كلية التراث الجامعة
المؤتمر العلمي السنوي الحادي عشر

طريقة مقترحة للولوج الآمن الى ملفات قواعد البيانات في تطبيقات العناية الطبية

د. سعد عبدالعزيز عبدالرحمن د. سناء احمد كاظم

كلية المأمون الجامعة

المستخلص

تعتبر العناية الطبية احدى المجالات المهمة التي تزايد الاهتمام بها مع التطور الكبير في تراسل البيانات وما يعرف بأنترنت الاشياء والذي تتشارك فيه جهات متعددة لتقدم خدمة معينة. الاتصال بين المريض والطبيب او مركز العناية الطبية يجب ان يكون مؤمن ودخول المريض لملفاته الطبية يجب ان يكون موثوق. في هذا البحث يتم اقتراح طريقة امنة للاتصال ودخول موثوق للمريض الى ملفاته الطبية. في هذه الطريقة يتم استخدام بعض المفاهيم لطرف معروفة مثل الالبتك كيرف وتشفير الجمال.

الكلمات المفتاحية: الالبتك كيرف, الولوج الموثوق, تشفير الجمال, العناية الطبية.

Abstract

Health care is one of the most important aspects which raises with the improvement of data communication and the internet of things were many parities join together to produce a service. The communications between the patient and his doctor or health care center should be secured and the access of the patient to his electrical medical files should be authentic . In this paper a new method is produced to secure this type of communication and provide the patient a secured access to his medical files. The method used some concepts of well-known algorithms like Elliptic curve and El-Gamal encryption.

Key words: Elliptic curve, access authentication, El-Gamal encryption, Health care.

1. Introduction

Due to the massive improvements in personal applications using Internet and the growth need for fast and secure access to personal files like bank accounts, medical files, educational files and others, many methods and strategies were produced to provide users need for fast and secure access[1]. Methods of cryptography and steganography have been used and improved frequently in the last few decades to improve internet applications and make them more applicable and useful for ordinary users[2].

Medical files have a special interest because of the sensitive information contained in such files. Accessing medical files should be restricted to those who are authorized like the patient himself and his doctor(s)[3]. therefore, security should be ensured here. One of the most effective methods for securing such files is by using secret key(s) for accessing and manipulating these information. The health care center (or a hospital or a doctor) may have many patients in its database[4]. To restrict each patient with only his data, a secured method is proposed using public and private keys between the patient and his health care center.

The proposed method combines two cryptography methods: Elliptic curve(EC) and El-Gamal encryption method.

2. Elliptic Curve (EC)

Elliptic curve system is mathematically complicated and needs finite field operations. Many researches worked on applying EC for its fast and complicated implementation.

The basic idea of EC depends on a scalar multiplication ($H \cdot P$), where P is a point on the EC used in a cryptosystem. Actually, scalar multiplication is a repeated addition operation on repeated point so that, the results of the EC system depends on number of repeating the process and this dependence is linear[5].

2-1 Elliptic Curve Public-Key Pairs

The process of producing the key of EC cryptosystem is as follows:

Suppose we have a set of points which is finite but very large (call it E). then suppose that if we have two points (P1,P2) from E we can produce a third point(P3) from the same set by P1(x1,y1)+P2(x2,y2)=P3(x3,y3). Now if we have a point M from E, then adding the point to itself will produce another point also in E, therefore we may have M+M, M+M+M, M+M+...+M. we may use an integer H which represent the number of repetitions used in finding the new point. The new point will be found by :R(x,y)= M(x1,y1) * H using the formula below:

$\Lambda = (3*x1^2+a) / (2*y1)$, where a is a coefficient.

$X= \Lambda^2 - 2*x1 \bmod p$

$Y= \Lambda (x1 - x) - y1 \bmod p$

The public key will be Q which is Q=M*H, while the private key L is a random number module E. so the key pair of EC is (L,Q) [6].

3. El-Gamal Encryption

El-Gamal encryption method produces a pair of numbers in each step (c1,c2) depending on a predetermined key. If a receiver has El-Gamal public key (y) where $y=g^x \bmod p$, and x is the private key and the sender wants to use this key in encrypting a message m. the process will be as follows[7]:

Compute c1 by : $c1= g^K \bmod p$, where g is any number less than p. $0<K<p-1$

Compute c2 by : c2= m. y^K mod p.

4. The Proposed method

The proposed method involves two sides: the medical care center (doctor, hospital,..) and the patient. Both will agree on a point G on the EC from E_P . the proposed method depends on EC key generation and El-Gamal encryption.

4-1 Medical care center(For each patient):

Take the first character of the patient first and last name.

Convert the two characters to a two digit hexa-number(h1h2,h3h4).

Select a random number K, from the interval (1..P) where P is the maximum limit of the Elliptic curve set E (E_P).

Select a point G in the curve to be shared by the medical care center and the patient.

Find Y_0 = K G

Send Y_0 to the patient.

Find (C_1,C_2) = K P_B, where P_B is the patient public key.

Find :

Y_1=C_1 h_1 mod P

Y_2=C_2 h_2 mod P

Y_3=C1 h_3 mod P

Y_4=C2 h_4 mod P

$T_H = Y_1 * h_1 + Y_2 *h_2 + Y_3 *h_3 + Y_4 *h_4$

Save the name of the patient in the database with its corresponding T_H.

4-2 Patient :

Select a random number n_B, from the interval (1..P) where P is the maximum limit of the Elliptic curve set E (E_P), then find the public key (P_B =G n_B).

Find (C1,C2)= Y_0 n_B , where n_B is the private key of the patient.

Take the first character of his first and last name.

Convert the two characters to a two digit hexa-number.

Encrypt the hexa-numbers as:

Y_1=C_1 h_1 mod P

Y_2=C_2 h_2 mod P

Y_3=C1 h_3 mod P

Y_4=C2 h_4 mod P

$T_P = Y_1 * h_1 + Y_2 *h_2 + Y_3 *h_3 + Y_4 *h_4$

Send T_P to the medical care center when trying to access his own medical files.

4-3 Verification of patient access:

The medical care center will receive T_P from the patient when he trying to access his medical files. This access will be verified as follows:

If TP =TH then : Access verified

otherwise : Access denied

The verification depends on the equalization of two parameters that are found with different keys (k and n_B). this verification depends on the following mathematical operation:

Since, for medical care center :

$(C_1,C_2) = K\ P_B$ and $P_B = n_B\ G$

And, for patient:

$(C_3,C_4) = Y0\ n_B$ and $Y0 = K\ G$

Then:

$(C_1,C_2) = K\ P_B \ = Y0\ n_B = (C_3,C_4)$

$(C_1,C_2) = K\ G\ n_B \ = K\ G\ n_B = (C_3,C_4)$

So:

$(C_1,C_2) = (C_3,C_4)$ and that implied the verification $T_H = T_P$

5. Implementation

Suppose P=23, then:

$E_{23}(1,1)$, E: $y^2 - x^2 + x + 1$ define over Z_{23} ,

For a=1 ,b =1 and $4a^3 + 27b^2 \bmod p \neq 0$ then

$4 * (1)^3 + 27*(1)^2 = 8 \neq 0$

The elliptic group Ep(a, b) = $E_{23}(1, 1)$ this include the points:

E23(1, 1) = (0, 1) (0, 22) (1, 7) (1, 16) (3, 10) (3, 13) (4, 0)
(5, 4) (5, 19) (6, 4) (6, 19) (7, 11) (7, 12) (9, 7)
(9, 16) (11, 3) (11, 20) (12, 4) (12, 19) (13, 7) (13, 16)
(17, 3) (17, 20) (18, 3) (18, 20) (19, 5) (19, 18)

The hexadecimal conversion of each alphabetical character is shown in table 1 below:

Table 1: Hexadecimal representation of English characters

A	41	O	4F
B	42	P	50
C	43	Q	51
D	44	R	52
E	45	S	53
F	46	T	54
G	47	U	55
H	48	V	56
I	49	W	57
J	4A	X	58
K	4B	Y	59
L	4C	Z	5A
M	4D		
N	4E		

Medical care center:
Suppose the patient name = "Ahmed Zaki"
X_1=A=41 → h1=4 , h2=1
X_2=Z=5A → h3=5 , h4=A
Let G = (1,7)
Suppose the public key of patient P_B = (0,22)
And the medical care center select its private key as K= 9, then:
Y_0 =KG = 7(1,7) = (9,16) , Sent Y_0 =(9,16)
(C_1,C_2)=K P_B =(19,5)
Y_1=C_1*h1 mod p =19*4 mod 23 = 7
Y_2=C_2*h2 mod p = 5 *1 mod 23 = 5
Y_3=C_1*h3 mod p = 19*5 mod 23 = 3
Y_4=C_2*h4 mod p = 5* 10 mod 23 = 4
T_H= 7*4 + 5*1 + 3*5 + 4*10 = 88
Save (Ahmed Zaki , 88)
Patient:
P_B =(0,22) , n_B =5
C_3,C_4 = Y_0 n_B = 5(9,16) = (19,5)
Name ="Ahmed zaki"
X_1=A=41 → h1=4, h2=1 , X_2=Z=5A → h3=5, h5=A
Y_1= 7 Y_2 = 5 Y_3=3 Y4= 4
T_P = 7*4 + 5*1 + 3*5 + 4*10 = 88
Send T_P when access is required.

6. Results and Analysis

By applying the proposed method on many patients, the results were as in table 2 below:

Table 2: Implementation of five patient

Patient name	n_B	G	K	P_B	(C_1,C_2) (C_3,C_4)	T_P T_H
Ahmed Zaki	3	(1,7)	5	(18,20)	(0,22)	152
Belal Sadak	4	(1,16)	3	(17,3)	(5,4)	142
May Ali	6	(3,10)	3	(12,4)	(6,19)	400
Yousif Fady	7	(3,13)	4	(11,20)	(21,20)	326
Ahmed Zaki	5	(1,7)	9	(0,22)	(19,5)	88

From table 2 , it is clear that when patients have the same name but with different private key or with different K, then the verification number TP will be different as well. Using the same private key by different patients with different names will produce different TP's. for different patients, even if the same K is used, the resulted TP's will be different. From all that, the uniqueness of verification number is ensured.

Conclusions

Guarding electronic medical files is one of the most important aspects in internet applications especially with the great improvements and usage of this field. The first step of securing medical information in a database is by securing the access to this information. Using verification technique for accessing medical database was used frequently in the last few years. In the proposed method the access verification depends on using public and secrete keys. These keys were produced and used by joining two concepts: EC points for its complexity and El-Gamal encryption for its simple but yet powerful basis. The results showed that, the verification number produced for different patients were different even if the names were the same, the private key, or even the K used by the medical care center, were the same.

References

[1] B. Lynn. The pairing-based cryptography library. http://crypto.stanford.edu /pbc/, June 2011. Version 0.5.12.

[2] 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 Security and Privacy in Communication Networks, volume 50 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pages 89–106. Springer Berlin Heidelberg, 2010.

[3] Ontario Hospital Association, "Protecting personal health information," webinar broadcast May 7 2013. Retrieved on July 2013 from http://ohaeducation.discoverycampus.com /elms /en /login.

[4] De Keijzer. MeDIA: Medical data management. Technical Report TR-CTIT-11-17, Centre for Telematics and Information Technology, University of Twente, Enschede, The Netherlands, 2011. ISSN 1381-3625.

[5] J.S. Milne," Elliptic Curves", BookSurge Publishers, 2006.

[6] Nick Sullivan, "A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography", CloudFlare , 24 Oct 2013.

[7] Andreas V. Meier, " The Elgamal Cryptosystem", http://www14.in.tum.de /konferenzen /Jass05 /courses/1/ papers/meier_paper.pdf, 2005.

[8] K. H¨ayrinen, K. Saranto, and P. Nyk¨anen. Definition, structure, content, use and impacts of electronic health records: A review of the research literature. International Journal of Medical Informatics, 77(5):291, 2008.

[9] Information and Privacy Commissioner of Ontario, "Unauthorized Access to Electronic Records," Presentation to Ontario Hospital Association, November 28 2012. Retrieved on May 16 2013 from http://www.ipc.on.ca/images/Resources/2012-11-28-OHA.pdf.

[10] Canadian HealthcareNetwork,"Privacy concerns adversely affect patient care outcomes,

survey finds," February 22 2012. Retrieved on July 17 2013 from http://www.canadianhealthcarenetwork.ca/healthcaremanagers/news/hospitalinstitutional/privacy-concerns-adversely-affect-patient-care-outcomes-survey-finds-13209.

[11] Ponemon Institute, Third Annual Benchmark Study on Patient Privacy & Data Security, December 2012. Retrieved on October 3 2013 from http://lpa.idexpertscorp.com/acton/attachment/6200/f-0033/1/-/-/-/-/file.pdf.

[12] Canada Health Infoway. "Cloud computing in health care" webinar broadcast February 13 2013. Retrieved on July 17 2013 from https://www.infoway-inforoute.ca/index.php/events/past-events-highlights/cloud-computing-in-health-webinar.