IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Lightweight Encryption AES, DES and RSA

1 Kritek Upadhyay, 2 Dhiraj Nikam, 3Ashvin Auti

1 Student, 2 Student, 3 Student,
CSE Department
MIT ADT, Loni Kalbhor, INDIA

Abstract: Data security has been a major concern in recent years. Encryption has emerged as a solution and is critical to the information security system. To protect the shared data, a variety of procedures are required. The current project focuses on using cryptography to safeguard data while it is being transmitted across a network. To begin, data must be encrypted using an encryption method in cryptography before being sent from sender to receiver in the network. The user then chooses the approach he wants to employ to decryption data. Second, the receiver can view the original data by employing the appropriate decryption algorithm (as determined by the user). Data encryption is used to send the key via email.

Index Terms **- AES, cryptography, steganography, RSA, DES, Encryption (E), Security and privacy (SP), homomorphic encryption (HE);**

I.INTRODUCTION

While using block chain technology to healthcare for efficient data sharing is inventive and disruptive, it is not a cure. For meeting the standards for SP, and the dangers of EMR data Instead, we contend that in-depth and comprehensive research is essential. A thorough understanding of the problems and the solutions Healthcare SP technology The block chain will bring direction and technological advancement. Cryptography is a powerful tool for safeguarding sensitive data. It's a way of storing and sending data in a way that only the people who need it can access and process it. E is progressing toward a future of limitless possibilities.

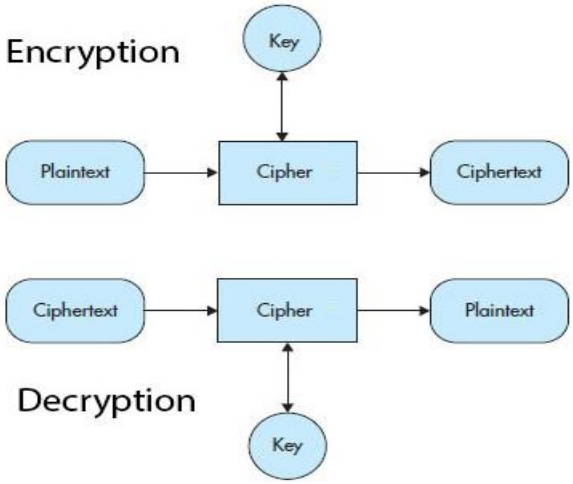

Figure 1: Cryptography

Symmetric-key Cryptography**:** A single key is shared by both the sender and the receiver. The sender encrypts plaintext and sends the cypher text to the receiver using this key. The receiver, on the other hand, uses the same key to decrypt the message and retrieve the plain text.

Public-Key Cryptography**:** In the previous 300-400 years, this has been the most groundbreaking thought. Two related keys are utilized in public-key cryptography. The public key can be freely transmitted, while the private key is kept hidden. The public key is used for E whereas the private key is utilized for decryption.

Hash Functions**:** This algorithm does not use a key. The plain text is hashed with a fixed-length hash value that prevents the plain text's contents from being recovered. Many operating systems also employ hash algorithms to secure passwords.

II.LITERATURE SURVEY

K. Anitha Kumari et.al [1] Carmichael's Theorem-based HE is our first proposed scheme, while Modified Enhanced HE is a modified version of Gorti's Enhanced HE Scheme. For clarity, the schemes are abbreviated as CTHE and MEHE. Both approaches are provably secure under the hardness of integer factorization, discrete logarithm, and quadratic residuosity problems.

Ömer Kasım et.al [2] This system encrypts writing and updating requests asymmetrically, whereas reading requests are symmetrically encrypted. This solution distinguishes the proposed method from previous studies. As a result of this solution, the system's overall performance has increased. Furthermore, because sensitive data is transferred to users using their private keys, the attacker cannot access the actual data in a cyber-attack. This result confirms that security and privacy rules are followed when accessing, writing, and updating electronic medical records.

Marielle Gross et.al[3] they discuss how block chain technology and privacy-preserving forms of computation could be the foundation for new ethical guidelines, given their ability to resolve fundamental tensions between our concurrent obligations to protect individuals' health data rights and to promote learning from health data for the benefit of society in this article.

R. Sendhil et.al [4] This study presents a fog-assisted health data transferring applications-based contextual fully HE techniques-based privacy preserving framework (CFHET-PPF). The proposed CFHET-PPF system combines three major totally HE algorithms to prevent bogus data injection.

Francis Dutil et.al [5] In order to deliver rigorous Privacy by Design services and impose a zero-trust data governance paradigm, we study the use of HE in the context of DL model training and prediction. First, we show how HE may be used to create predictions over medical images while also preventing illegal data reuse, and then we provide the results of a disease classification task using OCT images.

Huseyin Demirci et.al [6] To avoid the potential consequences of a data breach—which is a real risk nowadays—and to comply with existing data protection legislation, genomic data files should be encrypted and data processing procedures should be privacy-preserving. Algorithm may not scale up when applied to genomic data processing due to computation time inefficiency.

Yassine Abbar et.al [7] This article explores a selection of scenarios for surreptitiously scanning document corpora in both public and private environments, employing a trustworthy yet suspicious infrastructure. We integrate Fully Holomorphic Encryption (FHE) with other approaches like Symmetric Searchable Encryption (SSE) and Retrieval of Confidential Information to achieve acceptable system level performance (PIR). The study also goes into the prototypes that were produced to validate the method, in addition the results and their scalability.

Rui Zhang et.al[8] This article examines the security and privacy requirements for sharing of medical data via block chain, including the risks and requirements, in addition technical solutions and methods. We go over the security and privacy criteria and attributes that a set of criteria that must be completed in order to use the healthcare block chain to share electronic medical data.

Dr. A.C. Santha Sheela et.al[9] This authentication method is quite trustworthy, and it will make voting easier for people voters in many free societies, countries, elections have been a major source of worry. An election is seen as a procedure that effectively establishes the official structure of a country. It's a chance to pick the right leader and contribute to the country's progress. Furthermore, the authorities are anxious about the election's security and validity. Despite the fact that we use sophisticated computerized voting machines, the question of rigging arises frequently.

Chandra Thapa et.al [10] Security, privacy, and reliability of information are essential. Furthermore, healthcare data must be kept secure and private, according to government legislation and ethics agencies. Furthermore, the public, as the data source, desires secure, private, and reliable data. If they don't want to, they can opt out of submitting their data to the precision health system. As a result, precision health's effectiveness suffers because the public is the system's intended benefit.

III.PROPOSED SYSTEM

In our daily lives, lives, we move from one location to the next with writings, records on the internet are similarly recognized with puzzles. The PC key layout of PC guidelines plays a significant role in a cryptosystem that protects sensitive and confidential data. Verifying intuitive media data sight and sound information against variants of assaults against various types of ambushes may be a testing activity with expanded cryptanalysis. A security system using cryptographic and steganography technique.

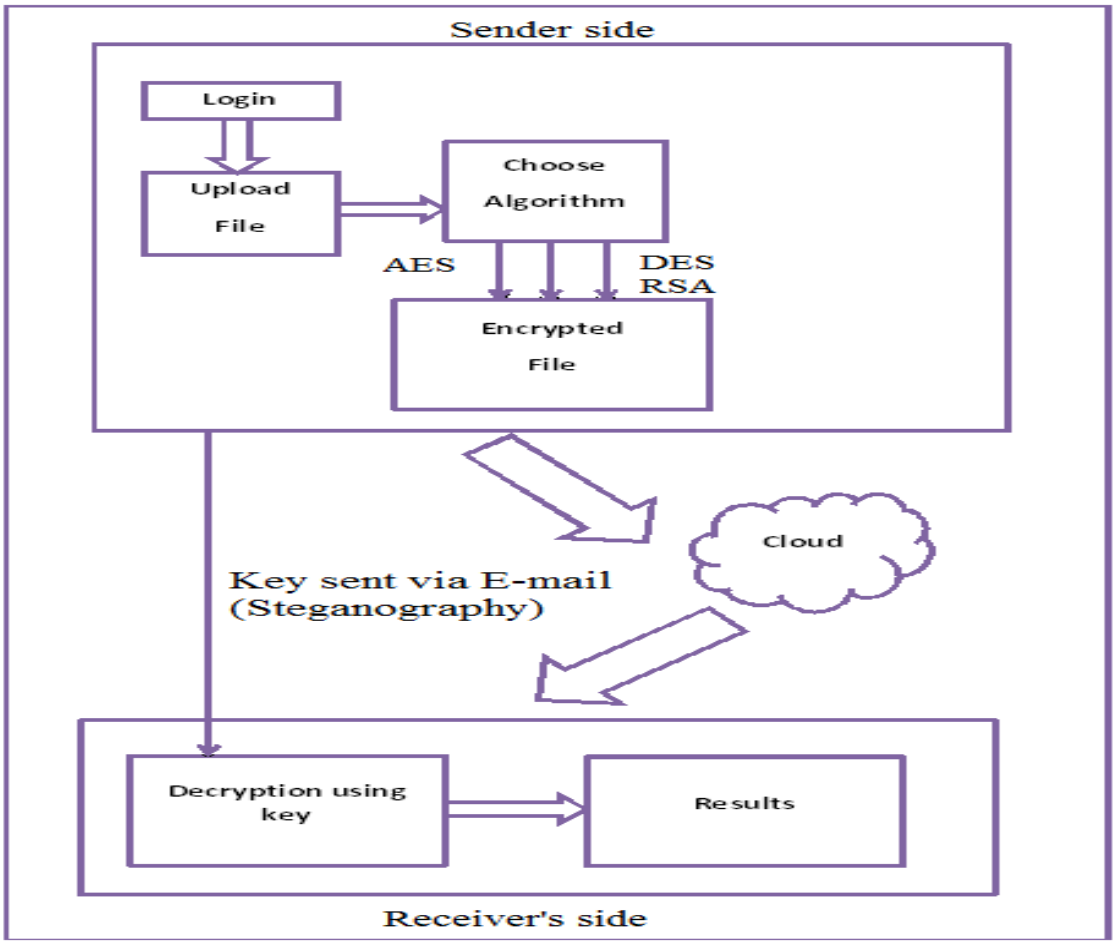

Figure 2: Proposed system

The website was created with the help of the Django framework allows users to register themselves. After registration, the user login into the portal via user ID and password. The user has been granted the option to choose any of the two algorithms for encrypting documents that they uploaded earlier. Cloud (firebase server) saves encrypted files, from where the receiver fetches file. To decrypt the document, the user will require a key, which will be emailed to the approved individual. Keys are encoded via steganography. Secret Messages can be buried in a variety of multimedia elements, such as text, images, and videos. Audio, photos, animations, video, and so on. In this system, we'll hide our key in an image.

Algorithm
AES Algorithm

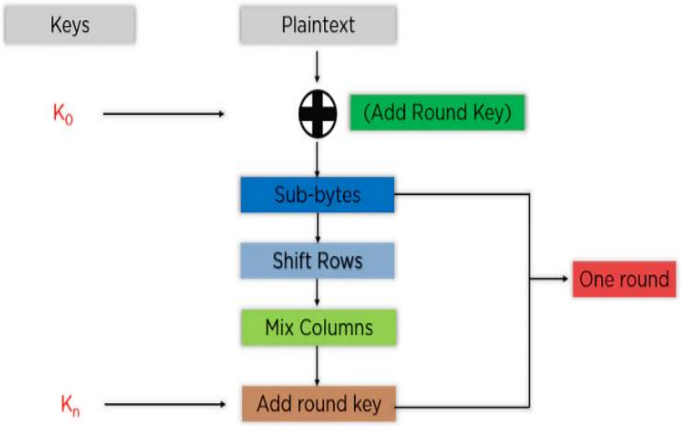

Figure 3: AES Algorithm

The key that was originally created is now enlarged into multiple round keys (number of rounds + one) of 128 bits by the key scheduler. The starting key is subjected to rotations, replacements, and an XOR operation with a predetermined round constant to calculate the round keys (stored in a table). AES is based on a four-by-four byte matrix called state. The state is subjected to many rounds of E, each involving four operations. Add Round Key, Substitution of Bytes (S-Layer), Shift Rows, and Mix Columns are

the operations (P-Layer). The round key is XORed with the state in the Add Round Key. Throughout the state, an 8 8 bits S-Box is used to accomplish the substitution layer. The permutation layer is created by rotating the matrix's rows (the final three rows) and multiplying the columns with a matrix (M).

DES Algorithm

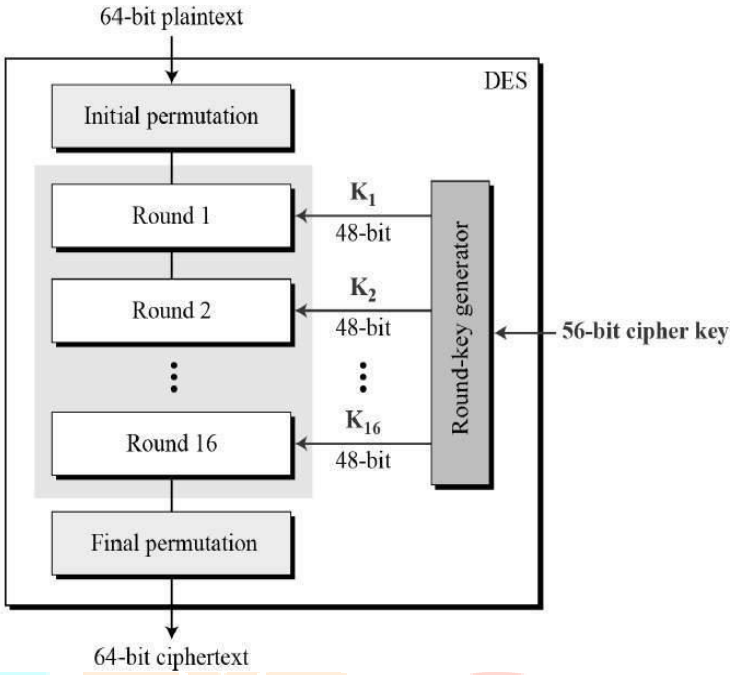

Figure 4: DES Algorithm

The DES is a block cypher technique that converts plain text in 64-bit blocks to cipher text using 48-bit keys. It's a symmetric key algorithm, which means it encrypts and decrypts data with the same key. The sender and receiver must both know and use the same private key because DES encrypts and decrypts messages using the same key. The more secure AES method has supplanted DES as the go-to symmetric key algorithm for the E of electronic data.

RSA Algorithm

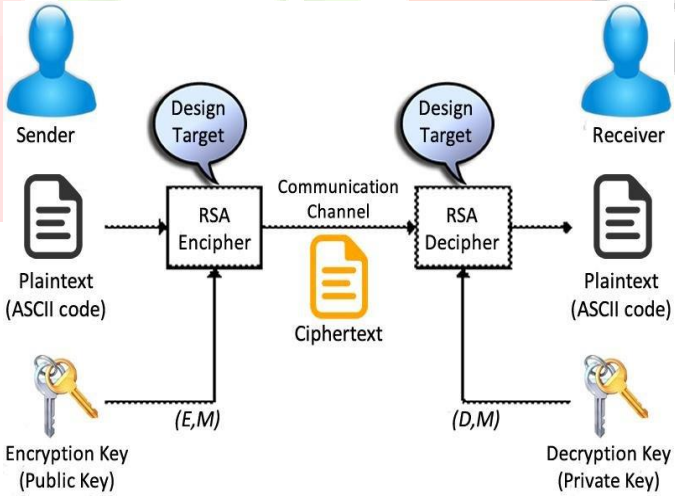

Figure 5: RSA Algorithm

Modern computers employ the RSA algorithm to encrypt and decrypt messages. It's an asymmetric cryptography algorithm. The presence of two separate keys is referred to as "asymmetric." This is also known as public key cryptography because one of the keys can be given to anyone.

IV.CONCLUSION

Each cryptographic algorithm has its own set of strengths and weaknesses. The cryptographic algorithm to be used must be chosen depending on the requirements of the application to be used. The AES algorithm can be chosen if confidentiality and integrity are important. The DES is the optimum option if the application's demand is network bandwidth. Hybrid cryptography and steganography have been used in this paper, and a stego picture has been created. . The message is encrypted using AES, DES, or RSA (depending on the user's preference). All of these encrypted files, including the encrypted message, encrypted key, and

encrypted digest, have been concatenated into a single message. For disguising the document in an image file, we used cryptographic algorithms such as DES, AES, and RSA, in addition the steganography approach.

V.ACKNOWLEDGMENT

We would also like to show our gratitude to the Dr. Nilesh R Marathe, Associate professor, MIT SOE, MIT ADT University for sharing their pearls of wisdom with us during the course of this research, We are also immensely grateful to our faulty of MIT SOE, MIT ADT University for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

1. K. Anitha Kumari, Avinash Sharma,2 Chinmay Chakraborty,3 and M. Ananyaa .” Preserving Health Care Data Security and Privacy Using Carmichael’s Theorem-Based Homomorphic Encryption and Modified Enhanced Homomorphic Encryption Schemes in Edge Computing Systems” Volume 10, Number 1, 2022.

2. Ömer Kasım. “An Efficient Ensemble Architecture for Privacy and Security of Electronic Medical Records” The International Arab Journal of Information Technology, Vol. 19, No. 2, March 2022.

3. Marielle Gross1, 2 · Robert C. Miller3.” Protecting privacy and promoting learning: block chain and privacy preserving technology should inform new ethical guidelines for health data” Accepted: 5 August 2021

4. R. Sendhil1, A. Amuthan. “ Contextual fully holomorphic encryption schemes-based privacy preserving framework for securing fog-assisted healthcare data exchanging applications” Accepted: 30 April 2021

5. Francis Dutil, Alexandre See*, Lisa Di Jorio, and Florent Chandelier.” Application of Homomorphic Encryption in Medical Imaging” 12 Oct 2021.

6. Huseyin Demirci 1 a, Lenzini Gabriele.” Privacy-preserving Copy Number Variation Analysis with Homomorphic Encryption” 2021.

7. Yassine Abbar1, Pascal Aubry2, Thierno Barry1, Sergiu Carpov4, Sayanta Mallick1, Mariem Krichen3, Damien Ligier3, Sergey Shpak3 and Renaud Sirdey2.” Cloud-based Private Querying of Databases by Means of Homomorphic Encryption”2021.

8. Rui Zhang, Rui Xue, and Ling Liu, Fellow.” Security and Privacy for Healthcare Block chains” 2021.

9. Dr. A.C. Santha Sheela, Ramya. G. Franklin ,” E-Voting System Using Homomorphic Encryption Technique” International Conference on Mathematical Sciences (ICMS 2020).

10. Chandra Thapa, seyit camtepe."Precision health data: Requirements, Challenges and existing techniques for data security and privacy" IEEE 2020.