Volume : 4 | Issue : 6 | June 2015 • ISSN No 2277 - 8179

Research Paper

Privacy in Mobile Health Network

Engineering

KEYWORDS : Mobile Health network, encryption, Digital signature

Athulya G S M.Tech CSE AWH Engineering College Calicut, India

ABSTRACT

One of the main application area of this mobile computing is the Electronic health care system or Mobile health system. This mobile health system has replaced paper based medical system due to its character like low cost, high accuracy and universal accessibility. Major component of ehealth systems include mobile devices to enable patient to physician communications. Through mobile, data send to the designated healthcare infra structure. If the data centre is compromised, patient's private data may be revealed. For providing security in such system should be enforced via encryption and the authentication of the users.

I. Introduction

Mobile Computing is a human–computer interaction in which computer is expected to be transport during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. One of the main application area of this mobile computing is the Electronic healthcare (eHealth) systems or mobile health system . This mobile health system have replaced paper-based medical systems due to its characters like low cost , high accuracy and universal accessibility. Major component of eHealth systems, applies mobile devices to enable patient-to-physician communications. For most mHealth systems, patients use sensors, implantable medical devices, and mobile to send medical data to the designated health care infra structure. If the data centre is compromised, patients private data may be revealed. For providing security in such system should be enforced via encryption and the authentication of the users.

II. Related Works

In [2] Carl Youngblood proposed Identity based Crypto graphy for the encryption of data. In [5] J. Bethencourt, A. Sahai, and B. Waters, proposed Ciphertext-policy attribute-based encryption for encrypting data. In [3] and [4] proposed a method to secure data in PHR. Recently, Linke Guo, Chi Zhang, Hefei Jinyuan Sun,and Yuguang Fang proposed,A Privacy-Preserving Attribute-based Authentication System for Mobile Health Networks[1].

III. Existing system

For encrypting and decrypting the data, the system uses RSA algorithm. It is an asymmetric cryptographic algorithm. Asymmetric means, there are two different keys used. This Rsa is also called public key cryptography, because one of them can be given to everyone. The RSA algorithm is

1. Choose two different large random prime numbers P and q
2. Calculate n=pq Where, n is the modulus for the public key and the private keys.
3. Calculate the totient: Ø(n) = (p-1)(q-1)
4. Choose an integer e such that 1 < e < Ø(n), and e is c
   prime to Ø(n), ie: e and Ø(n) share no factors other than 1; ie,
   gcd(e, Ø(n)) = 1 e is released as the public key exponent.
5. Choose d to satisfy de ≡ 1 (mod Ø(n)) d is kept as the private key exponent.

The message can encrypt by using c = m^e mod n and the decryption function is m = c^d mod n. After encrypting the data, it is stored in data centre.

The system describes encryption technique for providing privacy foe stored data. That is it represents a method of sharing public and private key. For the encryption it uses RSA algorithm .But disadvantage over this system is that, In case of signature, the ECDSA signatures and public keys are much smaller than RSA signatures and public keys of similar security levels. Also it does not give further advantage over patients like they cannot set a time interval where the physicians can access the data, or they cannot set who can access their data.So in proposed system for encryption RSA algorithm and for signing ECDSA algorithm is used.

IV. proposed system

One of the main application area of this mobile computing is the Electronic healthcare (eHealth) systems or mobile health system . This mobile health system have replaced paper-based medical systems due to its characters like low cost , high accuracy and universal accessibility. Major component of eHealth systems, applies mobile devices to enable patient-to-physician communications. For most mHealth systems, patients use sensors, implantable medical devices, and mobile to send medical data to the designated healthcare infrastructure. If a data center is compromised, patient's private data may be revealed. For providing security in such systems should be enforced via encryption and the authentication of the users.

When patients upload the file, it stored in cloud as a ciphertext. An encryption is performed over the uploaded file. After performing an RSA encryption over the file, the public(P_u) key and the private key(P_r) is stored in data base. An ECDSA is performed over the cipher text for providing a digital signature and this hash value is stored in database and the cipher text is stored in cloud.

When physicians download the file, first it searches the patient name whose files want to be downloaded. After getting a list of file he send a request to patient for checking that, if the patient provides a permission for the access of file or not. Once they provide permission, the physician can download the file from cloud. If the ECDSA verification is ok, then he can decrypt the cipher text and gets the original file.

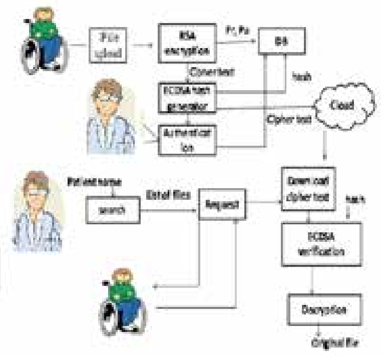

Fig 1. System Architecture

The ECDSA algorithm is, if Alice wants to send a signed message to Bob , Alice creates a key pair which consisting of a private key integer d_A randomly selected in the interval [1,n-1]and a public key curve point $Q_A = d_A * G$ where G elliptic curve base point and n integer order of *G*, means that n*G=0. For a message m, .

Calculate e=HASH(m)
2. Let z represents the leftmost bits of e
3. Select a random integer k from an intervel
[1,n-1]
4. Calculate the curve point $(x_{1,}y_1) = k*G$
5. Calculate $r = x_1 \bmod n$, if r =0 go back to
step 3
6. Calculate $s=k^{-1}(z+rd_A)\bmod n$, if s=0 go back to
step 3
7. The signature is the pair (r,s)

For Bob to authenticate Alice's signature he must have a copy of her public-key curve point QA.

1. Verify that r and s are integers in [1,n-1]. If
not, then the signature is invalid.
2. Calculate e = HASH(m)
3. Let z be the leftmost bits of e
4. Calculate $w = s^{-1} \bmod n$
5. Calculate u1 = zw mod n and u2= rw mod n
6. Calculate the curve point
(x1,y1) = u1*G + u2*QA
7. The signature is valid if $r \equiv x1 \pmod n$
Otherwise it is invalid

This is the encryption and signature generation algorithm used over the system. Main modules and their functions used in this system are,

1. Patient

Main functions of patient module are

- Signup
- File upload
- Allow access permission to physician
- Delete permission
- Time setting
- Download

2 Physicians

The main functions include in the Physician sides are

- Search
- View files
- Request
- Download

3. Server

The main functions include in the Server side are

- Registration
- Keys generation
- Sign generation

v. Conclusion

The system describes encryption technique for providing privacy foe stored data. That is it represents a method of sharing public and private key. For the encryption it uses RSA algorithm. Also it provide a digital signature, which is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message any signing method. Also it give further advantage over patients like they can set a time interval where the physicians can access the data, or they can set who can access their data.

REFERENCE

[1] Linke Guo, Chi Zhang, Hefei Jinyuan Sun, Yuguang Fang ,"A Privacy-Preserving Attribute-based Authentication System for Mobile Health Networks",in IEEE Transactions on Mobile Computing | [2] Carl Youngblood, "An introduction to Identity based Crypto graphy" | [3] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records," in Proc. ACM Workshop CCSW, New York, NY, USA, 2009, pp. 103–114 | [4] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Proc. SECURECOMM, Singapore, 2010, pp. 89–106. | [5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp. 321–334, 2007 | [6] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure," in Proc. ACM CCSW, New York, NY, USA, 2010, pp. 47–52. | [7] Kavitha Murugesan, Anjana.T.K, "Password Authentication Scheme Based On Shape and Text for Secure Sharing Of PHR Using ABE in Cloud", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013 | [8] M. Balamurugan, S. Chenthur Pandian and ,J. Bhuvana,"Privacy Preservation For File Sharing Scheme Using Secured File Block ID With Binary Trees", American Journal of Applied Sciences, 10 (1): 1-7, 2013 ISSN: 1546-9239 | [9] Shireesh Kumar Manda, B.HanmanthuPrivacy, "Preserving Support for Mobile Health Care using Message Digest", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 9, September 2013 ISSN: 2277 128X | [10] Apurva Mohan , David Bauer , Douglas M. Blough,"A Patient-centric, Attribute-based, Source-verifiable Framework for Health Record Sharing". | [11] http://en.wikipedia.org/wiki/Mobile_computing | [12] http://simple.wikipedia.org/wiki/RSA_%28algorithm%29