DATA SECURITY IN CLOUD COMPUTING USING HOMOMORPHIC ENCRYPTION

Prof.Smita Kulkarni
[1]Ashwini Jaiswal, [2]Asmita Gawandi, [3]Neha Deorukhkar,[4] Shubham Gunjal
Department of Information and Technology,
Terna Engineering College,
Navi Mumbai, 400706.

Abstract : Cloud Computing offers a number of benefits and services to its customers who pay the use of hardware and software resources (servers hosted in data centers, applications, software...) on demand which they can access via internet without the need of expensive computers or a large storage system capacity and without paying any equipment maintenance fees. An application of a method to execute operations on encrypted data without decrypting them which will provide us with the same results after calculations as if we have worked directly on the raw data. A homomorphic encryption scheme for securing data stored in cloud which allows user to operate on encrypted data directly without decryption.Use of ECC based homomorphic encryption (ECC-Elgamal) for the data storage and which outperforms other encryption techniques.

*Keywords***:** Cloud Computing, cryptography, security, Homomorphic encryption.

I. Introduction

Need of cloud to manipulate and manage data is increasing rapidly for sharing resources. It is financially beneficial to store data with a third party, the cloud provider. However, storing data on third party infrastructure poses risks of data disclosure during retrieval. Therefore, the data is stored in encrypted form. Encryption alone is not sufficient, as it provides security but reduces usability. Major advantage to be drawn from cloud computing is due to delegation of computation, but encrypting data would require sharing of keys with the third party performing computation on it, thereby increasing vulnerability. Hence, there is a need of feasible homomorphic schemes that allow user to compute on encrypted data, to verify a computation done by third party, to search an encrypted database, and so on.

The homomorphic encryption is first proposed by Rivest, Adleman and Dertouzos, regardless of whether the outsider can compute the information without decryption of ciphertext. At last, the consequences of the count are come back to the client. Following quite a while of diligent work, cryptography Gentry proposed the main full encryption conspire in view of perfect cross section, at that point the exploration advance of full homomorphic encryption conspire rapidly. Notwithstanding, the display development of the full homomorphic encryption scheme exists the accompanying issues: general society key is as well substantial, the extension rate of the figure content is huge and the figuring of the figure content is excessively tedious. RSA calculation is a homomorphism for augmentation operation, the comparing operation is additionally a multiplication, and Paillier calculation is a homomorphism for expansion operation. In this way, the plan can't be connected to the practice, and we propose the ECC based homomorphic encryption plot for these issues.

RESEARCH METHODOLOGY

1. EXISTING SYSTEM

Goldwasser-Micali partial homomorphic cryptosystem whose security is based on the quadratic residuosity problem and which allows homomorphic evaluation of a bitwise exclusive-or. This scheme has already been applied to the problem of securing biometric information. Other additive partial homomorphic encryption schemes that provide semantic security are Benaloh, Naccache-Stern, Paillier, Damgard-Jurik, Okamoto-Uchiyama and Boneh-Goh-Nissim. Some additively homomorphic encryption schemes use lattices or linear codes. For instance, the lattice-based encryption scheme introduced by Melchor, Gaborit and Herranz allows homomorphic computation of functions expressible as d-operand products of terms, each of which is a sum of inputs. Of particular interest to us is the Boneh-Goh-Nissim partially homomorphic encryption scheme, which allows evaluations of arbitrary 2-DNFs, i.e., functions whose evaluation requires one multiplication per term followed by an arbitrary number of additions of terms. The scheme is based on Paillier's earlier additive partially homomorphic scheme and bilinear pairing. As a consequence, the Boneh-Goh-Nissim scheme allows the secure evaluation of degree-two multivariate polynomials, with dot product computation being a particularly useful primitive arising as a special case. Paillier's scheme is the most efficient among currently known additively homomorphic schemes. Therefore, it is employed by some of our works as a building block or as a basis for comparison.

2. PROPOSED SYSTEM

Elliptic curve (EC) systems as applied to cryptography were first projected in 1985 severally by Neal Koblitz and Victor Miller. Elliptic curve cryptography [ECC] could be a public key cryptosystem. Each user includes a public and a personal key. The application which will be developed allows the user to register and login with the registered credentials while uploading any files to the users public cloud account. This application provides enhanced security to data using Homomorphic Encryption which is best suited for small to medium scale businesses. Elliptic curve cryptography [ECC] could be a public-key cryptosystem. each user includes a public and a personal key. Public secret's used for encryption/signature verification. Personal secret's used for decryption/signature generation. Elliptic curves are used as associate extension to alternative current cryptosystem. that's Elliptic Curve Diffie-Hellman Key Exchange and Elliptic Curve Digital Signature formula.

SignatureGeneration:

1. Calculate e=HASH (m), where HASH is a cryptographic hash function, such as SHA-1
2. Select a random integer k from $[1, n - 1]$
3. Calculate $r = x1 \pmod n$, where $(x1, y1) = k * B$. If $r = 0$, go to step 2
4. Calculate $s = k - 1(e + dAr)(\bmod n)$. If $s = 0$, go to step 2
5. The signature is the pair (r, s)
6. Send signature (r, s) to B cloud.

Encryption algorithm:

Suppose A wants to send to B an encrypted message.

i. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic group.
ii. A chooses another random integer, k from the interval [1, p-1]
iii. The cipher text is a pair of points PC = [(kB), (PM + kPB)]
iv. Send ciphertext PC to cloud B.

Decryption algorithm:

Cloud B will take the following steps to decrypt cipher text PC.

a. B computes the product of the first point from PC and his private key, dB * (kB)
b. B then takes this product and subtracts it from the second point from PC (PM + kPB) – [dB(kB)] = PM + k(dBB) – dB(kB) = PM
c. B cloud then decodes PM to get the message, M.

Signature Verification:

For B to authenticate A's signature, B must have A's public key PA

1. Verify that r and s are integers in $[1, n - 1]$. If not, the signature is invalid
2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate $w = s - 1 \pmod n$
4. Calculate $u1 = rw \pmod n$ and $u2 = rw \pmod n$
5. Calculate $(x1, y1) = u1B + u2PA$
6. The signature is valid if $x1 = r(\bmod n)$, invalid otherwise

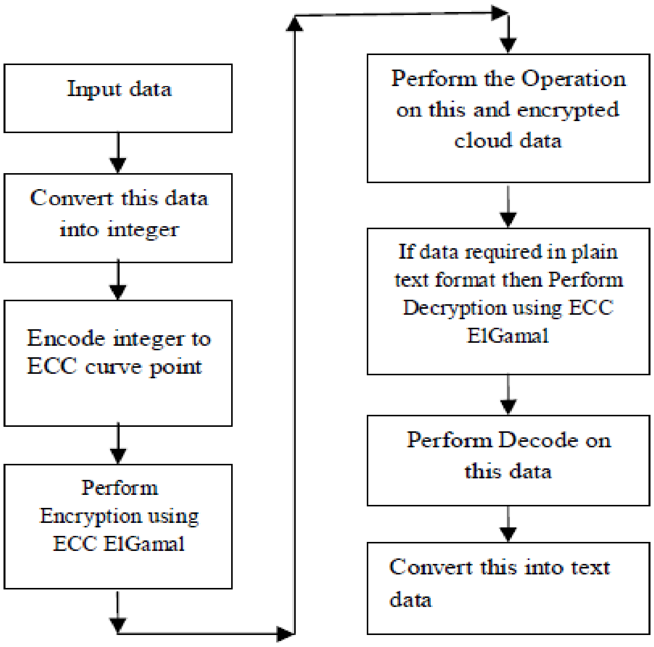
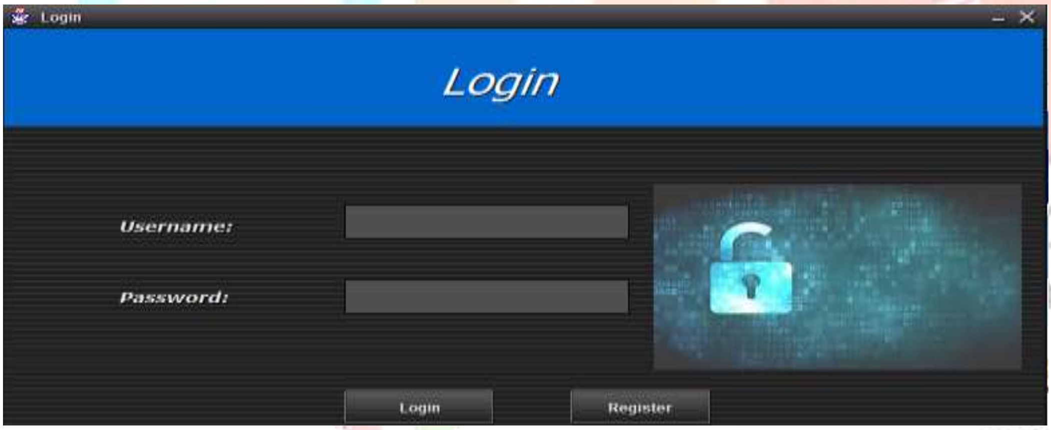
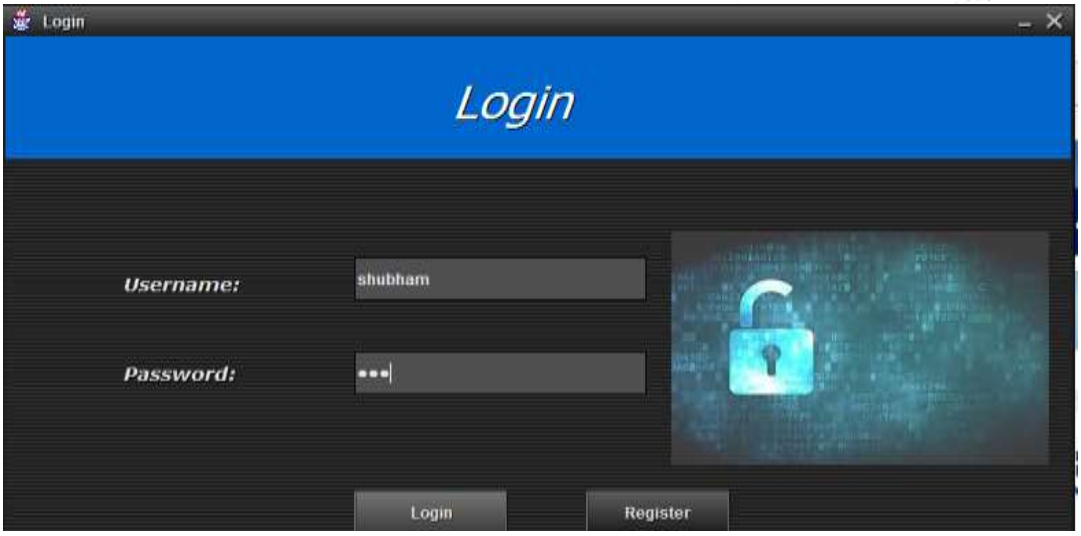

Input data
Convert this data into integer
Encode integer to ECC curve point
Perform Encryption using ECC ElGamal
Perform the Operation on this and encrypted cloud data
If data required in plain text format then Perform Decryption using ECC ElGamal
Perform Decode on this data
Convert this into text data

Fig :ElGamal Encryption System using Elliptic Curve

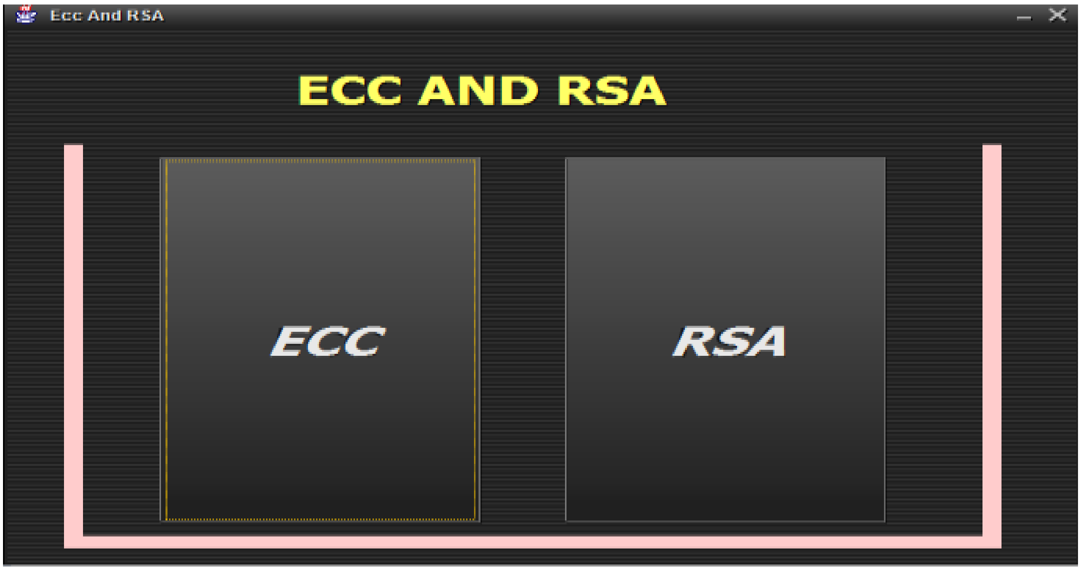
RESULT

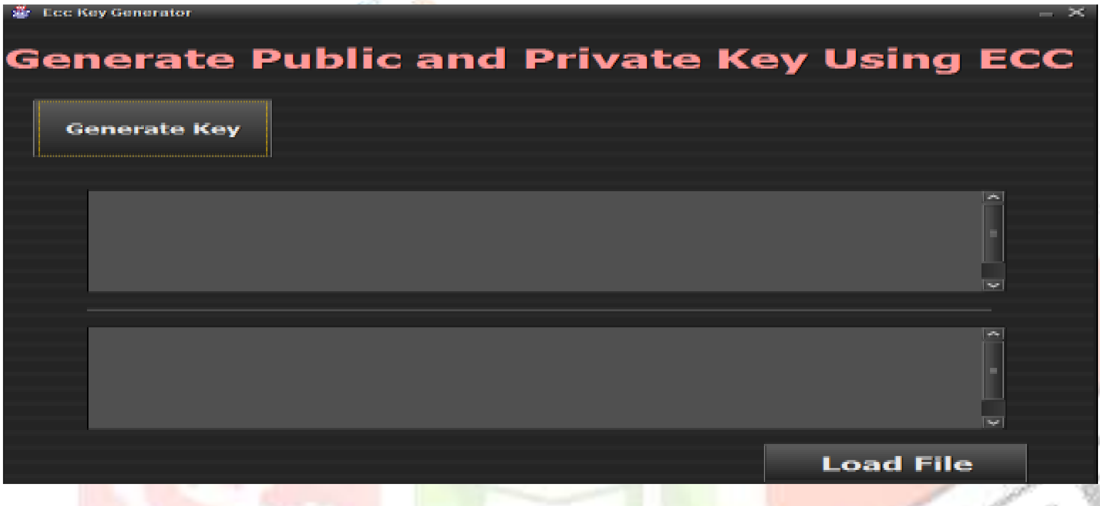


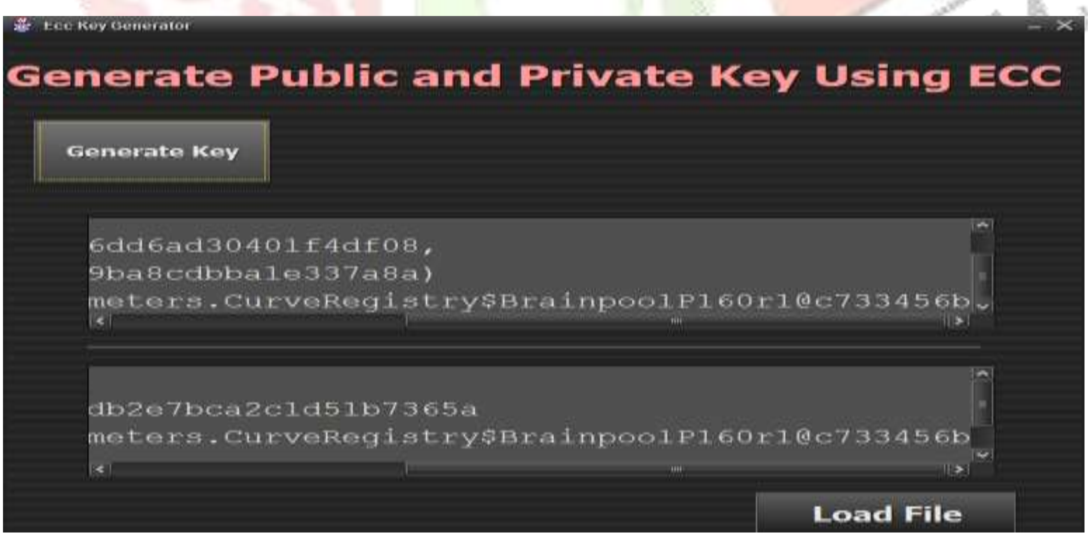


Username: shubham

Password: •••

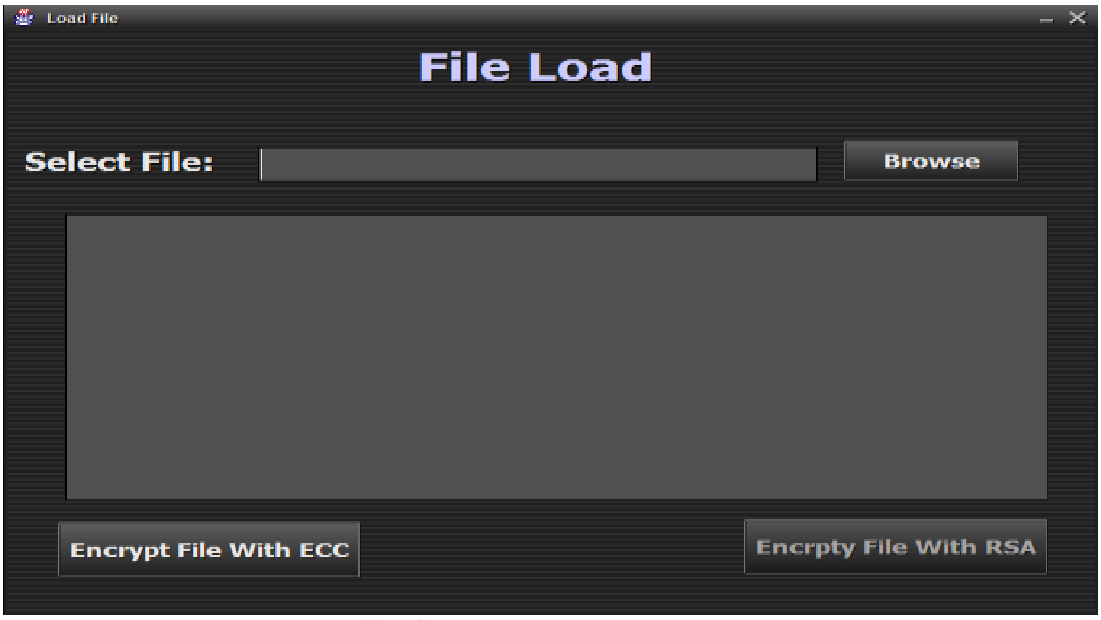


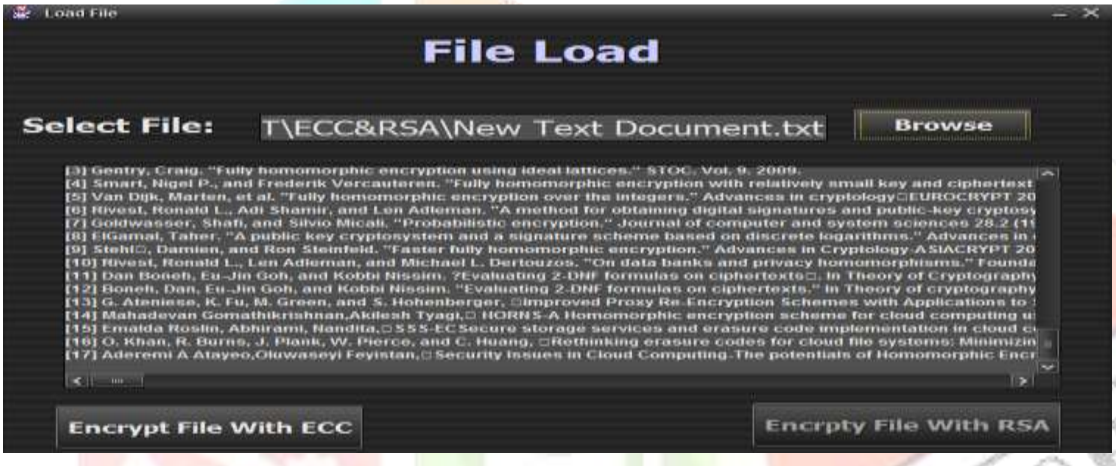




```
6dd6ad30401f4df08,
9ba8cdbba1e337a8a)
meters.CurveRegistry$BrainpoolP160r1@c733456b
```

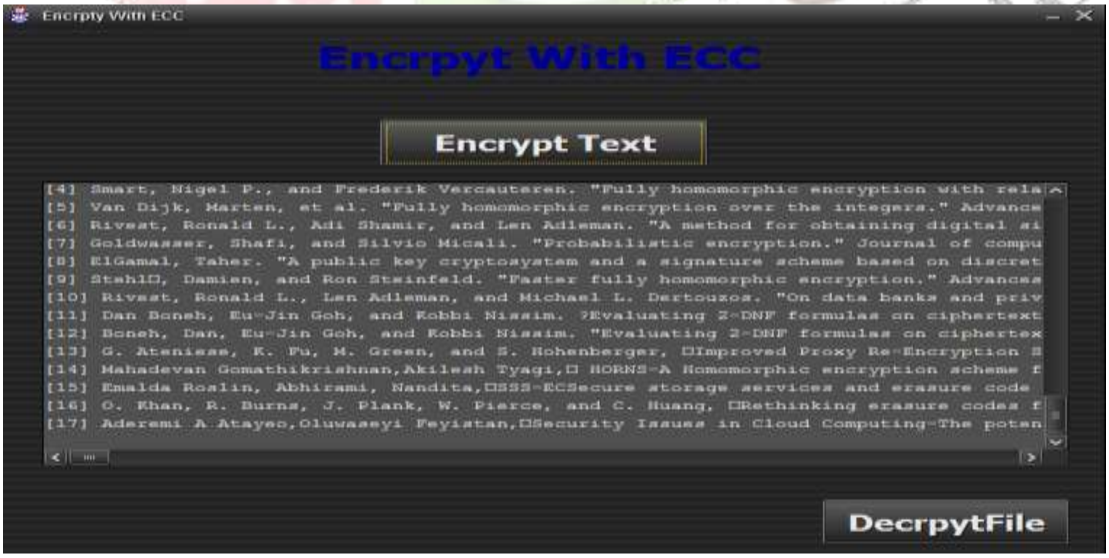
```
db2e7bca2c1d51b7365a
meters.CurveRegistry$BrainpoolP160r1@c733456b
```



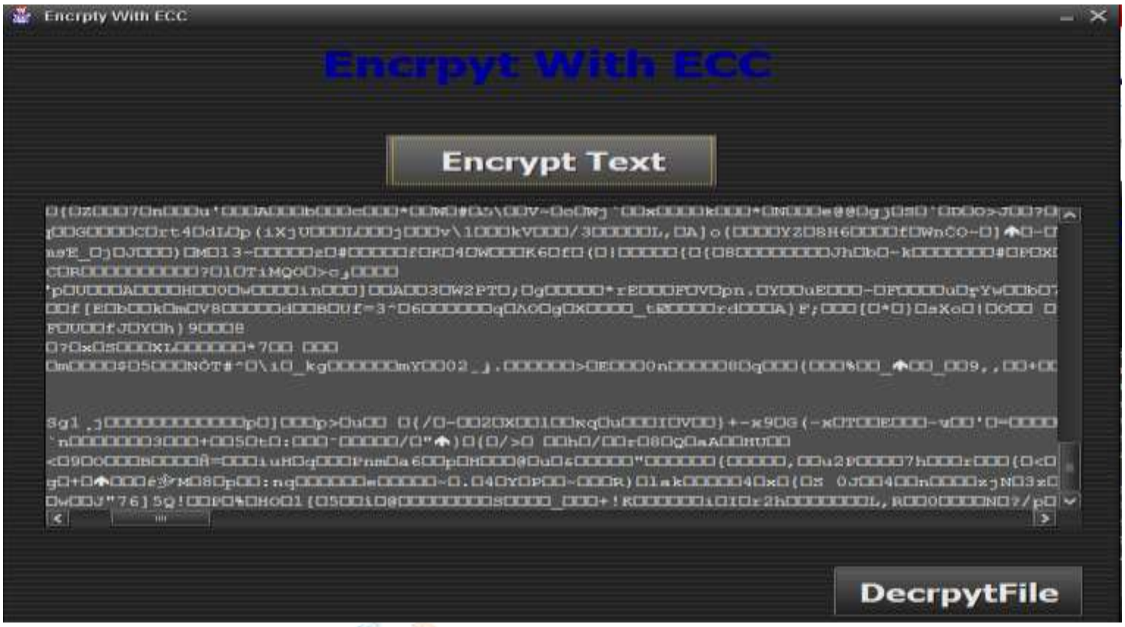


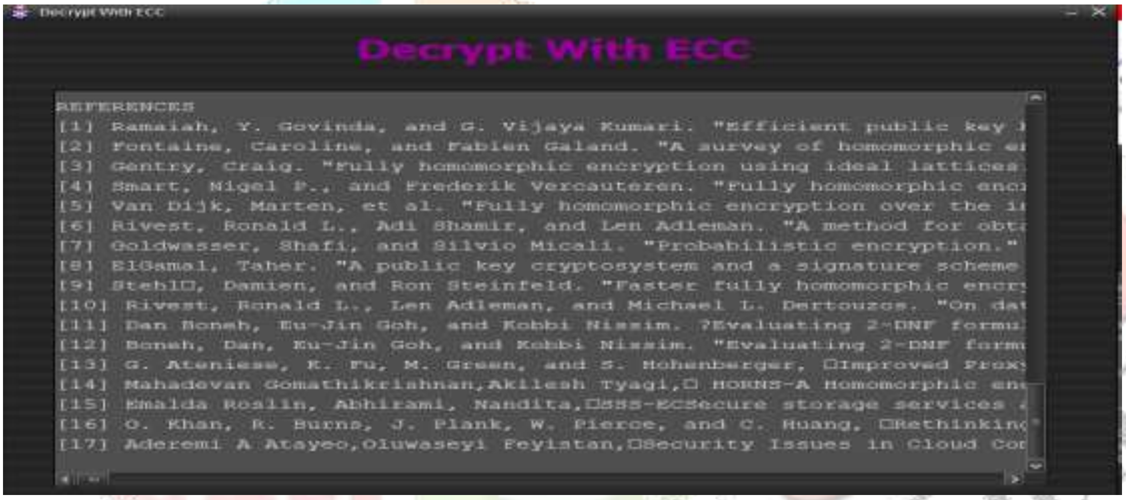
Select File: T\ECC&RSA\New Text Document.txt

```
[3] Gentry, Craig. "Fully homomorphic encryption using ideal lattices." STOC. Vol. 9. 2009.
[4] Smart, Nigel P., and Frederik Vercauteren. "Fully homomorphic encryption with relatively small key and ciphertext
[5] Van Dijk, Marten, et al. "Fully homomorphic encryption over the integers." Advances in cryptology□EUROCRYPT 20
[6] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosy
[7] Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption." Journal of computer and system sciences 28.2 (1
[8] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." Advances in
[9] Stehl□, Damien, and Ron Steinfeld. "Faster fully homomorphic encryption." Advances in Cryptology-ASIACRYPT 20
[10] Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. "On data banks and privacy homomorphisms." Founda
[11] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. ?Evaluating 2-DNF formulas on ciphertexts□. In Theory of Cryptography
[12] Boneh, Dan, Eu-Jin Goh, and Kobbi Nissim. "Evaluating 2-DNF formulas on ciphertexts." In Theory of cryptography
[13] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, □Improved Proxy Re-Encryption Schemes with Applications to
[14] Mahadevan Gomathikrishnan,Akilesh Tyagi,□ HORNS-A Homomorphic encryption scheme for cloud computing u
[15] Emalda Roslin, Abhirami, Nandita,□SSS-ECSecure storage services and erasure code implementation in cloud c
[16] O. Khan, R. Burns, J. Plank, W. Pierce, and C. Huang, □Rethinking erasure codes for cloud file systems: Minimizin
[17] Aderemi A Atayeo,Oluwaseyi Feyistan,□Security Issues in Cloud Computing-The potentials of Homomorphic Encr
```

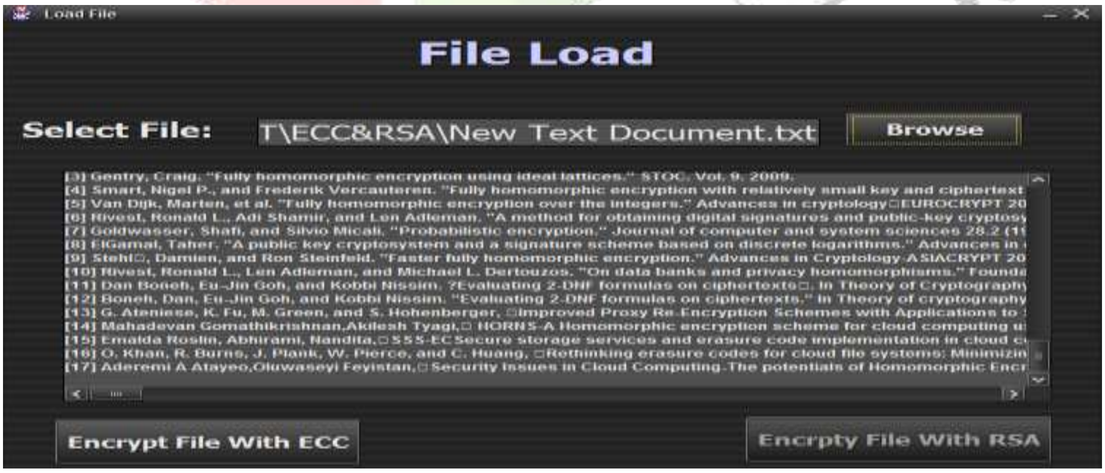


```
[4] Smart, Nigel P., and Frederik Vercauteren. "Fully homomorphic encryption with rela
[5] Van Dijk, Marten, et al. "Fully homomorphic encryption over the integers." Advance
[6] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital si
[7] Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption." Journal of compu
[8] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discret
[9] Stehl□, Damien, and Ron Steinfeld. "Faster fully homomorphic encryption." Advances
[10] Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. "On data banks and priv
[11] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. ?Evaluating 2-DNF formulas on ciphertext
[12] Boneh, Dan, Eu-Jin Goh, and Kobbi Nissim. "Evaluating 2-DNF formulas on ciphertex
[13] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, □Improved Proxy Re-Encryption S
[14] Mahadevan Gomathikrishnan,Akilesh Tyagi,□ HORNS-A Homomorphic encryption scheme f
[15] Emalda Roslin, Abhirami, Nandita,□SSS-ECSecure storage services and erasure code
[16] O. Khan, R. Burns, J. Plank, W. Pierce, and C. Huang, □Rethinking erasure codes f
[17] Aderemi A Atayeo,Oluwaseyi Feyistan,□Security Issues in Cloud Computing-The poten
```





```
REFERENCES
[1] Ramaiah, Y. Govinda, and G. Vijaya Kumari. "Efficient public key 
[2] Fontaine, Caroline, and Fabien Galand. "A survey of homomorphic e
[3] Gentry, Craig. "Fully homomorphic encryption using ideal lattices
[4] Smart, Nigel P., and Frederik Vercauteren. "Fully homomorphic enc
[5] Van Dijk, Marten, et al. "Fully homomorphic encryption over the i
[6] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obt
[7] Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption."
[8] ElGamal, Taher. "A public key cryptosystem and a signature scheme
[9] Stehl□, Damien, and Ron Steinfeld. "Faster fully homomorphic encr
[10] Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. "On da
[11] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. ?Evaluating 2-DNF formu
[12] Boneh, Dan, Eu-Jin Goh, and Kobbi Nissim. "Evaluating 2-DNF form
[13] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, □Improved Prox
[14] Mahadevan Gomathikrishnan,Akilesh Tyagi,□ HORNS-A Homomorphic en
[15] Emalda Roslin, Abhirami, Nandita,□SSS-ECSecure storage services 
[16] O. Khan, R. Burns, J. Plank, W. Pierce, and C. Huang, □Rethinkin
[17] Aderemi A Atayeo,Oluwaseyi Feyistan,□Security Issues in Cloud Co
```



Select File: T\ECC&RSA\New Text Document.txt

```
[3] Gentry, Craig. "Fully homomorphic encryption using ideal lattices." STOC. Vol. 9. 2009.
[4] Smart, Nigel P., and Frederik Vercauteren. "Fully homomorphic encryption with relatively small key and ciphertext
[5] Van Dijk, Marten, et al. "Fully homomorphic encryption over the integers." Advances in cryptology□EUROCRYPT 20
[6] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptos
[7] Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption." Journal of computer and system sciences 28.2 (1
[8] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." Advances in 
[9] Stehl□, Damien, and Ron Steinfeld. "Faster fully homomorphic encryption." Advances in Cryptology-ASIACRYPT 20
[10] Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. "On data banks and privacy homomorphisms." Founda
[11] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. ?Evaluating 2-DNF formulas on ciphertexts□. In Theory of Cryptograph
[12] Boneh, Dan, Eu-Jin Goh, and Kobbi Nissim. "Evaluating 2-DNF formulas on ciphertexts." In Theory of cryptography
[13] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, □Improved Proxy Re-Encryption Schemes with Applications to 
[14] Mahadevan Gomathikrishnan,Akilesh Tyagi,□ HORNS-A Homomorphic encryption scheme for cloud computing u
[15] Emalda Roslin, Abhirami, Nandita,□ SSS-EC Secure storage services and erasure code implementation in cloud c
[16] O. Khan, R. Burns, J. Plank, W. Pierce, and C. Huang, □Rethinking erasure codes for cloud file systems: Minimizin
[17] Aderemi A Atayeo,Oluwaseyi Feyistan,□ Security Issues in Cloud Computing.The potentials of Homomorphic Encr
```

CONCLUSION

In this paper, we propose a secure encryption scheme using elliptic curve cryptography. We empirically evaluated ECC based homomorphic encryption schemes for our proposed scheme and demonstrate that the algorithm performs better. Our secure scheme achieves better efficiency in terms of computation and communication cost as compared to RSA & Paillier scheme. Finally, we use the encryption scheme to calculate the horizontal co seismic deformation and the results prove that the proposed scheme is correct and high efficiency.

REFERENCES

[1] Ali, A. 2001.Macroeconomic variables as common pervasive risk factors and the empirical content of the Arbitrage Pricing Theory. Journal of Empirical finance, 5(3): 221–240.

[2] Basu, S. 1997. The Investment Performance of Common Stocks in Relation to their Price to Earnings Ratio: A Test of the Efficient Markets Hypothesis. Journal of Finance, 33(3): 663-682.

[3] Bhatti, U. and Hanif. M. 2010. Validity of Capital Assets Pricing Model.Evidence from KSE-Pakistan.European Journal of Economics, Finance and Administrative Science, 3 (20).