International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Secure Data Transaction using ECC in Corporate Environment

D. Sathiya, S. Albert Rabara

Abstract*: The encryption/decryption techniques are used to provide secure and fast data access. In this paper, we consider the data transaction from the user's mobile to company's server in the corporate environment with restricted accessibility at different levels of employees. To provide this secure and quick accessibility of data, we propose an ECC algorithm with DCT for different data types such as text, image, audio and video files. The efficiency of this approach is validated through encryption/decryption and throughput time analysis

***Index Terms*: Discrete Cosine Transform, Elliptic curve cryptography**

I. INTRODUCTION

Regulating individual user's access in a corporate database system based on their role in an organisation is an essential one, and it refers as Role Based Access Control[1]. For this purpose, the Organization should enable the security as view, add, update and delete based on user level by the actions of create, change, or discontinue roles of access privileges of individual users. Role-based access control with encryption satisfies Data confidentiality and integrity[2]. Confidentiality refers to protecting the information from disclosure to unauthorised parties, which means preventing sensitive information from reaching the wrong people. Integrity refers to protecting information from being modified by an unauthorised user to maintain the consistency, accuracy and trustworthiness of data. The security issues due to the absence of confidentiality are insider attack, outsider attack and access control issues and absence of integrity are unauthorised modification and deletion. The insider attack occurs by the database administrator because he may misuse all the privileges to access the database during maintenance. Outsider attacks related to exploitation of software vulnerability and also the activities like intrusion using login credentials, spoofing, side channelling and man-in-middle attacks. Access control issues occurlack of monitoring access control policies. The integrity issues happen at any level of data storage by unauthorised modification and deletion[1-3].

The corporate use the video, audio, image and text information to handle corporate data such as financial details, product design, company rules and regulation, working mechanism etc. This information should be accessed by the mobile user from their own mobile devices with a secure transaction between mobile devices and corporate servers. The different researchers have carried out a sample amount of work in their proposed work for a secure transmission of video, audio, image and text information individually[4-7]. Discrete cosine transform technique has been used by many researchers for image, audio and video encryption/decryption techniques as well as compression purpose. In this proposed work, we provide encryption and decryption of all kinds of data with ECC based security during data transmissions with discrete cosine transform technique.

Hence, to provide end to end security between Mobile and corporate Server for secure data access, Role-based access control policies are granted to a particular user in order to keep the information more confidential from an unauthorised user and for secure data access the ECC based encryption, and decryption operation is performed. The proposed security algorithms ensure the security properties data confidentiality, data integrity and role-based authentication.

The paper is organized as follows: Section 2 presents thecorporate environment and its access control. Section 3 presents the basics of the discrete cosine transform and Section 4 explains the ECC based security algorithms. Section 5 presentsResults and Discussion, and Section 6 concludes the paper.

II. CORPORATE ENVIRONMENT AND ACCESS CONTROL

The main units which we consider are Mobile Client (MC) and the Corporate Server (CS). The mobile device contains the client application that helps to establish secure connectivity with the corporate servers through 3G/4G network connection. The mobile user makes a request to access the employee data such as salary details, personal details and other sensitive services through the client application. Before processing the user's request, device authentication, user authentication is performed with MAC ID and User ID by a novel signcryption technique based on ECC.Additionally, the client application enables the configuration of security settings to protect the organisational data on the user's device. The details of the corporate environment are discussed in [15]. Access rights are defined for each Employee based on their designation. CEO can do all the operations such as view, add, update and delete; Managers can do view, add and update operations; Engineers can do view and addoperations and Workers can view their own details. The User ID information takes care of the secrets of the accessibility of data.These data transaction controlled and secured by ECC and DCT techniques in terms of encryption and decryption.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
D.Sathiya* ,Research Scholar, Computer Science Department, St.Joseph's College, Tiruchy, India.
S.AlbertRabara, Computer Science Department, St.Joseph's College, Tiruchy, India.

III. DISCRETE COSINE TRANSFORM

DCT transforms a time domain of a signal into its frequency components by only using the real parts of the Discrete Fourier Transform (DFT) coefficients. In the literature, the DCT coefficients are used to encrypt the different data files. Bouaziz et al. have implemented a MPEG video encryption algorithm based on DST coefficients of I-frames [8]. Hao Wang and Chong-Wei Xu [9] proposed a new lightweight, efficient, scalable and format compliant video encryption algorithm based on the DCT coefficients scrambling. They mentioned that the proposed encryption algorithm is basedon the concept of a permutation group. Scrambling DCT coefficients of the permutationgroups maintain the statistical property of DCT distribution so that the encryption does not suffer from DCT vulnerability attack. Narasimha et al., [10] have proposed a computationally efficient, yet secure video encryption scheme. It uses RC5 for encryption of the DCT coefficients. [11,12]. In this paper, we used DCT techniques for theencryption-decryption process of video, Audio and Image.

IV. ECC IMPLEMENTATION

The technique to protect multimedia files is by encrypting the multimedia itself, which is the main concern in mobile device applications and issues. Unauthorised users cannot read the data, and hackers or thieves will not be able to read encrypted data on mobile devices. This paper presents an implementation for using ECC in a mobile device for a multimedia file. The propose ECC algorithm focuses on increasing the security of the algorithm the multimedia for mobile phone.

NielKoblitz and Victor Miller[13] proposed the elliptic curve cryptosystem in 1985,and it was widely accepted around 2004. It is public key cryptography; the key sizes are smaller than the other system, and intractable[14]. So, it seems to be the best choice among the existing cryptographic techniques. In addition to that, the hardness of ECC relatively depended on thedifficulty of Elliptic Curve Discrete Logarithm problem. The formal and simple elliptic equation is of the form

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

$$4a^3 + 27b^2 \neq 0$$

$$x, y, a, b \in R$$

ECC based algorithms are designed for a different format of multimedia files (like video, audio, image and text) with DCT. The different kinds of input to the encryption/decryption algorithm are given below.

Video: The mathematical operation on video is done on the coordinates of each coefficient is considered for this manipulation. We consider the I-frames for this encryption and decryption process since it provides the access point of the image code data and are also the beginning of decades and are compressed based on common methods than the other frames P-frames and B-frames of the video stream. The effect will be the same on the frames P-frames and B-frames. The ECC parameters (a, b, G, p) are agreed between the sender and the receiver.

The sender uses the public key 'PUs ' of the receiver to generate the new coordinates (x2,y2) from the coordinates (x1=mk+J,y1=$\sqrt{x^3 + ax + b}$) (mod p) of a particular DCT coefficient 'PM'. The receiver uses the private key ' ks ' to decrypt the new coordinates back to the original coordinates(x1,y1) of the DCT coefficients. Finally, we obtain an encrypted video by browsing all the pixels of the I frame.

Audio: The DCT coefficient ofthe audio file is considered as input for this process and it iscalled asmessage m.

Image: The DCT coefficient of the pixel values of the imageis considered as input for this process, message m.

Text: The DCT coefficient of the ASCII value of each character of the text is considered as the inputmessage m for this process.

The message mis converted into the coordinates (x1=mk+J,y1=$\sqrt{x^3 + ax + b}$) (mod p)that is the point on the elliptic curve. Where k is a random positive integer, p$\geq$ mk, and J=0,1,2,3,…

The sender uses the public key 'PUs ' of the receiver to generate the new coordinates (x2,y2) from the coordinates(x1,y1) of a value of the audio file 'PM'. The receiver uses the private key ' ks ' to decrypt the new coordinates back to the original coordinates(x1,y1) of the value of the audio file. Finally, we obtain an encrypted audio/image/text by browsing all the values of the audio/image/text file.

In the proposed scheme, first, we generate an elliptic curve with at least 256 points and verify the user's identity using signcryption algorithm which consists Key generation, Signature generation and signature verification based on ECC. Second, the authorisation granting algorithm checks the accessibility for data requested by the user. The detailed steps of these algorithms are available in [15].The proposed algorithm is given below.

ECC based data access algorithm:

1. Generate an elliptic curve with 256 points.
2. Verify the user's identity using signcryption algorithm
3. Verify the user's accessibility of the particular data using the authorization granting algorithm
4. The menu displayed for the various role with user's query top-down menu
5. Encryption// Decryptionwith ECC and DCT
6. Go to step 4.

V. RESULTS AND DISCUSSION

We have implemented the proposed approach mobile with the help of Android Studio. The proposed system is communicated between the corporate database server and employee smartphone with the help of a web interface. The performance of the proposed system is tested with regard to the encryption/decryption runtime and throughput. Our solution is tested on a mobile with Qualcomm MSM8998 Snapdragon 835 processor @ Octa-core Kryo 4 x 2.45 GHz + 4 x 1.9 GHz, 8 GB Ram and on a server with INTEL QUAD CORE XEON E5-2630V3@2.4Ghz,16GB Ram.

The data access algorithm executes to show the details of the user's request, and it allows the user to view the particular data or delete or add or modify the data. The sample view of video, image and text of the production and sales department respectively are shown inFigure 1.

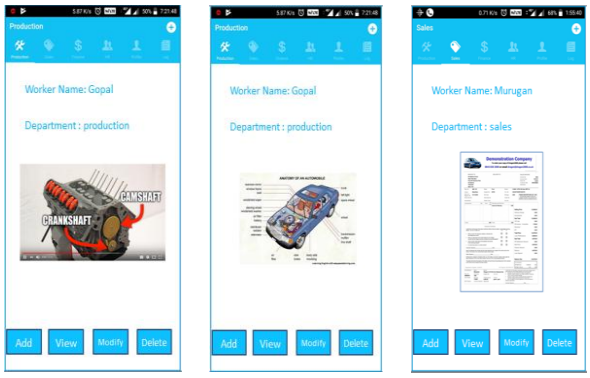

Figure 1 video, image and text files

The information such as design diagram, information about product design,working mechanism, financial details and company rules and regulations stored in corporate database are presented in different formats such as image(.jpg, .gif etc), audio(.mp3 etc), video(.mp4 etc), document(.txt, .doc. etc) and pdf respectively. After data retrieved from a database in the server, the requested data encrypted using ECC algorithm in authentication server and this data is transmitted to the mobile device in which the decryption process is made using the ECC algorithm. The encryption and decryption time and the throughput in these operations are presented.

The encryption and decryption time is depicted in Figure 2 taken by corporate apps for a different type of data. The encryption or decryption process may have any kind of data which can be used in a corporate environment, and the processing time may differ, which depends upon the data type. The encryption and decryption time for the multiple users (5, 10, 15, 20, 25 and 30 users) is shown in Figure 5.

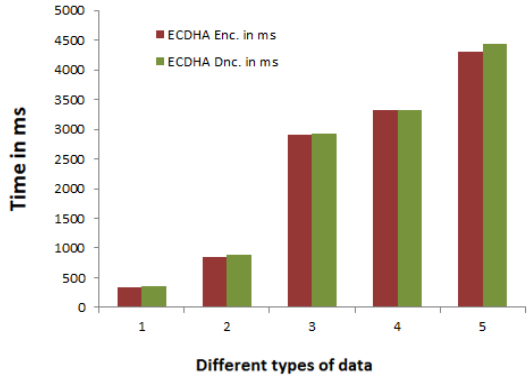

Figure 2 ECC Enc. /Dec. runtime

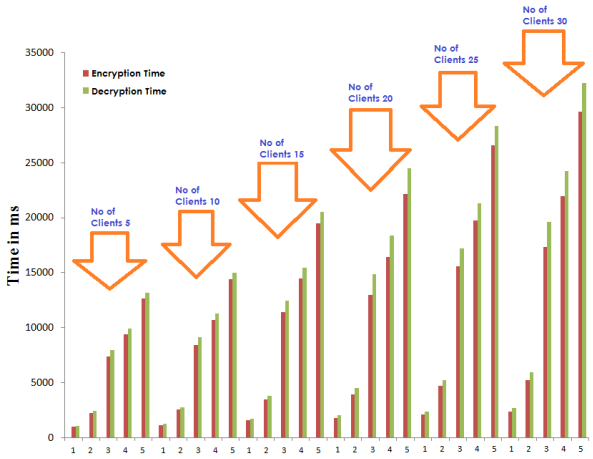

Figure 3 ECC Enc/Dec runtime for multiple users

The time taken for encryption or decryption process by corporate apps for a different number of users accessing different types of data is depicted in Figure 3. Depends on the number of users the process (encryption /decryption) time may differ, and it depends on the data type. For the smaller volume of data, the processing time is very less, and if the number of users is increased for the same type of data, the response time may increase. From the analysis, it is observed that the time taken for encryption is comparatively less with the decryption process since encryption processes the raw data(data in original format). But, in the decryption process, the cypher data has to be changed to original form hence the time is high.

Usually, the throughput of encryption is defined as the ratio between the size of the data which is going to be encrypted and the time taken for encryption by the ECC algorithm. Similarly, the throughput of decryption is termed as the ratio between the size of the data, which is going to be decrypted and the time taken for the decryption process by ECC. Here the throughput time is high for decryption than for the encryption since, in the decryption process, an additional process such as the fixing of the exchanged public key with the local private key consumes some time. The throughput for encryption and decryption operation for the single user is shown in Figure 4.

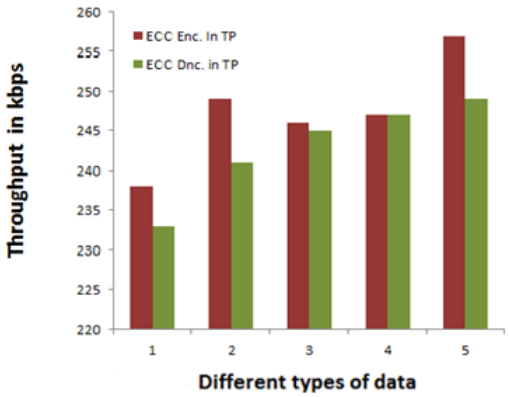

Figure 4Performance analysis based on Throughput

VI. CONCLUSION

In this paper, an ECC algorithm with DCT for data access in the corporate environment has been implemented. The main objective is to provide end to end data transaction from mobile to company server. The proposed technique has been tested from mobile to sever or otherwise with multiple users and different data files. The throughput and encryption/decryption time analysis of data transaction are shown in figures. The performance of this approach is praiseworthy, and it can be used in other mobile communication networks to provide enhanced data transaction.

REFERENCES

1. A. L. Pereira, V. Muppavarapu, and S. M. Chung, "Role-Based Access Control for Grid Database Services Using the Community Authorization Service," *IEEE Trans. Dependable Secure Comput.*, vol. 3, no. 2, Apr. 2006,pp. 156–166
2. K. K. Hingwe and S. Mary Saira Bhanu, "Hierarchical Role-Based Access Control with Homomorphic Encryption for Database as a Service," in *Proceedings of International Conference on ICT for Sustainable Development*, vol. 409, S. C. Satapathy, A. Joshi, N. Modi, and N. Pathak, Eds. Singapore: Springer Singapore, 2016, pp. 437–448.
3. E. Bertino, "Access Control for Databases: Concepts and Systems," *Found. Trends Databases*, vol. 3, no. 1–2, , 2010,pp. 1–14
4. R. Singh, R. Chauhan, V. K. Gunjan, and P. Singh, "Implementation of Elliptic Curve Cryptography for Audio Based Application," *Int. J. Eng. Res.*, vol. 3, no. 1, 2014,p. 6.
5. S. Bouaziz, R. Hadaji, and A. Mtibaa, "MPEG-2 and ECC Security in DCT Domain," vol. 11, no. 9, 2016.p. 5
6. D. P. Astya, B. Singh, and M. D. Chauhan, "Image encryption and decryption using elliptic curve cryptography," *Vol No*, p. 8, 2014.
7. L. Bhandari and M. A. Wadhe, "Speeding up Video Encryption using Elliptic Curve Cryptography (ECC)," vol. 2, no. 3, 2013, p. 6,
8. SamiaBouaziz, ramzihadaji, AbdellatifMtibaa, MPEG-2 and ECC security in DCT domain, International Journal of Applied Engineering and Research, 11(9) 2016, pp 6643-6647.
9. A. S. Tosun and W. Feng, "A light-weight mechanism for securing multi-layer video streams", Proc. IEEE International Conference on Information Technology: Coding and Computing., April, 2001, pp 157-161.
10. C. Narsimha Raju, GanugulaUmadevi, Kannan Srinathan and C. V. Jawahar. "Fast and Secure Real-Time Video Encryption", in. Proc. of the IEEE Sixth Indian Conference on Computer Vision, Graphics and Image Processing, 2008, pp257-264
11. Bhandari, Lekha, and AvinashWadhe. "Speeding up video encryption using elliptic curve cryptography (ECC)." International Journal of Emerging Research in Management &Technology 2.3 2013,pp24-9.
12. Singh, L. D., & Singh, K. M. (2015, January). Image encryption using elliptic curve cryptography. In Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), Procedia Computer Science (Vol. 54, pp. 472-481).
13. Scoot A Vanstone, Elliptic curve cryptosystem-the answer to strong, fast public-key cryptography for securing constrained environments. Information Security Technical Report, vol. 2. 1997.
14. Andreas Enge, Elliptic Curves and Their Applications to Cryptography: An Introduction. 1999.
15. D. Sathiya, S. Albert Rabara, T. Daisy Premila Bai, J. Ronald Martin, ECC based Signcryption Scheme for Corporate Environment through Mobile Communication System, International journal of pure and applied mathematics, 118(20), 2018, pp 449-456.

AUTHORS PROFILE

D Sathiya is doing Ph.D in Computer Science, St. Joseph's College (Autonomous),Tiruchirappalli, Tamil Nadu, India. She holds M.Sc. degree and M.Phill., degree from Bharathidasan University. She has authored/Co-authored 3 research papers which are published in refereed national and international journals and conferences. Her research interest is security in mobile database systems.

Dr.S.AlbertRabara is working as an Associate Professor in the Dept. of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli. He obtained his Ph.D Degree in Computer Science from Bharathidasan University. An expert in the field of Information and Communication Technology and Security, he is a consultant for several colleges in Tamil Nadu. He has 30 years of teaching and research experience and guided ten Ph.D Scholars. Published more than 100 papers in Journals, International and National Conference Proceedings, his research contribution is significant in IEEE, ACM and Springer Science publications and DBLP library catalogues. He is a member of editorial board of several International Journals and life time member Computer Society of India (CSI).