conclusion

In this paper, we designed a “Medicare” application which is a health monitoring system, which we can use to protect the privacy of the clients and also so that we can protect the intellectual property of the providers.

References

[1] P. Mohan, D. Marin, S. Sultan, and A. Deen, “Medinet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony.” Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society, vol. 2008, no. 3, pp. 755–758. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/19162765

[2] A. Tsanas, M. Little, P. McSharry, and L. Ramig, “Accurate telemonitoring of parkinson’s disease progression by noninvasive speech tests,” Biomedical Engineering, IEEE Transactions on, vol. 57, no. 4, pp. 884– 893, 2010.

[3] G. Clifford and D. Clifton, “Wireless technology in disease management and medicine,” Annual Review of Medicine, vol. 63, pp. 479–492, 2012.

[4] L. Ponemon Institute, “Americans’ opinions on healthcare privacy, available: http://tinyurl.com/4atsdlj,” 2010.

[5] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J. van Beijnum, and P. D. Stefanis, “End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust,” in PervasiveHealth, 2011, pp. 478–484.

[6] M. Delgado, “The evolution of health care it: Are current u.s. privacy policies ready for the clouds?” in SERVICES, 2011, pp. 371–378.

[7] N. Singer, “When 2+ 2 equals a privacy question,” New York Times, 2009.

[8] E. B. Fernandez, “Security in data intensive computing systems,” in Handbook of Data Intensive Computing, 2011, pp. 447–466.

[9] A. Narayanan and V. Shmatikov, “Myths and fallacies of personally identifiable information,”

Communications of the ACM, vol. 53, no. 6, pp. 24–26, 2010.

[10] P. Baldi, R. Baronio, E. D. Cristofaro, P. Gasti, and G. Tsudik, "Countering gattaca: efficient and secure testing of fully-sequenced human genomes," in ACM Conference on Computer and Communications Security, 2011, pp. 691–702.

[11] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, "Remote home health care technologies: how to ensure privacy? build it in: Privacy by design," Identity in the Information Society, vol. 3, no. 2, pp. 363–378, 2010.

[12] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008, pp. 111–125.

[13] "De-anonymizing social networks," in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2009, pp. 173–187.

[14] I. Neamatullah, M. Douglass, L. Lehman, A. Reisner, M. Villarroel, W. Long, P. Szolovits, G. Moody, R. Mark, and G. Clifford, "Automated de-identification of free-text medical records," BMC medical informatics and decision making, vol. 8, no. 1, p. 32, 2008.

[15] S. Al-Fedaghi and A. Al-Azmi, "Experimentation with personal identifiable information," Intelligent Information Management, vol. 4, no. 4, pp. 123–133, 2012.

[16] J. Domingo-Ferrer, "A three-dimensional conceptual framework for database privacy," Secure Data Management, pp. 193–202, 2007.

[17] T. Lim, Nanosensors: Theory and Applications in Industry, Healthcare, and Defense. CRC Press, 2011.

[18] X. Zhou, B. Peng, Y. Li, Y. Chen, H. Tang, and X. Wang, "To release or not to release: evaluating information leaks in aggregate human-genome data," Computer Security–ESORICS 2011, pp. 607–627, 2011.

[19] R. Wang, Y. Li, X. Wang, H. Tang, and X. Zhou, "Learning your identity and disease from research papers: information leaks in genome wide association study," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 534–544.

[20] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," UCLA Law Review, vol. 57, p. 1701, 2010.

[21] P. Institute, "Data loss risks during downsizing," 2009.

[22] P. Dixon, "Medical identity theft: The information crime that can kill you," in The World Privacy Forum, 2006, pp. 13–22.

[23] K. E. Emam and M. King, "The data breach analyzer," 2009, [Available at: http://www.ehealthinformation.ca/dataloss].

[24] E. Shaw, K. Ruby, and J. Post, "The insider threat to information systems: The psychology of the dangerous insider," Security Awareness Bulletin, vol. 2, no. 98, pp. 1–10, 1998.

[25] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in Usenix Security, 2011.

[26] Z. Wu, Z. Xu, and H. Wang, "Whispers in the hyper-space: High-speed covert channel attacks in the cloud."

[27] T. Kim, M. Peinado, and G. Mainar-Ruiz, "Stealthmem: system-level protection against cache-based side channel attacks in the cloud," in Proceedings of the 21st USENIX conference on Security symposium. USENIX Association, 2012, pp. 11–11.

[28] S. Dziembowski and K. Pietrzak, "Leakage-resilient cryptography," in Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on. IEEE, 2008, pp. 293–302.

[29] E. Shi, T. Chan, E. Stefanov, and M. Li, "Oblivious ram with o ((logn) 3) worst-case cost," Advances in Cryptology–ASIACRYPT 2011, pp. 197– 214, 2011.

[30] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO, 2001, pp. 213–229.