Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Elliptic Curve Cryptography Based Homomorphic End-to-End Encryption Security in Cloud Computing

A Secure Multiparty Data Sharing Networks Using Homomorphic Cryptography

Dr. G N Kodanda Ramaiah,
Professor, Dept. of E&CE,
Kuppam Engineering College, Kuppam, India,
gnk.ramaiah@gmail.com
Savita A Harkude
Research Scholar, Dept. of ETE,
Sir MVIT, Bangalore, India,
savita.harkude@gmail.com

Article Info
Page Number: 64 – 75
Publication Issue:
Vol. 71 No. 3s (2022)

Article History
Article Received: *22 April 2022*
Revised: *10 May 2022*
Accepted: *15 June 2022*
Publication: *19 July 2022*

Abstract

Cloud computing is turning into the principal computing model in the future because of its benefits, for example, high asset use rate and save significant expense of execution. The existing algorithms for security issues in cloud computing are basically advanced version of cryptography. Mainly cloud computing algorithm are concerning about data security and privacy preserving of user. To protect the privacy of data owner and data user the cryptographic data are shared and stored in cloud storage by applying HE-homomorphic encryption. According to environment of HE, this paper proposed a new hybrid algorithm by combining the two algorithms of cryptography i.e., AES and ECC with the concept of splitting algorithm. By the implementation of this hybrid algorithm, we will split any file into binary version and then after processing the cryptography technique. This hybrid algorithm provided higher protection against attacks over cloud storage and data sharing.

Keywords— Cloud computing, data security, Elliptic Curve Cryptography, Homomorphic encryption, Secure Multiparty Computation,

I. INTRODUCTION

In current conventional framework, there exist security issues for storing the information in cloud. Cloud computing security incorporates different issues like data loss, authorization of cloud, multi occupancy, inner threats, spillage, and so forth it isn't not difficult to carry out the safety efforts that fulfils the security needs of the all of clients. It is on the grounds that clients might have dissimilar security concerns relying on their motivation of utilizing the cloud services. Cloud service provider (CSP) has given a brilliant security layer for the owner

and user. The client needs to guarantee that there is no deficiency of information or misuse of information for different clients who are utilizing a similar cloud. The CSPs should be equipped for receiving by against digital assaults. Not all the cloud suppliers have the capacity of data protection. Different techniques are being carried out to annihilate the security issues in cloud storage of data. [1]

Customary models of information security have regularly centred around network-driven and perimeter security, often with tools such as intrusion detection systems and firewalls. However, this methodology doesn't give adequate protection against APTs, special clients, or other guileful kinds of safety attacks. [2] The encryption execution should join a robust key management solution for give affirmation that the keys are adequately secured. It's basic to review the whole encryption and key administration arrangement. Encryption works working together with other centre information security innovations, gleaning increased security intelligence, to deliver an inclusive hybrid approach to deal with ensuring sensitive information in or out of the cloud. [3]

Subsequently, any information driven methodology should combine encryption, key management, compact access controls, and security insight to ensure information in the cloud and give the imperative degree of safety. [4] By employing a hybrid approach that incorporates these basic components, associations can further develop their security posture more viably and effectively than by only concerning in solely on conventional organization driven security techniques. [5]

The Major Objectives of this paper are:

- To develop an enhanced technique for data protection in the Cloud
- To overcome the Challenges of Cloud Computing Security
- To develop a better strategy for secure data sharing through the Cloud.

The paper is divided into mainly six sections. Section one deals with introduction to research work with explanation of basic concepts in brief. Second section is about the related work that reviewed the existing studies which are useful as an exploratory data for the research work, and to evaluate the review for new framework designing. The third section deals with the explanation of proposed work used in the research study. In this section mainly the proposed methodology and algorithm research is explained. The fourth section described about the simulation designing and framework designing. In fifth section result are presented on basis of simulation factors as processed in section 3. Last section 6 contains conclusion of paper and future recommendations of the proposed work.

II. RELATED WORK

Cryptography is a technique for covering data to conceal it from unapproved clients [6]. Communicated information is clouded and delivered in a ciphertext design that is inexplicable and unreadable to an unauthorised user. A key is used to change figure text to plain text. This key is kept private and just authorised client can approach it [7]. Encryption is one of the safest ways to avoid MitM attacks because even if the transmitted data gets

intercepted, the attacker would be unable to decipher it. There exist information-theoretically secure schemes that probably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

The Shamir techniques[8] is utilized for image encryption and decoding using steganography. In first phasee Shamir techniques is encoding the original image. It is used for the encrypted the data. Boundary scanning techniques is used for the data hiding in a such way that hackers cannot hack the confidential data.

The algorithm uses[9] two secret keys are utilized for encryption and decode of data which we input it to. One for cover image and other for information. At first the image is uploaded and afterward it is encoded the image we input it by utilizing a secret key.

AES [10] utilizes the different variable key length as of 128bit, 192bit and 256bit. It performs Shift row transformation, SubBytes transformation, Add round keys and Mix columns with a simple bit wise XOR operation b\w state and round key.

RSA[10] has greater usefulness and AES is a lot quicker, it is smarter to consolidate these two: asymmetric cryptograph can be utilized to verify the parties and to concur on a key for symmetric encryption. Enormous information blocks are encoded utilizing faster AES calculation instead of slower RSA and securely appropriated utilizing RSA algorithm.

Elliptical curve cryptography[11] (ECC) depends on a public key cryptosystem put together that is with respect to elliptic curve hypothesis. ECC verification conspire is more appropriate for remote interchanges, similar to cell phones and smart cards, individual data like monetary exchange or some secret clinical reports, classified information where fundamental thought is to give secure information. ECC can be utilized to make more modest, quicker, and more effective cryptographic keys.

III. PROPOSED WORK

The Proposed system has its major aims towards confidentiality of data. In traditional ways the data is not stored on cloud in encrypted form because it will be needed at the time decryption process. In general, homomorphic encryption user can be able to execute computation on encrypted data. But in this work, it focuses on homomorphic encryption using ECC scheme. In proposed homomorphic encryption plot the size of code text is impressively decreased because of its smaller key size with same degree of safety like RSA. It propose ECC based homomorphic encryption plot for Semi Morphic Cryptography (SMC) issue that is drastically diminished reduced communication and computation cost. It shows that the scheme has advantages in communication consumption, privacy preservation and energy consumption. This strategy is blend of multiplicative homomorphic encryption calculations alongside binary splitting of data. [12]

A. Proposed Model

The proposed algorithm is an endeavour to introduce another methodology for complex encoding and decoding information dependent on equal programming so that the new

methodology can utilize numerous centre processor to accomplish higher speed with more significant level of safety. [13]

1. Encryption: In this process the information is transformed into such kind of data so that it is unintelligible to anyone but only to the envisioned recipient.
2. Decryption: In this process the encrypted information is transformed into the form of information so that it is intelligible again. Both encryption and decryption are the combined processes of cryptographic algorithm, The encrypted text is also called a cipher.
3. Splitting: this algorithm is the main core part of strategy used in this work for cloud security. Splitting algorithm divides files into more or at least two parts which don't have direct association with one another, but the parts of files must be accessed by the only data owner. And even the split parts of file must be recombined with one-another to get the original data.

With most current cryptography, the capacity to maintain encoded data secret is put together not with respect to the cryptographic calculation, which is generally known, yet on a number considered a key that should be utilized with the cryptographic algorithm to deliver an encoded result or to decode the encoded data. Decryption with the right key is basic. Decoding without the right key is undeniably challenging, and sometimes for all practical purposes. The work shows the areas that follow the present the utilization of keys for encoding and decoding. [14]

- Public-Key Encryption
- Symmetric-Key Encryption
- Key Length and Encryption Strength

B. Proposed architecture

The main important thing in this work is to ensure and maintain data storage security and data sharing security over cloud. The proposed architecture of the work performs the following steps as shown using (Fig. 1):

1) Initiate the implementation process
2) Take the data to upload over the cloud.
3) Encrypt the data using hybrid i.e., AES and ECC combined cryptography algorithm.
4) Store the encrypted file over cloud storage database as per data owner account with secret key.
5) Split the content of the data file uploaded in user account in binary version i.e., 0, 1 and store it over cloud or transfer into the receiver.
6) Receive the binary parts of file and join them using their split keys.
7) Perform clubbing (recombination of spilt files) and generate encrypted data.
8) Perform decryption using hybrid cryptography and generate the original message using the secret key shared only with authorized users.
9) End the process.

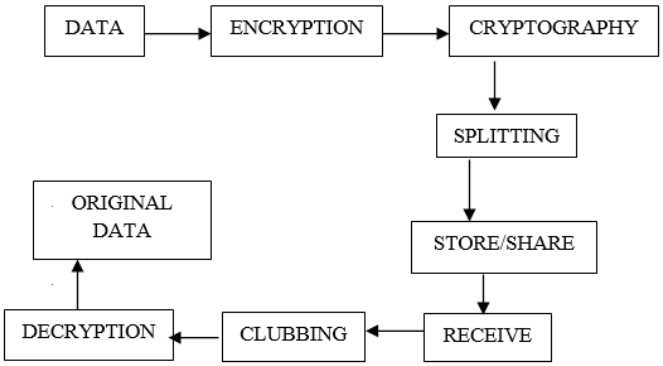

Fig.1: Flow chart of block diagram of proposed process

C. Proposed algorithm

After applying cryptography, the file wherein information is covered up is parted into "k" numbers and put away in arbitrarily selected servers.

These data sharing techniques depend on coding datasets into a binary (0,1) structure and afterward dividing this coded information among a selected group of secret users, every one of whom gets one portion of the split secret. The method of distributing the split information between participants is determined by the selected cryptographic algorithm. To recreate the split data, the endorsement of all members is needed, as is the combination of all shares of the split secret aimed at reconstructing the split information. After the data is recreated, there follows a course of decoding the data from the binary structure to the original form. [15]

Problem: A secret data D must to be divided into multiple parts such that information of “k” number of parts is required to recreate the secret data D.

Algorithm: File splitting and combining

In proposed algorithm, the original data is divided into different portions then encrypt it and shared it into different cloud. Then the divided part of data is recombined into original data and decrypted to original data using keys. Meta data required for searching the file parts.

The splitting and combining is done through the following steps

1. Initiate the process by uploading the document in the cloud.
   Upload a document by a user name: Monitor
   e.g., uploaded document: Test.doc
2. Accept document name and secret key
   e.g., Name of document: Test.doc
   Password: 12345
3. Generate special random number from the secret key, which fills in as the key.
   e.g., Secret key: Tes12

4. Split the document and the key into 2 parts as binary form of 0, 1.
   File splitting into two as
   Name: Monitor0, Monitor1

Secret keys: Tes1, Tes2 respectively

5. Encrypt the split part of the file with the split parts of the keys respectively.
   File encryption is done and stored in cloud.
6. Combine the splits to get the file.
   To download the original file, combine the splits parts of file using their respective split keys. And perform the decryption using secret key and then combine the spilt files into original document.
7. End

IV. SIMULATION FRAMEWORK

As per proposed scenario experimental setup is designed in three modules of cloud network for each user. The simulation framework of the proposed work is designed as per setup of the dynamic network using Python in software PyCharm 2021.2.1 and cloud server WampServer.

A. Experimental Design

On the basis of the process given in technique, we will add the splitting technique with cryptography to optimize and derive the improved security in data sharing. A parallel event driven test framework, PyCharm 2021.2.1 using WampServer was utilized for deriving the expected results of proposed model. The usage comprises of well-ordered configuration. Find the modules below:

Module 1

- The client will send access request to cloud server from client machine. A connection is established between sender and receiver using cloud network.

Module-2

- Login- The login page will help user and the admin to sign-in to system with username and password that is authorized by server.
- Key Selection- The key selection is done based on user logged into the system with encryption and decryption of data.
- Uploading- Here the user will select the file to be uploaded into the system with proper credentials.
- Computations –On the basis of file selected, computations are executed and outcomes of execution are moved to encryption components.
- Encrypt and store- The encryption is performed on the user data or system executed data are stored in cloud.

Module-3

- Splitting: In this phase the file uploaded by user will be split into two parts as per binary version of algorithm
- Decrypt- Using the secret or private key provided by server and shared to both sender and receiver the encrypted file with be decrypted by user to its original content.

- Clubbing: In this section once the file is decrypted the split file will be combined to original file.
- Retrieve- This section displays the data requested by the user at the clients end by retrieving the same from the cloud store.

B. Experimental scenario

Experimental scenario using python implementation:

Experimental scenario shows the process of implementation of proposed algorithm in PyCharm and cloud storage in dataset

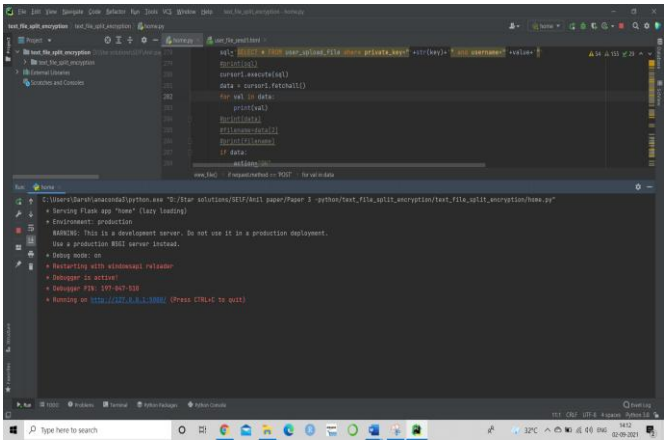

Fig.2: Implementation of proposed algorithm in PyCharm

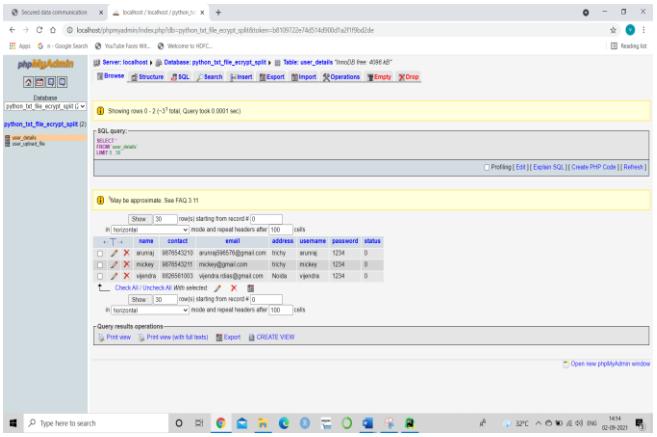

Fig.3: Users and admin details in Cloud storage

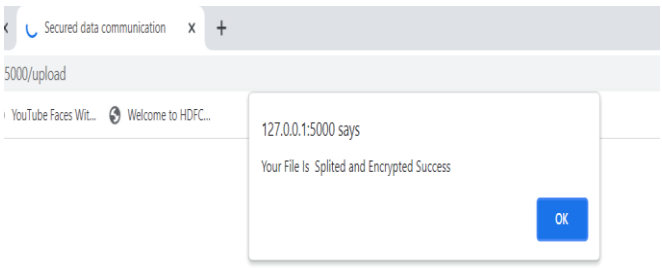

Fig.4: Backend message of Splitting process

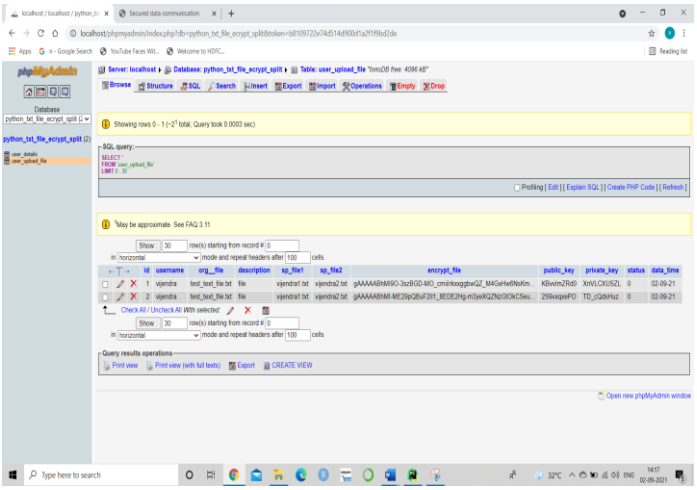

Fig.5: Binary version of files splitting stored in cloud storage

V. RESULT

Simulation results have demonstrated the process of proposed work by taking an example prototype as shown in below figures. The results shown are as below

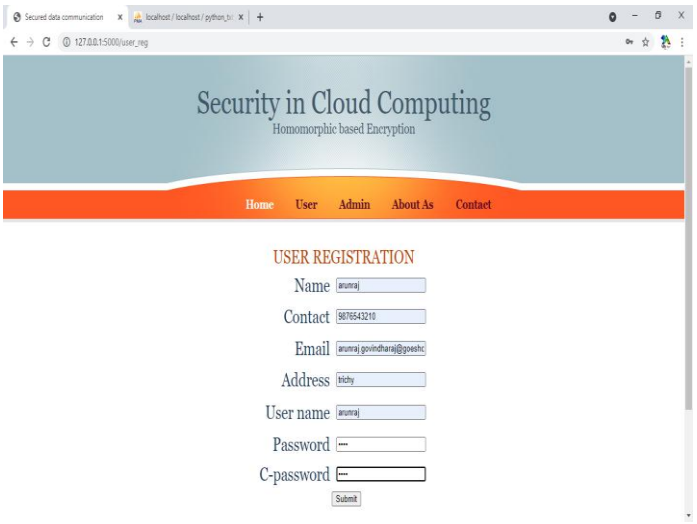

Fig.6: User registration page

After user registration user will login to his account by using registered username and password. After login user can transfer data to sender through uploading it to cloud.
Upload file select your folder any text file

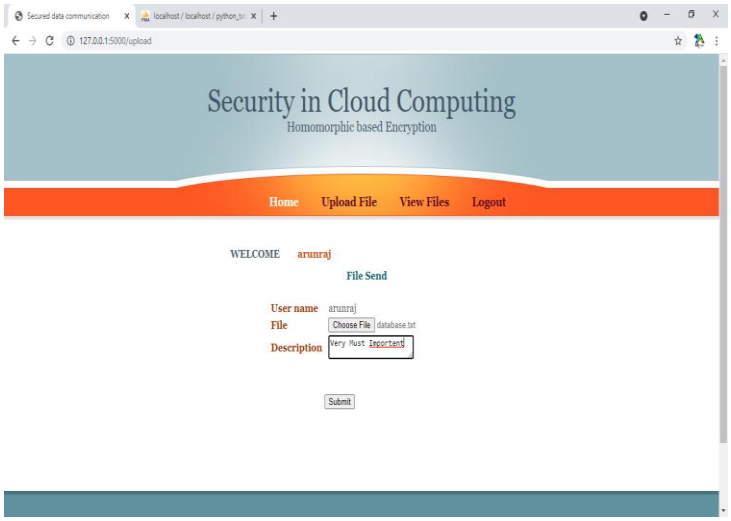

Fig.7: any database file uploading by user

After receiving “Upload success” pop-up message

View: List of uploaded database files with their decryption link

Click on decrypted link private key put the field. Finally output show encrypted file and original file. Check the encrypted file using private key

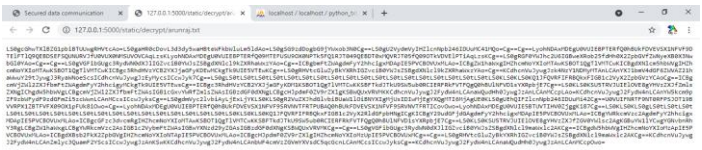

Fig.8: Output of Encrypted file on uses end

Original file

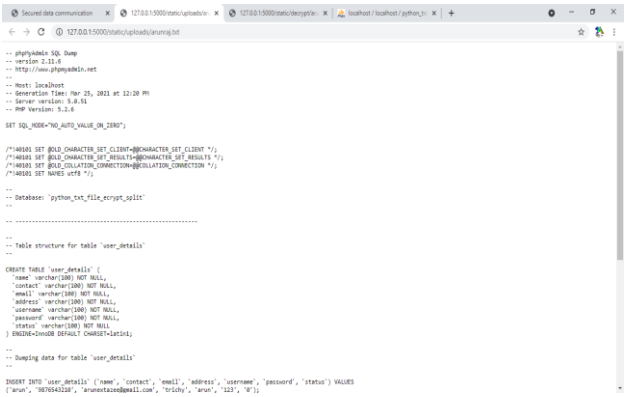

Fig.9: Output of original file

Admin pages

Fig. 10: Admin view of uploaded file details by user

Fig.11: List of encrypted files on website

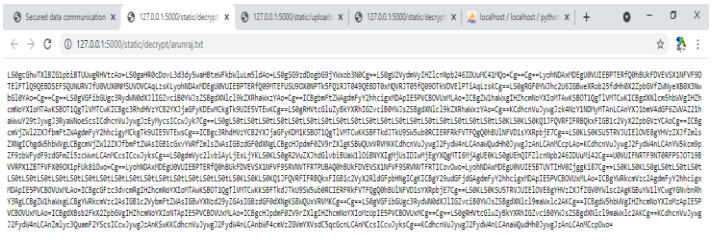

Fig.12: Output of encrypted files server end

VI. CONCLUSION

In cloud computing security the basic algorithm used for generating keys using cryptography are AES and RSA. Although the symmetric algorithms which encapsulate the operations (like searching over metadata) in decrypted content are needed for cloud computing security activities. These algorithms also enhanced by maintaining the confidentiality of the content and the user. Security is a significant prerequisite in distributed computing while we talk about data storage. There are number of existing procedures used to carry out security in cloud. In this paper the work proposed a new hybrid algorithm by combining the two algorithms of cryptography i.e., AES and ECC with the concept of splitting algorithm. This hybrid algorithm provided higher protection against attacks over cloud storage and data sharing. By the implementation of the hybrid algorithm, we will split any file into binary version and then after we process the encryption and decryption technique using security keys.

In this paper, our main concern is to enhance the data confidentiality and by implementing splitting algorithm we are doing that. For future work will be considering some problems related to time and cost calculation and comparisons to other existing algorithms

.

REFERENCES

[1] Felix Bentil, Isaac Lartey “Cloud Cryptography - A Security Aspect” International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 10 Issue 05, May-2021

[2] Deepak Jain & Nidhi Singh, “Providing Security using Encryption and Splitting Technique over Cloud Storage” International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, June, 2018

[3] Lidia Ogiela, “Cryptographic techniques of strategic data splitting and

[4] secure information management” AGH University of Science and Technology, Cryptography and Cognitive Informatics Research Group, 30 Mickiewicza Ave., PL-30-059, 2015

[5] Nikita Dhule et al, “Secret Splitting Scheme: A Review” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 59-64

[6] Stallings, William. Cryptography and Network Security (6^{th} Edition). Pearson, 2014

[7] Ravikumar M.Raypure, Vinay Keswani "Implementation For Data Hiding Using Visual Cryptography " International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Vol. 04 Issue: 07 July -2017

[8] Aiswarya pradeep, D Vinotha "Data Hiding in Image Encryption by using Logistic Mapping Algorithm " International Journal of Engineering Science and Computing, Vol. 7 Issue No.4, April 2017

[9] Abdullah Al Hasib, Abul Ahsan Md. Mahmudul Haque " A Comparative study of the Performance and security issues of AES and RSA Cryptography " Third 2008 International Conference on Convergence and Hybrid Information Technology, Vol. 5, Issue. 2, pp.91 – 95, 2008

[10] Himja Agrawal, Prof.P.R.Badadapure "A Survey Paper On Elliptic Curve Cryptography " International Research Journal of Engineering and Technology (IRJET) e ISSN: 2395 -0056 Vol. 3 Issue: 04 | Apr-2016

[11] J.N., Aws and Z.F. Mohamad. Use of Cryptography in Cloud Computing. Conference Paper published in IEEE November 2013.

[12] Sayli Tambe, Dattaram Naik, Vaibhav Parab, Siddhesh Doiphode "Image Steganography Using Uniform Split and Merge Technique" 2017 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS), Vol. 2, Issue. 2, pp.39 – 41 may 2017

[13] P. Garg, M. Sharma, S. Agrawal and Y. Kumar, "Security on Cloud Computing Using Split Algorithm Along with Cryptography and Steganography" nternational Conference on Innovative Computing and Communications, Lecture Notes in Networks and Systems 55, Springer Nature Singapore Pte Ltd. 2019

[14] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati " A new modified version of AES based algorithm for image encryption" 2018 International Conference on Electronics and Information Engineering (ICEIE 2018), Vol. 4, Issue. 3, pp.161 – 165, 2018

[15] Muthulakshmi P, Shathvi K, Aarthi M, Seethalakshmi V (2016) Encrypted image with hidden data using AES algorithm. Int J Sci Eng Technol Res (IJSETR) 5(4) ISSN: 2278-7798