International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 10th Apr 2019. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-04

Title: SECURED FILE SHARING OVER CLOUD IN MODULAR WAY USING MULTILAYERED ENCRYPTION STANDARDS AND STEGANOGRAPHY TO AVOID DATA BREACH

Volume 08, Issue 04, Pages: 155–161.

Paper Authors

DINESHSURISETTI, I.RAVI KUMAR, DR. M. JAMES STEPHEN

Wellfare Institute of Science Technology and Management, Visakhapatnam, A.P

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SECURED FILE SHARING OVER CLOUD IN MODULAR WAY USING MULTILAYERED ENCRYPTION STANDARDS AND STEGANOGRAPHY TO AVOID DATA BREACH

[1]DINESHSURISETTI,[2]I.RAVI KUMAR, [3]DR. M. JAMES STEPHEN
[1]B.Tech Scholar, Dept. of CSE, Wellfare Institute of Science Technology and Management, Visakhapatnam, A.P
[2]Assistant Professor, Dept. of CSE, Wellfare Institute of Science Technology and Management, Visakhapatnam, A.P
[3]Professor,Dept. of CSE, Wellfare Institute of Science Technology and Management, Visakhapatnam, A.P
[1]dineshsurisetti@gmail.com, [2]ravirk1228@gmail.com, [3]jamesstephenm@yahoo.com

Abstract:
We proposed a system to avoid data confidentiality even when there occurs a data breach at public domain on cloud, by using some principle function of steganography, encryption with numerous algorithms with receiver's authentication protocols to yield a secured and reliable file sharing model. .With the Help of clouds, Files are store over them, it acts as buffer. But most of the time Files are encrypted once or not encrypted at all which could lead to vulnerability in file sharing. Our aim is to overcome such vulnerabilities by introducing multiple Public Keys assigned to one file. Which would be helpful not only while sharing a File , but also will decrease the chances of sophisticated hackings , files can be divided into 'n' modules which will be assigned to 'n' different keys which will potentially increase the security of a file by 'n' times.

1. Introduction:

File Sharing Mechanism is a key role to be played in day to daily life. Every Day billions of Files are shared securely over one end to another. With the Help of clouds, Files are store over them, it acts as buffer. But most of the time Files are encryptedonce or not encrypted at all which could lead to vulnerability in file sharing. Our aim is to Overcome such vulnerabilities by introducing multiple Public Keys assigned to one file. Which would be helpful not only while sharing a File , but also will decrease the chances of sophisticated hackings , files can be divided into 'n' modules which will be assigned to 'n' different keys which will potentially increase the security of a file by 'n' times.

'n' modules = 'n' Keys

Greater the value of 'n' higher will be the File security.

Data breaches that end up in the media spotlight are a small fraction of total breaches. A quick web search finds that companies that are commonly seen as impenetrable (Google, Amazon, Apple, etc.)

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

have all been breached (and these are only the few that have been reported).[1]

2. Existing System:

For file sharing, IPFS (Inter Planetary File Sharing) is used in existing system. It mainly uses Blockchain technology, it bound to Module Traversing, uses Asymmetric Encryption, generates public key to access file. The complete file is encrypted using single key and generates public key in this system. The usage of RAM is more as complete file has to be placed on RAM.

3. Proposed System:

3.1 Idea:

- Sharing files via the internet has been troublesome when it comes to security. We introduced a solution to solving some of these problems. This will not only avoid data breaching but also avoid data leakage when it falls into the wrong hands.
- The multilayer algorithm ensures a though composition to decrypt a file. There are more than 70, 55 x 10^{84}(seventy septenvigintillion) different combinations of Encryption keys, and you just need one of those for the file.
- Salient Features:
  - We provide 2-Factor Authentication
  - a solution to store encrypted data
  - Backup Security Encryption
  - Dividing a file into modules is always safer as it lowers the risk factor of "man in middle" attack.
  - In addition each module is assigned with its own unique key providing more security to the files.
  - Modulation also helps in less consumption of RAM while Encrypting, thereby letting other tasks run normally.

Our encryption obeys symmetric encryption which assigns each block of data with a unique key, which ensures dual layering. Receiver will receive an image of a size roughly 200kb, the file will be decrypted and be presented in a selected folder.

IPFS(Inter Planetary File Sharing)	Our Method
> Uses Blockchain Technology	> Similar but with more Ease
> Bound to Module Traversing	> Module Traversing
> Asymmetric Encryption	> Symmetric Encryption
> Generates Public Key to access File.	> Checks for authenticity, which makes direct Interaction of file without the use of a KEY.
> Whole File is Encrypted using single Key and generates Public Key	> Chunks of File is Encrypted using Different Unique Keys.

fig: Comparison with existing system techniques

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3.2 System Architecture:

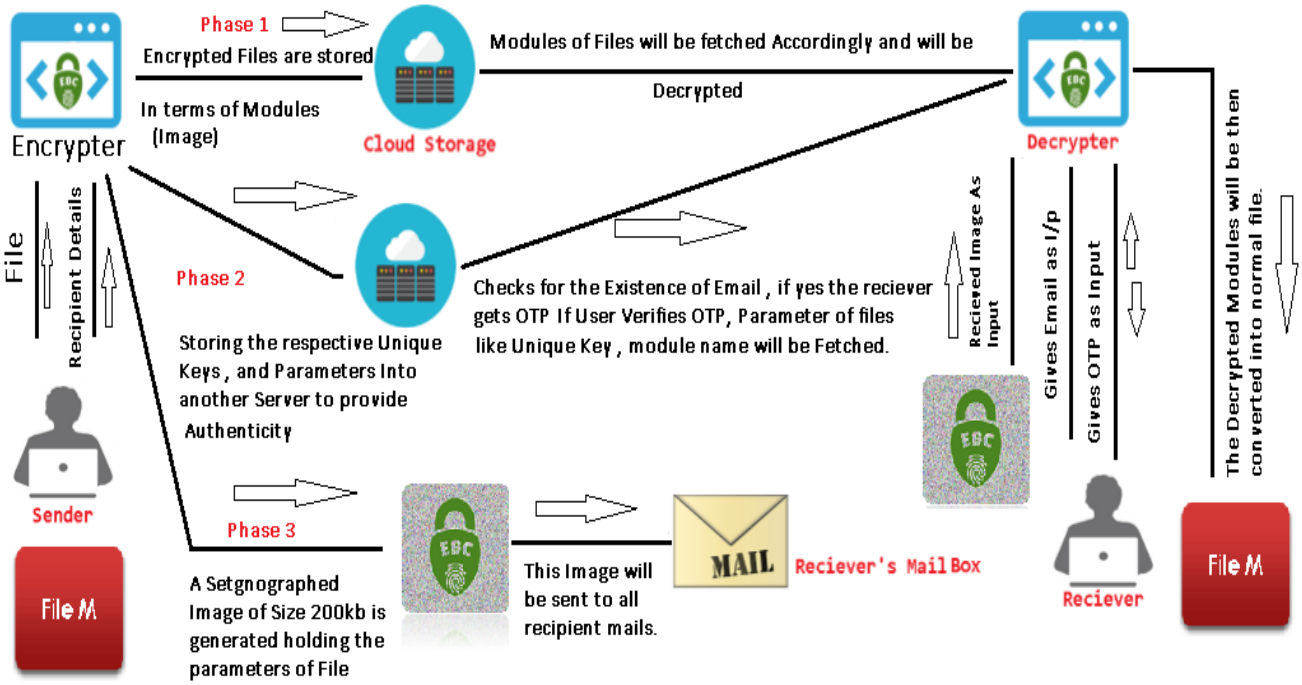


fig: system architecture

NOTE: These Steganographed images of modules are formed in RAM and are not stored in Secondary Memory which will not let the user know about the existence of the modules.

3.3 Modules Description:

3.3.1 Encryption:

1. The file, along with the recipient list, is first read and divided into *'n'* different module (example 'n'=9).
2. Each module is then assigned with a unique KEY string, which's length is ranging from 32-50 characters.
3. Each module then undergoes encryption using different algorithms which involves a unique file encoding ASCII pattern.
4. These modules are linked internally in a sequential manner and then are separately formed into an Image.
5. These images are then stored over Cloud.
6. The final EBC card is then obtained as output. Irrespective of the input file size, the encrypted files will always be 165KB, which can be transported anywhere very easily.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

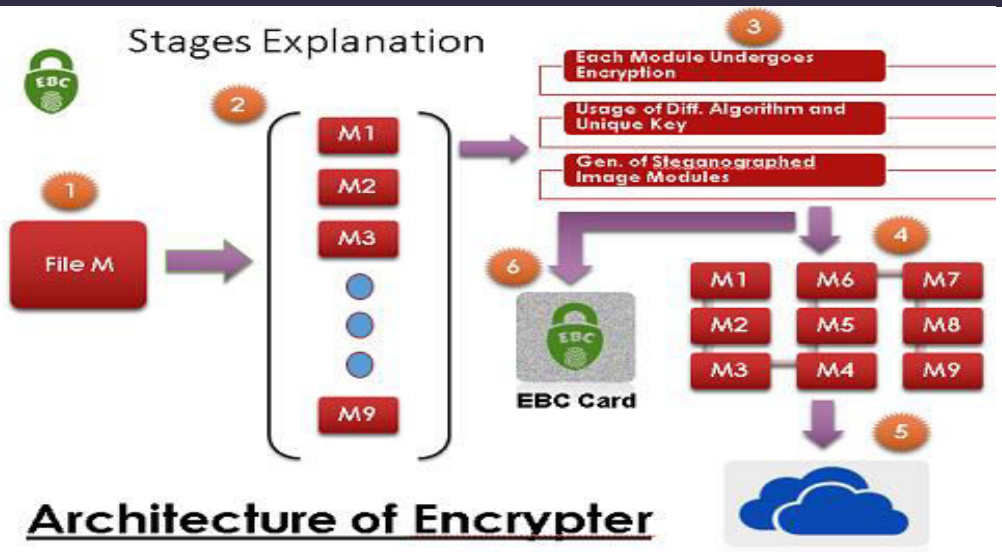


fig: encryption architecture

3.3.2 Decryption:

1. The received EBC card is placed along with receiver's email address as Input.
2. The recipient list is checked to ensure whether the provided email has permission to access the shared file.
3. If the recipient's email address has permission, the OTP will be sent to the corresponding receiver's phone number, provided by the Sender.
4. When approved, all the corresponding files will be retrieved from the backend records; modules will be called from the cloud and then will undergo decryption accordingly.
5. The decrypted files will be saved in a "Decrypt Dumps" Folder.

NOTE: Modules are retrieved in RAM and are not stored in secondary Memory which will not let the receiver know about the existence of the modules.

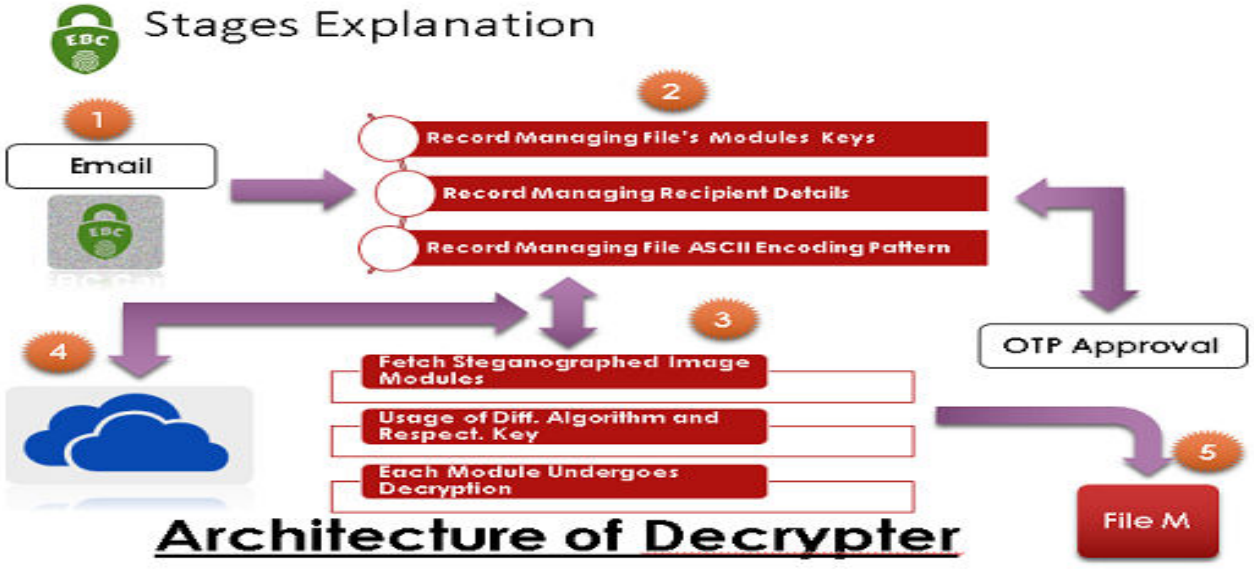


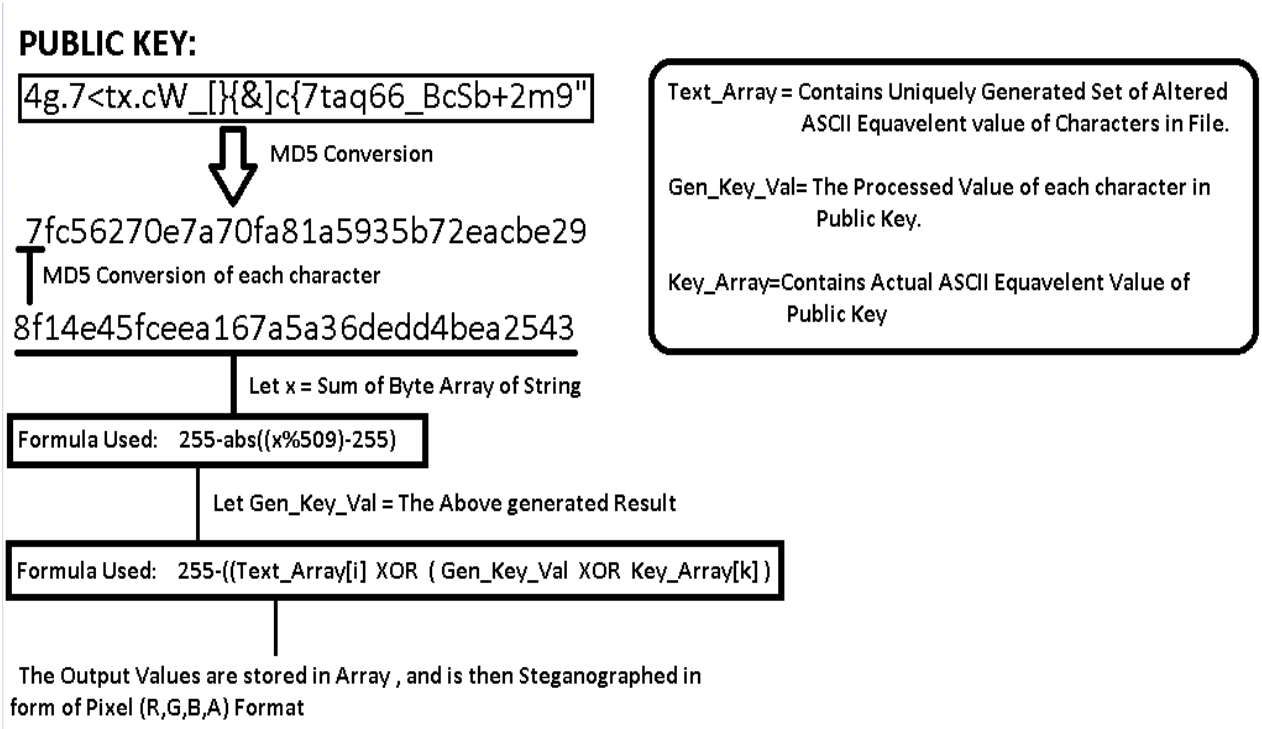
fig: decryption architecture

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3.4 Methodology:

3.4.1 Algorithm:

- ➔ Taking in consideration of Altered ASCII Values SET which is uniquely generated every time.
- ➔ Dividing the Files into Chunks of EQUAL SIZES, The each Chunk holding Values are converted into their respective ASCII Value from the uniquely generated Altered ASCII Set and are stored in Matrix.
- ➔ The Keys are Encoded using the below mentioned Formulas Which Consists of Repeated Usage of MD5 Conversion , Conversion of String into Byte Array , Conversion of String into it's respective ASCII Equivalent Array , Performing XOR operations.



- ➔ Formation of Image on RAM (Main Memory) itself without actually storing it On HDD.
- ➔ Linking of Each Chunks Internally
- ➔ Converting Chunks in the form of Image

3.4.2 Implementation:

Platform: Python

API's:

- Google API
- Drop Box API
- SMS API

Packages or Libraries:

- io, random, time, os, way2sms,drop box, Gmail, tempfile, shutil, sub process,sys,zlib,base64,hashlib,math,

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

gspread,pprint,oauth2client.service_account,itertools,ast,tqdm,PIL,coloramа,termcolor,pyfiglet

Python is a Light Weight Programming Language serves multiple purposes while dealing with complex Calculations, Integrating with online Web API's.

4. Results:

Total File Size: 47.7 MB

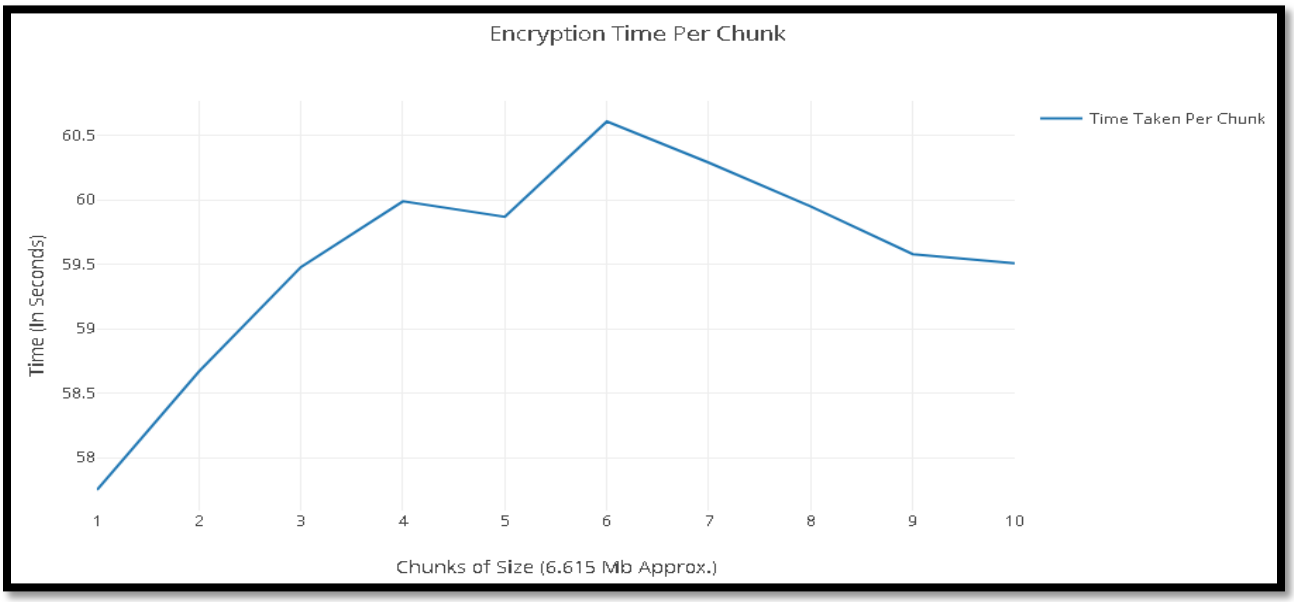
Output Sum of Chunks File Size: 67MB (approx.)

Increase in Size: 27.9%

Average Calculated Encryption Time: 6.615 MB / Min (approx.)

Improvement Techniques(Yet to be tested):

- ➔ Usage of Vectorization which could possibly make it 300 times faster than current Speed.
- ➔ Implementation of Multithreading Concept which can be used to achieve Parallel Processing.



4.1Current Problem and its Solution:

❖ Is your data secured when a Data Breach Happens?

From the recent Analysis of Data Breach it is clear that 96% of the breaches were "Unsecured Breaches" where the data was not encrypted.

The only remaining 4% of Breaches were "Secured Breaches" where the data was encrypted.

Development in technology increases every day, yet no one knows how to stop the increase in security breaches.

5. Conclusion:

- ▶ Instead of focusing on IOT (Internet Of Things), we gave priority to EOT(Encryption Of Things).
- ▶ Our aim is to reduce the number of breaches by providing security to stored files, by using encryption at the premature level itself.

6. References:

[1]https://medium.com/west-stringfellow/cybersecurity-guide-how-to-secure-your-corporation-4f19768d0f39
[2]https://onlinelibrary.wiley.com/doi/full/10.1002/widm.1211