Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

ISSN NO. 2320-5407

Article DOI: 10.21474/IJAR01/16613
DOI URL: http://dx.doi.org/10.21474/IJAR01/16613

RESEARCH ARTICLE

SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

Ashwin Satheesh Kumar[1], Anfah K.[1], Hariharan T.[1], Rosna Parveen[1], Sizan Mahmud[1] and Dr. Sonal Sharma[1,2]

1. Department of CSE CTIS, Faculty of Engineering and Technology, JAIN (Deemed-to-be-University) Karnataka 562112, India.
2. Associate Professor School of CSE.

Manuscript Info

Manuscript History
Received: 05 February 2023
Final Accepted: 09 March 2023
Published: April 2023

Abstract

Our project aims to provide secure file storage for users on the cloud (specifically on AWS S3) by utilizing a hybrid cryptography approach. This involves encrypting files using both AES and RSA algorithms, with the user receiving the encryption key through email. To further enhance security, the key will be hidden behind an image or within a PDF document using steganography techniques. Additionally, the files stored in the S3 bucket will also be encrypted, but instead of encrypting the contents of the file, we will encrypt the file format itself. The file format can be decrypted using the GHE decryption key and software, which will be made available to end-users. Overall, our project aims to provide a robust and secure solution for cloud-based file storage.

Introduction:-

In today's digital age, the majority of people rely on the internet and mobile storage devices to send and receive data. However, despite knowing that personal information can be compromised, many individuals neglect to encrypt their data. Information security has always been crucial, but with technology's increasing control over various aspects of our daily lives, it has become even more critical. Cryptography serves as a crucial security layer by translating messages into an unreadable format for unauthorized third parties. Our program's ultimate goal is to develop highly secure AES and RSA cryptography algorithms that are low power, high-throughput, and reliable in real-time. While cloud-based internet security provides an outsourced solution for secure data storage, security breaches often occur due to employee error. It is crucial to enhance user security to improve data storage safety. Around the world, there is an increasing demand for cloud-based solutions, including secure data storage and for full business processes. Therefore, this study aims to explore the effectiveness of hybrid cryptography in securing cloud-based data storage and preventing data breaches caused by employee errors [10].

Literature Survey

BIJETA SETH,SURJEET DALAL,VIVEK JAGLAN,DAC-NHUONG LE,SENTHILKUMAR MOHAN,GAUTAM SRIVASTAVA. INTEGRATING ENCRYPTION TECHNIQUES FOR SECURE DATA storage in the cloud(2020)

This paper centers around the integration of Hybrid cryptography with a cloud storage system. The authors provide insights into a new architecture's implementation, which can provide an improved level of security for outsourcing information in a cloud computing environment that involves multiple independent cloud providers. The framework includes dual encryption and data fragmentation techniques that facilitate the secure distribution of information in a

Corresponding Author:- Ashwin Satheesh Kumar
Address**:-** Department of CSE CTIS, Faculty of Engineering and Technology, JAIN (Deemed-to-be-University) Karnataka 562112, India.

multi-cloud environment. The authors have addressed various concerns related to this area, particularly those concerning integrity, security, confidentiality, and authentication [3]

BILAL HABIB, BERTRAND CAMBOU, DUANEBOOHER, CHRISTOPHER PHILABAUM. PUBLIC KEY EXCHANGE SCHEME THAT IS ADDRESSABLE

(PKA)(2017)

The objective of the PKA encryption scheme is to complement, or replace, existing Public Key Infrastructures (PKI). In this scheme, the initialization step is based on the secure exchange of addressable cryptographic tables between the communicating parties. These tables are generated either with random numbers, or with arrays of addressable Physical Unclonable Function (PUFs). The subsequent communications between the parties can therefore occurs over untrusted channels, by exchanging dynamically generated public keys. Private keys are, generated independently with all communicating parties using their cryptographic tables, and the shared public keys. The private keys are combined with methods such as the Advanced Encryption Standard (AES) to encrypt and decrypt the communication between users. The generation of private keys is done without mathematical computations that are potentially vulnerable to quantum computers using algorithms such as the one developed by Shor. PKA is fast and requires approximately 800 CPU clock cycles. We implemented, and tested the PKA dynamic key exchange scheme in legacy systems to secure PC-to-PC communication, and PC to smart card communication with AES [2]

PUNAM V. MAITRI, ARUNA VERMA. SECURE FILE STORAGE USING HYBRID CRYPTOGRAPHY (2016)

This paper focuses on how files are securely stored using cryptography. It also discusses the drawbacks of just using just one cryptographic algorithm and a method of securing user data stored on the cloud by utilizing hybrid cryptography algorithms. The authors propose a tool that encrypts files using both AES and RSA, and the user receives the key via email. [5]

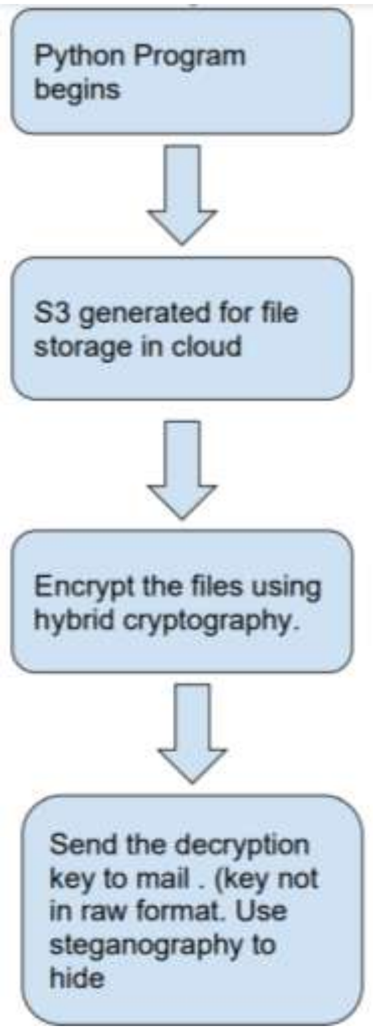
Objective:-

To make a secure file storage system in the cloud using hybrid cryptography

Proposed Methodolgy:-

Step 1: Execute the python program
Step 2: Console login for end users.
Step 3: Files will be moved to your secure storage bucket
Step 4: Hybrid encryption process will begin. Any two of the best symmetric and asymmetric encryptions will be chosen [3,5]
Step 5: The contents of the file won’t be encrypted rather the file format would be encrypted
Step 6: Key is sent directly to your email ID [5]
Step 7: It uses steganography to send the key [5]
Step 8: Decryption software will only be with the end users

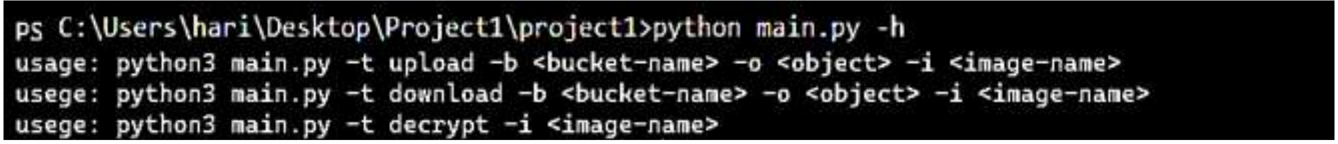
System Design
Flow Chart:


Python Program begins
S3 generated for file storage in cloud
Encrypt the files using hybrid cryptography.
Send the decryption key to mail . (key not in raw format. Use steganography to hide

Hardware And Software Requirements
1. 32-bit or a 64-bit Computer
2. Windows, macOS or Linux
3. Python 3 and above for the source code
4. Mail Trap for mailing services
5. AWS S3 for cloud storage services

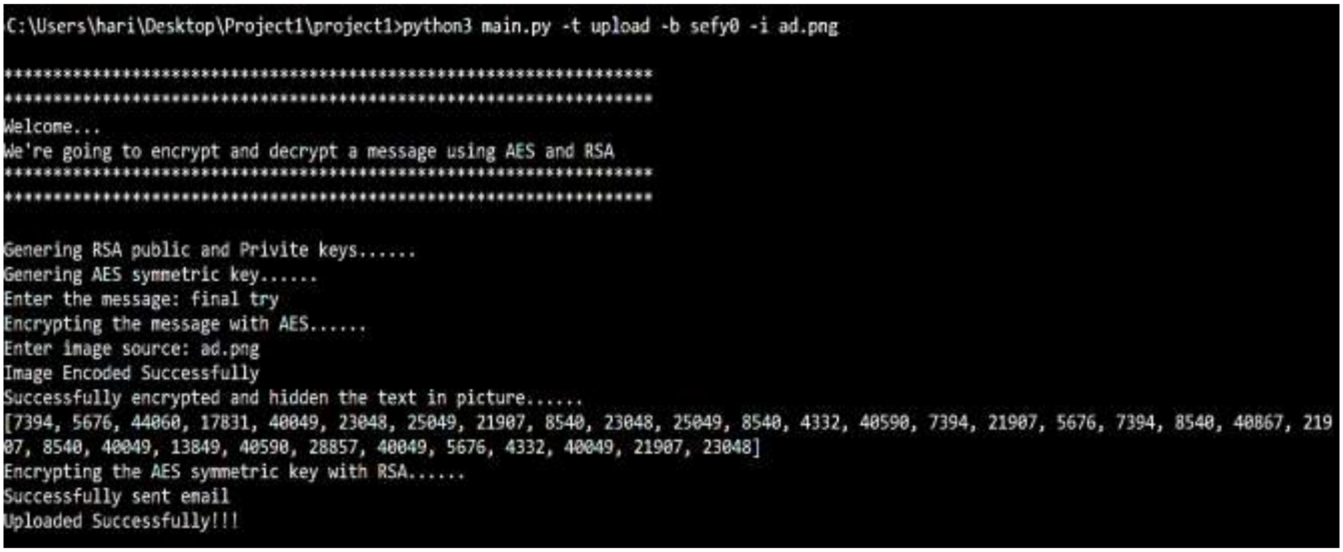
Results:-

1.Call help by running main code with -h para meter



```
ps C:\Users\hari\Desktop\Project1\project1>python main.py -h
usage: python3 main.py -t upload -b <bucket-name> -o <object> -i <image-name>
usege: python3 main.py -t download -b <bucket-name> -o <object> -i <image-name>
usege: python3 main.py -t decrypt -i <image-name>
```

2.Uploading our file into the AWS s3 bucket

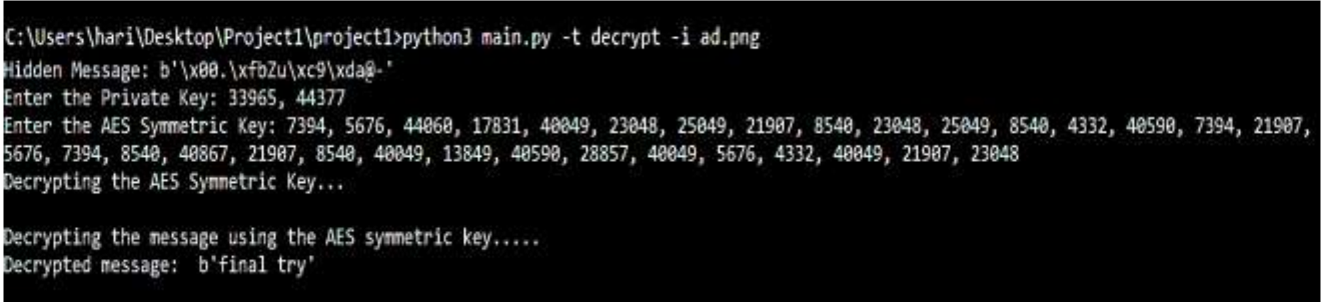


```
C:\Users\hari\Desktop\Project1\project1>python3 main.py -t upload -b sefy0 -i ad.png

*****************************************************************
*****************************************************************
Welcome...
We're going to encrypt and decrypt a message using AES and RSA
*****************************************************************
*****************************************************************

Genering RSA public and Privite keys......
Genering AES symmetric key......
Enter the message: final try
Encrypting the message with AES......
Enter image source: ad.png
Image Encoded Successfully
Successfully encrypted and hidden the text in picture......
[7394, 5676, 44060, 17831, 40049, 23048, 25049, 21907, 8540, 23048, 25049, 8540, 4332, 40590, 7394, 21907, 5676, 7394, 8540, 40867, 219
07, 8540, 40049, 13849, 40590, 28857, 40049, 5676, 4332, 40049, 21907, 23048]
Encrypting the AES symmetric key with RSA......
Successfully sent email
Uploaded Successfully!!!
```

3.Decrypting the encrypted file by loading it from s3



```
C:\Users\hari\Desktop\Project1\project1>python3 main.py -t decrypt -i ad.png
Hidden Message: b'\x00.\xfbZu\xc9\xda@-'
Enter the Private Key: 33965, 44377
Enter the AES Symmetric Key: 7394, 5676, 44060, 17831, 40049, 23048, 25049, 21907, 8540, 23048, 25049, 8540, 4332, 40590, 7394, 21907,
5676, 7394, 8540, 40867, 21907, 8540, 40049, 13849, 40590, 28857, 40049, 5676, 4332, 40049, 21907, 23048
Decrypting the AES Symmetric Key...

Decrypting the message using the AES symmetric key.....
Decrypted message:  b'final try'
```

Conclusion:-

The project described involves implementing a two-stage encryption algorithm that offers high security, scalability, confidentiality, and ease of accessibility for multimedia content on the cloud. The second stage of the algorithm is critical as it involves a randomly generated key that provides greater security than conventional encryption systems. The resulting ciphertext is stored in the cloud, and it is extremely difficult to recover the original content without the random asymmetric key. The proposed algorithm has wide applications and protects information from side-channel attackers who attempt to grab data from the cloud. As a result, your content is kept safe in the cloud using this algorithm

References:-

1. Schenieronsecurity.https://www.schneier.com/academic/blowfish/.Lastaccessed31Oct2017
2. Bilal habib, Bertrand Cambou, Duanebooher, Christopher Philabaum. Public key exchange scheme that is addressable (pka)(2017)
3. BijetaSeth,SurjeetDalal,VivekJaglan,Dac-Nhuong Le,SenthilkumarMohan,Gautam Srivastava. Integrating encryption techniques for secure data storage in the cloud (2020)
4. NgweTT,PhyoSW(2015)Hybridcryptosystemfordatasecurity.IntJAdvElectronComput Sci 2(6)
5. Punam V. Maitri, Aruna Verma. Secure file storage using hybrid cryptography (2016)
6. Vasundhara S (2017) The advantages of elliptic curve cryptography for security. Glob J Pure Appl Math 13(9):4995–5011. ISSN 0973-1768
7. KamaraS,LauterK(2010)Cryptographiccloudstorage.LectNotesComputSci6054:136–149
8. Bansal VP, Singh S (205) A hybrid data encryption technique using RSA and blowfish for cloud computing on FPGAs. In: 2nd international conference on recent advances in engineering computational sciences (RAECS), Chandigarh, pp 1–5

9. MaitriPV,VermaA(2016)Securefilestorageincloudcomputingusinghybridcryptography algorithm. In: International conference on wireless communications, signal processing and networking (WiSPNET), Chennai, pp 1635–1638
10. Chinnasamy P, Deepalakshmi P (2018) Design of secure storage for health-care cloud using hybrid cryptography. In: 2nd international conference on inventive communication and computational technologies (ICICCT 2018). IEEE Xplore Compliant-Part number: CFP18BAC-ART; ISBN 978-1-5386- 1974-2.