IJCTA, 9(36), 2016, pp. 649-661

An Empirical Study on the Analysis of ECC implementation in BYOD Healthcare System

C.R. Bharathi*

Abstract : Medical records are the most important evidences for reducing the risk on re-hospitalization. Good patient care and health outcomes are often ensured with accurate, complete, clear and timely documentation of history of health problems and treatments undertaken including discharge summary, laboratory reports, prescribed medications and so on. But, the traditional method of documentation on hospitals is often based on paper or form of paper which is hard to maintain and may often be lost. The unavailability of patients past records may lead to negative consequences of wrong treatment. Moreover, the delay in attaining test reports and communication discrepancies among doctors, patients and nurses may also cause errors during the treatment process. Hence, in this paper an attempt is made to implement BYOD (Bring Your Own Device) in public health systemfor the successful process of medical records amongst the people involved in patient care. In addition, BYOD is at the risk of security breaches which cause problem of security and privacy of patient information to be addressed with. Hence, the paper also addresses the issues with BYOD security with an advanced Elliptic Curve Cryptography for secure transmission of data.

Keyword : ECC, Elgamal Key Agreement , Key Generation, Point Addition, Elliptic Curve, Key Exchange, BYOD.

1. INTRODUCTION

The rising of technology integration has significantly changed the way we communicate, access information and conduct of our routine activities, which results in the need of trends that could be adopted faster than ever. The increased use of wireless data transmission through electronic devices such as laptops, smart phones and tablets encounters the concept of Bring Your Own Device (BYOD) which allows the user to bring their own device to enhance data transmission for variety of purposes that increase productivity and user satisfaction. BYOD can be viewed as software program which can be facilitated as downloaded or installed software, native software in the device, or web application software.

The applications of BYOD are certainly promising in the areas including education, business, and medical care. Implementation of BYOD in public health centres holds immense potential to transform the medical sector, enable agility and encourage innovative ways of interacting with patients and medicos. The key is to approach BYOD holistically responding the patients requirements by considering the security on both sides. The aim of this project is to develop a recommender system for deploying secured BYOD in public health centres of Indian smart cities so as to maintain patients information not only with hospital server but also to transfer to patients device for future references. BYOD in healthcare brings lot of advantages for both patients and medicos point of view that includes:

- Faster delivery of medical reports (scan, X-Ray, Laboratory Results)
- Faster manipulation of patient recovery
- Ease of maintenance of patient summary and history

* Assoc. Prof., Dept. of ECE,Vel Tech University

The initiation on bringing BYOD in clinical transformation enables the opportunities for physicians in finding solutions to patient's problems irrespective of their physical locations. Access to real-time information of patient data ensures the physician to take effective decision on treatment. The digitization of clinical documentation benefits the patients to have an up-to-date medical history to better understand their condition and recovery. The faster transmission of laboratory reports saves time and reduces manual efforts. Though the advantages of implementing BYOD in medical transcriptions are extremely high, the issues related with the disclosure of patient details is also high. The confidentiality of patient medical records must be ensured with the secure transmission of data. Hence, in this paper, an elliptic curve cryptographic system is employed for securely keeping and sharing the medical data. The scope of this paper is defined as the following:

- To facilitate a well-defined User Authentication Management
- To offer a Secure Environment through User Security Management
- To Enhance a User Policy Management to manage user activities

2. REVIEW OF LITERATURE

Sansurooh et al [1]. have analyzed the current state of problems and challenges of implementing BYOD in healthcare environment where the privacy and security requirements are indeed essential. The authors have discussed the risks of security breaches that could be possible in healthcare centres and demonstrated that the issue is not merely technology based and needs a wider methodology that is comprehensive of technology that requires an expansive and social based perspective. The risks specific to healthcare apart from the capacity, workflow integration, and information sensitivity of mobile devices are device security and application security. The authors have claimed that the BYOD environment should be understood better for providing sufficient and acceptable protection.

Nykvist [2] have presented a case study into the use of mobile devices in a science unit, where the students bring their own devices to the classroom and use them in lectures, tutorials and workshops. The author has highlighted number of challenges faced by both students and teaching staff with the implementation of BYOD such as access to common software, data storage, retrieval and presentation, network infrastructure and familiarity with multiple platforms. The author has claimed that the changing nature of education through ICT caters to the needs of students.

Revenaugh et al. [3] have examined BYOD projects at IBM, CISCO, CITRIX and Intel and have integrated the analysis to build a success model for BYOD implementation. The authors have revealed the potential challenges for the organizations that decide to develop and implement BYOD policies which can be majorly categorized into five as security, mobile device management, device selection, training and support. The success model is built by combining organizational and individual impact over the employee satisfaction and contribution.

Afreen [4] has analyzed on how BYOD is helpful in higher education, as the personal devices used in educational institutions are increased. The author has suggested the most important factor that has to be considered over the deployment of BYOD at educational institutions is to define a distinct policy guideline model that suits the best for the institution. The author has suggested that the institutes have to subscribe various programming and should develop applications for teaching purposes with proper licensing.

Sangroha et al. [5] have introduced an approach to secure corporate data inside and outside the company premises when implementing BYOD strategy. The authors have proposed three different solutions such as MDM (Mobile Device Management), MAM (Mobile Application Management) and Encryption/Decryption techniques to monitor, secure and manage the devices that are registered with BYOD. The software's enrolls user personal devices by presenting the features of device registration, connection setup, user authentication and cryptography mechanisms, and keeps log of user history and digital certificates to monitor for violations.

3. METHODOLOGY

The transformation of patient medical records between the parties involved in healthcare system must be done in a secure manner. The concept of cryptography plays an inevitable role for protecting patient data. Hence, as a part of BYOD policy, the methodology of the proposed system consists of three major elements for the secure construction of BYOD in health care system such asformation of elliptic curve, Point Multiplication and modified elgamalkey agreement protocol.

3.1. Formation of Elliptic Curve Cryptography

1. Declare p, A, B
2. for ($x = 0$; $x < p$; x ++)
   compute $x^3 + Ax + B \bmod p$
3. for($y = 0$; $y < p$; y ++)
   compute $y^2 \bmod p$
4. extract the value of y where $y^2\% p = x$ and store the points x, y in two vectors X and Y respectively
5. plot and connect the x, y coordinates that forms the elliptic curve e over the geographical field G_p

Figure 1: Pseudo Code for Basic ECC setup

1. Let e be the elliptic curve formed by the equation $y^2 \bmod p = x^3 + Ax + B \bmod p$
2. Let $p_1(x_1, y_1)$ and $p_2(x_2, y_2)$ are two points on the curve where p_1 and $p_2 \neq \infty$
3. If($x_1 = x_2$) and ($y_1 \neq y_2$) then $p_1 + p_2 = \infty$
4. If($x_1 \neq x_2$) then
   $x_3 = m^2 - x_1 - x_2$
   $y_3 = m(x_1 - x_3) - y_1$ where $m = y_2 - y_1/x_2 - x_1$
5. If($p_1 = p_2$) and ($y_1 = 0$) then $p_1 + p_2 = \infty$
6. If($p_1 = p_2$) and ($y_1 \neq 0$) then
   $x_3 = m2 - 2x_1$
   $y_3 = m(x_1 - x_3) - y_1$
   Where $m = 3x_1^2 + A/2y_1$
   //Note: $p_1 + \infty = p1$

Figure 2: Psuedo Code for Point Addition

Elliptic Curve Cryptography is an asymmetric key cryptosystem which is formed from the notion of standard elliptic curve equation $y^2 = x^3 + Ax + B$ [6]. where x and y are the coordinates of the curve points and A and B denotes the constants. The curve is drawn over a geographical prime field G_p that reduces mod p in each step to obtain the points that forms an elliptic curve which is used then used to obtaina third point from a consecutive addition or doubling of two points. Moreover, a new point ∞ is also introduced and used in the group operation. Fig.1. presents the basic ECC stepup algorithm for constructing the elliptic curve. Once when the obtainment of curve points is over, the points are added with each other for constructing an addition table from where the keys are generated for EC Cryptography. There are certain criterions need to be followed for adding two points $p_1 + p_2 = p_3$, the algorithm presented in Fig. 2. explains the criterions for point addition [7]. As ECC is an asymmetric key cryptography, both sender and receiver have public and private keys. Point multiplication is yet another important calculation on ECC

which is helpful for multiplying the public key with the private key. Let $p_1(x_1, y_1)$ and s_k are the public and private keys of the sender then there need to the occurrence of point multiplication with s_k. (p_1). Point multiplication is the repetitive addition or doubling of a given point p_1 heading to s_k. Supposing if the private key of the sender is 8 means the point multiplication ($8 \times p_1$) would be $p_1 + p_1 = 2p_1$, $2p_1 + 2p_1 = 4p_1$, $4p_1 + 4p_1 = 8p_1$. The output of point multiplication results another point in the addition table.

1. Let Bp be the randomly chosen base point from the curve points
2. Set sender private key ski where $0 < sk_i < p$
3. Set receiver private key skj where $0 < sk_j < p$
4. Compute sender public key $pk_i = sk_i \times B_p$ and forward to receiver
5. Compute receiver public key $pk_j = sk_j \times B_p$ and forward to sender
6. Sender: receive pk_j, Compute K= $pk_j \times k_i$, and Encrypt message M with modulo inverse of M with K
7. Receiver: receive pk_i, compute K= $pk_i \times k_j$ and Decrypt message M with modulo inverse of K

Figure 3: The proposed Modified Elgamal Key Agreement Protocol

3.2. Modified Elgamal Encryption Protocol

Key agreement upon the sender and receiver is done by choosing a Base point B_p from the curve points which to be multiplied with their respective private keys *sk*. The resultant point serves as a public key *pk* for the opposite ends. The session key K is then computed by multiplying sk and *pk*. The sender encrypts the message M with modulo inverse of M with key K and the receiver decrypts the message M with modulo the inverse of K. In this work, a modified Elgamal encryption protocol is proposed to enhance the security of the data by adding an increased step of mod inverse of message M with key K.

4. EXPERIMENTATION

ECC implementation in BYOD is experimented by developing a web based BYOD healthcare system. The architecture of BYOD healthcare system is majorly categorized into three major divisions such as User Authentication Management, User Security Management and User Policy Management which are described in the subsequent section. Fig.4. depicts the proposed architecture of BYOD healthcare system.

4.1. User Authentication Management (UAM)

The distinct users of the BYOD healthcare system are recognized as physician, patient, health assistant, admin and diagnostician. User registration is mandatory for every user who takes part in the system. Users are given a username and a password at the successful completion of registration and their information is updated in the database. Every registered user is considered as an authorized user of the system. The role of UAM is to authenticate the login credentials of user by verifying the database on every login.

4.2. User Security Management (USM)

End- to- End security of BYOD healthcare system is ensured by USM. USM employs ECC for imparting high level security over the transmission and storage of user data along with modified Elagamal Key agreement protocol. Enforcement of USM starts on the submission of login credentials till the end of the session. USM generates session keys for being agreed upon the parties involved in the communication and also takes care of encryption/decryption of data using the keys. The illustration on ECC with modified Elgamal key agreement protocol is given below:

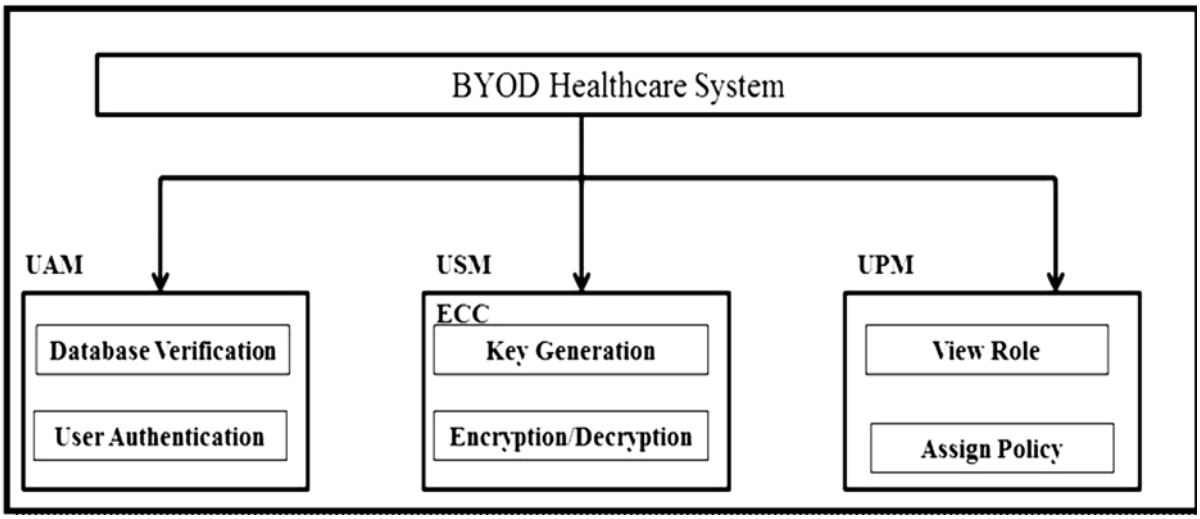


Figure 4: Proposed Architecture of BYOD Healthcare System

Consider an Elliptic curve E_{11} (1, 6) that originates the equation

$$y^2 = x^3 + x + 6 \quad (1)$$

To find the *x* and *y* coordinates of elliptic curve, replace the values of *x* from 0 to 10 on to equation (1) to extract y^2 and identify the possible values of y that could be paired with *x*.The curve points the forms an elliptic curve for the equation E_{11}(1,6) are (2,4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9), and ∞. An addition table is constructed using the curve points in the next step, for the purpose of simplifying the task of point multiplication. As it is discussed, point multiplication is achieved through repetitive addition of points.

Point Addition

$P_1 = (2, 4)$

and $P_2 = (3, 5).$

The addition of $P_1 + P_2 = Q$ is derived as follows:

$x_1 = 2,$

$y_1 = 4$

and $x_2 = 3,$

$y_2 = 5$

$$m = \frac{y_2 - y_1}{x_2 - x_1} = m = \frac{4-5}{3-2} = 1$$

$$x_3 = m^2 - x_1 - x_2 \Rightarrow 1^2 - 2 - 3 \Rightarrow 1 - 5 \Rightarrow -4\%\ 11 \Rightarrow 7$$

$$y_3 = m(x_1 - x_3) - y_1 \Rightarrow 1(2 - 7) - 4 \Rightarrow -5 \Rightarrow 4 \Rightarrow -9\%11 \Rightarrow 2$$

Hence, in E_{11}(1,6) the addition of points $P_1 + P_2$, (2,4) + (3,5) = (7,2)

Modified Elgamal Encryption :

Let p = 11, base point G = (3, 5) on curve $y^2 = x^3 + x + 6$

A chooses k_i = 10 and publishes 10G = (8, 8)

Encryption :

B wants to send a message M = 6 to A:

- B chooses a random *kj* = 5 and calculates 5*10G = (5,9), where he takes the key K = 5
- B sends A the pair(C1, C2),where
  - C1 = 5G = (2,7)
  - C2 = K*M^{-1} mod p = 5*2mod q = 10 mod 11=10

Decryption :

A calculates 10*(2, 7) = (5, 9) getting K = 5

A calculates the inverse of K^{-1} mod 11 = 9

A decrypts by inversing C2* K^{-1} mod 11 = 10*9 = 90 mod 11 = 2^{-1} = 6

4.3. User Policy Management (UPM)

Each recognized user in BYOD healthcare system has certain access policies with respect to their roles. The primary concern of UPM is to monitor and regularize the access policies without any violation discrepancies. The access polices of the recognized users are defined in table.1 which shows the activities that are assignedto the user role.

Table 1

BYOD Access Policy

S. No	*Role*	*Access Policy*
1.	Physician	• View Patient Description • View Appointment • Suggest Diagnostics Tests • View Diagnostics Report • Suggest Medication • Direct Follow-ups • Write summary
2.	Patient	• Register problem • Download diagnostic test reports • Download medication • Download summary
3.	Health Assistants	• View Medication • View Follow-up
4.	Diagnostician	• View tests • Submit tests

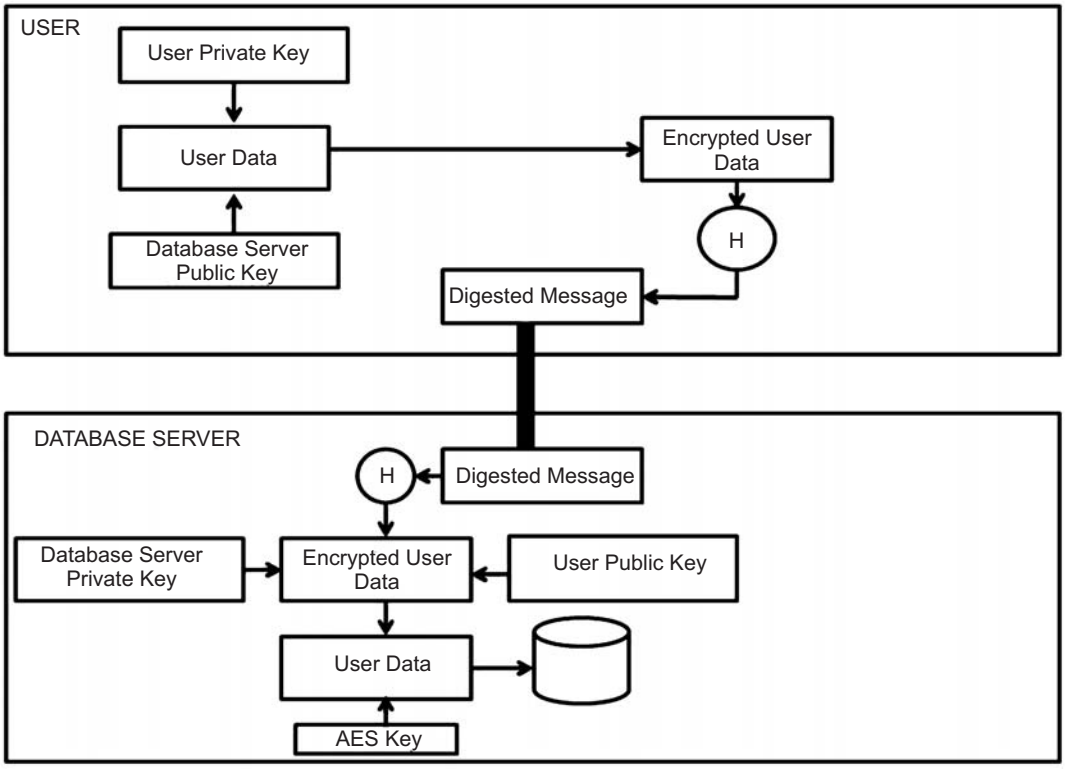


Figure 5: ECC-AES Collaboration on Data Storage

One of the significant contributions of this paper is the implementation of ECC with modified Elagamal key agreement protocol for securing the BYOD healthcare system. ECC is alone sufficient for the communication between clients, but offers only partial support on data storage as the key for storing and retrieving data in the database must be same. To overcome this issue, an additional AES symmetric key algorithm is developed for performing database operations. Moreover, SHA 1(Secure Hash Algorithm 1) a message digestion algorithm is applied to ensure the integrity of user data from source to destination. Fig.5. depicts the exchange of data between user and database server.

5. RESULTS AND DISCUSSION

Fig. 6.*a*. depicts the web portal of BYOD healthcare system that consists the entry point of user to get access to the system. As the roles of the user are distinct the inputting information on the registration are also distinct. Hence, the registration form of the system is designed to be variedbetween user categories. Fig.6.*b*. denotes the registration form of physician which requires the information such as password, name, gender, date of birth, mail id, mobile number, qualification, Specialization and years of experience. In contrast, the information that are necessitated for the patient are password, name, gender, date of birth, mail id, phone number, problem description and Consultant Physician as shown in Fig. 6.*c*. The system is made to generate automatic userid's according to the role of user.

Only the registered user can login to the system. Unlike registration, the login form for all users is same and expects the user to enter their userid and password. USM on the client machine encrypts the login credentials of the user and forwards them to UAM. UAM authenticates the credibility of the user by decrypting them with help of USM on the server. Once when the authentication of the user is successfully verified, UAM transfer the control to UPM, Else an 'invalid user' error message is thrown. Fig. 7.*a*. shows the login form of the user and the result produced by UAM is displayed in Fig.7.*b*.

Figure 6 : (*a*) BYOD Gateway **(*b*) Registration - Physician** **(*c*) Registration - Patient**

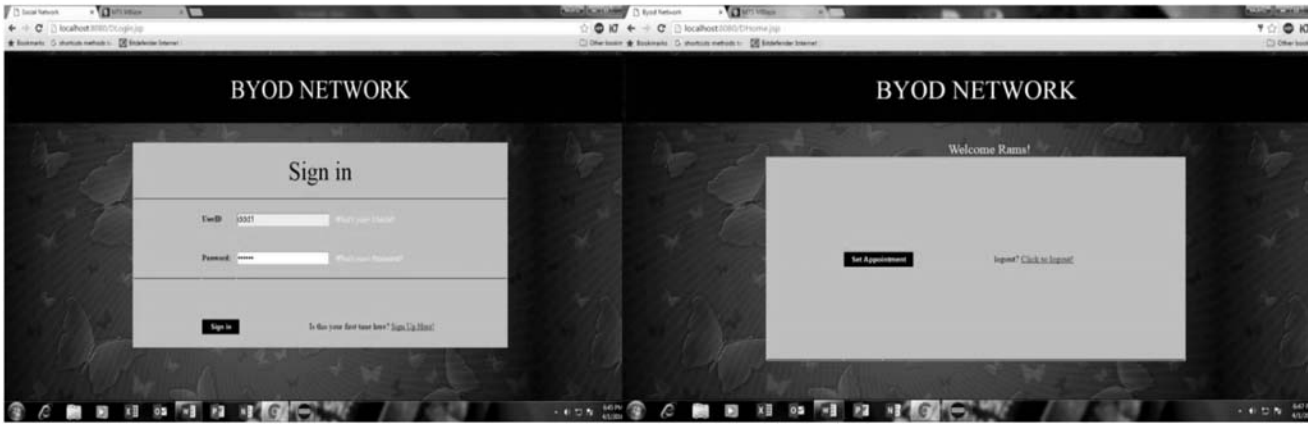
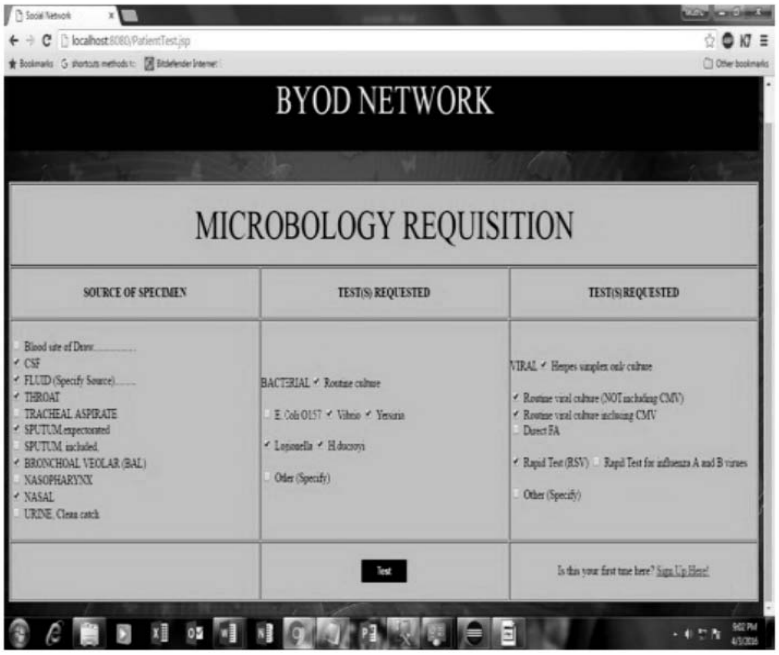


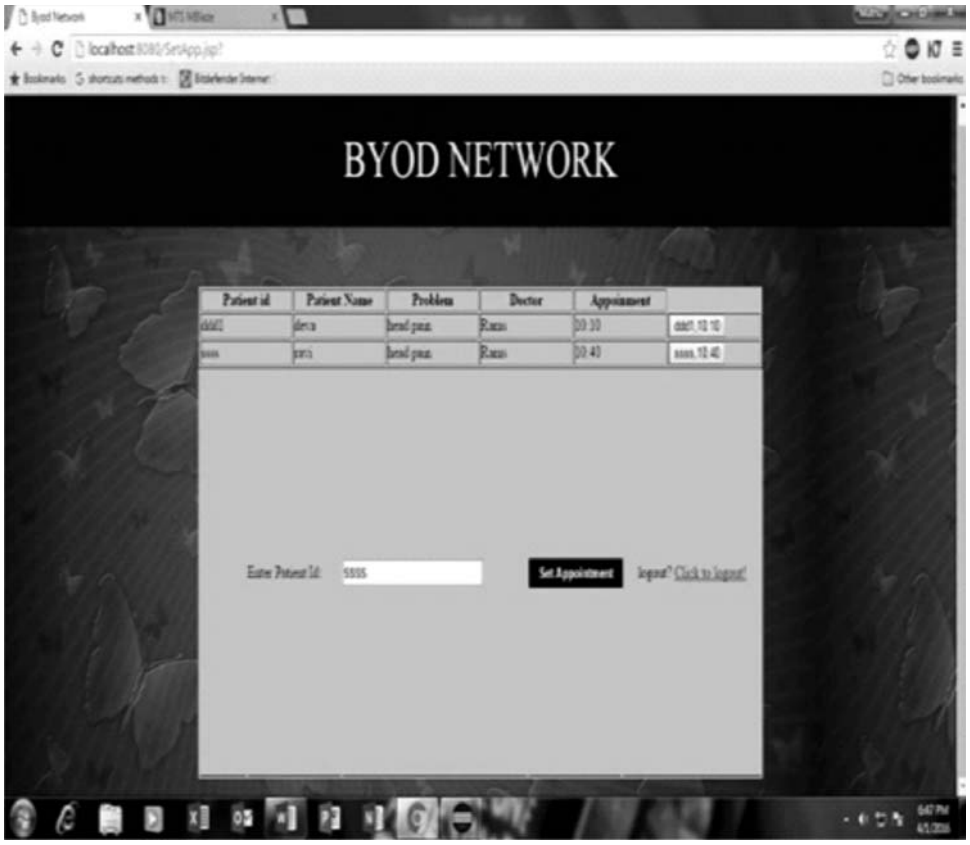
Figure 7. (*a*) User Login **(*b*) User Authentication**

UPM holds an access policy table that contains a set of précised activities of the user according to their role. When the user is authenticated, UPM identifies the role of the user and fetches the access policy that is defined for the user by displaying them on the user screen. It then distributes the activity pages that arerequested by the user without any violation caused on the access policy. Fig.8.*a*. represents access policy of the role 'physician' and the corresponding access pages. The access policies of the physician are view appointment, view patient description, suggest lab tests, view lab reports, write medication, write follow-ups and finally write patient summary. Fig.8.*c*. denotes one of the activity pages of physician, view appointment that consists of patient id, patient name, problem description, tentative appointment schedule of the patients. Fig.8.*b*. denotes a yet another activity pages of the physician such as suggest lab test, which describes the name of the tests to be conducted on the patient for effective treatment.

Figure 8 : (*a*) Access Policy-Physician



(*b*) Suggest Lab Tests Activity - Physician



(*c*) View Appointment Activity - Physician

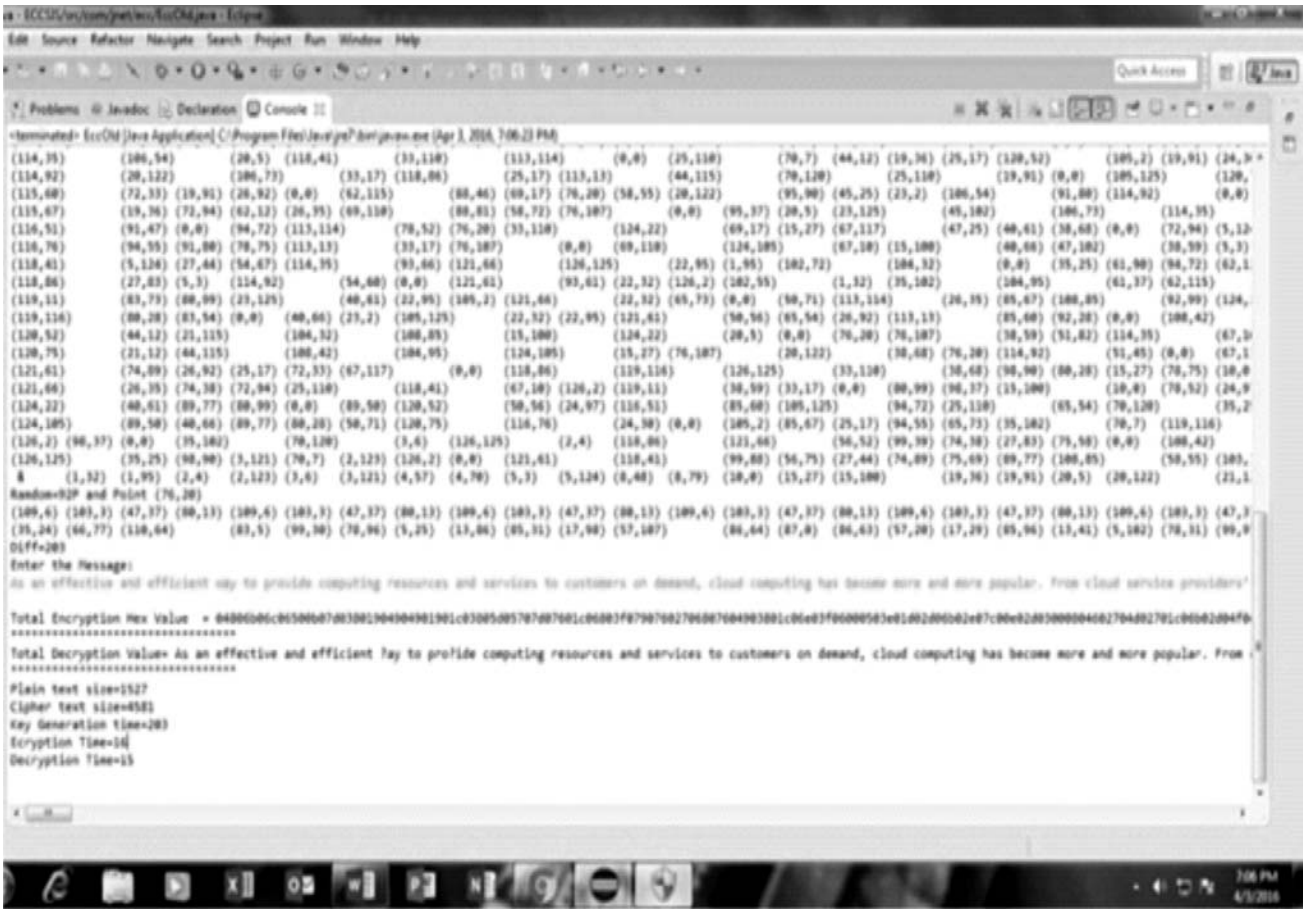
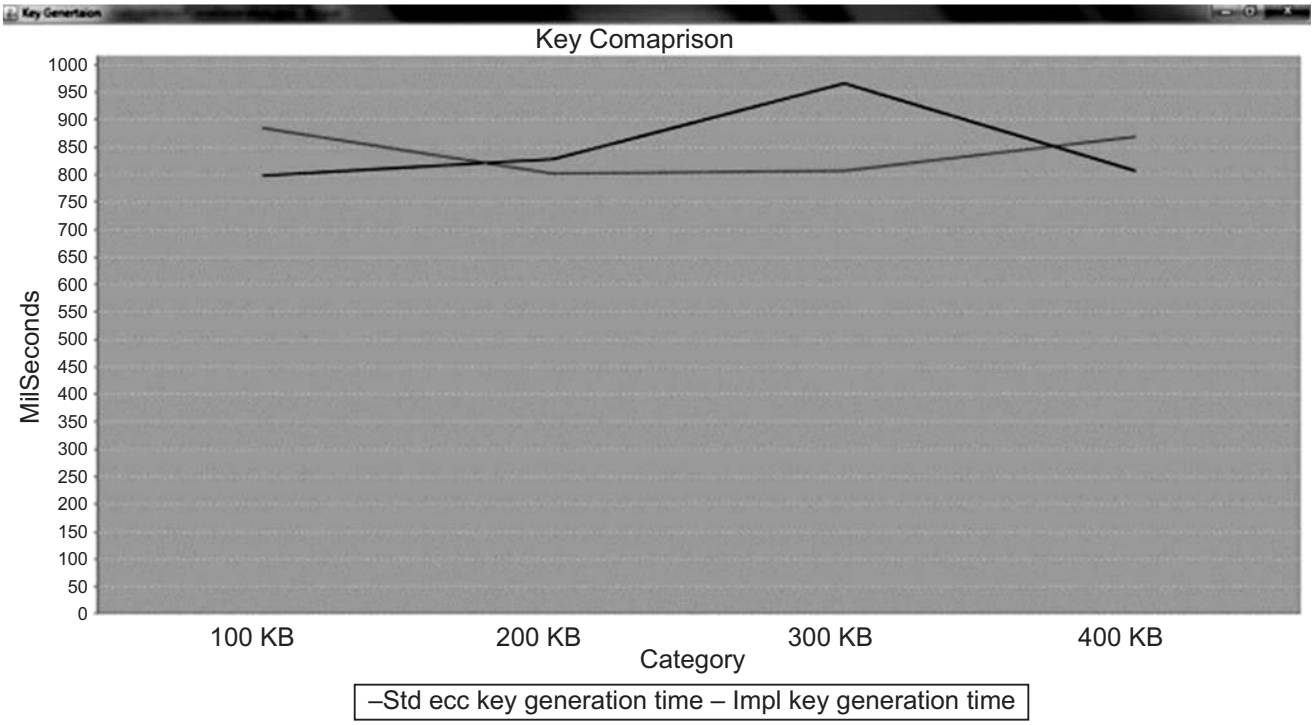
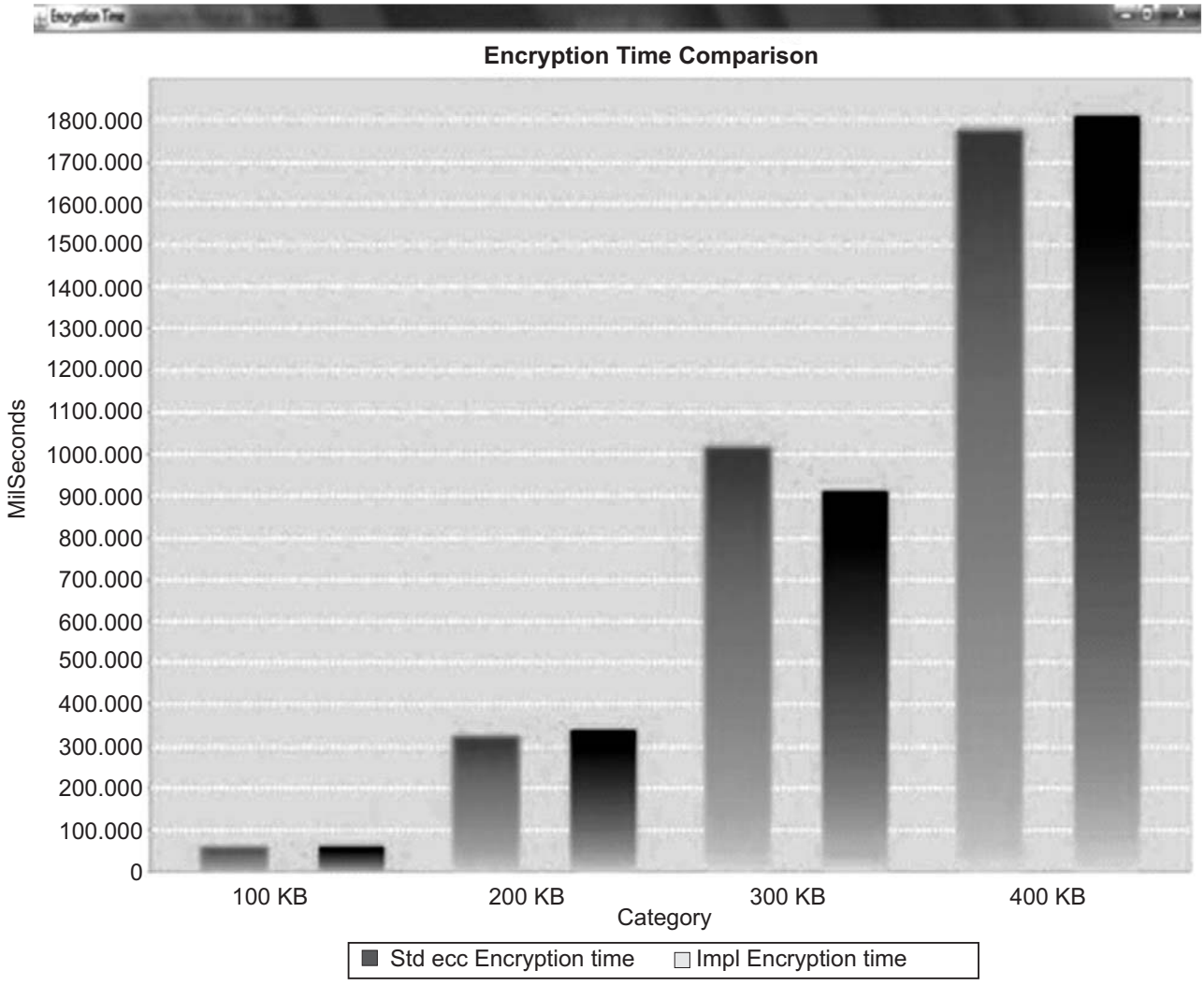


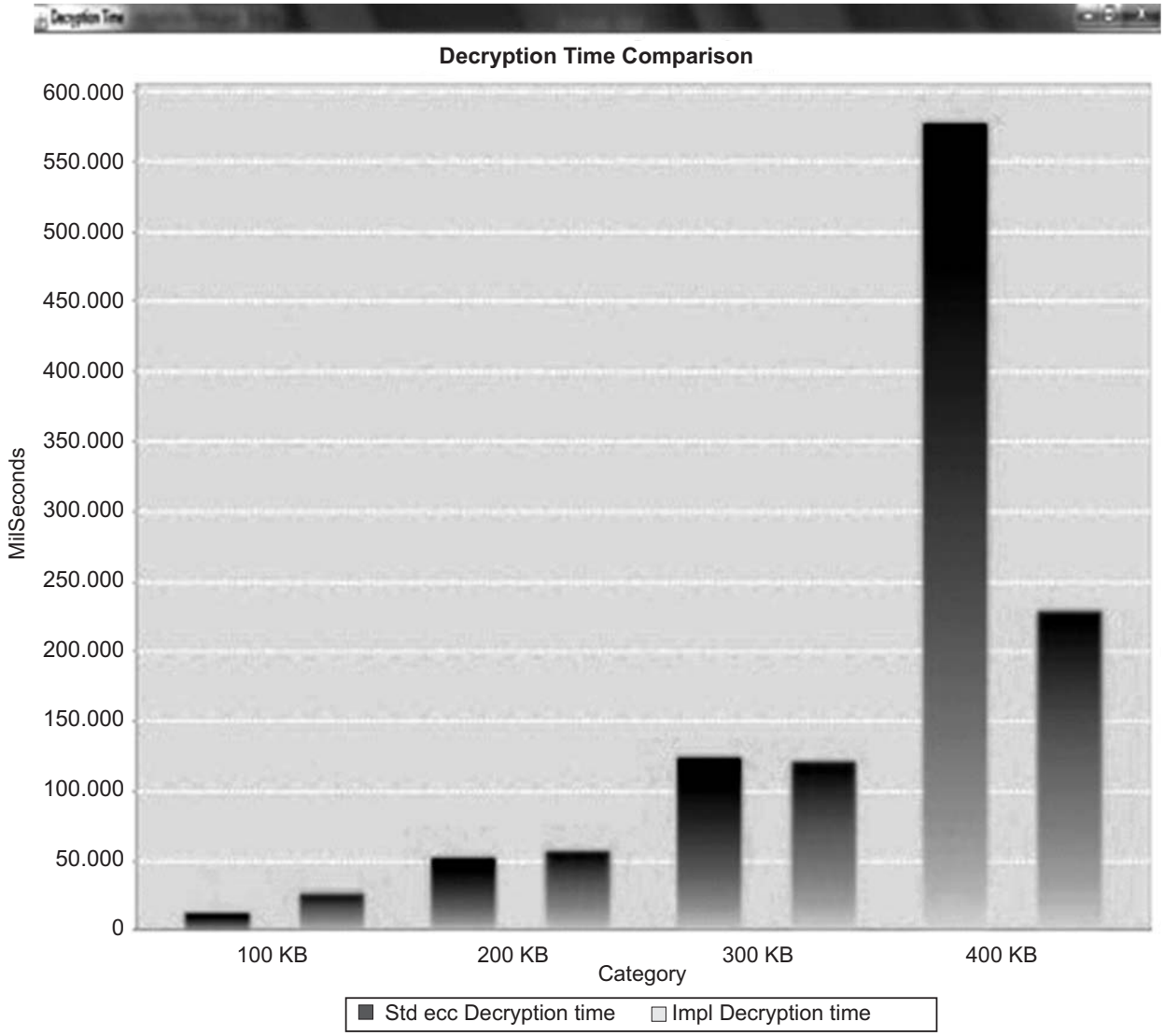
Figure 9: (*a*) Generation of Key Points



(*b*) Key Generation Time Comparison Modified Elgamal Vs Standard Elgamal

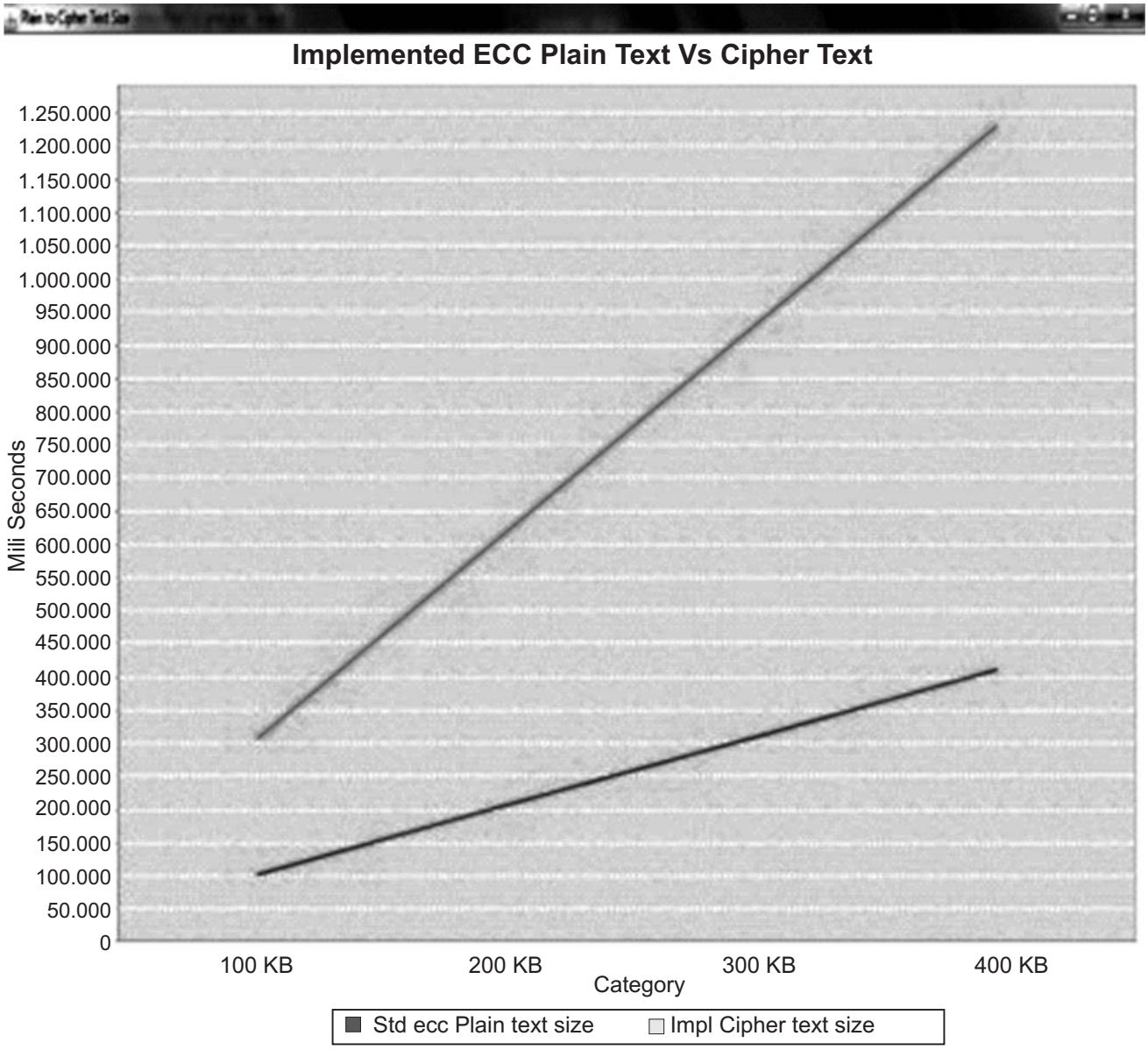


(*c*) Encryption Time Comparison



(*d*) Decryption Time Comparison

The crucial segment of this paper is the implementation of ECC with modified Elgamal key agreement protocol. The performance of the ECC with modified Elgamal key agreement protocol is compared with ECC with standard Elgamalkey agreement protocol based on the traditional cryptography validity criterions such askey generation time, encryption/decryption time, plain text size and cipher text size. The more the time taken for encryption and decryption is the more the security of the system is. As the proposed method implements modulo inverse operation on both stages of encryption and decryption, it offers additional security on user data and protects users from different types of network threats such as man-in the- middle, eaves dropping and so on. The cipher text of the improved Elgamal encryption doubles the size of the plain text over encryption which initiates a positive sign on the proposed work. In addition, the key generation time of both the modified Elgamal and standard Elgamal means the same as it is generated from the notion of ECC. But, there is a variation between encryption and decryption time because the underlying the mechanism of proposed work adds an additional step of inversing the message takes an additional time for both encryption. The comparative study of Modified and standard Elgamal over five transactions has been captured and presented in Fig.9.*a*.shows the ECC key generation table, Fig.9.*b*.represents the key generation of time, Fig.9.*c*. denotes the encryption time, Fig.9.*d*.depicts the key generation and Fig.9.*e*. portrays the plain text and cipher text comparison.



(*e*) Plain Text Vs. Cipher Text Comparison

Table 2

Comparative Analysis of ECC with Modified ElgamalVs. Standard Elgamal

Metric	*ModifiedElgamal*	*Standard Elgamal*
Plain Text Size	1527	1320
Cipher Text Size	4581	2972
Key Generation Time	203	184
Encryption Time (in sec)	16	12
Decryption Time (in sec)	15	10

Table. 2. describes a sample comparative study with one simple transaction of data between the clients and proves the ecstasy of modified Elgamal key agreement protocol by satisfying the requirements of cryptographic metrics.

6. CONCLUSION

Most of the computer researches are carried out on majority of topics related to medical sciences as the computer based techniques are more prevalent in analyzing biological concepts. This research project is a computerized solution for medical oriented issues that brings in contact of people of computer and medical professionals. Moreover, the devices that are to be used in this project are the personal devices of the participants which are most convenient for ease of use. The interdisciplinary nature of this research is valuable not only for immediate benefits of the project but also for keeping the door opened to diverse extension of medical claim, insurance and so on. Moreover the issues related with BYOD security can be addressed with the proposed ECC with modified Elgamal encryption as the results have proven an enhanced security of BYOD than the standard techniques.

7. REFERENCES

1. Sansurooh, K. and Williams, P.A., 2014. BYOD in ehealth: Herding cats and stable doors, or a catastrophe waiting to happen?.
2. Nykvist, S.S., 2012. The trials and tribulations of a BYOD science classroom. In Proceedings of the 2nd International STEM in Education Conference (pp. 331-334). Beijing Normal University.
3. Lance, D. and Schweigert, M.E., 2013. BYOD: Moving toward a More Mobile and Productive Workforce.
4. Published Paper in the title of " Automatic detection of lung cancer nodules by employing intelligent fuzzy cmeans and support vector machine ", Biomedical Research
5. Published Paper in the title of "Cognitive Computational Semantic for high resolution image interpretation using artificial neural network", Biomedical Research.