IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 3, Ser. II (May. – June. 2023), PP 33-40
www.iosrjournals.org

Integrated Framework Of AES, RSA And Steganography Technique For Data Security

[1]Yash Thakur,[2]Sunita Joshi,[3]Dr.Arvind Kumar, [4]Jassica Khera,
[1] yta0088@gmail.com,School of Computer and Applications, Manav Rachna International Institute of Research and Studies, Faridabad
[2]Ms. Sunita Joshi,Assistant Professor,sunita.fca@mriu.edu.in, School of Computer and Applications, Manav Rachna International Institute of Research and Studies, Faridabad
[3]Dr. Arvind Kumar,Associate Professor,akdangi@gmail.com, School of Computer and Applications, Manav Rachna International Institute of Research and Studies, Faridabad
[4] jasicakhera09@gmail.com,School of Computer and Applications, Manav Rachna International Institute of Research and Studies, Faridabad

Abstract
Recent years have seen a rise in the importance of network security. Encryption has appeared as a preparation and is critical to the procedure of statistics sanctuary schemes. Our data is protected by encryption, which guarantees that it can only be accessed by the intended recipient and prohibits data modification or tampering. Several techniques and procedures have been developed in order to reach this level of security. The proposed technique uses hybrid of AES256-GCM, RSA and steganography. The proposed framework would convert plain text into ciphertext by encrypting it using a hybrid of three encryption algorithms to ensure the highest security of the data.

Date of Submission: 28-05-2023 Date of Acceptance: 08-06-2023

I. INTRODUCTION

Now that the Internet offers vital information, Tens of millions of people are able to communicate with one another through security becomes a concern when technology is employed more and more in commerce really crucial problem to address. There are numerous factors numerous uses, ranging from safe commerce, to security payments for private communications, as well as safeguarding passwords.

The most popular method of transforming data so that nobody can read it, but only those with interesting knowledge (sometimes referred to as a key) that enables them to transform the data back to its distinctive decipherable structure, is known as encryption.

Since encryption empowers you to safeguard the information you don't believe others should approach securely, it is urgent. Organizations use it to defend business mysteries, states use it to get characterized data, and many individuals use it to protect individual data from forestalling things like fraud.

Data security utilizes an assortment of uninhibitedly open encryption procedures. Both symmetric (private) and topsy-turvy (public) key encryptions fall under this classification. Information is scrambled and decoded involving a single key in symmetric or mystery key encryption. Two private and public keys are used in hilter kilter keys.

II. RELATED ALGORITHMS

DATA ENCRYPTION STANDARD (DES)

- Data Encryption Standard (DES), a symmetric-key block cypher encryption technique, was developed by IBM in the early 1970s and standardised by NIST in 1977. DES uses 64-bit blocks of plaintext and a 56-bit key to create the ciphertext. The plaintext is subjected to a number of substitutions and permutations by the algorithm using a Feistel network. The particular set of replacements and permutations that are utilized throughout the encryption process are chosen using the key.
- Although DES was frequently used for secure communication and data encryption, its comparatively tiny key size eventually made it susceptible to brute-force attacks. As a result, the Advanced Encryption Standard (AES) took its place in 2001. Yet, DES was a significant advancement in the history of cryptography and opened the door for the creation of more sophisticated encryption techniques.

Blowfish

- The Blowfish symmetric key block cypher algorithm was developed by Bruce Schneier in 1993. It is widely utilised in many different applications, including the encryption of private information including files, passwords, and messages.
- The algorithm operates by breaking up the input data into 64-bit blocks and running a series of rounds that involve substitution and permutation operations. Blowfish is a very strong encryption method since its keys range in length from 32 to 448 bits.
- Blowfish has been extensively analyzed and is considered to be a highly secure encryption algorithm, with no known vulnerabilities. It is also relatively fast and efficient, making it a popular choice for various encryption applications.

III. LITERATURE REVIEW

This framework is designed to encrypt and decrypt plain text into ciphertext. "Assuming somebody acquires information on the mystery key, the individual in question can use the way to unscramble every information that was scrambled with the key. No encryption technique is secure. Given information on the calculation and sufficient opportunity, assailants can recreate most encoded information" (Jain, Y.K., and Ahirwal,R.R., 2010). The strength of the calculation keeps it from assaults.In the present "web age," a period of quickly evolving advances, security concerns are of prime significance given that fraud and

extortion occasions are expanding forcefully. Protecting the security of any Basic Data (CI) is a difficult errand in any continuous application

(Mali, Latika Desai and Suresh, 2018) . Cryptography, Steganography, Watermarking, fingerprinting, and so forth have been stylish as of late. Calculations for cryptography are powerless to programmers. This has emphasized the need to install steganography utilizing video, sound, advanced pictures, and so on that are moderately difficult to break. Srinivasan, Gowthaman, and Kanakraj indicated that "Computerized sound, video, and pictures are progressively outfitted with recognizing however subtle imprints, which might contain a secret copyright notice or chronic number." They foster an RSA Hilter kilter key cryptographic strategy that includes a consciousness of the mystery key to the proprietor, hence making the security powerful (Srinivasan K., Gowthaman T. andKanakraj J., 2017). Of the new advancements, we additionally track down fake brain organizations (ANN) looking like the human cerebrum being applied in different areas like Bioinformatics, financial exchange expectations , clinical science, weather conditions gauging, etc. Cryptography is one field where the ANN is essential [6]. In the ANN engineering educational experience can be altered to produce more compelling encryption frameworks given criticism. Steganography procedures are likewise being applied to secure biometric information in fingerprints. Creators like Douglas et al. have introduced a basic examination of the designated and blind steganalysis procedures for breaking steganography strategies (Douglas, M., Bailey, K. and Leeney, M., 2018). Additionally, questions about cloud registration over the web involve serious security issues (Tirthani, N. and Ganesan, R., 2014). The fact that cryptography makes it profoundly grounded steganography consolidated can make information safer. Crafted by Soria-Lorente and Berres shows a novel steganographic technique that depends on the pressure standard according to the JPEG and the utilization of the Entropy Thresholding strategy. In order to generate a collection of pseudorandom numbers that are paired in nature, their suggested steganographic calculation combines a public key and a secret key, showing the addition spot of parallel succession components of a mystery message (S.Berres and A. Soria-Lorente,

2017). Kim, Chang, and Yang suggested that the data stowing away (DH) be allowed to inject restricted material, copyright data, and commentary into various forms of media like pictures, sounds, videos, or texts. They add that "a guard dog should not be able to detect the inserted information, and in the meantime, the privileged information needs to remain stowed away in a cover signal without discovery from steganalysis devices" (Kim C., C. C. Chang, C. N. Yang and Zhang J. Baek, 2018).

Bhardwaj and Vaishali Sharma three degrees of safety viz. "first is given by supplementing the mystery message, second by stowing away supplemented secret message in cover picture pixels that are chosen arbitrarily by utilizing pseudo arbitrary number generator and third by utilizing reversed piece LSB technique (Bhardwaj, R. and Sharma, V., 2016). Below are the findings of various research papers. *A Study of Encryption Algorithms AES, DES and RSA for Security*: They compared how well each performed using merely the time it took to encrypt and decode data using three distinct encryption methods, including the AES, DES, and RSA algorithms. Also, they show the outcomes of assessments of each algorithm's efficiency. based on the testing findings and the textual content documents employed. *Efficient Encryption Techniques in Cryptography Better Security Enhancement:* They suggested looking into encryption methods and talked about their process and constraints. Huffman coding, B2G, and G2B are used for encryption. They also described a variety of transpositional techniques, such as simple columnar, easy row, route cypher, and transposition. *An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security:* They supplied a fresh set of encryption guidelines and used a block cypher generation technique. To analyse and create findings, they

recommended using calculation with different plaintexts inside the same key (DPSK) mode. The results show that the proposed set of rules operates more quickly than the current set of rules for the same key length and for the same amount of data. *Asymmetric Encryption Techniques for Securing Internet of Things (IOT) Applications:* The Internet of Things (IoT) applications are secured using a variety of asymmetric encryption algorithms, which are all thoroughly reviewed in this paper. Elliptic Curve Cryptography (ECC), Paillier, and RSA are only a few of the several methods that the writers evaluated and assessed for strengths and shortcomings. The application of asymmetric encryption in the context of IoT is also discussed in the article, along with its opportunities and limitations. *A Comprehensive Study on Symmetric Encryption Techniques for Secure Data Communications:* This study provides a thorough overview of the various symmetric encryption methods that are employed for safe data transmission. The authors examined and contrasted the benefits and drawbacks of various algorithms, including the Advanced Encryption Standard (AES), Blowfish, and Triple Data Encryption Standard. (3DES). The most recent advancements and fashions in the field of symmetric encryption are also covered in the article.

IV. IMPLEMENTED TECHNOLOGIES IN PROPOSED APPLICATION

AES256-GCM

- AES256-GCM is an encryption technique that is frequently used and offers high security for data protection. The symmetric encryption algorithm known as AES uses the same key for both encryption and decryption. AES stands for Advanced Encryption Standard. The key size, which is 256 bits, is indicated by the "256" in AES256-GCM.
- A symmetric key cryptographic block cipher's mode of operation is called GCM, or Galois/Counter Mode. Data secrecy and data authenticity are both provided by the authenticated encryption method GCM. In other words, in addition to being encrypted, the data also has a cryptographic tag that enables the recipient to confirm that it was not altered during transmission.
- Network security, secure communication protocols, and data storage encryption are just a few of the uses for AES256-GCM. Because of its security and dependability, it is commonly regarded as a very powerful encryption method.
- AES256-GCM is efficient in that it can be implemented in hardware and software platforms without requiring a lot of processing power, which is one of its advantages. This makes it a well-liked option for a variety of applications.

RIVEST-SHAMIR-ADLEMAN (RSA)

- It is common practice to employ the public-key encryption algorithm RSA (Rivest-Shamir-Adleman). It bears the last names of Ron Rivest, Adi Shamir, and Leonard Adleman and was created in 1977. Data transmission over the internet is frequently encrypted and decrypted using the RSA algorithm.
- There is a private key and a public key for every RSA user. The public key is made available to anyone who wants to send encrypted messages to the user, while the private key is kept secret and used only by the user to decrypt communications.
- RSA is frequently used in key exchange systems and digital signatures. Despite intensive analysis, no effective way to defeat RSA encryption has been discovered. However, to maintain security, it's crucial to employ suitably high key sizes as future advancements in computing power could make RSA vulnerable to attack.

STEGANOGRAPHY

- Steganography is the art of hiding a message or piece of information within another medium—like a picture, audio file, or text—so that only the person to whom it is intended remains aware of its presence. By making the message appear to be a harmless or unimportant file, steganography seeks to conceal the message's existence rather than its substance.
- Steganography can be used for both legitimate and illegitimate purposes. In the digital world, it is often used to hide sensitive information or to evade detection by authorities. However, it can also be used for legitimate purposes, such as watermarking, copyright protection, and authentication.
- Detecting steganography is a challenging task as it requires analyzing the structure of the cover medium and looking for patterns that are not typical of the medium. Various tools and techniques have been developed to detect steganography, including statistical analysis, entropy analysis, and visual inspection. However, these methods may not always be effective against advanced steganography techniques.

PYTHON

Python is a significant-level, deciphered programming language utilized for the overwhelming majority of uses, including AI and manufactured reasoning, web improvement, and logical processing. It is eminent for

its clarity, comprehensibility, and use, making it an incredible choice for fledgling and prepared software engineers. Python's enormous standard library, dynamic engineer local area, and clear, brief linguistic structure simplify learning and grasping, giving clients admittance to various apparatuses and assets. The way Python is cross-stage permits it to work on various working frameworks, including Windows, macOS, and Linux.

PYBASE64

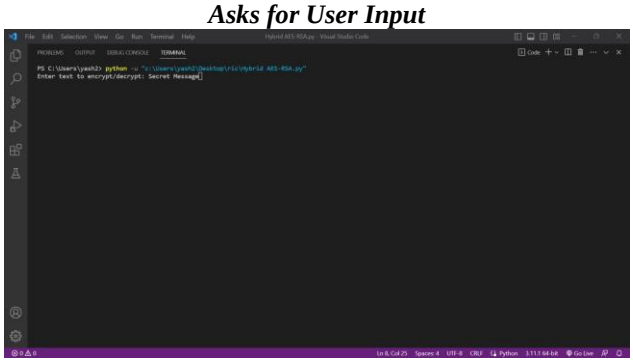
- PyBase64 is a Python module that offers capabilities for Base64-based binary data encoding and decoding. A binary-to-text encoding system called Base64 displays binary data as ASCII strings. This is helpful when transferring binary data via channels like email or websites that can only handle ASCII characters.
- B64encode and B64decode are the two primary operations offered by the PyBase64 module. The base64-encoded version of the input data is returned as a bytes object by the b64encode function, which accepts a bytes-like object as input. The b64decode method takes a bytes object that has been Base64-encoded and returns the binary data in its original form.

TKINTER

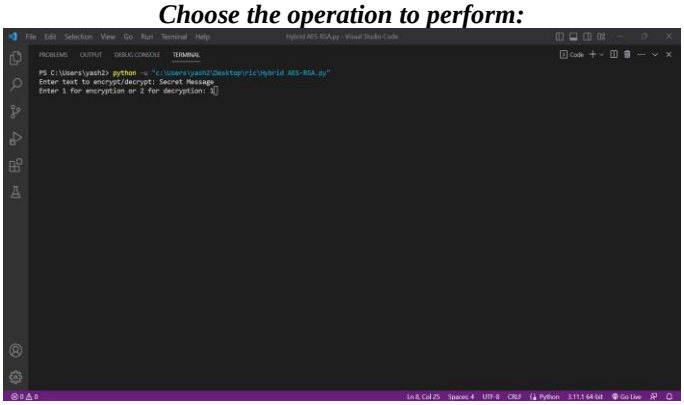
A built-in Python package called Tkinter is used to make graphical user interfaces (GUIs). The window that is produced when a Tkinter program is executed and acts as the user's primary interface is referred to as the Tkinter screen. It is possible to add different widgets to the screen, including buttons, labels, text boxes, and more. With built-in features, the screen can be adjusted, maximized, minimized, and closed. In general, the Tkinter screen is a crucial component in creating user-friendly and Python applications.

V. WORKING OF THE PROPOSED APPLICATION

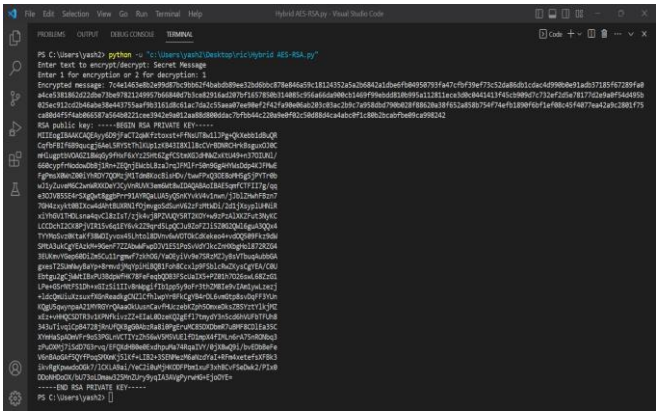
Asks for User Input



Choose the operation to perform:

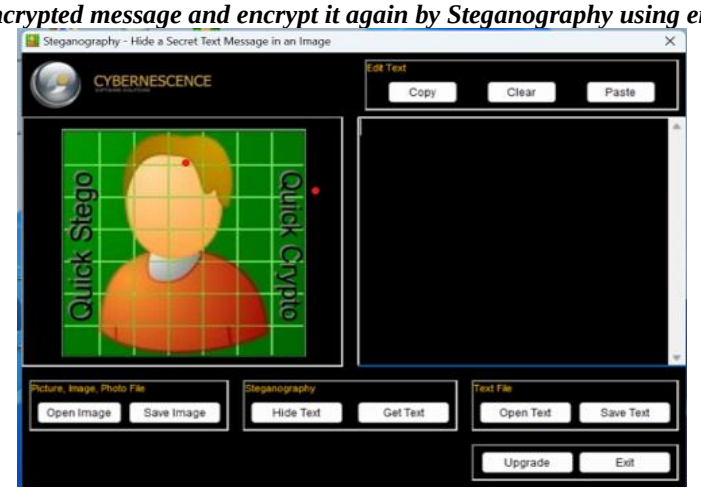


Output of operation:
Encrypted message along with RSA private key:



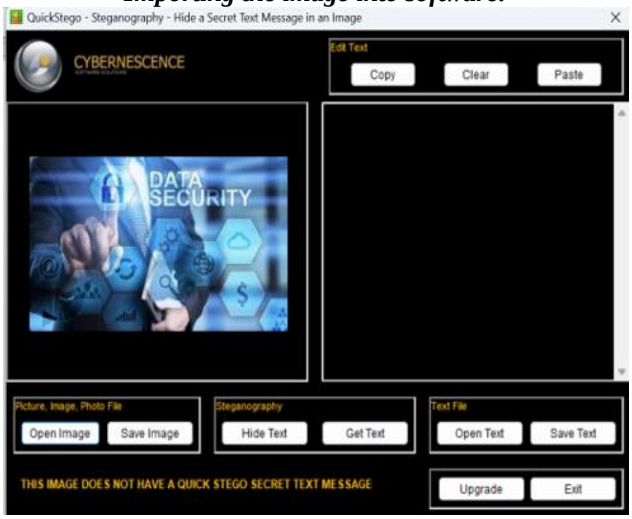
Steganography:

Now we take the encrypted message and encrypt it again by Steganography using encryption software:

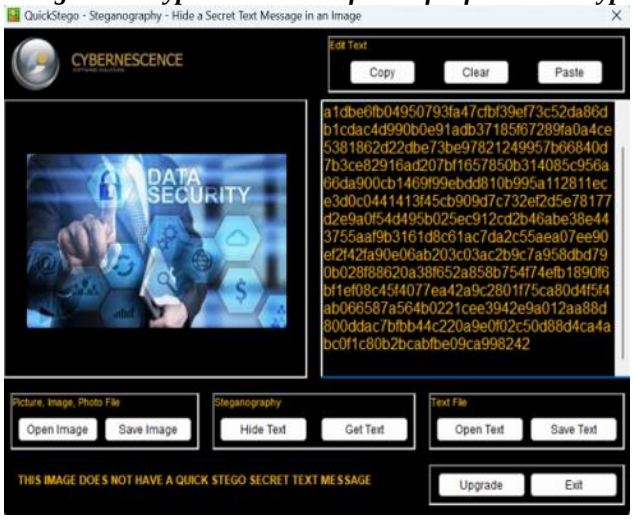


The image in which the AES-RSA encrypted message will be encrypted again:

Importing the image into software:

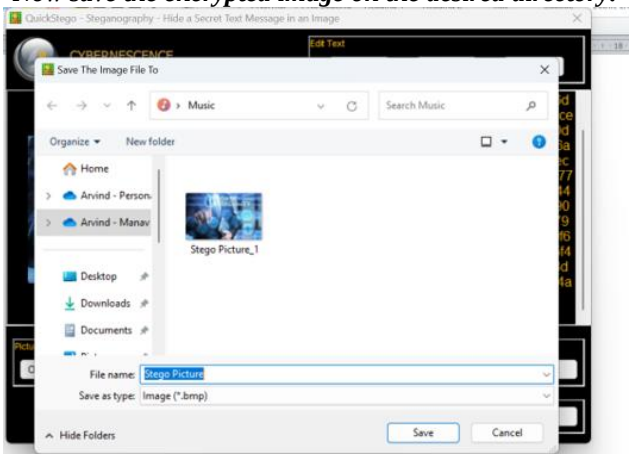


Importing the encrypted text into software for further encryption:



By clicking on the Hide Text message we encrypt the text into image:

Now save the encrypted image on the desired directory:



VI. CONCLUSION AND FUTURE SCOPE

In this paper, a Python based GUI-Application which uses a hybrid of AES256-GCM and RIVEST-SHAMIR-ADLEMAN (RSA) algorithms was successfully designed and implemented to encrypt and then further encrypted using Steganography to ensure highest security. Working of applications are given as well along with brief explanations of the technologies used in the development and working of the application. This hybrid technique ensures the high level of security in encryption.In the extensive working of this work might be applied the fusion of different data security methodology and algorithms for the vast and complex level of data security.we can apply steganography and cryptography fusion inside the fiestel structure also to increase the level of complexity of the data security

REFERENCES

[1]. "Implementation of Encryption and decryption Methodologies" – Lohit
[2]. H, Dr. Umarani C
[3]. "A Study of Encryption Algorithms AES, DES and RSA for Security" - Dr. Prerna Mahajan & Abhishek Sachdeva
[4]. "A Symmetric Key Cryptographic Algorithm" – Ayushi
[5]. "A Secure and Fast Approach for Encryption and Decryption of Message Communication" - Ekta Agrawal, Dr. Parashu Ram Pal
[6]. "Cryptography Algorithms: A Review" - Anjula Gupta, Navpreet Kaur Walia
[7]. "Efficient Encryption Techniques in Cryptography Better Security Enhancement" - Reema Gupta
[8]. "Efficiency and Security of Data with Symmetric Encryption Algorithms"- Chehal Ritika, Singh Kuldeep
[9]. "Evaluating The Performance of Symmetric Encryption Algorithms" - Elminaam, Diaa Salama Abd, Abdual Kader, Hatem Mohamed & Hadhoud, Mohiy Mohamed
[10]. "A Novel Approach for Data Encryption Standard Algorithm" - Prashanti.G, Deepthi.S & Sandhya Rani.K.
[11]. "Using the RSA as as an asymmetric non-public key encryption algorithm in the shamir three-pass protocol" - Dian Rachmawati & Mohammad Andri Budiman
[12]. "GUI implementation of image encryption and decryption using Open CV-Python script on secured TFTP protocol" - K. Rasool Reddy & Ch Madhava Rao
[13]. "Cryptft+ : Python/Pyqt based File Encryption & Decryption System Using AES and HASH Algorithm" - Dongho ShinWoori Bae[...]Hyung-Woo Lee
[14]. "Evaluation of cryptographic key generation performance using evolutionary algorithm" - M. Ragavan & K. Prabu
[15]. "Implementation of Elliptic Curve Cryptography over a Server-Client network" - S. B. Bore Gowda
[16]. "A Double-Key Based Encryption-Decryption Process for Stronger Secured Message Transactions" - Md Ismail Jabiullah, AA Md Monzur Ul Akhir, Muhammed Rasheduzzaman
[17]. "An innovative near-field communication security based on the chaos generated by memristive circuits adopted as symmetrical key" - Colin Sokol Kuka, Yihua Hu[...]Mohammed Alkahtani
[18]. "Augmenting natural language processing for selective encryption in mobile ad hoc network" - Ajay Kushwaha, Megha Mishra, Subhash Chandra Shrivastava
[19]. "Implementation of the Gauss-Circle Map for encrypting and embedding simultaneously on digital image and digital text" - M. T. Suryadi, Yudi Satria, Azzam Hadidulqawi
[20]. "Simulation of a secure optical communication system using different optical modulation schemes coupled with Rivest-Shamir-Adleman algorithm" - Soumit Banerjee, Appala Ventaka Ramana Murthy
[21]. "Method for hiding text data in an image" - G.B. Turebaeva
[22]. "Information Encryption and Decryption Analysis, Vulnerabilities and Reliability Implementing the RSA Algorithm in Python" - Rocío Rodriguez G, Gerardo Castang M, Carlos A. Vanegas
[23]. "Designing and Implementing Cloud Security Using Multi-layer DNA Cryptography in Python" - Md Irfan Alam, Satya Narayan Singh
[24]. "A Secure Messaging for Internet of Things Protocol based RSA and DNA Computing for Video Surveillance System" - Saba S. Ibraheem, Ali H. Hamad, Ali Sadeq Abdulhadi Jalal
[25]. "A Novel Multiplicative Substitution Cryptosystem" - Vemulapalli Rajesh,
[26]. V. Panchami.
[27]. "Password generation mechanism using DNA and RNA processing" - Anand Mahendran, Siddharth Chatterjee, V. Vijayarajan

[28]. “Analysis of Secure Transfer of Healthcare Data using Fog Computing” - Arshath Bilai Ramzan Ali, Paramasivam Alagumariappan
[29]. “Extended Information Hiding Procedure in Cloud Computing Environment using Random Security Codes”-A.K.Dangi & A.Gupta
[30]. “Asymmetric Encryption Techniques for Securing Internet of Things (IOT) Applications” - K. Praveen
[31]. "A Comprehensive Study on Symmetric Encryption Techniques for Secure Data Communication" - S. K. Parida
[32]. "Efficient and Secure Encryption for Electronic Health Records in Cloud Computing" - H. S. Ali
[33]. "A Novel Double Encryption Scheme for Securing Medical Images in Cloud Computing" - H. Ghasemzadeh .
[34]. “Information Security Using the Ensemble Approach of Steganography and Cryptography”-A.Kumar &A.Gupta