International Journal of Advancements in Technology

Gharte et al., Int J Adv Technol 2017, 8:1
DOI: 10.4172/0976-4860.1000179

Review Article OMICS International

Medicare

Saurabh Gharte*, Simarpreet Bagga, Virendra Deore and Akshay Jadhav

The ICFAI University, Dehradun, India

***Corresponding author:** Gharte S, The ICFAI University, Dehradun, India, Tel: +919997655162; E-mail: saurabhgharte15@gmail.com

Received date: December 05, 2016; **Accepted date:** December 26, 2016; **Publication date:** January 21, 2017

Abstract

(Mobile Health) mHealth care monitoring system which applies mobile communications and cloud computing technologies and provides feedback decision support; this has been considered as a revolutionary approach for improving the healthcare quality and also lowers the cost of healthcare. But on other hand it has a serious risk on client's privacy and the intellectual property of the service provider, which would reduce the adoption of this technology. This paper would solve this big issue related to security and also design an application having cloud computing technology which would preserve the privacy of the client's and the associated service providers. This paper would focuses on the technology called "AES" (Advanced Encryption Standard) to implement security. Lastly, the security and the performance which will be implemented show the effectiveness of the proposed system.

Keywords: mHealth(Mobile Health); Privacy; AES algorithm; Encryption; Decryption; Private key

Introduction

Wide development of electronic devices such as mobiles, I-pads, tabs, etc which is known as smart devices now a day's; along with the implementation of sensors which are available at low cost have proved to be beneficial for improving the quality the health services. Remote mobile healthcare monitoring has already been successful and is a very good example of mobile Health (mhealth) application specially I the developing countries. Microsoft has launched a product Remote Monitoring System has beed designed the health status of cardiovascular and diabetes diseases in remote areas [1]. In such remote healthcare monitoring system, client deployed portable sensors in wireless body sensor networks which collected psychological data, such as BP (Blood Pressure), BR (Breathing rate), and ECG/EKG (Electrocardiogram), Blood Glucose. The psychological data then collected can be sent to the server which is centrally placed, which could in return run the various web medical applications and the return it to the respective client. The applications have various different functionalities which range from sleep pattern analyzer, physical activity assistance, exercises, to cardiac analysis system which then provide consultation related to medical treatment [2]. As the cloud computing technology is evolving as a new trend in the market, many different solutions can be thought of by using SaaS (Software as a Service) model along with the pay as you go business model in cloud computing, which would allow different companies to go ahead with their in the healthcare market. Automated decision support algorithms have along with cloud assisted healthcare monitoring system are being considered as a future trend [3].

Cloud assisted mHealth monitoring system offer an opportunity to improve the quality of the service of healthcare reduces the cost, but there are some hurdles in turning this technology into a reality. Without properly looking into the data management in the mHealth system, the client's privacy could be at a great risk during the process of collection of data, storage, diagnosis, communication and computing the results. A recent survey shows that 75% of Americans consider their privacy very important [4,5].

There are some existing privacy laws such as HIPPA (Health Insurance Portability and Accountability Act) give protection to the personal health record, but the main drawback of the is that is not applicable to the cloud computing technology [6]. There are many companies who have their own personal interest in collecting the client's personal data [7,8] and further share it with the insurance companies, or research institutes, or even to the government agencies.

The privacy mechanisms which are traditional provide the mechanism by simply removing the client's personal identity information or by using various anonymization techniques. But then these techniques fail to serve as a good protection mechanism because of the increasing diversity and increasing amount in the Personal Identifiable Information (PII) [9-13]. The proposed mobile monitoring system gives a good opportunity so as to collect a good and larger set of medical information, so as to identify the individual. Many recent research and studies show that an individual can be recognized from his blood pressure [14-16].

One the major problem with the privacy and security is the computational workload which is involved with the cryptographic techniques. With the presence of the cloud computing technology, it will be easy to shift the load of the computational computation on the cloud [17-20]. To achieve this very effectively and without any compromise to the privacy of the client and security of the client's data is a big challenge, and should be investigated properly.

Our proposed system will mainly focus on the insider attacks, which can be either malicious or non-malicious. For example an insider could be an employee or a healthcare worker who might enter this business for this own selfish needs or some criminal purpose [21,22]. The attacks which are done by the insider are proved to be more dangerous than the attacks done by the outsider [23,24]. Thus the attacks done by the insider are much tougher to handle because the attacks might be done by the professionals or the criminals who might be expert at the attacks and also expert at escaping the intrusion attack.

In this paper we will be designing a system known as "Medicare". We will firstly identify he problems related to the design of privacy protection and then the solutions will be provided. So that we understand it without any problem we will start with the basic structure so that we can understand all the possible privacy schemes. After understanding the privacy scheme we will give an improved solution to the privacy scheme observer by us. In AES algorithm, the keys will be generated between the client and the doctor. The data will be encrypted using the key generated and the decryption process will also be done be using the same key. The key will not be stored on the cloud. It will be with the respective client and the doctor. Once the communication starts between the doctor and the client the exchange of the data done will also be in the encrypted form. For that purpose also the key will be generated. In short 2 keys will be generated i.e. first key for authentication purpose and the second key for the purpose of the safety of the data exchange done between the client and the doctor.

System Model

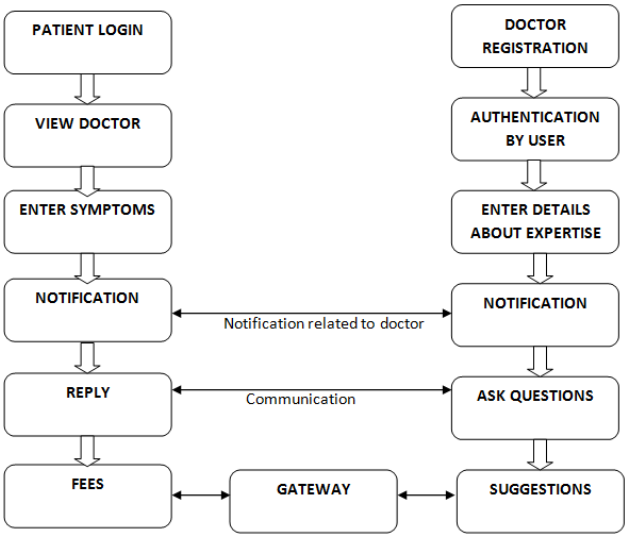

Figure 1: 7 different modules of medicare.

We would first like to elaborate our paper "Medicare". Medicare consists of 7 different modules. The modules are as follows (Figure 1):

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 user (patient) and the doctor. The doctor's registration will have all the details of the doctor such as his qualification, specialization, etc. and the user's registration will include his name, mobile number, password, gender, age, 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 client and the doctor will be done. The authentication of the client will be done by the generation of the OTP which will be sent to the client on his mobile number. The authentication of the doctor will be done by the administrator itself. The admin will personally check the details of the doctors, their degree, their qualification, their clinic or their respective hospitals. Forget password module also comes along with this module. If the user forgets his password he can get a recovery mail at his mail id by the admin. Next module is the notification module. If the doctor sends the report or gives the reply to the client and if the client is not available or is busy somewhere, the client will get the notification. 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. One additional module to our application will be the Image upload/download module. The doctor, after generation of the report can send the report to the client in an image format. For this purpose we will be using FTP (File Transfer protocol) which is by default a secure protocol for transferring files. Cloud Server is used for storing all the data and will also act as offline storage. All the data in the encrypted format will be stored at the cloud [25-30].

Algorithm Used

AES (Advanced Encryption Standard)

AES stands for Advanced Encryption Standard. This algorithm is a symmetric encryption algorithm. The two cryptographers Joan 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 means conversion of 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. This process converts the cipher text into plain text which is again in readable format.

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

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

Mathematical Model for AES Algorithm

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

Success case:

Failure case:

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

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.

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. Mohan P, Marin D, Sultan S, Deen A (2008) Medinet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony. IEEE 3: 755-758.
2. Tsanas A, Little M, McSharry P, Ramig L (2010) Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests. Biomedical Engineering 57: 884-893.
3. Clifford G, Clifton D (2012) Wireless technology in disease management and medicine. Annual Review of Medicine 63: 479-492.
4. Ponemon L (2010) Americans' opinions on healthcare privacy.
5. Dhukaram AV, Baber C, Elloumi L, van Beijnum BJ, Stefanis PD (2011) End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust. Pervasive Health.
6. Delgado M (2011) The evolution of health care it: Are current U.S. privacy policies ready for the clouds? SERVICES.
7. Singer N (2009) When 2+ 2 equals a privacy question.
8. Fernandez EB (2011) Security in data intensive computing systems. Data Intensive Computing.
9. Narayanan A, Shmatikov V (2010) Myths and fallacies of personally identifiable information. Communications of the ACM 53: 24-26.
10. Baldi P, Baronio R, Cristofaro ED, Gasti P, Tsudik G (2011) Countering gattaca: efficient and secure testing of fully-sequenced human genomes. Computer and Communications Security.
11. Cavoukian A, Fisher A, Killen S, Hoffman D (2010) Remote home health care technologies: how to ensure privacy? build it in: Privacy by design. Identity in the Information Society 3: 363-378.
12. Narayanan A, Shmatikov V (2008) Robust de-anonymization of large sparse datasets. IEEE.
13. Narayanan A, Shmatikov V (2009) De-anonymizing social networks. Computer Society.
14. Neamatullah I, Douglass M, Lehman L, Reisner A, Villarroel M, et al. (2008) Automated de-identification of free-text medical records. BMC 8: 32.
15. Al-Fedaghi S, Al-Azmi A (2012) Experimentation with personal identifiable information. Intelligent Information Management 4: 123-133.
16. Domingo-Ferrer J (2007) A three-dimensional conceptual framework for database privacy. Secure Data Management 4721: 193-202.

17. Lim T (2011) Nanosensors: theory and applications in industry, healthcare, and defense.
18. Zhou X, Peng B, Li Y, Chen Y, Tang H, et al. (2011) To release or not to release: evaluating information leaks in aggregate human-genome data. Computer Security.
19. Wang R, Li Y, Wang X, Tang H, Zhou X (2009) Learning your identity and disease from research papers: information leaks in genome wide association study. ACM.
20. Ohm P (2010) Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review 57: 1701.
21. Reese P (2009) Data loss risks during downsizing. Symantec official blog.
22. Dixon P (2006) Medical identity theft: The information crime that can kill you. World Privacy Forum.
23. Emam KE, King M (2009) The data breach analyzer.
24. Shaw E, Ruby K, Post J (1998) The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin 2: 1-10.
25. Green M, Hohenberger S, Waters B (2011) Outsourcing the decryption of abe ciphertexts. Usenix Security.
26. Wu Z, Xu Z, Wang H (2012) Whispers in the hyper-space: High-speed covert channel attacks in the cloud.
27. Kim T, Peinado M, Mainar-Ruiz G (2012) Stealthmem: system-level protection against cache-based side channel attacks in the cloud.
28. Dziembowski S, Pietrzak K (2008) Leakage-resilient cryptography. 49th Annual IEEE Symposium.
29. Shi E, Chan T, Stefanov E, Li M (2011) Oblivious ram with o ((logn) 3) worst-case cost. International Conference on the Theory and Application of Cryptology and Information Security, Springer Berlin Heidelberg.
30. Boneh D, Franklin MK (2001) Identity-based encryption from the weil pairing, in CRYPTO.