Web Application for Issuing of Government Documents using Elliptic Curve Cryptography

Chetana Zambare[1], Vaishnavi Nibrad[2], Pranjali Shivramvar[3]
[1, 2, 3] AISSMS IOIT, Pune

Abstract- *Need of personal documents is increased to take advantage of government facilities. For issuing documents manually there are lots of aspects of corruption that cannot be seen easily. This project offers a mechanism by which user can issue his documents online instead of doing it manually at his native place. An efficient and secure environment is necessary for issuing government documents and makes it available for real time access. For security purpose documents are encrypted in the form of image and for sharing purpose they are stored on the cloud. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. This project also offers sharing of documents among government offices. In proposed system we are going to use Elliptical Curve Cryptography for ciphering images. ECC provides smaller key size. Thus thereby requiring lesser storage and processing time.*

Keywords- Cloud computing, Security, ECC, Image Encryption.

I. INTRODUCTION

People think that issuing of documents is hectic task. Paper introduces an idea of issuing the documents from anywhere. People no longer need to issue documents manually. Keeping the information in the form of hard copied documents lead to many problems such as loss of documents, document forgery, etc. To avoid these problems we can keep the documents in the form of soft copy. Handling of documents in the form of soft copy is convenient but at the same time it is not secure. The paper focuses on providing the security to the documents. Documents are stored on cloud in the form of images. For securing the images, store them on cloud in encrypted form. Encryption is the process of conversion of original form into other form called cipher form. Cipher form cannot be read by anyone without converting it into original form known as decryption. This paper concerned with the technology known as Elliptic Curve Cryptography for encryption and decryption process.

II. LITERATURE SURVEY

1. Robshaw and Yin compared RSA digital signature with a key size of 1024 bit and ECDSA with 160 bit length key in 1997, in a RSA laboratory. After comparing both algorithms according to storage requirements and computational speed they found ECC signature generation is seven times faster than RSA signature [1]. So using ECC instead of RSA improves the performance of internet exchange gains enhancement thoughtlessly.
2. ECC provides encryption functionality requiring a smaller percentage of the resources required by RSA and other algorithms. In most cases, if key length is longer, the more protection that is provided, but ECC can provide the same level of protection with a smaller key size than RSA. Since smaller keys as in ECC require fewer resources of the device to perform the mathematical tasks.
3. Mohammad Montazerolzohour et al [2] in Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application compare ECC algorithm with 160 bit key size against RSA algorithm with 1024 bit key size in a multipurpose smart card.
4. Kamlesh Gupta et al [3] in "ECC over RSA for Asymmetric Encryption: A Review" demonstrated the ECC is more cost efficient method to perform encryption for portable devices and to secure image transmission over internet and provide good security with smaller key sizes.
5. P.R.Vijayalakshmi et al[4] in "Performance analysis of RSA and ECC in identity-based authenticated new multiparty key agreement protocol " compare Elliptic Curve Cryptosystem (ECC) and RSA by computing execution time and memory size for encryption and decryption process and analyzed performance with different key sizes and variable word lengths.
6. Nils Gura et al[5] in Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs states that as compared to RSA smaller key sizes, faster computation, memory, energy and bandwidth savings are offered by ECC.
7. Swadeep Singh et al[6] in Comparison of Cryptographic Algorithms: ECC RSA finds that properties of ECC are stronger against various attacks in wireless networks. Signature generation for ECC becomes comparatively faster than RSA system.
8. NAS [7] Technical Report on A Survey of Elliptic Curve Cryptosystems gives a deep introduction of how elliptic curves have been applied to public key cryptography. It

also introduces the bridge between mathematical terms of elliptic curve and its cryptographic applications.

9. Ali Soleymani et al[8] in An Image Encryption Scheme Based on Elliptic Curve and a Novel Mapping Method states that multimedia data types, such as images, videos, and audio, large sizes and high data rates so that it require a short key size and high security cryptosystem. ECC is acceptable choice for these real time multimedia applications.
10. Smithashree K et al[9] in Image Encryption Using Efficient Elliptic Curve Cryptography proposed the FSR (Feedback Shift Register) method to generate key they also obtained encrypted images by taking input as plain images and computed and analysed correlation coefficient of the input and encrypted images.

Table 1. Key Comparison

Symmetric Key Size	ECC Key Size	RSA and Diffi-Hellman Key Size
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	521	15360

III. ARCHITECTURE

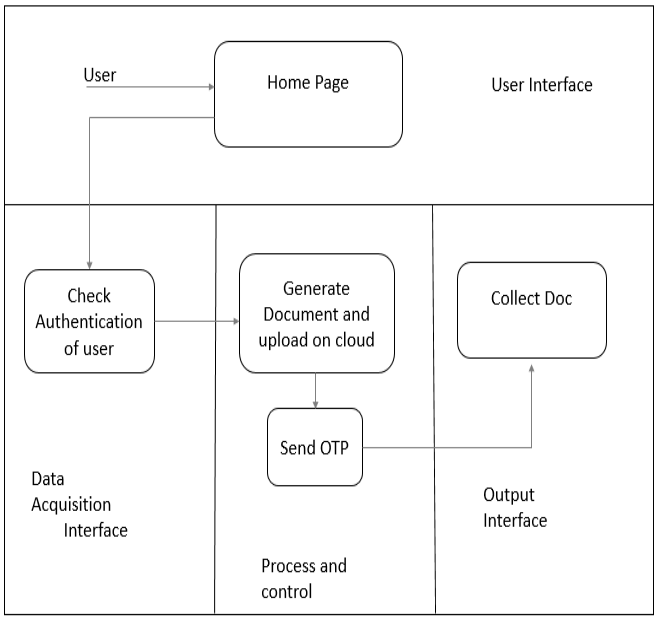

Figure 1. Architecture Diagram

Figure 1 shows the architecture view of the proposed idea. Using the web application user can send the request to government officer for issuing of documents online. After that government officer check the authentication of user and proceed further. If user is authentic then document will be generated and stored on cloud in the form of encrypted image using Elliptic Curve Cryptography. At the same time officer send OTP to the user which is a decryption key. Using this key user can decrypt the document.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

As compare to other public key cryptosystem it is possible to achieve same security level with smaller key size using Elliptic Curve Cryptography therefore it require less storage and processing time. Informally, an elliptic curve is a kind of cubic curve but whose solutions are confined to a region of space. The general equation of an elliptic curve looks like:

$y^2 = x^3 + ax + b$ [1]

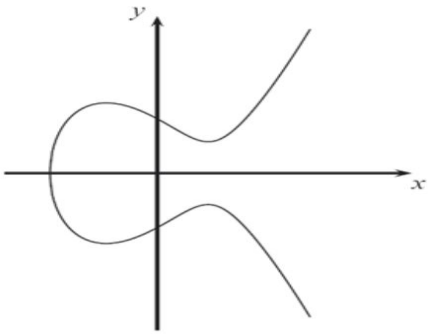

Figure 2. Elliptic Curve

.

A prime number p and a generator point a are given along with the equation of the curve. The operation exploited for key selection in elliptic curve cryptography comes from considering elliptic curve as an abelian group with points as elements.

Point addition: It states that to add two points P and Q we draw a line PQ through them and find the third point of intersection –R of that line and reflect it over the axis of symmetry of the curve. The resultant point R will give the addition of the two points.

V. APPROACH

The complete process followed by us can be summarized by the following flowchart:

1. Encryption Process:

a) Select the image to be converted. .
b) Convert the image into matrix form.
c) Generate the random number using number generator n.
d) The image matrix is divided into n parts.
e) Generate another random number which can be use to divide each element of every matrix. This division

produces quotient and remainder.

f) Koblitz encoding [3] is used to generate points on the curve.
g) The points are encrypted.
h) Encrypted image is produced

2. Decryption Process:

a) Encrypted image is received by receiver.
b) To get the points on the curve decryption is performed.
c) To get the elements of matrix decoding is done.
d) All the elements of matrix are multiplied by random number.
e) To get the original image all the matrices are merged.

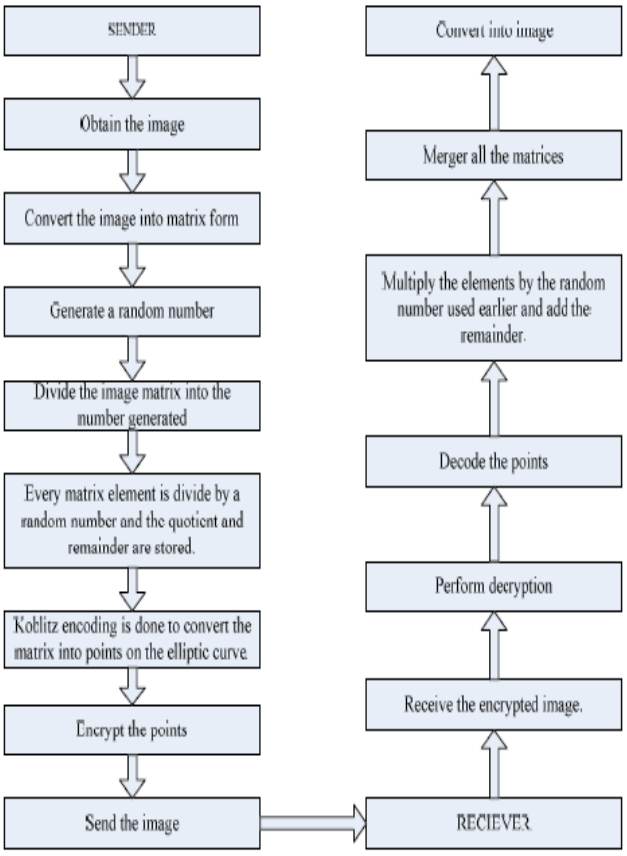

Figure 3. Flowchart

VI. CONCLUSION

ECC provides better security than other cryptographic techniques. One of the most important problem is with storage constraints. So that ECC with smaller key size is very important. While uploading the document on cloud it is encrypted to be secure. As compared to RSA, ECC provides faster computations, reduce power consumption and saving memory space and bandwidth. For mobile phones ECC is better because mobile having limited processing power.

REFERENCES

[1] Nikita Gupta, Vikas Kundu, Neha Kurra, Shivani Sharma, Bhagyashree Pal, "Elliptic Curve Cryptography for Ciphering Images ", IEEE, 2015

[2] Maryam Savari, Mohammad Montazerolzohour, Yeoh Eng Thiam, "Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application", 2012

[3] Kamlesh Gupta, Sanjay Silakari, JUET, Guna, UIT, RGPV, "ECC over RSA for Asymmetric Encryption: A Review ", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011

[4] P.R.Vijayalakshmi, K. Bommanna Raja, "Performance Analysis of RSA and ECC in Identity- Based Authenticated New Multiparty Key Agreement Protocol", ICCCA, 2012

[5] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz , "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs ", Sun Microsystems Laboratories

[6] Swadeep Singh, Anupriya Garg, Anshul Sachdeva, "Comparison of Cryptographic Algorithms: ECC RSA", International Journal of Computer Science and Communication Engineering

[7] "A Survey of Elliptic Curve Cryptosystems, Part I: Introductory ", NAS Technical Report - NAS-03-012 August 2003.

[8] Ali Soleymani, Md Jan Nordin, Azadeh Noori Hoshyar, Zulkarnain Md Ali, Elankovan Sundararajan, "Image Encryption Scheme Based on Elliptic Curve and a Novel Mapping Method", International Journal of Digital Content Technology and its Applications(JDCTA) Volume7, Number13, Sept 2013

[9] Smithashree K, Sujatha M, "Image Encryption Using Efficient Elliptic Curve Cryptography ", International Journal of Innovative Research in Computer and Communication Engineering

[10] Ruchika Markan, Gurvinder Kaur, "Literature Survey on Elliptic Curve Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering,2013