Design and Development of Framework to Secure Healthcare Data

Anita Chaudhari[1]; Mayank Nagora[2], Mayur Rane[3], Murtuza Hafizjee[4], Jagruti Goswami [5]

[1,2,3,4,5]John College of Engineering and Management, Mumbai, India,

ABSTRACT

In today’s world security in cloud computing technology is a developing area. For cloud computing technology services, it is a matter to discuss. Encryption of data is required before it is kept in reserve on the cloud. ECC algorithm is being used instead of known and popularized RSA for data encryption for providing security services. Because of its additional benefits with regards to less memory usage, smaller key size of encrypted data and lower central processing unit time. We had proposed framework to secure patients data. Main drawback of existing system is Patient had to carry reports in hard copy, so whatever prescriptions given by doctors will be encrypted and will be uploaded on cloud . If any one wants to download specific patients report , they should have secret key , so only authentic user can access record.

Keywords: Elliptic Curve Cryptography, Rivest-Shamir Adleman**.**

1.Introduction

These days protecting not only the documents and the text files, but also pictures, audio files, video files and many more on hard disk are now moderately ending due to variation of cloud. To grasp all of the digital data the virtual repository is complete with the necessity for added repository. Here as stated by the needs of the user the data processing center, in the context, visualize the reference. Then the client can utilize it to reserve document and then display even as repository. Actually, the method might extent over different hosts. A web-based user interface is used for accessing cloud storage services. A single virtual cloud storage system is being build by cloud storage architectures. The following are the risks when data is stored on the cloud:

1.The chance of illegal entry to the data is increased when the allocated data is stored at the multiple places.

2. Drastically increase in the count of people with access of memory.

3. The amount of grid gets expanded above that the statistics progress. Data reserved on cloud requires a WAN connection to link them both LAN or SAN.

4.Possibility of distributing of storage and networks with more users to access the data.

The majority of the systems utilizes a union of methods in order to protect document, along with:

1. Encrypted code means the procedure in which the data or the useful documents is translated into top secret cipher which protects the original detail of the document.

2. Validation processes, is to prove that something is based on facts.

3. Basically authorization, is a procedure in which the users are permitted or refused with access to different types of network plans based on their specification. We can also say that, as the owner of our house, we have entire rights to our properties resources and we can also permit other people the right to access it.

What is ECC?

ECC is Elliptic Curve Cryptography. It follows the concept of asymmetric key cryptosystem which means in this we use public and private key concept same as we use in RSA and non ECC algorithms. The most important advantage of this is that it provides equal security with smaller key size for example if RSA uses 3072 bits, same security is being provided by ECC within 256 bits. It makes use of Elliptic curves. These are defined by some cubical functions. RSA and Diffie – Hellman are the most public-key encryption methods used as coexistence technology. Thus in this project, we have two structure - Doctors and Patient. Doctors can also open patients' files as pdf and view them. Patients' data can be downloaded from the portal as pdf and also the data can be shared with patients' from the portal itself. Doctors can send code to patients which can be used to open files. Once the code is sent it displays the code sent successfully. The patient receives file on mails where the key is attached with a file which can be used to open the encrypted file.

2.Material and Methods

2.1 Review of Literature

In this paper, the purpose was to display the amount of time taken for generating signatures and also ECC has minor and not so much effective than RSA[4]. In this paper, survey of ECC algorithm in operation by inquiring into its consumption in SSH, TLS[5]. Provides a clear understanding between ECC and RSA based on the advantages and applications[6]. Provides study the safety related data of end customers in server [7].Provides how to secure data in cloud computing system [8].

Discussed about DNA computing which is used to improve the safety of ECC[9].ECC is fast and powerful cryptography system based on its performance and various applications[10].Designed system was not totally based on keys and in addition To same unencrypted text it resulted in separate fixed key[11]. From the review, we compared both ECC and RSA and hence we came to a conclusion that ECC provides very less expenses above RSA[12]. Symmetric algorithms are more quicker and secured than asymmetric algorithm [13]. Safety methods has reduced the ordinary method on the basis of space values and PSNR values. ECC is significant option for providing data safety[14-15]. Whatever useful information which is being uploaded on the cloud needs to be protected[16].

2.2 Key Geration of ECC

It is Asymmetric (Public &Private) key Cryptosystem. It is equal security as RSA.ECC makes use size of elliptic curve. ECC is small size than RSA.Elliptic curves are defined by some mathematical function .

$y^2 = x^3 +ax+b$

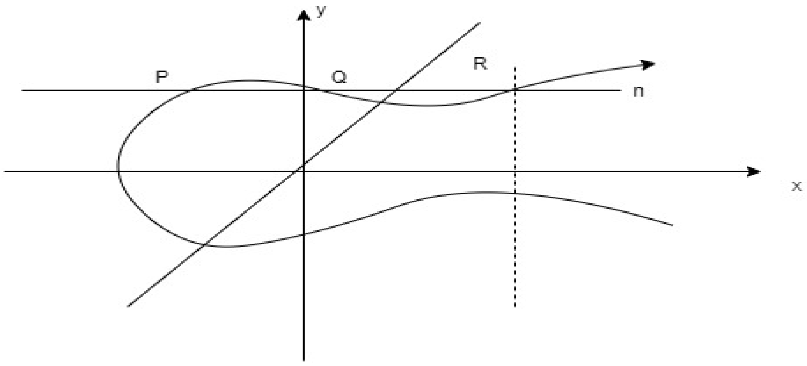


Figure 1.ECC Algorithm

It is very simple for example, if we calculate from A to B, then we cannot calculate from B to A, as it will be extremely difficult. So, this is what trapdoor function says that it is not difficult to calculate or determine in a single direction and thus it is extremely difficult to determine in finding its inverse.

Let E_p (a, b) be the elliptic curve
Comsider the equation
Q $=K_p$
K_p ---> Q (Q is point on curve)
Q,P ---> K (Discrete log limit m problem for Elliptic curve)

Key Exchange
Let see ECC key exchange between two parties i.e. sender and the receiver.
We have two global public Elements, G and E_q (a, b)
E_q (a, b) : This is the elliptic curve along with variables a , b and q, where a , b are the constants and q can either be prime number or an integer of the form 2^m .
G : This is the point which lies on the curve.

Key Genration
Now we will do key generation of user A:
Firstly we select private key of n_A ,
Where ,value of (n_A< n)
Then we need to calculate public key $P_{A,}$
Where, $P_A = n_A * G$
Here, n_A is the private key and G is the generator point.
Similarly, we do key generation of user B:
Firstly, we assume private key of $n_{B\ ,}$
Where, value of (n_B< n)
Afterwards, we need to generate public key of $P_{B\ ,}$
Where , $P_B = n_B * G$
Now we will do key exchange simply,
So, user A needs to calculate a secret key.
Let us say , $K= n_A * P_B$
Similarly, user B needs to calculate a secret key.
Let us say, $K= n_B * P_A$
Thus, the values of both K will be same and hence the key exchange procedure is successfully executed.

ECC Encryption
Suppose, the message be M.
Firstly we encode M the message into a coordinate format which lies over an elliptic curve.
And let the point be named as Pm.
Hence we can say that the point is encrypted successfully.
For simply encryption we are going to choose any positive numeric called K.
And the coded message generated be as,
$C_m = K_G - P_m + KP_B$
Here, for encryption, public key of B is used and thus, this generated point will be sent to the receiver.

ECC Decryption
Now for decryption,
Simply, it multiplies 1st point in the pair with receivers secret key as,
$K_G * Pn_B$
Where private key of B is used for decryption.
And after decrypting it, we will subtract it from 2nd point in the pair as,
Pm $+KP_B - (K_G * n_B)$
But we also know from previous equation that,
$P_B = n_B * G$
So, $P_m + KP_B - KP_B$
Simply we get the original point as $P_{m.}$ Thus, receiver gets the same point.

3.Methodology

Our research mainly focuses on securing patient data and reduces doctors time in writing presriptions.

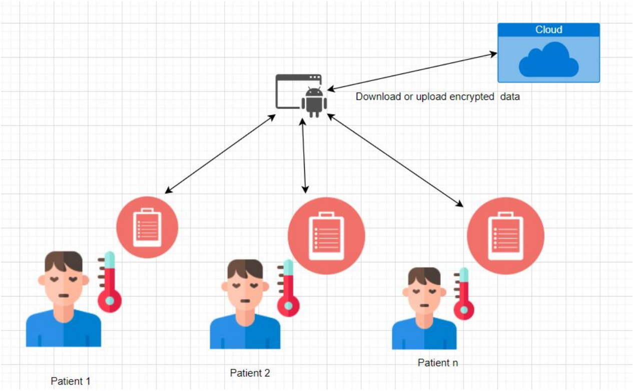


Figure 2. Proposed Methodology

The proposed system of implementing ECC to improve security in cloud storage determines that multiple patients needs to enter the key received with file on mail and hence the downloaded file can be viewed by the patients.

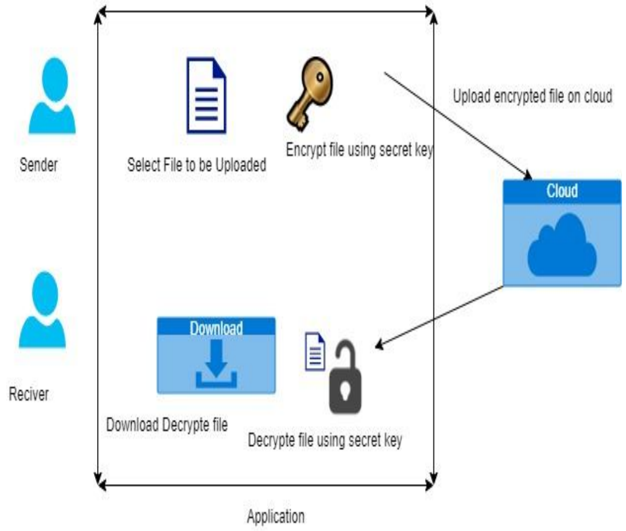

Sender
Select File to be Uploaded
Encrypt file using secret key
Upload encrypted file on cloud
Cloud
Reciver
Download
Download Decrypte file
Decrypte file using secret key
Application

Figure 3. Processing of Application

The process shows that the sender or we can say doctors send the useful information on mail where a secret key is attached with file which can be used to open the file.On the receiver’s end, once the key is entered file can be viewed.

4.Assumptions

The key size is calculated in bits is then converted into bytes.

Here, 8 Bit = 1 Byte

For encrypted code size we need :

[[size of the key / 8] – 11]

For decrypted code size we need :

[size of the key / 8]

Following are the size of the key along with the similar safety measures for Elliptic curve Cryptography and Rivest, Shamir, Adleman :

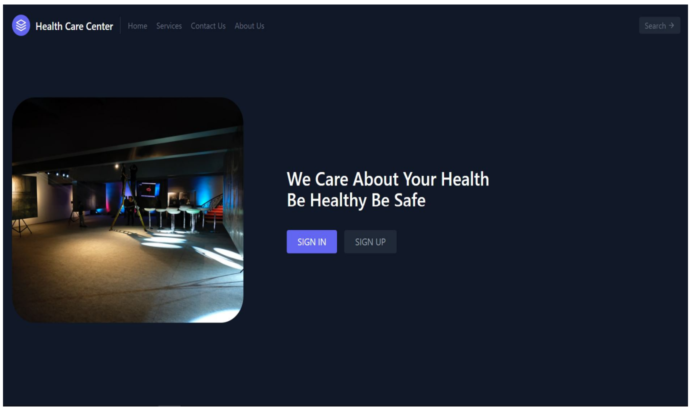
Table No.1 [9]

Elliptic curve Cryptography	Rivest, Shamir, Adleman
160 bits	1024 bits
224 bits	2048 bits
256 bits	3072 bits
384 bits	7680 bits
512 bits	15360 bits

Constant: In comparison to execution and property of the RSA and ECC encryption algorithms, the parameters used here are as follows:

1. Generation of key time
2. Encrypted of key time
3. Decrypted of key time

5.Result and Discussion



We Care About Your Health
Be Healthy Be Safe

Figure 4. Home Page

The following is a health care portal this first result displays the signup page for doctors where they can sign up and register themselves. Once the doctor clicks on the sign-up, the registration form pops up where a doctor can fill in his/her personal details. Once registration is done doctor can use his/ her login credentials and login to the website.

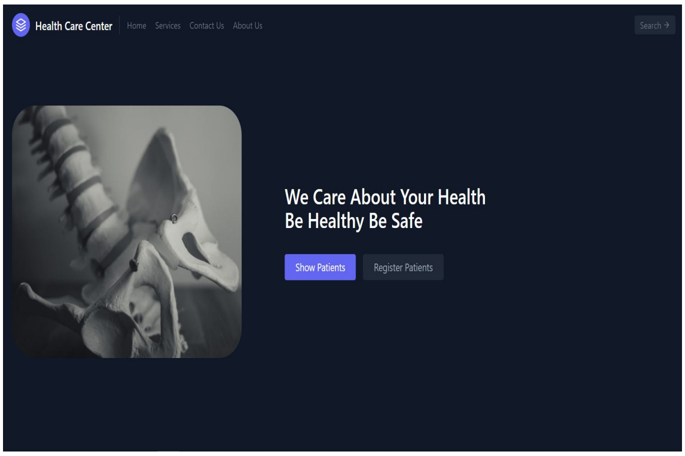
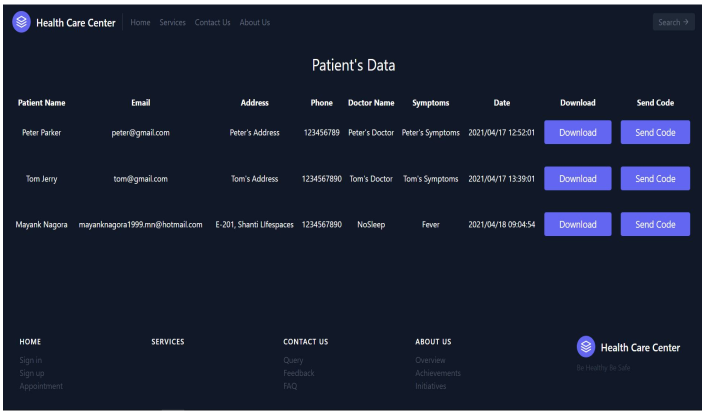


Figure 5. Details

On the home page, it displays two buttons, shows patients and add patients. When show patients are clicked it displays the patients which the doctor has consulted to date. If add patients are clicked it opens up with patient register form where every required detail for consultation of patient is filled by a doctor. Doctors can also open patients' files as pdf and view them.

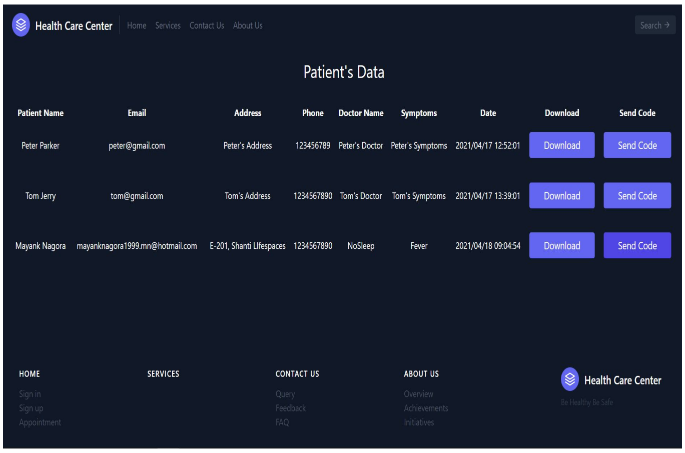


Patient's Data

Patient Name	Email	Address	Phone	Doctor Name	Symptoms	Date	Download	Send Code
Peter Parker	peter@gmail.com	Peter's Address	123456789	Peter's Doctor	Peter's Symptoms	2021/04/17 12:52:01	Download	Send Code
Tom Jerry	tom@gmail.com	Tom's Address	1234567890	Tom's Doctor	Tom's Symptoms	2021/04/17 13:39:01	Download	Send Code
Mayank Nagora	mayanknagora1999.mn@hotmail.com	E-201, Shanti LIfespaces	1234567890	NoSleep	Fever	2021/04/18 09:04:54	Download	Send Code

Figure 6. Patient Data

PDF can be opened by choosing the pdf file and then it can be viewed.Patients' data can be downloaded from the portal as pdf and also the data can be shared with patients' from the portal itself. Once the file is completely downloaded it displays the file downloaded successfully.

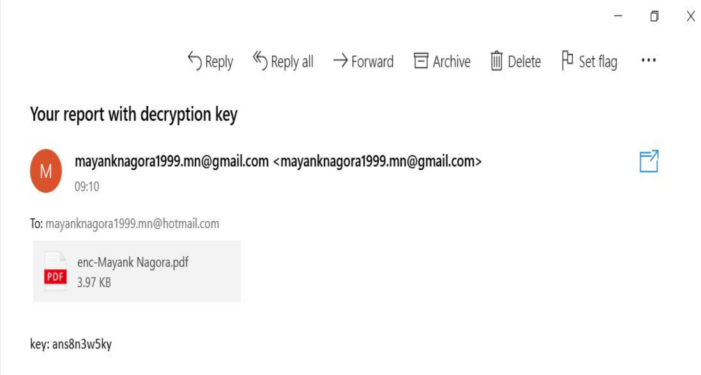


Patient's Data

Patient Name	Email	Address	Phone	Doctor Name	Symptoms	Date	Download	Send Code
Peter Parker	peter@gmail.com	Peter's Address	123456789	Peter's Doctor	Peter's Symptoms	2021/04/17 12:52:01	Download	Send Code
Tom Jerry	tom@gmail.com	Tom's Address	1234567890	Tom's Doctor	Tom's Symptoms	2021/04/17 13:39:01	Download	Send Code
Mayank Nagora	mayanknagora1999.mn@hotmail.com	E-201, Shanti Lifespaces	1234567890	NoSleep	Fever	2021/04/18 09:04:54	Download	Send Code

Figure 7. Patient Data

Doctors can send code to patients which can be used to open files. Once the code is sent it displays the code sent successfully. The patient receives file on mails where the key is attached with a file which can be used to open the encrypted file.



Your report with decryption key

mayanknagora1999.mn@gmail.com <mayanknagora1999.mn@gmail.com>

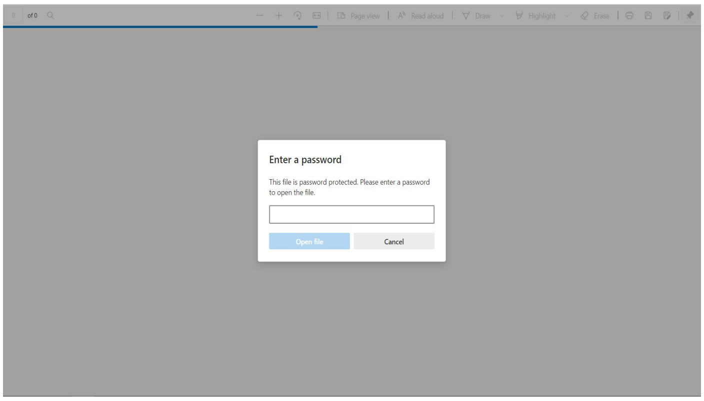
09:10

To: mayanknagora1999.mn@hotmail.com

enc-Mayank Nagora.pdf
3.97 KB

key: ans8n3w5ky

Figure 8. Decrypted Data1



Enter a password

This file is password protected. Please enter a password to open the file.

Figure 9. Decrypted Data2

The Patient receives file on mails where the key is attached with a file which can be used to open the encrypted file. Before downloading patient needs to enter the key received with a file in the mail. Once the key is entered a file can be downloaded. Once file is downloaded it can be viewed here.

7.Conclusion

Elliptic Curve Cryptography is a easy and faster way to get secure communication. Elliptic Curve Cryptography is much faster than RSA algorithm. ECC provides greater security than RSA. ECC future is much brighter than today's technology. The ECC has smaller key sizes and has lesser complexness as today's technology. The most important advantage of ECC is that it provides equal security with smaller key size. However, in the upcoming years cryptography will be figured on the basis of ECC because of the fact that RSA is probably impractical and unprofitable in the course of time.

8.Reference

[1] Elliptic curve cryptography, https://en.wikipedia.org/wiki/Elliptic_curve_crpography

[2] RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm)

[3]JavaTM Cryptography Extension (JCE), Reference Guide. http://docs.oracle.com/javase/1.5.0/docs/guide/security/jce/JCERefGuide.html

[4]Haodong Wang,Qun li,"Efficient Implementation of Public key cryptosystem on mote sensor",Department of Computer Science, College of William and mary.

[5]Joppe W.Bos,Alex Halderman,Nadia Heniger,Jonathan Moore,"Elliptic curve cryptography in practice",Microsoft Research,University of Michigan.

[6]Sharad kumar varma,Dr.D B Ojha,"A descussion onElliptic curve cryptography and Its Application",Research Scholer,Mewar University.

[7]Jai Cui, Yudong Qi,Bei Hong,Qinghua Chen,"Research on cloud computing daasecurity basedon ECHD ",Department of weapons Science and Technology,Naval Aeronautical and Astronautical University Yantai,China.

[8]Dr,S.Selvi,"An Efficientt Hybrid Cryptography model for cloud data Security",Professor,Department of Computer Science,Coimbatore,India.

[9]Fatima Amounas,Hussain Sadki,Moha Hajar,"An more efficient Approch of ECC Encyption algorithm using DNA Computing",R.O.I group,Computer Scienece Department,Moulay Ismai'l University.

[10]Wendy Chou,"ECC and Its Application to mobile Device",Unversity of Maryland.

[11]Ajay Bhushan,"Trasnform operator random generator delimiter based encryption standard ",M.Tech in Information Technolgoy,Galgotias college of Engineering and Technology.

[12]Ravi Gharshi and Suresha,"Enhancing security in cloud storage using ECC algoritham",Departmentof Computer science and Engineering,Reva Institute of Technology and Mangment,Banglore.

[13]Omkar Abood,Shawkat Guirguis,"A survey of cryptography Algoritham",Deparment of Information Technology, Institute of Graduate Studies and Researches,Egypt.

[14]G Prakash,Dr.M Kannan,"Enhacing security in cryptographic smart cards through elliptic curve cryptography and optimized modified matrix encoding algoritham", Department of Information technology ,Anna University Chennai.

[15]Himija Agerwal," A survey paper on Elliptic Curve Cryptoraphy",Dept of E&TC,Imperial College of Engineering and Research,Pune,India.

[16]Eng.Hashem H.Ramadan,Moussa Adamou Djamilou,"Using Cryptography Algoritham to secure Cloud Computing Data and Services".Master in Computer Science Indian Acacdamy Degree College,Banglore,India.

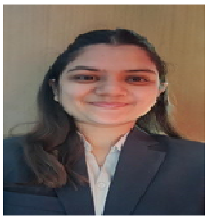
Author

[1]**Anita Chaudhari** is an Assistant Professor in Department of Information Technology ,St. John College of Engineering and Management , Mumbai. She received Bachelors degree from pune university in 2009 and Masters degree from Mumbai university in 2013.Currently pursuing Ph.D from Mumbai University. Her current research focuses on network security, Internet of Things.

[2]**Mayank Nagora**, is currently pursuing his Bachelor's of Engineering (B. E.) in Information Technology (IT) from St. John College of Engineering and Management (SJCEM), Palghar, India. His Area of interest include React,MongoDB and Firebase

[3]**Mayur Rane**, is currently pursuing his Bachelor's of Engineering (B. E.) in Information Technology (IT) from St. John College of Engineering and Management (SJCEM), Palghar, India. His Area of interest include Networking,MongoDB and Cloud Computing

[4]**Murtuza Hafizjee**, is currently pursuing his Bachelor's of Engineering (B. E.) in Information Technology (IT) from St. John College of Engineering and Management (SJCEM), Palghar, India. His Area of interest include Java Script, HTML and CSS



[5]**Jagruti Goswami**, is currently pursuing her Bachelor's of Engineering (B. E.) in Information Technology (IT) from St. John College of Engineering and Management (SJCEM), Palghar, India. His Area of interest include Java Script HTML and CSS.