IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE MESSAGE TRANSFER USING ECC ALGORITHM

[1]A.Regina Elizabeth, [2]P.Darlin Jena, [3]T.Deepika, [4]V.Jemiladevi[5]N.Karthika

[1]*Faculty*, [2,3,4,5]*UG Scholar*

Computer Science and Engineering

Jayaraj Annapackiam CSI College of Engineering, Nazareth, India.

Abstract: A Secure Message Transfer Using ECC Algorithm is a web based application. The Elliptical Curve Cryptography(ECC) algorithm enables secure message sharing by encrypting and decrypting data using elliptic curve over finite fields. Compared to more established public- key cryptography algorithms like RSA,ECC is a kind of PKC that is thought to be more efficient and safe. Using encryption technology to transform messages into unreadable formats that can only be decoded by the intended receiver with right decryption key is a common practice in secure message sharing. Even if the message is intercepted by an attacker, encryption ensures that they won't able to read it. When sending private or sensitive information like financial information, medical records, or personal details, secure message sharing is very crucial. Data protection benefits both people and organization from data breaches and other forms of cyber attacks.

Index Terms **- ECC, PKC, Encryption, Decryption.**

I. INTRODUCTION

ECC takes its structure from its ability to ensure data transmission in one of the apploudable manners. With its key size being significantly smaller than that of many other encryption algorithms like RSA, It is yet a commendable one for its efficiency. One of the greatest assets of a human can be his cognitive abilities. To think in a manner that no bot or machine or another human for that manner can is something to be astounded about and taken effectively advantage of. This cognitive ability is best utilized during the authentication process of the system. The authenticated user uses his cognitive abilities to log in on to his account created with selecting certain provided co-ordinates obtained from an elliptic curve equation to remember while you are logging in. By testing a user ability to recall the coordinates they chose before logging in, this facilitates user authentication. After the authentication procedure, data is encrypted using elliptic curve cryptography, whose merits have already been covered in this introduction. With the help of the Diffie-Hellman Key exchange mechanism ,the encryption is carried out with the creation of a shared –secret key on both sides. The method aids in opening a line of communication between the users involved in the connection that has since been made. Since a text is being delivered through the channel in encrypted form, which is a coordinate, this makes it much more challenging to decipher. Finally, a decrypted version of the cipher text is produced. At the other end, received. In contrast to other public key encryption methods that employ substantially bigger keys, elliptic curve cryptography uses smaller keys for encryption. Elliptic Curve Cryptography's 164-bit key grows its capacity for data security up to that of roughly a 1,204-bit key encryption technology.

BASIC TERMS IN CRYPTOGRAPHY:

- Plaintext
- Cipher text
- Encryption
- Decryption
- Key

CLASSIFICATIONS OF CRYPTOGRAPHY:

Encryption algorithms can be classified into two broad categories:

- **Symmetric**
- **Asymmetric**

Asymmetric Encryption:

Asymmetric encryption, often known as public-key cryptography, encrypts and decrypts a message while safeguarding it against unauthorized access or use using a pair of linked keys: a public key and a private key.

II. LITERATUREREVIEW

O Shoewu and Segun., discuss how to secure GSM data by using encryption, decryption, the transmission module, and demodulation in a remote domain. This article focuses on using elliptic curve cryptography(ECC) to encrypt and decrypt instant messages while keeping in mind that the ultimate goal is to safeguard the integrity, reliability, and security of instant communication. The goal of the study is to improve the consistency of message quality when conveyed over distances, and to that end, ECC encryption and decoding algorithms have been chosen to distinguish/check their effectiveness based on three major considerations: speed, key length and quality.

Ruchika and Guruvinder., described how it is crucial for some associations to prevent unauthorized access to corporate data structures. One of the big mystery zones is security communication.. The most recent development in network security is cryptography using elliptic curve architectures, which relies on discrete logarithmic problems and elliptic curve number-crunching.ECC plans are public key based systems that provide key exchange methods, encryption, and outstanding marks.

Laiprakhpam et al., proposed a present a solution that eliminates the high strategy of mapping the characters to relative foci in the elliptic curve. The plain content's corresponding ASCII estimates are combined properties serve as the elliptic curve cryptography's contribution. This new method keeps a strategic distance from the pricey mapping process and the requirement for the sender and beneficiary to share the same query database. The algorithm is designed to be used to scramble or decode any script the uses recognisable ASCII vales.

Plain text is transformed using Cryptography to make it secure and impervious to hackers. Public key Cryptography known as elliptic curve was created. Established in 1985 by Neal Koblitz and Victor Miller. The curve equation of the form will be used in elliptic curve cryptography. $Y2 = X3 + axe + b$ It is referred to as the weierstrass equation, where a and b as a constant $4A3+27B2=0$. Based on the intractability of specific mathematical puzzles, Public-Key cryptography is used. Assuming that it is challenging to factor a huge integer made up of two or more large prime factors, early Public-Key systems are secure. Finding the discrete logarithm of a random elliptic curve element with respect to a widely known base point is known as the "Elliptic Curve Discrete Logarithm Problem (ECDLP) " and is considered to be infeasible for elliptic curve-based protocols.

The main advantages of elliptic curve cryptography is a reduced key size, which reduces the need for storage and transmission. Curve group with a large modulus and proportionally larger key might offer the same amount of security as an RSA-based system. A 256-bit elliptic curve Public key, for instance, ought to offer equal security to a 3072-bit RSA public key.

III.PROPOSED SYSTEM

Data security is crucial whenever it is sent as an image, text, or file. Effective multi-key encryption and decryption methods like the ECC algorithm are required. In this project, data is transferred securely by encryption and decryption using the ECC method

Advantages:

- Smaller key size
- Quicker processing
- Better resistance to attacks
- Better scalability

KEY SIZE COMPARISION IN BITS

Symmetric	ECC	RSA
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

IV.RESEARCH METHODOLOGY

Secure Message Transfer Using ECC Algorithm is emphasize the significance by putting an algorithm which is relatively easy for implementation and it gives impressive response. In our work, we are having three modules such as Key generation, Encryption, Decryption.

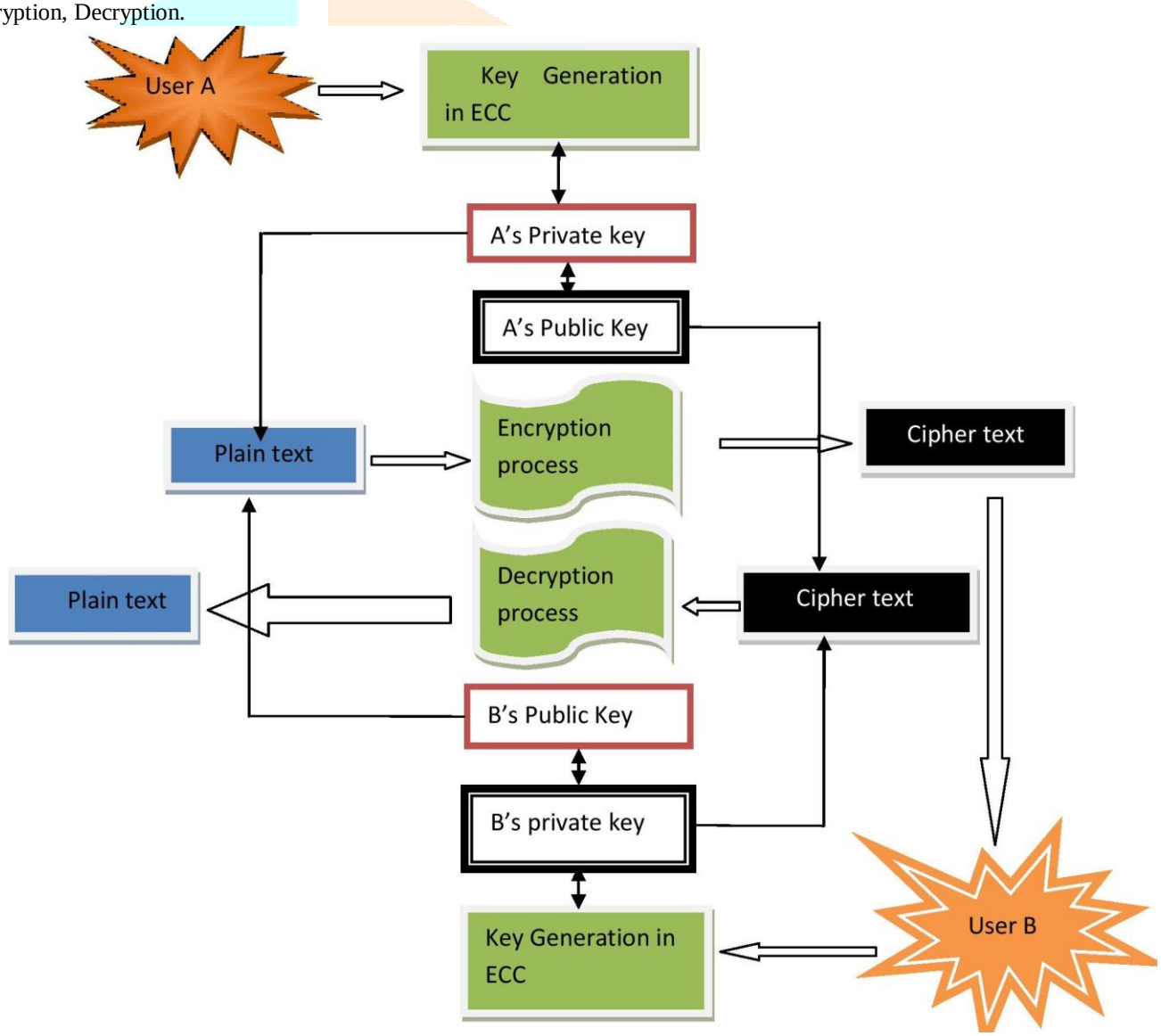

Fig.1 Architecture Diagram

4.1 Key Generation

Both the sender and receiver produce a private key and public key. The key is utilised both when the cypher text is being decrypted and when the plain text is being encrypted.

Global public elements

Eq(a, b) - Elliptic curve with the parameters a, b and q,

q - Prime or an number in the form of 2m or

G – point on the elliptic curve with a big value n for the order

Key Generation for User A

Private key n_A n_A< n

calculate public key P_A. P_A=n_A×G

Key Generation for User B

Private key n_B n_B < n

Calculate public key P_B P_B=n_B ×G

User A calculates secret key using the formula K = n_A×P_B

Calculation of the secret key by the user B K=n_B ×P_A

4.2 Encryption

Encryption is the process of changing Plain text into Cipher Text. With the help of cryptography, private messages can be sent via an unsafe channel.

A selects a random positive integer k to create the cipher text Cm, which is made up of the following pair of points, to encrypt and deliver the message Pm to B.

Cm = { KG, M+K PP_B}

4.3 Decryption

Decryption is the term for the opposite of encryption. Cipher text is transformed into plain text during this process. In order to recover the original message from a non-readable message (Cipher Text), cryptography requires a decryption algorithm at the recipient side.

A has utilised PM, B's public key. B multiplies the first point in the pair by B's Private key and subtract the result from the second point to decrypt the cipher text.

$$K_G \times n_B$$

$$C_{2\_} - K_G \times n_B$$

$$M+K\ P_B - K_G * n_B$$

$$M + K\ P_B - K\ P_B = M$$

M is the plaintext.

V. RESULTS AND DISCUSSION

ECC is a useful method for protecting data on mobile devices because they have limited storage or battery life. Algorithms with asymmetric keys are available. It does not, however, guarantee message authentication. Along with the missing key, a secure channel is required for message transmission. Otherwise, there is a greater risk of invasions and attacks. The key size and speed become a serious issue for the traditional RSA cryptosystem. This technique uses smaller keys to encrypt messages. However, this system makes the encryption less strong. ECC is useful because it provides good security with a smaller key, not just in resource-constrained environments related to mobile phones, pagers, or sharp card devices that have limited memory, limited protection of limit, and required support on successful PCs. ECC provides message authentication as well. The transmitter and beneficiary should both be utilizing comparable technology, and both should be changing at the same time, as this is the most crucial factor in employing this technique for safe correspondence. This ensures thorough verification, the ability to precisely decode the Message at the time of transfer, and protection against later attempts to decode the Message by others. ECC can be effectively used in this manner to secure and confirm the correspondence between the parties. The transmission of messages from one cell phone to the next without interruption is possible. Above all, sensitive data-containing communications are stored securely and remain so even if a mobile device goes bad The beneficiary has the ability to decipher a message once upon receipt, but never again. High levels of confidentiality must be maintained, and while doing so, the message data must be protected from misuse. As a result, it supports the secure, end-to-end exchange of data without data corruption..

5.1. Sample Screenshots

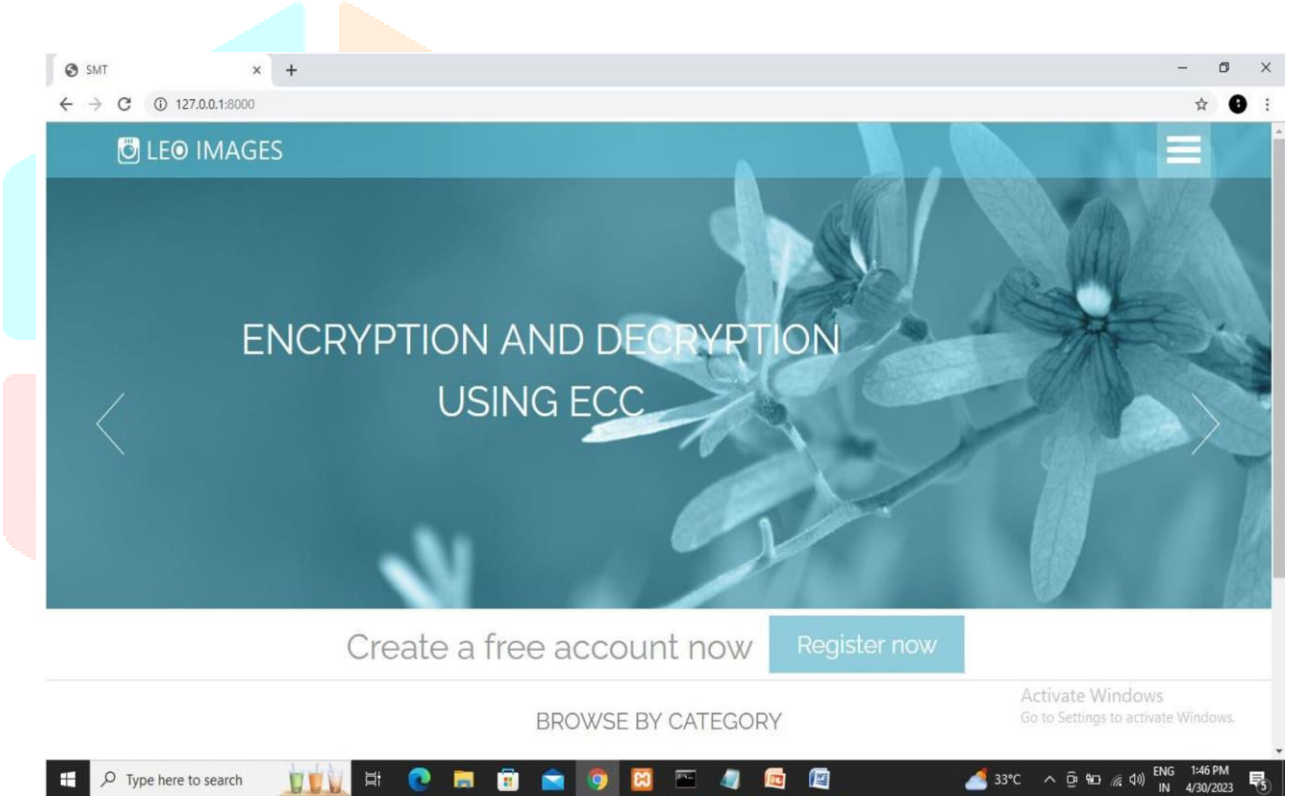

Fig 2. HOME PAGE

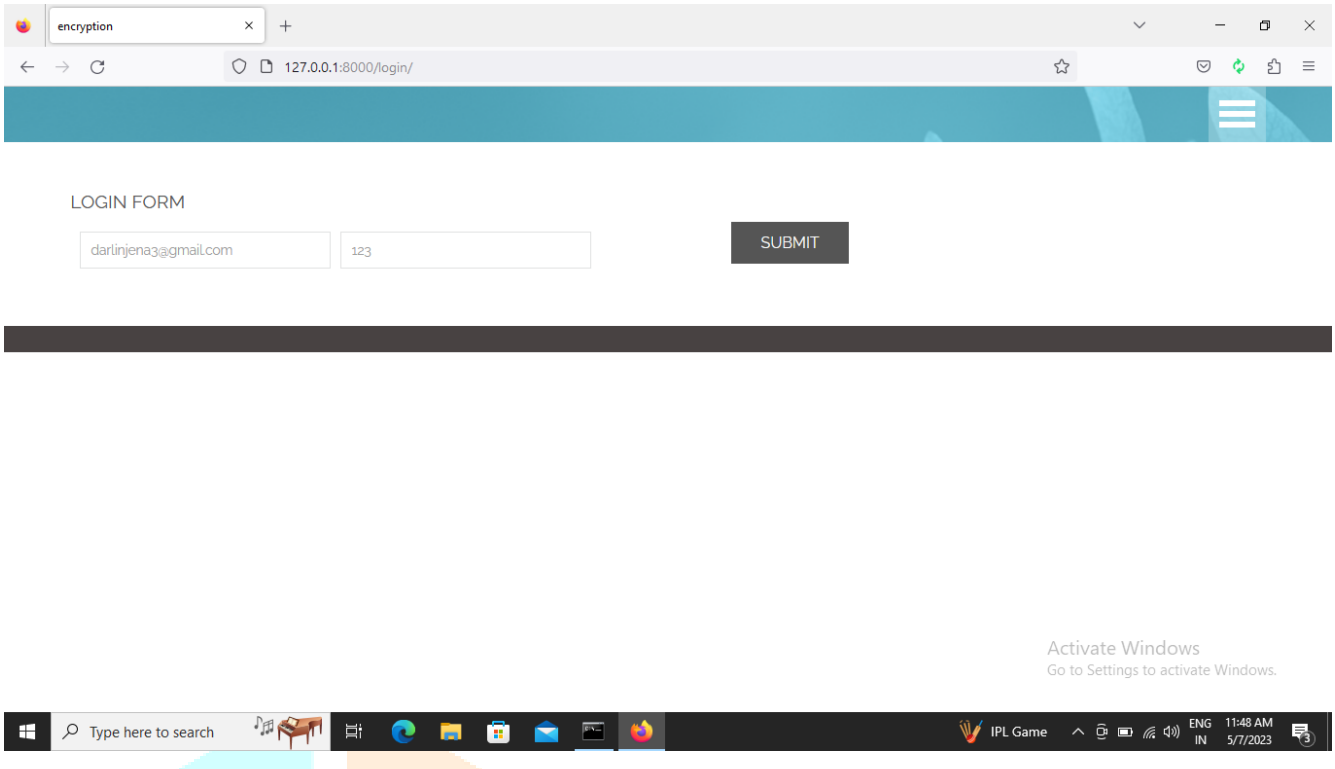

Fig 3.LOGIN PAGE

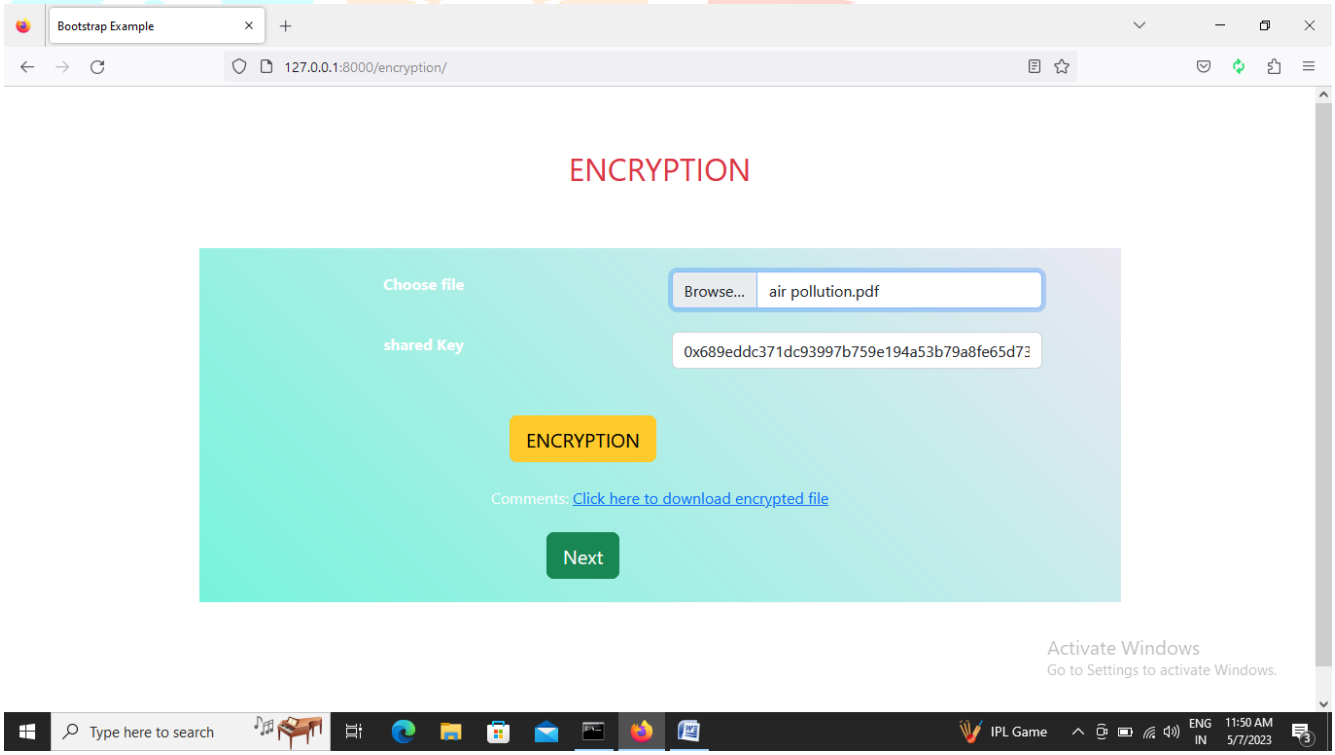

Fig 4. ENCRYPTION PAGE

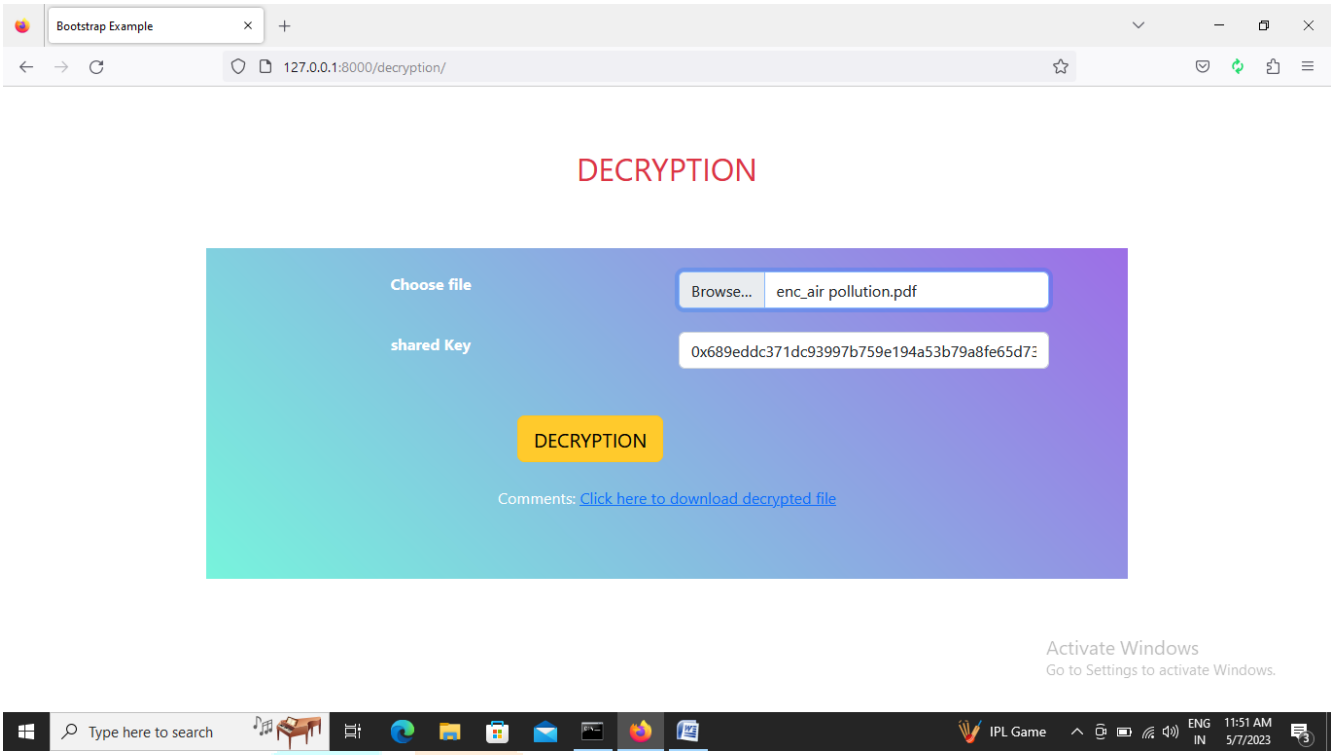

Fig 5. DECRYPTION PAGE

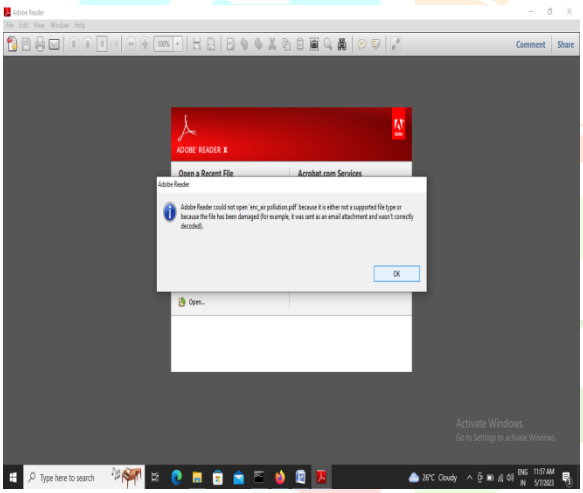

Fig **6.. ENCRYPTED**

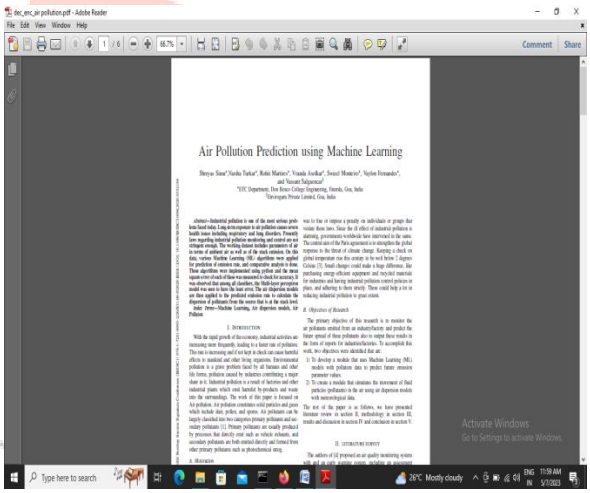

Fig.**7. DECRYPTED**

VI .FUTURE ENHANCEMENT

Transfer of Secure Messages To assist those who want to protect their photographs, files, and music, the ECC algorithm is utilized. Scalability and enhanced defence against attacks The inclusion of video files is for future improvement.

VII. ACKNOWLEDGMENT

The management of our college and our family members, who have supported and helped us at various stages of this project work, deserve our sincere gratitude.

REFERENCES

[1] Burguera, S. Nadjm- Tehrani, & U. Zurutuza(2011). Crowdroid is an Android malware detection system based on behavior. SPSM@CCS.

[2] N.S> Chaudhari and N.Saxena(2012), a GSM network method for sending SMS that is safe. CUBE.

[3] H. Eberle, N. Gura, A. Patel, S.C. Shantz,& A. Wander(2004). Comparing RSA and elliptic curve cryptography on 8-bit processors. CHES.

[4] D. Hankerson, A. Menezes,& S.Vanstone(2004). Elliptic curve cryptography reference.

[5] Jadhav, M.A., and M.M. Kolhekar (2011). Elliptic curve cryptography is used for Text and Image.

[6] In 2010, Koblitz, N. Cryptosystems using Elliptic curves.

[7] Laiphrakpam Khumanthem Manglem singh Dolendrosingh. Elliptic curve cryptography is used implement Text Encryption http://www.sciencedirect.com/science/article/pii/S 1877050 915013332

[8] Miller, V.S. (1985). Elliptic curves are used in cryptography. Segun O. Olainwo and O. Shoewu, "Securing Text Messases Using Elliptic Curve, " CRYPTO. "Cryptography and Orthogonal frequency division multiplexing "Securing Text Messages Using Elliptic Curve Cryptography and Orthogonal Frequency Division Multiplexing (http://www.academia.edu/5383818)