An Enhanced Privacy and Security to Outsourced Public Cloud Storage

Nakshatra Saxena[1], Pallavi Marulkar[2] , Roshan Talap[3] , Khushbu Pandey[4]
BE, Dept. Student of Computer Engineering, PHCET,
Pillai HOC College of Engineering & Technology,
Rasayani

***Abstract*- With growth in technology, the use cloud computing is increasing day by day. Mainly large companies are associated with computing because of its cost effective way. The on demand services which can be accessed anytime and anywhere can be achieved by advanced computing platform. Cloud computing depends on sharing of resources to realize coherence and economies of scale, similar to a public utility. Due to this increasing demand for more cloud services, there is an ever growing threat of security becoming a major issue. Cloud computing poses privacy considerations as a result of the service supplier will access the info that's within the cloud at anytime. It cloud accidently or deliberately alter or delete information. The Advanced Encryption Standard(AES), and the Rivert -Shamir-Adleman (RSA) algorithms are the main popular encryption schemes that guarantee confidentiality and authenticity. The AES provides encryption and decryption to the data as it has 10 rounds for 12-bit keys, 12 rounds for 192-bit keys and RSA generally helps in distribution of keys. According to the work in this paper,a hybrid encryption algorithm based on these two security algorithm is introduced and implemented on a cloud platform which will have high execution rate.**

***Keywords:-** Cloud computing, Encryption, key encryption, Advanced standard encryption, Rivest-Shamir-Adleman*

I. INTRODUCTION

Cloud Computing has rapidly changed the IT industry .Enterprise outsourced data and compute services to cloud as cloud provides on demand computing resources in pay per fashion. In fact cloud computing is a scalable environment .Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. The company which provides cloud computing services is known as Cloud Service Provider (CSP). It is responsible to provide requested services on-demand to data owners or users. Data owner is an entity of person who is willing to outsource data to cloud. The data outsourced to cloud is associated with Infrastructure as a Service (IaaS) layer of cloud. The data owner is mainly worried that cloud is untrusted and security issues about the data which is outsourced .while enjoying the convenience of sharing data via cloud storage, users are more and more involved regarding accidental information leaks within the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in iCloud). To address users' concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud. Many working came for securing cloud , for confidentiality. There are some Third Party Auditing (TPA) based services and other schemes like Provable Data Possession (PDP) for secure storage in cloud computing. In this paper, cryptography based solution is available to enhance the privacy and security of outsourced data. Outsourcing is a method to obtain good and services from Third Party Supplier instead of in place of internal Source. Encryption Standard (AES) algorithm, information dispersal algorithm and secure hash algorithm are used appropriately to protect cloud data and achieve confidentiality, availability, security and privacy. By combining those three in encoding and decoding procedures enhanced security is achieved besides making the operations faster. As no single method can provide complete security, we found it useful for improving cloud storage security.

II. RELATED WORK

A. Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage:

Author-HuiTian, Yuxiang Chen, ChinChen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen and Jin Liu. 2016 IEEE

It achieve secure auditing in clouds and induce significantly fewer costs of storage, communication and computation.

B. Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation:

Author- Tao Jiang, Xiaofeng chen and jiang Ma 2015.

The objective of this paper is to secure and efficient shared data integrate auditing for multi-useroperation for ciphertext database.

C. Data Security for Cloud Computing with Double Layer Encryption Algorithm based on DNA and AES:

Author- Aura Raj, Ram Charan Kesireddi and Shruti Gupta 2015, In this paper new double layer cryptographic technique has been proposed which combines the novel DNA algorithm with the most secure AES algorithm.

D. An Analysis of the Cloud Computings Ssecurity Problem:

Author- Yibin Li, KekeGau, LongfeiQiu, MeikangQiu and Hui Zhao 2016

In this paper Role BasedEncryption (RBE) is used for Internet of Things (IOT) data.

III. EXISTING SYSTEM

Existing system uses three algorithm that is AES (Encryption Standard Algorithm), information dispersal algorithm, Secure hash Algorithm. While moving towards the conception of on-demand service, resource pooling, shifting everything on the distributive environment, security is the major obstacle for this new dreamed vision of computing capability. Our system permits a sender to send associate encrypted message to a receiver through a cloud storage server. The sender solely must recognize the identity of the receiver however no different info (such as its public key or its certificate). The receiver must possess 2 things so as to rewrite the ciphertext. The first issue is his/her secret key keep within the pc. The second thing is a unique personal security device which connects to the computer. It is not possible to rewrite the ciphertext while not either piece. More significantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any ciphertext. This can be done by the cloud server which might at once execute some algorithms to change this ciphertext to be un-decryptable by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decode any ciphertext at any time. The security and potency analysis show that our system isn't solely secure however conjointly sensible.

A. Problem Statement

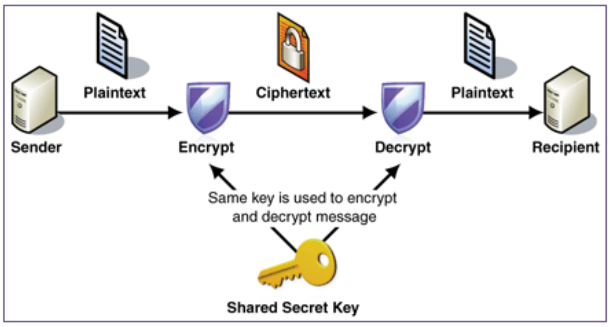
User users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. The company which provides cloud computing services is known as Cloud Service Provider (CSP). It is responsible to provide requested services on-demand to data owners or users. The data owner is mainly worried that cloud is untrusted and security issues about the data which is outsourced . Data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in iCloud. In this paper, cryptography based solution is available to enhance the privacy and security of outsourced data. Outsourcing is a method to obtain good and services from Third Party Supplier instead of in place of internal Source. Encryption Standard (AES) algorithm, information dispersal algorithm and secure hash algorithm are used appropriately to protect cloud data and achieve confidentiality, availability, security and privacy..

IV. PROPOSED SYSTEM

There area unit two sorts of cryptography algorithmic rules- symmetric-key algorithmic rule and asymmetric-key algorithm. For symmetric-key algorithm, the same cryptographic key is used for both encryption and decryption, in comparison to asymmetric-key algorithm symmetric-key algorithm like AES is usually high speed and low RAM requirements, but because its the same key both encryption and decryption, its big problem of key transport from encryption side(sender) to decryption side(receiver). For asymmetric-key algorithmic rule, it requires two separate keys, one of which is secret(or private) and one of which is public. Although totally different, the two parts ofthis key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature.

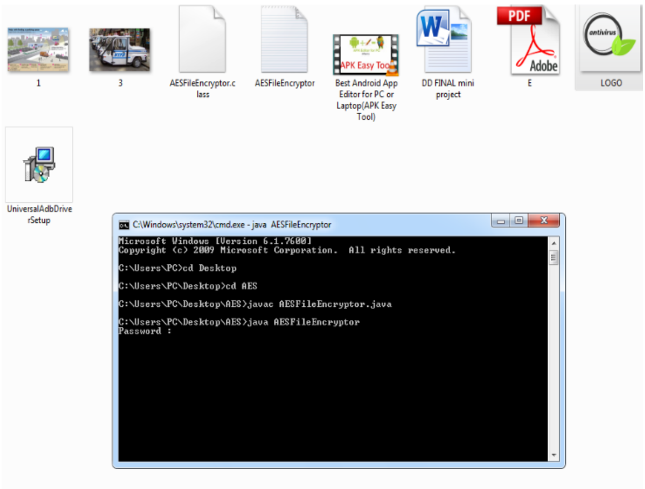
V. IMPLEMENTATION

Cloud Computing will become safer mistreatment cryptographical algorithms. Cryptography is that the art or science of keeping messages secure by changing the info into non clear forms. But the present cryptographical algorithms area unit single level cryptography algorithms. Cyber criminals can easily cracked single level encryption. Hence we propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage.

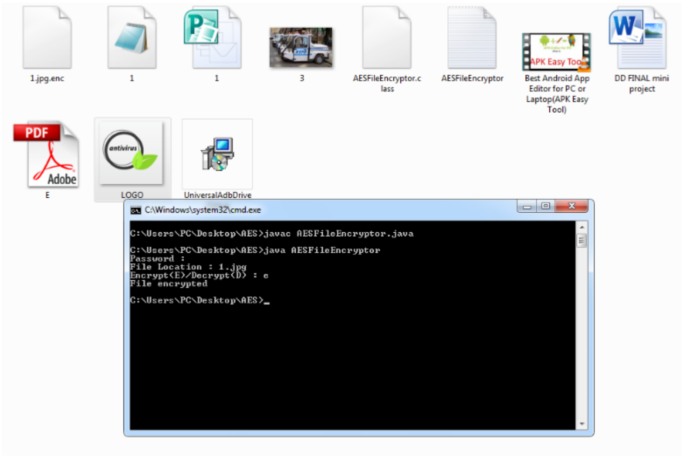


As our proposed algorithm is a Multilevel Encryption and Decryption algorithm. Thus, in our projected work, only the authorized user can access the data. Even if some persona non grata (unauthorized user) gets the info accidentally or designedly, he should need to decode the info at every level that could be a terribly tough task while not a valid key. It is expected that using multilevel encryption will provide more security for Cloud Storage than using single level encryption.

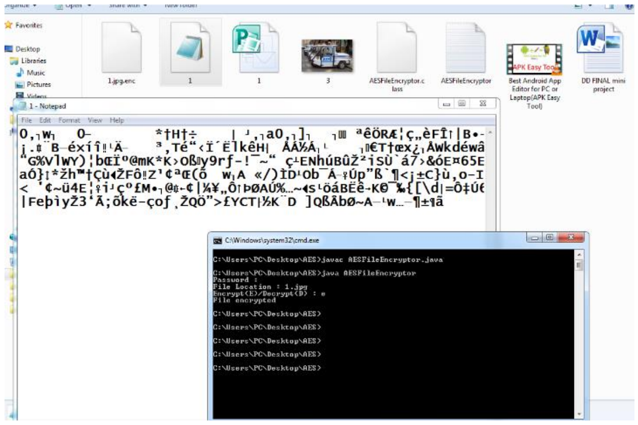
OUTPUT


1
3
AESFileEncryptor.class
AESFileEncryptor
Best Android App Editor for PC or Laptop(APK Easy Tool)
DD FINAL mini project
E
LOGO
UniversalAdbDriverSetup
C:\Windows\system32\cmd.exe - java AESFileEncryptor

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\PC>cd Desktop

C:\Users\PC\Desktop>cd AES

C:\Users\PC\Desktop\AES>javac AESFileEncryptor.java

C:\Users\PC\Desktop\AES>java AESFileEncryptor
Password :
```

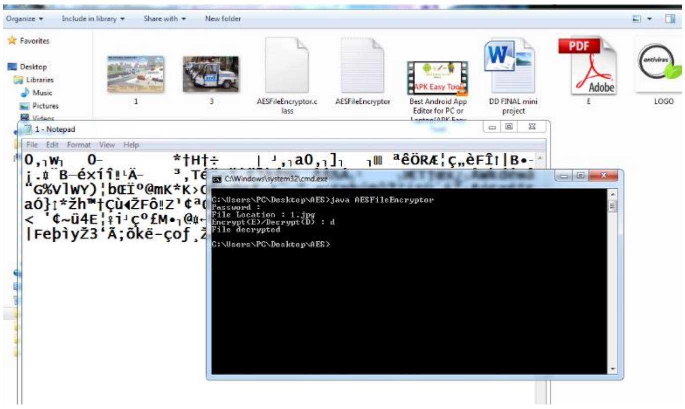


```
C:\Users\PC\Desktop\AES>javac AESFileEncryptor.java

C:\Users\PC\Desktop\AES>java AESFileEncryptor
Password :
File Location : 1.jpg
Encrypt(E)/Decrypt(D) : e
File encrypted

C:\Users\PC\Desktop\AES>_
```

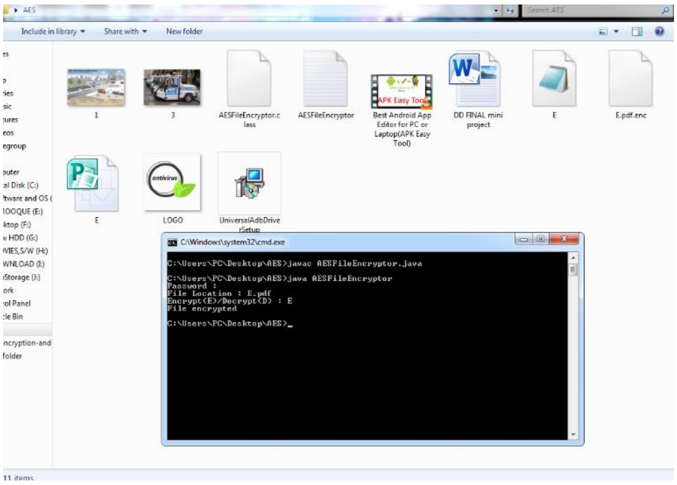


```
0,┐W┐   0─          *†H†÷     | ┘,┐a0,┐]┐   ┐▯ ªêÖRÆ¦ç„èFÎ↑|B•-
¡.‡¨B─éxíî‼└Ä─      ³,Té“‹Ï´ËlkêH| ÅÁ½Á┐└     ┐▯€T†œx¿┐Åwkdéwâ
“G%VlWY)¦bŒÏº@mK*K›Oß▯y9rƒ-!¯~“ ç┴ENhúBûŽ²ïSÙ`á7›&óE¤65E
aÓ}↕*žh™†Çù◄ŽFô‼Z'¢ªŒ(õ  w┐A «/)ÌD┴Ob¯Á─♀Úp”ß`¶<¡±C}ù,o-I
< '¢~ü4E¦♀ï┘çº£M•┐@‡←¢|¼¥„Ô↑ÞØAÚ%…~◄s└öáBËê→K©¯‰{[\d|=Ô‡Ú€
|FeþìyŽ3‘Ä;õkë-çoƒ¸ŽQÖ”>£YCT|½K¨D ]QßÂbØ~A─└w…─¶±¶ã
```

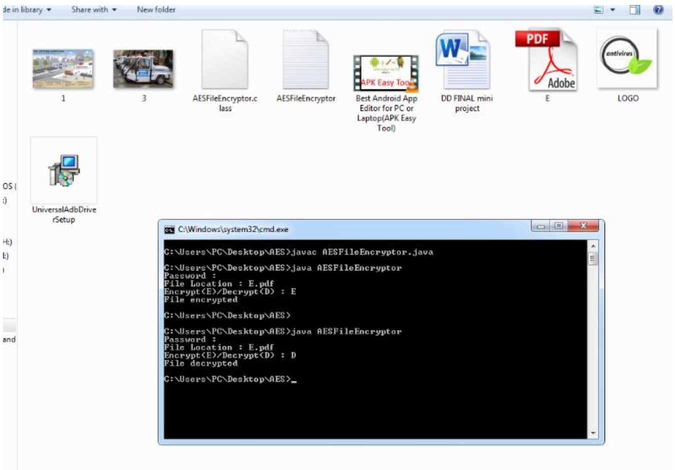
```
C:\Users\PC\Desktop\AES>javac AESFileEncryptor.java

C:\Users\PC\Desktop\AES>java AESFileEncryptor
Password :
File Location : 1.jpg
Encrypt(E)/Decrypt(D) : e
File encrypted

C:\Users\PC\Desktop\AES>

C:\Users\PC\Desktop\AES>

C:\Users\PC\Desktop\AES>

C:\Users\PC\Desktop\AES>

C:\Users\PC\Desktop\AES>
```



```
C:\Users\PC\Desktop\AES>java AESFileEncryptor
Password :
File Location : 1.jpg
Encrypt(E)/Decrypt(D) : d
File decrypted

C:\Users\PC\Desktop\AES>
```



```
C:\Users\PC\Desktop\AES>javac AESFileEncryptor.java

C:\Users\PC\Desktop\AES>java AESFileEncryptor
Password :
File Location : E.pdf
Encrypt(E)/Decrypt(D) : E
File encrypted

C:\Users\PC\Desktop\AES>_
```



```
C:\Users\PC\Desktop\AES>javac AESFileEncryptor.java

C:\Users\PC\Desktop\AES>java AESFileEncryptor
Password :
File Location : E.pdf
Encrypt(E)/Decrypt(D) : E
File encrypted

C:\Users\PC\Desktop\AES>

C:\Users\PC\Desktop\AES>java AESFileEncryptor
Password :
File Location : E.pdf
Encrypt(E)/Decrypt(D) : D
File decrypted

C:\Users\PC\Desktop\AES>_
```

ENC Key

A. *Requirement Analysis*

- Hardware Requirement :
  - Processor – i3 2.4 Ghz
  - Ram – 4GB DDR
  - Hard Drive – 256 GB
- Software Requirement :
  - OS – Windows 7 or above
  - Tool – Eclipse IDE

B. *Dataflow Diagram*

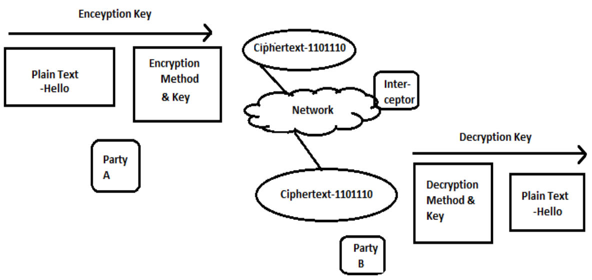


Figure 3: Dataflow Diagram

VI. RESULTS

The obtained results of the proposed technique are viewed in this section. The execution was done with Eclipse And encryption and decryption is done . Test performed on Various file formats to encrypt and decrypt the file (of any file format). This File have been taken by giving the file path and it is encrypted by giving a key . The file can be taken from any drive (c,d) or any location by giving the path.

AES and RSA algorithm are used. This algorithms are used to Encrypt and decrypt the data. This is implemented by using Amazon EC2 as cloud platform and Amazon S3 as storage service for outsourcing data. This system is more secured and privacy prone system.

VII. CONCLUSION

In this paper the quality of cloud storage security is been increased . As we know that the cloud storage is not that trusted , it is really important to protect and secured the cloud for the owner of cloud. There are two groups involved they are CSP(Cloud Service Provider) and owner of the data. Cloud service providers (CSP) are companies that offer network **services**, infrastructure, or business applications in the cloud and owner of data is who data is been owned or to be store in the cloud. We have used different cryptographic algorithm to give privacy and security to cloud. Here we have used Two major algorithms that are AES and RSA, AES is used for encryption and decryption and RSA is used for encoding and decoding the procedures. This framework is more secured in terms of encryption, decryption ,uploading the data and downloading the data.

REFERENCES

[1] HuiTian, Yuxiang Chen, Chin-Chen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen and Jin Liu,. (2016). Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage. IEEE, p1-14

[2] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma. (2015). Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation.IEEE, p1-12.

[3] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma. (2018). Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation.IEEE, p1-12.

[4] Dr. Anitha Patil *, Govind Rao Mettu .(2018).An Enhanced Privacy And Security To Outsourced Public Cloud Storage.ISSN