EAI Endorsed Transactions
on Pervasive Health and Technology

Research Article EAI.EU

Cloud-based Secure TeleMedicine Information System using Crypto-Biometric Techniques

Dindayal Mahto[1,*], Dilip Kumar Yadav[2]

[1]SASTRA Deemed-to-be University, Thanjavur, Tamil Nadu, India
[2]NIT Jamshedpur, Jharkhand, India

Abstract

INTRODUCTION: TeleMedicine Information System (TMIS) uses information and communication technology (ICT) for providing remote medical consultations. Taking the benefits of ICT, a sick person may distantly get regular telecare medical consultations with his/her remote medico. The backbone of ICT is the Internet, which is open-standard architecture. Due to the openness of the architecture, there are many security vulnerabilities to the TMIS.
OBJECTIVES: To provide secured telemedicine consultation between a sick person and a medico and, to maintain the privacy of the sick person information.
METHODS: This paper proposes a security enhancement to the TMIS using crypto-biometrics fusion, which consists of Elliptic Curve Cryptography (ECC) algorithm and iris biometrics. The paper also compares the efficiency of ECC with the Rivest-Shamir-Adleman (RSA) algorithm.
RESULTS: The result of the simulation proves that the offered model provides a high level and robust security than RSA based model.
CONCLUSION: This paper provides robust user authentication and achieves the data confidentiality of the TMIS, which uses a cloud computing system for its smooth functioning and wider scope.

Received on 30 September 2019; accepted on 25 October 2019; published on 13 November 2019

Keywords: Elliptic Curve Cryptography, RSA, Iris Biometrics, Asymmetric-key Cryptography, Patient, Doctor

doi:10.4108/eai.13-7-2018.163837

Abbreviation

CS	Cloud Server
CKP	Checkup Process
CSK	Common Secret Key
CSP	Cloud Service Provider
EC	Elliptic Curve
ECC	EC Cryptography
ECDHKX	EC Diffie-Hellman Key eXchange
HP	Health-care Provider
HPUP-M	HP Upload Process for MD
HPUP-SP	HP Upload Process for SP
MD	Medico/Doctor
PBK	Public Key
PVK	Private Key
RSA	Rivest Shamir Adleman
SP	Sick-Person/Patient
SPUP	Sick Person data Upload Process
TMIS	TeleMedicine Information System
TTP	Treatment Process

1. Introduction

The term telemedicine literally means “healing at a distance”, was introduced by the American Thomas Bird in the 1970s. The origins of this technology, however, date back to the beginning of the 20th century. [33]. Telemedicine offers a sick person the opportunity to interact with his medico, even though they live in faraway places. The sick person gets a digital prescription after consultation with the medico, which allows the sick person to take adequate medication and precautions for their care and thus enjoys a healthy

[*]Corresponding author. Email: dindayal.mahto@gmail.com

life. Telemedicine works based on communication channels such as the Internet or Intranet. Such communication channels, however, are based on open source technologies. Because of this openness, certain confidentiality issues are activated when exchanging sensitive information, such as sick person data and medication. The privacy of the information of the sick person while communicating in TeleMedicine Information System (TMIS) must be maintained. In order to maintain privacy of TMIS, this paper uses ECC with iris biometric. Stakeholders' private keys must be confidential, non-sharable, and secure. There is a need for larger cryptographic keys than the prevailing key sizes because of a rapid breakthrough in cryptanalysis. Larger key size, however, has many issues, such as difficulties in remembering, entering into or storing in the system. When keys are kept somewhere, the keys may get stolen/lost. This paper suggests a model using iris biometric to produce cryptographic keys to tackle the above-mentioned problems. Such keys are digitally created as and when a sick person and a medico need. Ultimately, the generated cryptographic keys are used to enforce ECC in telemedicine for the security of sensitive information traffic.

The following is the structure of this article. Section-II discusses similar research and reviews of literature. Section-III explains ECC. Section-IV discusses iris biometrics. Section-V discusses cloud computing. Section-VI explains the suggested system. Section-VII explains a case study based on the suggested system. Section-VIII describes the suggested approach's security analysis and its conclusion is outlined in Section-IX.

2. Similar Research and Review of Literature

Online consultations of telemedicine system between specialists and referring medicos develop novel ideas which can be applied to sick person in timely and hassle free manner for providing best treatment to the sick person[14]. Communication can be considered as the main ingredient in medical care [29]. A survey has been conducted for the telemedicine system, which suggests that the telemedicine still requires some time to become ubiquotous e- service. Different barriers have been studied with the help of earlier published works. There are some pioneer obstacles, such as technology-specific barriers, strategies for change management, and alternative delivery by telemedicine and contact between sick person and provider [31]. A practical and secure telemedicine system for user mobility is proposed [30], in which the system uses symmetric key cryptography for providing confidentiality between Patient and Doctor. This system generates a session key for every session between Patient and Doctor. The session key generation, distribution, and management are tedious task for the key generator i.e. Home Server (HS). Other case in which HS and Remote Server (RS) work as intermediary between Patient and Doctor, here also the Patient authentication with RS is time taking and problematic if the RS may behaves maliciously. The main issue with symmetric key cryptography is key distribution. Kumar et al. [16] propose cloud-assisted TMIS, which suggests a strong secure authentication system and manages a good resource efficiency. A protocol for efficient digital image telemedicine protection is proposed [32] using D[W/C]T (Discrete Wavelet/Cosine transform). Nonetheless, [32]'s paper suggests only digital image protection, with no related solution for text-based data available. Several researchers have exemplified in the literature on how cryptographic models are implemented using biometric-based keys. Biometric traits produce these keys. The following is a short analysis of a few selected papers: Hao et al. [9] used iris-based biometric cryptographic keys to depict the implementation of the 128-bit AES cryptography model, which first produces genuine IrisCodes and then creates a regenerated binary digit known as the biometric key of up to 140 bits. Yao-Jen et al. [4] proposes face-based cryptographic-key generation. The main problem with face biometric is that after certain years shape and size of face changes, and then False Rejection Rate increases. Monrose et al. [28] proposes voice-based cryptographic key generation, there is a risk of recording the voice-based password and later imposter can use it. Other implied crypto-biometric approaches are given in [1, 8, 17–22, 34].

3. ECC

Elliptic curves that are not directly related to ellipses are cubic equations in two variables similar to the equations used to calculate integrals of ellipses in arc lengths. The generalized EC cubic equation is as follows:

$$y^2\ (mod\ prm) = x^3 + ax + b\ (mod\ prm) \qquad (1)$$

where, 'a' and 'b' are the coefficients and 'prm' is a large prime digit of desired security length of the EC, and the discriminant, $\Delta = 4a^3 + 27b^2 \neq 0$. The $\Delta \neq 0$ requires the formation of a group and thus the use of the elliptic curve to implement cryptography. ECC is a method for public-key cryptography [7], proposed by two authors independently (Neil Koblitz [15] and Victor S. Miller [27]) in late 1985. In ECC, first of all, each character of the message must be converted into the form of a point(x, y). In this way, as many points as the length of the message are generated. Such generated points are encrypted and decrypted by ECC algorithm. ECC is regarded as an RSA algorithm competitor. The RSA cryptography's security is dependent on the

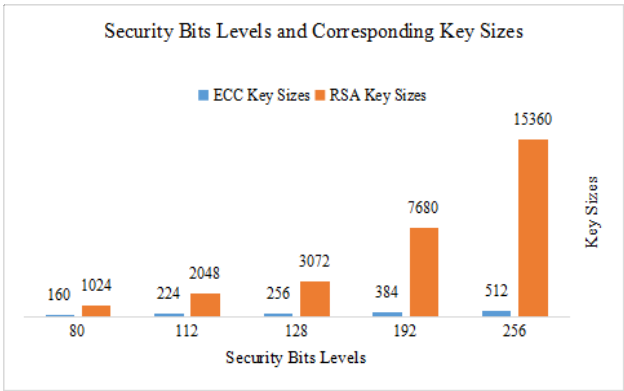


Figure 1. Key Size (NIST Recommended)[2]

IFP (Integer-Factorization-Problem), and ECC's security is dependent on the ECDLP (Elliptic-Curve-Discrete-Logarithm-Problem). ECC's main selling point to RSA is that famous technique to crack the ECDLP takes full exponential time, whilst it takes sub-exponential time to resolve RSA's IFP. ECC has a complex numerical calculation that helps to provide better safety per bit with less key length than RSA. It means that, with comparable protection rates, significantly smaller parameters are used in ECC than RSA. The comparative data is shown in Fig. 1. This figure shows the key sizes to be needed by RSA for safety bit level 80, 112, 128, 192, 256 as 1024, 2048, 3072, 7680, 15360, while by ECC as 160, 224, 256, 384, 512 respectively.

4. Iris-Biometrics

An eye is a visual organ. An eye consists of several components. One of the important components is an iris, which is shown in Fig. 2. Referring to Fig. 2 of an eyeball, the sclera is a white portion, the pupil is the dark-black part in the middle, and the iris is a mixture of colored pigment, found between sclera and pupil. Because of iris's distinctive features, large quantities and non-counterfeiting [9] texture pattern [5], it offers a highly reliable and accurate user recognition tool compared to other biometrics characteristics [6]. IrisCode is produced after finding the surrounding boundary between the portions of iris and pupil and the outer boundary between the iris and the sclera portions of the image of the eyeball. An iris is located as [9, 10, 13] do and then the localized characteristic, in turn, generates the IrisCode. The IrisCode eventually helps to generate cryptographic keys. The steps for IrisCode generation are shown in Fig. 3.

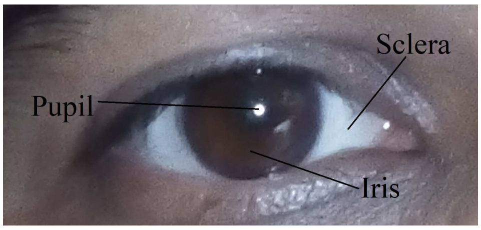


Figure 2. Eyeball's iris

5. Cloud Computing

The ICT provides the platform to flourish the cloud computing technology. Cloud computing is on-demand service facilities available through the Internet or Intranet, which provides many services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS)[26]. Due to its pay-per-use model of licensed computing resources as well as software services, Cloud Computing is expanding its client base [12]. An organization, can use, these services as use and pay basis. These type of rental services helps an organization optimize its resources, minimize the cost of ever-growing IT infrastructure and software. One of the important services of cloud computing is SaaS, which helps an organization run a business application without any breakdown. This paper suggests a system for TMIS, which uses the PaaS service of the cloud computing system. The Cloud computing platform provides many services for different business applications to execute smoothly without any breakdown. One such recent application uses the cloud computing platform to generate an automated query system[11].

6. Suggested System

The Fig. 4 reflects the solution proposed. In this system, there are four different actors/units: the sick person, the reliable Health-care Provider, the Medico, and the Server hosted on a cloud computing environment. The system consists a Health-care Provider Upload Procedures (HPUP_SP or HPUP_M) for a Sick Person and a Medico, a Sick Person data Upload Process (SPUP), a Treatment Process (TTP) and a Checkup Process (CKP).This system uses the iris biometrics characteristics of the sick person, health-care provider, and the medico to generate their private and public keys, and then those keys are utilized in ECC to ensure the safety of traveling messages related to medical consultation between the sick person and the medico. The SP uses MD's PBK to encrypt plain-message, and this cipher-message is then sent to the MD. When the MD decrypts and receives a plain-message, then the MD understands the SP's issue and writes a prescription. The plain-prescription is encrypted by the MD using

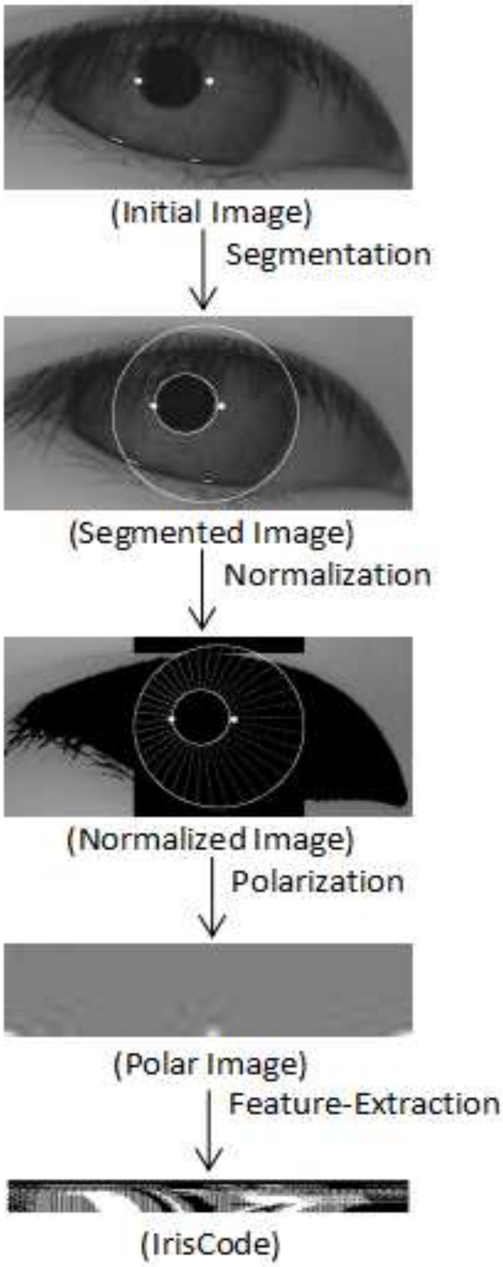


Figure 3. Steps for generating IrisCode

the SP's PBK, and this generated cipher-prescription is then sent to the SP. In this way, the cycle is formed and their messages are kept securely sent.

A. Steps for the suggested system

In this system, all parties need two keys i.e. PVK and PBK. This scheme focuses primarily on the confidentiality of information security services using ECC. The receiver's PBK is used by the sender for encrypting the message, while, receiver's PVK is used by the receiver himself for decrypting the cipher message.

The PVKs of HP, MD, and SP get generated from hash-values of their IrisCodes. The cloud server uses a random number of the desired length as its PVK.

A CSP is approached by a HP and then they use the ECDHKX protocol to generate their PBKs, and a common secret-key (CSK) for them gets calculated using their PBKs.

In a similar way, MD and the HP, and, SP and the HP, use the ECDHKX protocol to generate their PBKs, and further their CSKs get calculated based on their PBKs.

The HP works as a trusted facilitator of medical infrastructure/services for the SP and the MD. The HP also coordinates them to the cloud server.

After an initial round of key-exchanges, the HP uses medico's PBK to encrypt the cloud server's PBK and send this encrypted data to the MD.

In a similar way, the HP uses the SP's PBK to encrypt the cloud server's PBK and sends this encrypted data to the SP.

In the CSP side, the CS stores the incoming ciphertext with a suitable bookmark in its database so that the CS can later recognize this ciphertext immediately. The bookmark may contain subject, sender, receiver, date and time. Only decryption happens when a user requests the data, and then the CS matches the incoming request of the user with the stored bookmark and decrypts the corresponding ciphertext with the help of ECC using its own PVK. This decrypted message is immediately sent to the requester. After sending the decrypted message, there is no availability of the decrypted message at the CS side, however, the corresponding ciphertext of the decrypted message still persists in the database. This way of storing and managing the data prevents insider attacks or other related attacks to the data-at-rest.

(i) In the HPUP-M phase, the HP encrypts MD's basic information and the MD's PBK, using the CS's PBK and then HP uploads this ciphertext to the CS.

(ii) In HPUP-SP phase, the SP approaches HP for treatment. First of all, as mentioned above, their keys get generated and exchanged. After that, the HP inspects the SP and then encrypts this inspected report and the SP's PBK, using the CS's PBK, and finally, HP uploads this ciphertext to the CS.

(iii) In the SPUP phase, the SP encrypts a request message to view his inspected report, using the CS's PBK, and then SP uploads this ciphertext to the CS. The CS decrypts this ciphertext using its own PVK. This decrypted plaintext is then encrypted with the help of ECC using SP's PBK.

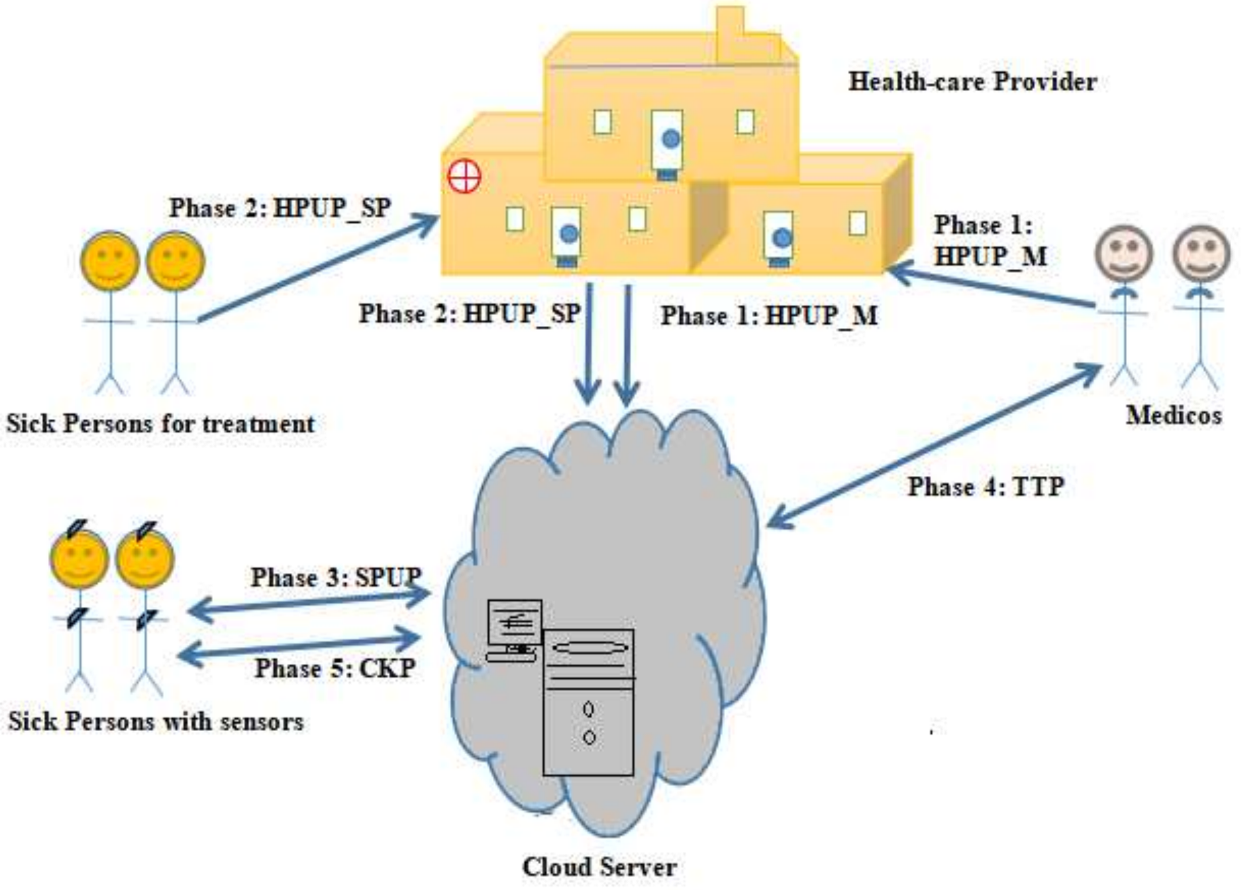


Figure 4. Cloud-based Secure TMIS

Finally, the resultant ciphertext is sent to the SP. The SP decrypts the ciphertext using his own PVK and gets his inspected report. Later, the SP encrypts his body sensor's information using the CS's PBK. Then the SP uploads this ciphertext to the CS.

(iv) In the TTP phase, the MD encrypts a message regarding the treatment of the SP, using CS's PBK, and then the MD sends this ciphertext to the CS. The CS decrypts this ciphertext using the own's PVK, and then CS encrypts the required information of the SP using the MD's PBK, and then the CS sends the resultant ciphertext to the MD. At the MD side, the MD decrypts this ciphertext and reads the details of the SP. After going through the details of the SP, the MD encrypts the digital prescription and other diagnosis reports of the SP using CS's PBK, and then the MD uploads this ciphertext to the CS.

(v) In the CKP phase, the CS receives the ciphertext from MD regarding the SP and then the CS gets the plaintext after decrypting it using own's PVK. Once getting the decrypted prescription and diagnosis reports of the SP, the CS encrypts the same using the SP's PBK and then the CS sends this ciphertext to the SP.

In this way, a confidentiality of the message is achieved amongst the stakeholders. If they need to exchange further information, then they have to follow the step-iii through step-v.

B. Key Exchange using ECDHKX

I. Steps for generating PBK and CSK of users, the CS and the HP

Global public elements

(i) Both the users, CS and HP, opt a large prime digit of desired security length, 'prm', as well as other parameters such as 'a' and 'b', which satisfy the above equation number 1:

(ii) A reference point: R(x, y), is chosen from points of the EC.

The CS - key generation

(i) Private key of the CS:
PVK_{cs} = a random number of the desired length.

(ii) Public key of of the CS:
$PBK_{cs}(x, y)= PVT_{cs} * R(x, y)$.

The HP - key generation

(i) Private key of the HP:
PVK_{hp} = the HP's hash-value of his IrisCode.

(ii) Public key of of the HP:
$PBK_{hp}(x, y)= PVT_{hp} * R(x, y)$.

Calculation of a CSK between user, the CS and the HP

(i) CSK for the CS:
$CSK_{cshp}(x, y) = PVK_{cs} * PBK_{hp}(x, y)$.

(i) CSK for the HP:
$CSK_{cshp}(x, y) = PVK_{hp} * PBK_{cs}(x, y)$.

II. Steps for generating PBK and CSK of users, the MD and the HP

Global public elements

(i) Both the users, MD and HP, opt a large prime digit of desired security length, 'prm', as well as other parameters such as 'a' and 'b', which satisfy the above equation number 1:

(ii) A reference point: R(x, y), is chosen from points of the EC.

The MD - key generation

(i) Private key of the MD:
PVK_{md} = the MD's hash-value of his IrisCode.

(ii) Public key of of the MD:
$PBK_{md}(x, y)= PVT_{md} * R(x, y)$.

The HP - key generation

(i) Private key of the HP:
PVK_{hp} = the HP's hash-value of his IrisCode.

(ii) Public key of of the HP:
$PBK_{hp}(x, y)= PVT_{hp} * R(x, y)$.

Calculation of a CSK between users, the MD and the HP

(i) CSK for the MD:
$CSK_{mdhp}(x, y) = PVK_{md} * PBK_{hp}(x, y)$.

(i) CSK for the HP:
$CSK_{mdhp}(x, y) = PVK_{hp} * PBK_{md}(x, y)$.

III. Steps for generating PBK and CSK of users, the SP and the HP

Global public elements

(i) Both the users, SP and HP, opt a large prime digit of desired security length, 'prm', as well as other parameters such as 'a' and 'b', which satisfy the above equation number 1:

(ii) A reference point: R(x, y), is chosen from points of the EC.

The SP - key generation

(i) Private key of the SP:
PVK_{sp} = the SP's hash-value of his IrisCode.

(ii) Public key of of the SP:
$PBK_{sp}(x, y)= PVT_{sp} * R(x, y)$.

The HP - key generation

(i) Private key of the HP:
PVK_{hp} = the HP's hash-value of his IrisCode.

(ii) Public key of of the HP:
$PBK_{hp}(x, y)= PVT_{hp} * R(x, y)$.

Calculation of a CSK between users, the SP and the HP

(i) CSK for the SP:
$CSK_{sphp}(x, y) = PVK_{sp} * PBK_{hp}(x, y)$.

(i) CSK for the HP:
$CSK_{sphp}(x, y) = PVK_{hp} * PBK_{sp}(x, y)$.

C. Message encryption

The sender encodes plain-message into EC points, $P_{msg}(x, y)$. These EC points get encrypted by sender using the ECC alongwith receiver's PBK. Then the encrypted points are sent to the receiver. The steps for encoding and encrypting are mentioned below:

(i) Each character of a plain-message (msg) gets converted as 0,1,2,3,4,5,6,7,8,9 (for decimal digits), 10, 11,. . . , 34, 35 (for upper case alphabets), 36, 37, . . . 60, 61 (for lower case alphabets), 62, 63, 64 . . . . . . 90, 91 (for special symbols).

(ii) The ECC Encryption module of the sender generates $P_{msg}(x, y)$ from the msg.

(iii) This module uses a temporary variable, h, which gets initialized as,

$$h = 1\%\ CSK's\ x - coordinate \tag{2}$$

[the CSK(x, y) point gets generated for the sender and the receiver during the ECDHKX phase].

(iv) The x-coordinate, of the EC point, is calculated as,

$$x = msg * h + i \tag{3}$$

where, the value of the variable, i, considers from 1 to h-1.
An integral value, y, get calculated, based on the value of x, such that the values of x and y, must satisfy equation number 1. If equation number 1 is not satisfied by these x and y values, then the value of the variable, i, is incremented to 1, and then the same process is applied until the equation number 1 is satisfied.
In this way, whole msg is converted into different EC points(x,y).

(v) The cipher-message consists two EC points such as,

$$C_{\text{msg}} = ((k * R(x,y)), (P_{\text{msg}} + k * PBK(x,y))) \tag{4}$$

where the PBK(x, y) is the receiver's public-key, and the intermediary variable, k, is randomly selected an integer value by the sender.

(vi) The sender sends this cipher-message to the receiver.

D. Message decryption

The receiver gets cipher-message, then it decrypts plain-message from cipher-message using decryption module, which requires its own's PVK. Steps for decrypting the cipher-message are given below:

(i) The receiver gets C_{msg}.

(ii) The receiver multiplies the point1 of the cipher-message with its own's PVK, and, then subtracts the resultant point from the point2 of cipher-message:
The C_{msg} is expressed as,

$$= (P_{\text{msg}} + k * PBK(x,y)) - (k * PVK * R(x,y)) \tag{5}$$

$$= (P_{\text{msg}} + k * PVK * R(x,y)) - (k * PVK * R(x,y)) \tag{6}$$

After subtracting, the P_{msg} is left, which is the plain-message point.

(iii) The decoding of the plain-message is done as,

$$msg = floor((P_{\text{msg}}(x) - 1)/h) \tag{7}$$

where, the variable, h, gets value, based on equation number 2, and the floor function produces the greatest integer <= x.

(iv) The msg is the decrypted-message.

(v) Finally, the msg is uncoverted into corresponding decimal digits (from 0,1,2,3,4,5,6,7,8,9), upper case alphabets (from 10, 11,. . . , 34, 35), lower case alphabets (from 36, 37, . . . 60, 61), and special symbols (from 62, 63, 64 . . . . . . 90, 91).

These encryption and decryption processes are followed for all the communications to be made between different stakeholders in the TMIS.

7. A sample implementation of the communication security between the users, the sender and the receiver

This implementation proposes to improve the security enhancement of TMIS using ECC with iris biometrics. As mentioned above, the cryptographic keys of ECC are generated with help of eyeball IrisCodes for the sender and the receiver, except, the CS gets its PVK key based on a random integer.

A. Use of ECDHKX for generating and exchanging the keys like PBK, CSK.

The steps are given below:

Global public elements

(i) Both the sender and the receiver, choose values of ECC's parameters such that, a large prime digit, prm=8191, a=10, b=17, R(x, y)=(9, 3510).

The ECDHKX module evaluates the equation number 1, as per the values chosen for the ECC. The equation looks like,

$$y^2\ mod\ 8191 \;=\; (x^3 + 10 * x + 17)\ mod\ 8191 \tag{8}$$

where, prm>3, and the discriminant, $\Delta = 4 * 10^3 + 27 * 17^2 \neq 0$.

User, the SP - key generation

(ii) Private key of the SP: PVK_{sp} = 4680.

(ii) Public key of of the SP:
PBK_{sp}(6454, 7641) = 4680 * (9, 3510).

The CS - key generation

(i) Private key of the CS: $PVK_{cs} = 4818$.

(ii) Public key of of the CS: $PBK_{cs}(4329, 5845) = 4818 * (9, 3510)$.

Calculation of a CSK between users, the SP and the CS

(i) CSK for the SP:
$CSK_{spcs}(x, y)$
$= 4680 * (4329, 5845) = (820, 7879)$.

(i) CSK for the CS:
$CSK_{spcs}(x, y)$
$= 4818 * (6454, 7641) = (820, 7879)$.

B. The SP, a sender of a message to the CS

(i) The SP got some issues and he expresses the same as plain-message, **Patient: Hello Sir, I am not feeling well, have headache and stomach pain, kindly suggest some medicines for me.**

(ii) **Encoding process:** the encryption module at the SP side, do encoding of the plain-message into plain points based on the equation number 3, a sample encoded output is shown in the Fig. 5.

(iii) **Encryption process:** the generated plain points get encrypted with the help of the CS's PBK using the equation number 4, a sample cipher-message output is shown in the Fig. 6.

(iv) Once the cipher-message gets generated, and then, the same is sent to the CS.

C. The user, CS, a receiver of the cipher-message, sent by the SP

The CS receives a cipher-message from the SP, which is to be sent to the SP's MD for further diagnosis.

(i) **Decryption process:** the CS, decrypts the cipher-message of the SP with the help of decryption module of ECC using its own PVK. This module uses the equation number 5. Once decryption gets done successfully, the plain-points are generated, as shown in the Fig. 5.

(ii) **Decoding process:** the CS, decode the plain-points into plain-message as per equation number 7. Finally the plain-message is unconverted into the corresponding original message, which is the **Patient: Hello Sir, I am not feeling well, have headache and stomach pain, kindly suggest some medicines for me.**

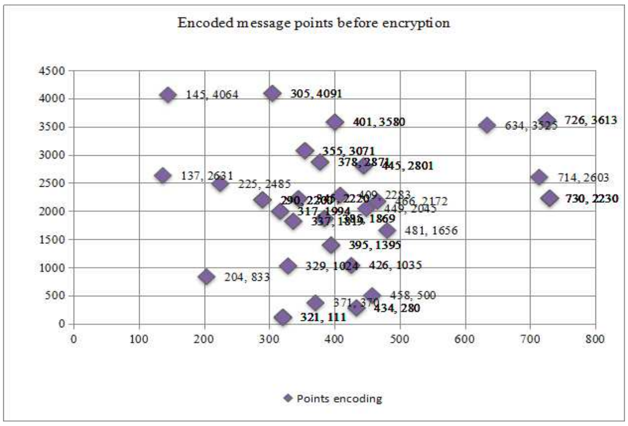


Figure 5. Encoded-points for mentioned plain-message

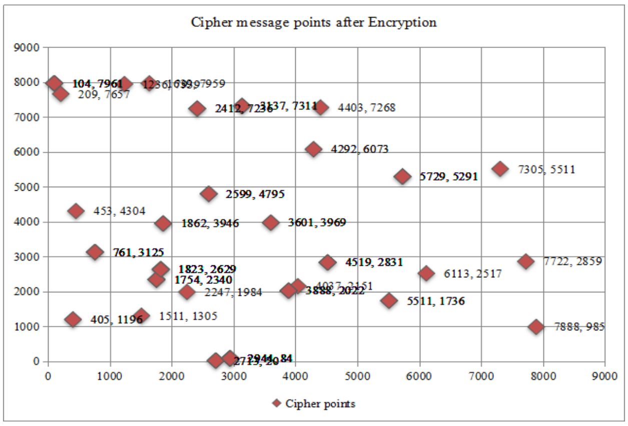
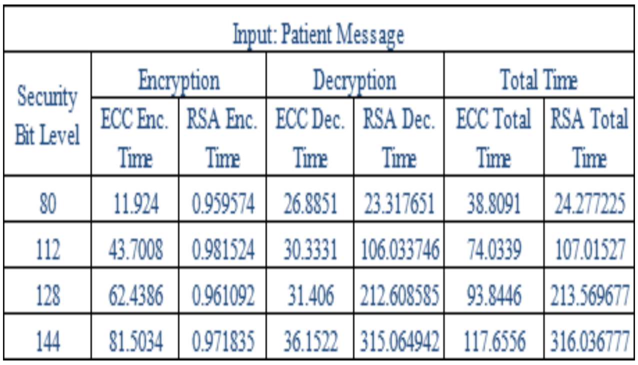


Figure 6. Cipher-points for above mentioned encoded-points

The CS also follows the same process for encrypting the plain-message of the SP and uploads the cipher-message to the MD. The MD gets the cipher-message and decrypts the same with his PVK using ECC. Once he understands the issues of the SP, he follows the same process of encrypting the response and uploads it to the CS. Then the CS decrypts back the plain-message sent by the MD. The CS encrypts this decrypted message with SP's PBK using ECC and sends it to the SP. In this way, the communication cycle is maintained.



Input: Patient Message						
Security Bit Level	Encryption		Decryption		Total Time	
	ECC Enc. Time	RSA Enc. Time	ECC Dec. Time	RSA Dec. Time	ECC Total Time	RSA Total Time
80	11.924	0.959574	26.8851	23.317651	38.8091	24.277225
112	43.7008	0.981524	30.3331	106.033746	74.0339	107.01527
128	62.4386	0.961092	31.406	212.608585	93.8446	213.569677
144	81.5034	0.971835	36.1522	315.064942	117.6556	316.036777

Figure 7. Time efficiency of ECC and RSA

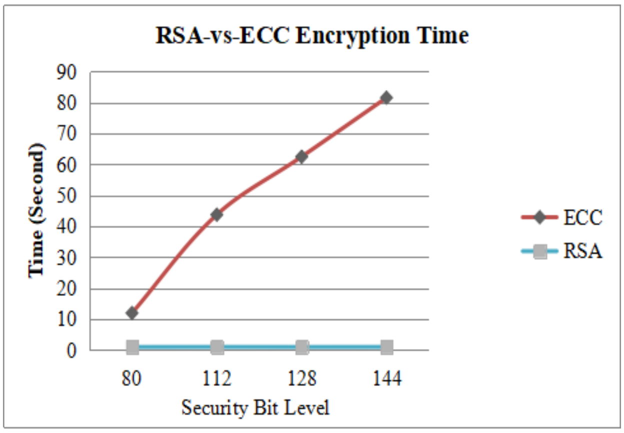


Figure 8. Encrytion time (in sec.) of ECC and RSA

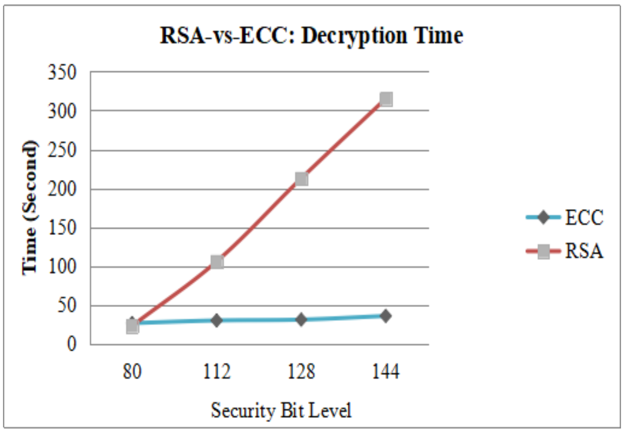


Figure 9. Decryption time (in sec.) of RSA and ECC

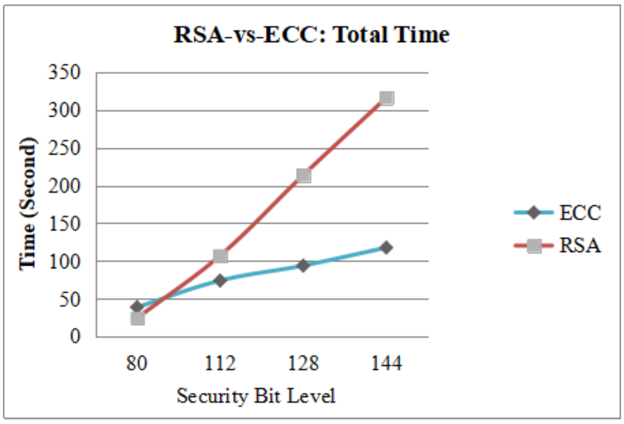


Figure 10. Total time (in sec.) of ECC and RSA

8. Security Analysis

Cloud computing is a very scalable and strong model for small and medium business enterprises, who do not want to spend too much on ever-growing and changing hardware and software systems. However, they still want the benefit of these changing nature of the ICT systems. Cloud computing helps such enterprises to concentrate on their business without worrying about the ICT related changing/damaging systems. Cloud computing provides services to these enterprises as per their usage basis. This proposed model focuses on usage of the PaaS of cloud computing. This paper implements ECC for cloud-based TMIS security, in which all PVKs of the stakeholders are generated from their eyeball irises, except the CS, which generates a value for its PVK from a random number generator. Once their PVKs are ready, they generate their PBKs using the ECC and calculate their CSKs also. There are mainly four stakeholders in this system, they are, the CS, the HP, the SP, and the MD. This paper allows them to securely exchange medical-related information. The CASIA Iris Image Database (CASIA-Iris) [3] is referred to download the iris samples, which are used to validate the proposed model. The iris biometric features provide the most accurate and speed system for identifying a person. This paper also implements RSA with similar type of data for analyzing the performance of it. The efficiency of ECC and RSA is shown in Fig. 7 and in Figs. 8-10. The simulation result shows that RSA is very powerful in encryption and slow in decryption whereas ECC is slow in encryption and very fast in decryption. Overall, as shown in Fig. 10, ECC is more efficient than RSA [23–25].

9. Conclusion

This article suggested a cloud-based TMIS security model, which provides secure online medical consultations between the SP and the MD via the CS. The HP acts as a trusted third party for providing healthcare services, which connects all other stakeholders to securely transmit healthcare information. The proposed model uses the eyeball irises of all stakeholders except the CS to generate their PVKs, and then they get their PBKs and CSKs on the basis of those PVKs. The CS uses a random number as its PVK of the desired length. The eyeball irises are very accurate biometric systems, which are formed at the early stage of the baby in the womb, and since then, they are unique always, unless or until there is no damage done to the irises. Sometimes these irises get damages, due to eye-related diseases. In such cases, the proposed model allows generating strong PVKs of the desired length based on a random number generator, so that the same can not be easily guessed by the attackers. Upon implementation of the proposed models using ECC and RSA, this paper concludes that the model based on the ECC offers greater protection with less key length than the model based on RSA. At the CS side, this model does not store plain-messages of the TMIS in its database except the bookmarks. The bookmarks help in matching the desired message and then the CS decrypts that cipher-message and sends it to the requester. Hence this model also provides security to the data-at-rest from insider-attacks or other related attacks.

References

[1] Bansal N, Mahto D, Yadav DK. Enhanced RSA Key Generation Modelling Using Fingerprint Biometric, 2018, Vol. 8(5): 3922- 3926, DOI 10.29042/2018-3922-3926. Helix.

[2] Barker E, Barker W, Burr W, Polk W, Smid M. Recommendation for key management part 1: General (revision 3). NIST special publication. 2012 Jul 10;800(57):1-47.

[3] CASIA Iris Image Database, http://biometrics.idealtest.org/

[4] Chang YJ, Zhang W, Chen T. Biometrics-based cryptographic key generation. In2004 IEEE International Conference on Multimedia and Expo (ICME)(IEEE Cat. No. 04TH8763) 2004 Jun 27 (Vol. 3, pp. 2203-2206). IEEE.

[5] Daugman J. New methods in iris recognition. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics). 2007 Sep 24;37(5):1167-75.

[6] Daugman J, Downing C. Epigenetic randomness, complexity and singularity of human iris patterns. Proceedings of the Royal Society of London. Series B: Biological Sciences. 2001 Aug 22;268(1477):1737-40.

[7] Diffie W, Hellman M. New directions in cryptography. IEEE transactions on Information Theory. 1976 Nov;22(6):644-54.

[8] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. InInternational conference on the theory and applications of cryptographic techniques 2004 May 2 (pp. 523-540). Springer, Berlin, Heidelberg.

[9] Hao F, Anderson R, Daugman J. Combining crypto with biometrics effectively. IEEE transactions on computers. 2006 Aug 7;55(9):1081-8.

[10] Hollingsworth KP, Bowyer KW, Flynn PJ. The best bits in an iris code. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2008 Aug 1;31(6):964-73.

[11] Jangiti S, Swathi G, Ravi L, Vijayakumar V, Subramaniyaswamy V. Automated question extraction and tagging for cloud-based online communities. International Journal of Web Based Communities. 2019;15(3):212-24.

[12] Jangiti S, Sriram VS, Logesh R. The role of cloud computing infrastructure elasticity in energy efficient management of datacenters. In2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) 2017 Sep 21 (pp. 758-763). IEEE.

[13] Jogi SP, Sharma BB. Methodology of iris image analysis for clinical diagnosis. In2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom) 2014 Nov 7 (pp. 235-240). IEEE.

[14] Kedar I, Ternullo JL, Weinrib CE, Kelleher KM, Brandling-Bennett H, Kvedar JC. Internet based consultations to transfer knowledge for patients requiring specialised care: retrospective case review. Bmj. 2003 Mar 29;326(7391):696-9.

[15] Koblitz N. Elliptic curve cryptosystems. Mathematics of computation. 1987;48(177):203-9.

[16] Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. Telematics and Informatics. 2019 May 1;38:100-17.

[17] Mahto D, Yadav DK. Network security using ECC with Biometric. InInternational Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness 2013 Jan 11 (pp. 842-853). Springer, Berlin, Heidelberg.

[18] Mahto D, Yadav DK. Enhancing security of one-time password using elliptic curve cryptography with biometrics for e-commerce applications. InProceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT) 2015 Feb 7 (pp. 1-6). IEEE.

[19] Mahto D, Yadav DK. Enhancing security of one-time password using elliptic curve cryptography with biometrics for e-commerce applications. InProceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT) 2015 Feb 7 (pp. 1-6). IEEE.

[20] Mahto D, Yadav DK. Security improvement of one-time password using crypto-biometric model. InProceedings of 3rd International Conference on Advanced Computing, Networking and Informatics 2016 (pp. 347-353). Springer, New Delhi.

[21] Mahto D, Yadav DK. One-time password communication security improvement using elliptic curve cryptography with iris biometric. International Journal of Applied Engineering Research. 2017;12(18):7105-14.

[22] Mahto D, Yadav DK. A Secure One-Time Password Authentication Scheme using Elliptic Curve Cryptography with Fingerprint Biometric. Journal of Engineering and Applied Sciences. 2017.

[23] Mahto D, Khan DA, Yadav DK. Security analysis of elliptic curve cryptography and RSA. InProceedings of the world congress on engineering 2016 Jun 29 (Vol. 1, pp. 419-422).

[24] Mahto D, Yadav DK. RSA and ECC: a comparative analysis. International journal of applied engineering

research. 2017 Oct;12(19):9053-61.

[25] Mahto D, Yadav DK. Performance Analysis of RSA and Elliptic Curve Cryptography. IJ Network Security. 2018 Jul 1;20(4):625-35.

[26] Mell P, Grance T. The NIST definition of cloud computing, 2011.

[27] Miller VS. Use of elliptic curves in cryptography. InConference on the theory and application of cryptographic techniques 1985 Aug 18 (pp. 417-426). Springer, Berlin, Heidelberg.

[28] Monrose F, Reiter MK, Li Q, Wetzel S. Cryptographic key generation from voice. InProceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001 2000 May 14 (pp. 202-213). IEEE.

[29] Ong LM, De Haes JC, Hoos AM, Lammes FB. Doctor-patient communication: a review of the literature. Social science & medicine. 1995 Apr 1;40(7):903-18.

[30] Rezaeibagha F, Mu Y. Practical and secure telemedicine systems for user mobility. Journal of biomedical informatics. 2018 Feb 1;78:24-32.

[31] Scott Kruse C, Karem P, Shifflett K, Vegi L, Ravi K, Brooks M. Evaluating barriers to adopting telemedicine worldwide: A systematic review. Journal of telemedicine and telecare. 2018 Jan;24(1):4-12.

[32] Singh J, Patel AK. An effective telemedicine security using wavelet based watermarking. In2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) 2016 Dec 15 (pp. 1-6). IEEE.

[33] Strehle EM, Shabde N. One hundred years of telemedicine: does this new technology have a place in paediatrics?. Archives of disease in childhood. 2006 Dec 1;91(12):956-9.

[34] Zhang L, Sun Z, Tan T, Hu S. Robust biometric key extraction based on iris cryptosystem. InInternational Conference on Biometrics 2009 Jun 2 (pp. 1060-1069). Springer, Berlin, Heidelberg.