JES
Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

AN UPGRADED VERSION OF DATA PROTECTION COMBINED WITH CRYPTOGRAPHY

Adiba Firdous[1], Dr. Mohammed Sanaullah Qaseem[2]

[1]PG Scholar, Dept of CSE, Nawab Shah Alam Khan college of Engineering and technology, Hyderabad, TS.
adibafirdous507@gmail.com

[2]Professor, Dept of CSE, Nawab Shah Alam Khan college of Engineering and technology, Hyderabad, TS

Abstract: Information Security has constantly been an amazingly noteworthy angle with respect to forestalling unapproved access, destruction or examination of ordered data. Today every field on the planet uses sight and sound information. There is need to confirm the arranged information used in these zones. There are different approaches to manage secure information. One of them is Homomorphic Encryption (HE), which is the main hiding the information inside other data with the ultimate objective that there is no perceptible change in spread information. The assistant strategy for confirming information is cryptography, an encryption framework which scrambles the information into a wrote structure which is overall insinuated as figure. Both Homomorphic Encryption and Cryptography have their own one of a kind ideal conditions and limitations. Regardless of the way that the two techniques offer security, to incorporate various layers of security it is constantly a respectable practice to use Cryptography and HE together. So when cryptography and HE are used together, it results in multi-layer security model. The key objective of the proposed work is to give extra layer of security by showing cryptography nearby HE to encode and embed the mystery information to be sent over a non-secure channel.

I. INTRODUCTION

Cryptography, an encryption procedure which disarrange the data into some specific structure with the goal that lone expected client can peruse and process it. Homomorphic Encryption is demonstration of concealing messages so that the main beneficiary can make out the presence of the message [1]. Cryptography and Homomorphic Encryption got little consideration in registering. Numerous figures to be demonstrated powerless against the cryptanalytic assaults and numerous stega-methods are effectively noticeable. Subsequently the need emerges to give better security by joining these two methods. Here, if there should be an occurrence of bombing the Homomorphic Encryption framework, discharge message stay safe as a result of encoding system. Homomorphic Encryption isn't a trade for cryptography but instead to enhance it. The proposed model gives a double layer of security where cryptography and Homomorphic Encryption structure the internal and external layers of security individually. It primarily comprises of four phases to be specific encryption, implanting, extricating and unscrambling. Encryption and Embedding is finished by the sender where the mystery information is first scrambled utilizing a cryptographic calculation to change over the plain content into a figure, after which the figure is inserted into the spread record to conceal its quality as appeared in figure 1. This paper is on the correlation of Homomorphic Encryption calculations LSB and RDH with the execution of cryptography as an external layer.

II. OVERVIEW OF CRYPTOGRAPHY

This area gives various types of cryptography systems like AES, DES, RC4, RSA and Homomorphic Encryption methods like picture, sound, video, system and content Homomorphic Encryption.

- **CRYPTOGRAPHY**

Symmetric Key Algorithms [4]: In this calculation, a similar key is utilized by transmitter and the recipient to scramble and unscramble the message individually.

- **RC4**

RC4 is a symmetric key stream figure created by Ron Rivest. It is notable for its effortlessness and speed in its product. It utilizes variable key length commonly somewhere in the range of 40 and 2048 bits. Here the information stream is XORed with the created key arrangement.

- **AES**

AES otherwise called Rjindael's calculation. AES is a symmetric square figure planned by Vincent Rijmen and Joan Daemen distributed in 1998. The variable key length are 128, 192 and 256 bits. Two sorts of hashing calculations can be utilized in particular: SHA1 (Secure hashing Algorithm 1) Digest Size: 160 bits, Block Sizes: 512 bits, Rounds: 80 and MD5 (Message Digest 5) Digest Size: 128 bits, Block Sizes: 512 bits, Rounds: 4

- **3DES**

The triple data encryption algorithm (TDEA) is a Symmetric key square figure. It applies DES (Data

Encryption Standard) multiple times to every datum square. It utilizes a Key pack that comprises of 3 keys K1, K2, AND K3 each 0f 56 bits. DES is universal, simple to actualize in both equipment and programming. Deviated Key Algorithm: In this calculation the sender and the client utilize distinctive keys to encode and unscramble. The deviated key we utilized here is RSA.

- **RSA**

RSA is a public-key cryptosystem, asymmetric key algorithm. RSA is developed by Ron Rivest, Adi Shamir,
and Leonard Adleman in 1977. Here sender and receiver use different keys to encrypt and decrypt.

III. METHODOLOGY

In the proposed work, the confidential text will be encrypted with the AES encryption and the key, which will be used for decryption, by using following modules:

- Admin
- Application Owner
- Broker
- User

➢ **Admin**

Administrator is the main module. Administrator login and make the numerous mists as indicated by details. He will make dealer for each cloud. Administrator can compute the nature of administration, security of administration and asset assignment. Discover the hazard examination between various applications.

➢ **Application owner**

Application proprietor is the subsequent module. First he will enroll and login. After login he can demand for numerous mists to the application then he will contact the merchant's of each cloud and send particulars and view principle insights regarding agent. On the off chance that any client demand for the application he can affirm the client. Give administration to the client as indicated by the application.

➢ **Broker**

Specialist is the third module of the venture. Specialist is the middle person among cloud and application proprietor. He can see the application proprietor solicitation and particulars. He will advance the solicitation to administrator and reaction from administrator to application proprietor.

➢ **User**

Client is the fourth module of the venture. First client will enroll with various applications and login. Client can use the administrations of the application and client can store or share the information as per the mists which is accessible to that application. Client subtleties and data is verified dependent on the security levels given by the application.

Sequence Diagram:

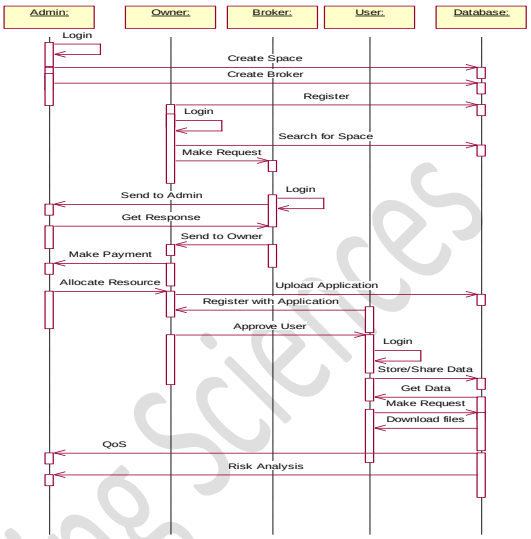

Fig. 1. Sequence Diagram

System Architecture

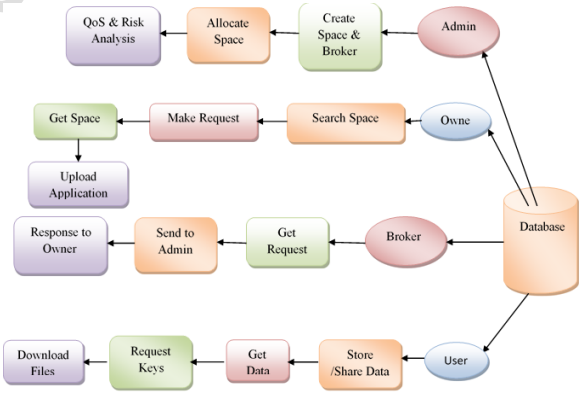

Fig. 2. System Architecture

IV. RESULT

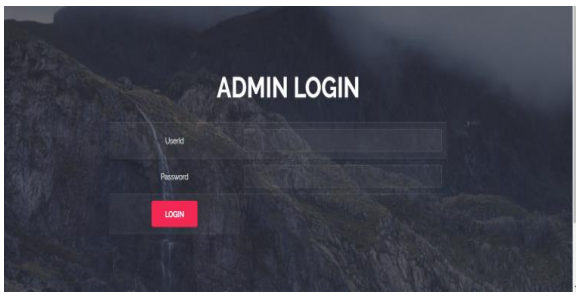

Fig. 3. Admin Login Page

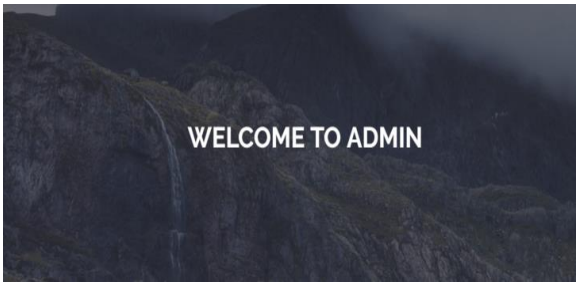

Fig. 4. Admin Welcome Page

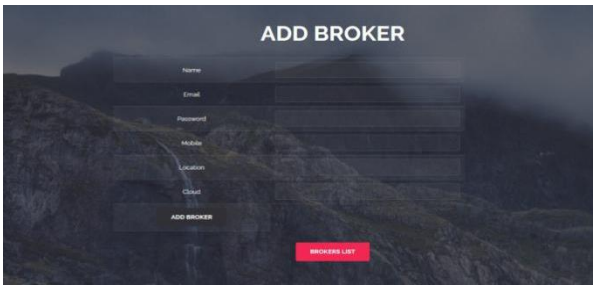

Fig. 5. Add Broker

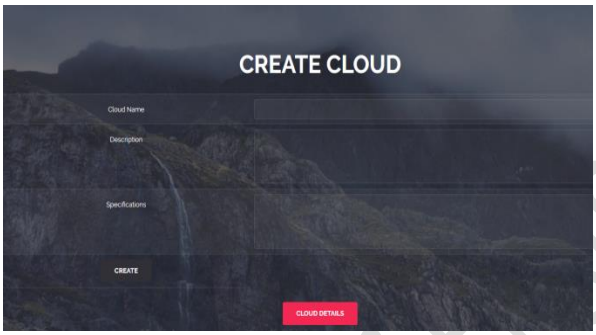

Fig. 6. Create Cloud Page

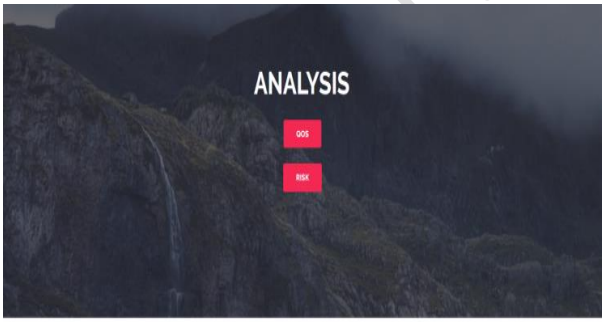

Fig. 7. Admin Analysis Page

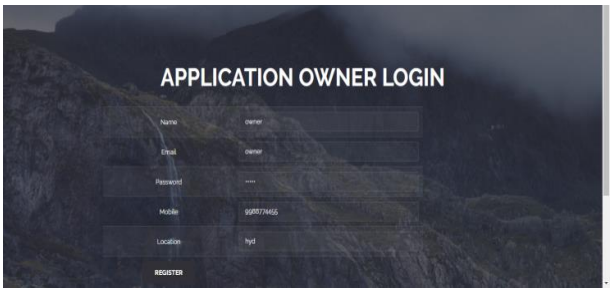

Fig. 8. Application Create Page

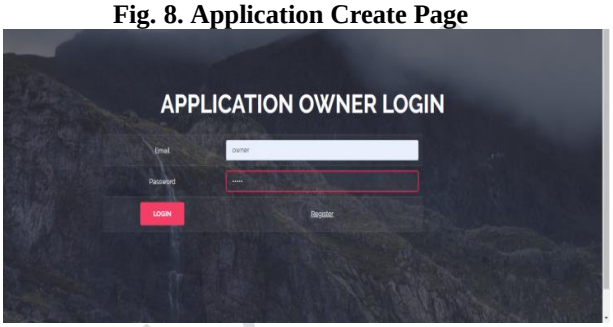

Fig. 9. Application Owner Login Page

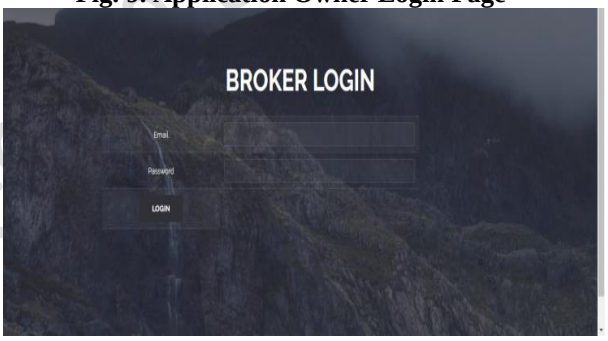

Fig. 10. Broker Login Page

V. CONCLUSION

Today, HE isn't executed in progressively broad ways anyway it might be used as the best security mechanical assembly. The standard issue of the present world is to check their private information; the methodologies used at present are either cryptography or HE, are not capable to confirm this information. Proposed count includes the usage of cryptography with HE by giving stunned security to the mystery data. Assessment of LSB, RDH and Improved RDH counts with twofold security model is viewed. The proposed count gives better results for concealing pictures in double level security.

In spite of the way that the image quality can be secured with high PSNR, visual quality can scarcely be improved. By definitely viewing the visual quality, the technique of RDH can be better improved to achieve the more pleasant results.

REFERENCES

[1] CERN Large Hadron Collider Computing Grid - http://wlcg.web.cern.ch.

[2] The iPlant Collaborative: Cyberinfrastructure for Plant Biology - http://www. iplantcollaborative.org.

[3] University of Missouri Electron Microscopy Core Facility - http://emc.missouri.edu.

[4] W. Kim, P. Sharma, J. Lee, S. Banerjee, J. Tourrilhes, S-J. Lee, and P. Yalagandula, "Automated and Scalable QoS Control for Network Convergence", *Proc. of ACMINM/WREN*, 2010.

[5] R. B. Antequera, P. Calyam, S. Debroy, L. Cui, S. Seetharam, M. Dickinson, T. Joshi, D. Xu, and T. Beyene., "ADON: Application-Driven Overlay Network-as-a-Service for Data-Intensive Science", *IEEE Trans. on Cloud Computing*, 2016.

[6] C. Irvine,T. Levin, "Quality of Security Service", *Proc. of Workshop on New Security Paradigms*, 2000.

[7] S. Lindskog, "Modeling and Tuning Security from a Quality of Service Perspective", *PhD Thesis*, Chalmers Univ. of Tech., 2005.

[8] E. Dart, L. Rotman, B. Tierney, M. Hester, J. Zurawski, "The Science DMZ: A Network Design Pattern for Data-Intensive Science", *Proc. of IEEE/ACM Supercomputing*, 2013.

[9] "Security and Privacy Controls for Federal Information Systems and Organizations", *NIST SP800-30 Technical Report*, 2013.

[10] W. Pieters, T. Dimkov, D. Pavlovic, "Security Policy Alignment: A Formal Approach", *IEEE Systems Journal*, Vol. 7, No. 2, pp. 275-287, 2013.