ENHANCING DATA SECURITY USING CRYPTOGRAPHIC TECHNIQUES IN PUBLIC CLOUD STORAGE ENVIRONMENTS

Dr. P. Maragathavalli[1], Assistant Professor[2]
Department of Information Technology, Pondicherry Engineering College, Puducherry, India.

Abstract

Cloud computing becomes an evolving technology which offers services to its users over the internet. Cloud storage is a model of data storage, which is maintained and backed up remotely and made feasible from multiple distributed and connected resources. Since cloud computing stores the distributed resources and data in the public environment, security has become the main hurdle which is hindering the deployment of cloud environments. Due to the security issues in cloud many users are reluctant to use it for personal and sensitive data storage. Since cloud storage is third party storage it needs special data security solutions than traditional third party storage's. In this paper we use a technique called Modified Advanced Encryption Standard (M-AES) algorithm in order to enhance the cloud storage security. In this technique the encryption and decryption uses same key which makes the data more protected from unauthorized user to access the data from the cloud. The encryption and decryption process will be completely cloudy (opaque) to the user. The security parameters such as confidentiality, trustworthiness and integrity in group sharing framework play a major role. The implementation results demonstrate the efficiency and analysis of our proposed system, using the multimedia (text, images, audio) data is provided.

Keywords: cloud computing, cryptographic algorithm, data security, security issues, user authentication.

1. Introduction

Cloud is a multi-tenant environment, where resources are shared. Cloud computing has reached popularity and developed into a major trend in IT. Cloud storage is networked data storage where data is stored in pools that span multiple servers and are generally managed and hosted by third parties rather than being hosted on dedicated servers. Storing information in a third party's cloud system causes severe involvement on information confidentiality. There are many advantages in using cloud storage. A notable advantage of cloud storage is data accessibility. Once a data is stored in the cloud, it can be accessed any time, any place as long as there is network access.

As cloud environment becomes more mature as there are more applications and storage services provided by the cloud, it is therefore important to foresee that the security for data protection in the cloud should be further increased. Security is generally perceived as a huge issue in cloud. A wide variety of security threats have been found in the cloud environments due to the vast amount of data stored on cloud servers.

The severity of damage tends to depend on the sensitivity of the data exposed. Some of the security issues which is faced by the cloud computing includes data integrity and data theft. Cloud storage security processes should address the security controls the cloud provider will incorporate to maintain the user's data security, privacy and compliance with necessary regulations.

This paper is concerned in identifying the major data security and privacy concerns of cloud storage systems and provides the solution. To keep data secure, the important needed protection is encryption. Encryption methods utilize complex algorithms to hide cloud-protected information. To decipher encrypted files, receivers need the encryption key.

In the existing system [2] Joseph K. Liu, Kaitai Liang and Willi Susilo used two factor mechanisms for cloud security. In two-factor data encryption protection, there should be two necessary things required to decrypt the file. First, the user needs to have a secret key which is stored in the computer. Second, the user should have a unique personal security device which will be used to connect to the computer (e.g., USB, Bluetooth). It is impossible to decrypt the cipher text without either piece. The second factor involved in protection is revocability. Once the security device is stolen or reported as lost, this device is revoked. That is, using this device can no longer decrypt any cipher text in any circumstance. We have analysed the recent developments in two factor secret key formations, future trends in cloud environment. In this paper, we propose a technique named Modified AES mechanism for providing security to the cloud data.

This paper is organized as follows: the section 2 discusses about the related work, section 3 describes about the proposed work followed by implementation in section 4, next section 5 analyses the results with the system description, section 6 concludes the paper followed by references.

2. Related work

Sulton Aldossary, William Allen [1] proposed Identity Based Encryption (IBE), Attribute Based Encryption and Public Based Encryption. The jpeg images were encrypted. It is based on the metrics of Secured cloud storage and Data vulnerability to internal and external threats was the drawback in this system.

Dr. S.S. Manikandasaran [3] proposed a Public key cryptography. The data set which was used is audio and images. It is based on the metrics of data interception and the limitations are insiders attacks are very difficult to identify and also very tough to protect data.

Kire Jakimoski [2] proposed a Secure Socket Layer (SSL) technology. The data set which was used is Mp3, video. It is based on Enforcement of encryption policy to protect sensitive data and it is based on the drawbacks of not concentrated on security issues.

R. Velumadhava Rao, K. Selvamani proposed RSA encryption algorithm. The text file documents were shared and encrypted. It is based on the metrics of Supports access of larger files and Transmission of data is not proper in this work. Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy proposed a Time-based one-time password, Automatic block protocol. Existing text documents was used. It is based on the metrics of less data loss and the major drawback is minimal usage of password.

In most of the papers mentioned above they used encryption techniques such as Identity Based Encryption (IBE), Public Key Encryption (PKE) and Attribute Based Encryption (ABE).

The Identity Based Encryption is a public-key cryptosystem which is based only on valid public key. IBE solutions may rely on cryptographic techniques that are insecure against code breaking quantum computer attacks. The Private Key Generator (PKG) generates private keys for users; it may decrypt and/or sign any message without authorization. This implies that IBE systems cannot be used for nonrepudiation.

The Public Key Encryption can encrypt a message using the public key of the receiver, but such a message can be decrypted only with the receiver's private key. Because of the computational complexity of asymmetric encryption, it is usually used only for small blocks of data and only protects what it's designed to protect.

The Attribute Based Encryption is a public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. ABE systems have few drawbacks such as non-efficiency and non-existence of attribute revocation mechanism. The above mentioned techniques concentrates on the data loss, storage maintenance and data interception. They can be improved by giving additional security to database and authentication issues so that the time can be utilized effectively. By giving additional security, parameters such as confidentiality, integrity and privacy can be improved.

3. Proposed system

The proposed system of group sharing framework, in which the users can share file with individual member or group of members, uses a technique called Modified AES for file encryption and decryption which is an important primitive of symmetric block cipher algorithm. As such it is a type of symmetric encryption which uses same key for encrypting and decrypting, so both the sender and receiver must know and use the same secret key. This means that a sender who has access to the public parameters of the system can encrypt a message. The receiver obtains decryption key from a sender who needs to be trusted as they generate secret key for every user. The system architecture of the proposed work is described below in the Figure1.

The objective of this system is to enhance security for data which is stored in the cloud, reduce violations, and minimize encryption and decryption time and improve the parameters associated with the data security. The group sharing framework consists as follows:

1. File Sharing in Social Networking
2. Encryption using Modified AES Algorithm
3. Decryption using Modified AES Algorithm

3.1 File Sharing in Social Networking
Social Networking consists of admin and the user. The Figure 2 shows the flow of the operations involved in this phase. The process starts at login for already registered user or register for new user. Once the user has registered, the user has the authority to send request, to accept request, to create group and to access the files which are uploaded by their friends. The admin has the authority to approve the files which were uploaded, to access the details of the user.

3.2 Encryption using Modified AES Algorithm
Encryption is the process of converting data into an unintelligible form by making use of a key or password. The data is made useless without the corresponding decryption key or password. The file uploaded by sender gets encrypted and stored in the database. The Advanced Encryption Standard (AES) is a symmetric block cipher which uses single key for both encryption and decryption process. In Modified-AES algorithm, the modification is done by totalling the Initial Permutation step, takes from DES (Data Encryption Standard), in order to enlarge the encryption performance. This modification undoubtedly increases the efficiency of encryption.

To overcome the problem of high calculation and computational cost, we modify the Advanced Encryption Standard (AES), to reduce the calculation of algorithm and for reducing the time taken for encryption as well as decryption. In Modified-AES encryption and decryption process resembles to that of AES, in account of number of rounds, data and key size. Mixcolumn step gives better security but it takes large calculation that makes the encryption algorithm slow. We add the permutation step instead of Mixcolumn step to overcome the drawback of high calculation.

3.3 Decryption using Modified AES Algorithm
Same sequence of encryption transformations is applied on decryption structure as which is applied in encryption structure. The transformations i.e. Inv-Bytesub, Inv-Shiftrows, Inv-Mixcolumns, and Addroundkey permit the type of key schedules to be matched for encryption and decryption. Here it must be noted that the Mixcolumn reverse operation requires matrix elements. So we go for InvPermutation process instead of Inv-Mixcolumns. One such type of brute force attack is “Search Attack” in which it covers all possible combinations of a character set and ranges of password length. To prevent such attack, we produce a fake file when an incorrect OTP is entered.

4. Implementation

The implementation of the proposed system works as follows:

4.1 File Sharing in Social Networking
Social Networking phase consists of following functionalities
4.1.1 Sending Request and Confirming Friends
When a user logs in, he/she can send requests to another user by searching their profile names. Accordingly, the result will be displayed below it. If a person has given request, it will be shown in the pending request; so that the user can accept or reject according to his/her wish. After accepting requests, they can view each one’s profile.

4.1.2 Session Timeout

A session remains alive even when the users do not perform any action on a web site during certain interval of time. Security vulnerabilities related to authentication occurs. The vulnerabilities are not known to be fixed yet and it is a threat to the users. Hence a short timeout of 2 minutes is given, if the user does not refresh or request a page within the time-out period, the session ends and it goes to the login page.

4.1.3 File Sharing

The user can share file that has been already uploaded by him/her and can share files with his/her friends in two ways. The Figure 3 shows the flow of the operations involved in this phase. One way is to select the friends individually in the friends list and another way are to create a group and sharing the files in the group. OTP with file name will be generated and send to the corresponding mail-ID. The Figure 4 shows the sender sharing a file to their friend. The respective user can download the file by entering the correct OTP.

4.2 Encryption using Modified AES Algorithm

The user can upload or download files in a social network. The user can upload files in any format (except video files). The uploaded files will be encrypted using Modified AES Algorithm. The encrypted file gets decrypted and made accessible by the receiver if and only if receivers enters the secret key (OTP) correctly.

The Modified - AES algorithm is divided into four steps and it is designed in such a way that it can take any combination of data and is flexible for key size of 128 bits. The four blocks combines to one round of Modified-AES. The four steps that we use for ModifiedAES Algorithm are:

- Substitution bytes
- ShiftRows
- Permutation
- AddRoundKey

AES Encryption:

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
    begin

        byte state[4,Nb]
        state = in
        AddRoundKey(state, w[0, Nb-1])


        for round = 1 step 1 to Nr–1


            SubBytes(state)
            ShiftRows(state)
            MixColumns(state)
            AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])


        end for
        SubBytes(state)
        ShiftRows(state)
        AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

        out = state


    end
```

M-AES Encryption:

```
Cipher(bytebegin in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)]) 
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w[0, Nb-1])
    for round = 1 step 1 to Nr–1
        SubBytes(state)
        ShiftRows(state)
        Permutation(state)
        AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
    end for
    SubBytes(state)
    ShiftRows(state)
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
    out = state
end
```

Substitution Bytes, Shiftrows and Addroundkey remain the same as it is in the AES. The Permutation step is used instead of Mixcolumn. Permutation tables are used in the DES algorithm. The inputs to the IP table consist of 128 bits. Modified-AES algorithm takes 128 bits as input. The Substitution Bytes and ShiftRows steps of Modified-AES are taken as 128 bits whereas the Permutation step also interpreted as 128 bits. After permutation process, the complete set of 128 bits is taken and then remaining steps of algorithm are performed. The Figure 5 shows the encrypted format of JPEG file where the actual content of the image is hidden and it should be decrypted to view the original content.

4.3 Decryption using Modified AES Algorithm

The decryption process for Modified-AES algorithm involves, Inv-Bytesub, Inv-Shiftrows, InvPermutation, and the AddRoundkey, which are performed in 10 rounds as it is in the encryption process. If we take the inverse permutation it gives again the original bits, the output result is a 128-bit original text. When the user enters the correct OTP, the decrypted file gets downloaded. Whenever Search attack occurs, fake file get downloaded. So it will be difficult for the attacker to know when he has guessed correctly and therefore the user has to enter the OTP correctly. From Figure 6, it is depicted that wrong file is downloaded when incorrect OTP is entered by the user.

AES Decryption :

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
    for round = Nr-1 step -1 downto 1
        InvShiftRows(state)
        InvSubBytes(state)
        AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
        InvMixColumns(state)
    end for
    InvShiftRows(state)
    InvSubBytes(state)
    AddRoundKey(state, w[0, Nb-1])
    out = state
end
```

```
M-AES Decryption :
InvCipher(byte in[4*Nb], byte out[4*Nb], word
w[Nb*(Nr+1)]) begin
            byte   state[4,Nb]
            state = in
            AddRoundKey(state, w[Nr*Nb,
            (Nr+1)*Nb-1]) for round = Nr-1 step -1
            downto 1 InvShiftRows(state)
                  InvSubBytes(state)
                  AddRoundKey(state, w[round*Nb,
                  (round+1)*Nb-1])
                  InvPermutation(state)
            end for
            InvShiftRows(state)
            InvSubBytes(state)
            AddRoundKey(state, w[0, Nb-
            1]) out = state
      end
```

5 Results and discussion

In the experiments, different file size ranges from 100 K byte to 1000 K bytes were encrypted. The performance metrics considered for experimentation are Encryption and Decryption Time. The encryption time for Modified AES is less when compared to the other existing algorithms which are shown in Figure 7. The decryption time for Modified AES is less when compared to the other existing algorithms which are shown in Figure 8. The encryption and decryption process using Modified AES algorithm reduces high calculation and improves the security.

Encryption Time = Time taken for transformation of cipher text from plain text

Decryption Time = Time taken for transformation of plain text from cipher text

In Table 2 it is depicted that the measure of security in terms of low, medium and high. By considering the security parameters such as confidentiality, trustworthiness and integrity, the security in proposed work is comparatively higher than the existing system. In proposed work, we increase confidentiality by encrypting the data using Modified AES algorithm, trustworthiness is improved by sharing the files only with the friends and integrity is increased by providing OTP for each file which is to be downloaded.

6 Conclusions

In this paper, a technique called Modified Advanced Encryption Standard (M-AES) has been proposed in order to enhance the data security. The proposed M-AES improves the confidentiality of the data by providing additional authentication information such as fake file for incorrect OTP, file sharing group.

By assigning unique secret for each individual user in a group enhances security as well as reduces the time taken for a single file transaction. The implementation of M-AES reduces the encryption and decryption time when compared to the existing IBE and PKE. In version of security analysis and experimental results, our proposed encryption scheme is fast and on the other hand it provides good security and adds very less overhead on the data, this today is the requirement of most of the multimedia applications.

References

1. Sulton Aldossary and William Allen (2016), "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", *International Journal of Advanced Computer Science and Applications,* pp. 485-498.

2. Joseph K. Liu, Kaitai Liang and Willi Susilo (2016), "Two-Factor Data Security Protection Mechanism for Cloud Storage System", IEEE Transactions on Computers, Vol. 65, No. 6, pp. 92-104.

3. Dr. S. S. Manikandasaran (2016), "Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage", *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS),* Vol. 6, No. 1, pp. 498-503.

4. KireJakimoski (2016), "Security Techniques for Data Protection in Cloud Computing", *International Journal of Grid and Distributed Computing,* Vol. 9, No. 1, pp. 49-56.

5. Apurva R. Naik and Lalit B. Damahe (2016), "Enhancing Data Security and Access Control in Cloud Environment using Modified Attribute Based Encryption Mechanism", *International Journal of Computer Network and Information Security*, Vol. 10, pp. 53-60.

6. K. Subramanian and F. Leo John (2016), "Data Security in Single and Multi-Cloud Storage", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, No. 11, pp. 46-52.

7. Nithya Chidambaram, Pethuru Raj and K. Thenmozhi (2016), "Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique", *International Journal of Digital Multimedia Broadcasting*, pp. 1-7.

8. D.I.George Amalarethinam and B. Fathima Mary (2016), "Confidentiality Technique for Enhancing Data Security in Public Cloud Storage using Data Obfuscation", *International Journal of Computer Technology and Applications*, Vol. 9, pp. 107-113.

9. Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy (2016), "A secure cloud storage system combining time-based one-time password and automatic blocker protocol", *El-Booz et al. EURASIP Journal on Information Security*, Vol. 13, pp. 1-13.

10. RamalingamSugumar and SharmilaBanu Sheik Imam (2015), "Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage", *Indian Journal of Science and Technology*, Vol. 8, No. 23, pp. 1-5.

11. R. VelumaDhavaRaoa and K. Selvamanib (2015), "Data Security Challenges and Its Solutions in Cloud Computing", *International Conference on Intelligent Computing, Communication & Convergence*, pp. 204-209.

12. Santanu Chatterjee and Ashok Kumar Das (2015), "A Secure and Effective Access Control Scheme for Distributed Wireless Sensor Networks*", International Journal of Communication Networks and Distributed Systems*, Vol. 14, No. 1, pp. 40-73.

13. Aized Amin Soofi, M. Irfan Khan and Fazal-e-Amin (2014), "A Review on Data Security in Cloud Computing", *International Journal of Computer Applications*, pp. 1-9.

14. Zhu, G.J. Ahn, H. Hu and S.S. Yau (2014), "Dynamic Audit Services for Outsourced Storages in Cloud", *IEEE Transactions on Services Computer*, pp. 1-8.

15. Ashok Kumar Das and VangaOdelu (2014), "An Efficient Access Control Scheme in User Hierarchy based on Polynomial Interpolation and Hash Function", *International Journal of Communication Networks and*

Distributed Systems, Vol. 12, No. 2, pp. 129-151.

16. Yang, X. Jia, K. Ren and B. Zhang (2013), “Effective Data Access Control for Multi-Authority Cloud Storage Systems”, *IEEE Transactions Information Forensics Security*, pp. 1-9.

17. Young jun Ren, Jiang Xu and Jin Wang (2013), “Designated-verifier Provable Data Possession in Public Cloud Storage”, *International Journal of Security and its applications*, Vol. 7, No. 6, pp. 11-20.

SL. NO	AUTHOR S & YEAR	TITLE OF THE PAPER	JOURNAL / CONFER ENCE NAME	TECHNI QUES OR METHOD S USED	PARAME TERS CONSIDE RED	DATA SET USED	DIS ADVANT AGES
1.	Y.Zhu, G.J.Ahn,H. Hu and S.S.Yau	Dynami c audit services for Outsour ced storages in Cloud	IEEE Transacti ons on Services Computi ng, 2014	Efficient approach es based on probabili stic query and periodic variety	Dynamic audit, storage security, integrity and verificatio n.	mp3,.txt	Untrusted storage of Cost
2.	Ramalinga m Sugumar and SharmilaB anu Sheik Imam	Symmetr ic Encrypti on Algorith m to Secure Outsourc ed Data in Public Cloud Storage	Indian Journal of Science and Technolog y, Vol. 8, No. 23, 2015	Public key Cryptogra phy	Time, Efficiency, Optimality	Existin g Text documen ts	Less Interaction with users
3.	Santanu Chatterjee and Ashok Kumar Das	A Secure and Effective Access Control Scheme for Distribut ed Wireless Sensor Networks	Internation al Journal Communic ation Networks and Distributed Systems, Vol.14, No.1, 2015	Formal Security Verficatio n Widely Accepted Automated Validation of Internet Security Protocols and Applicatio ns (AVISPA) tool	Confidential ity, Efficiency	Existing text documen ts	Not secure against node replication attacks

4.	KireJakimoski	Security Techniques for Data Protection in Cloud Computing	International Journal of Grid and Distributed Computing Vol. 9, No. 1, 2016	Secure socket layer(SSL) Technology	Reliability	.mp3, videos	Not concentrated on security Issues
5.	Dr. S.S. Manikandasaran	Security Attacks And Cryptography Solutions for Data Stored in Public Cloud Storage	IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol.6, No1, 2016	Public key Cryptography	Authenticity	Downloaded audio and video images	Insiders' attacks are very difficult to identify and also very tough to protect data
6.	Sulton Aldossary, William Allen	Data Security, Privacy , Availability and Integrity in Cloud Computing: Issues and Current Solutions	International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016	Identity Based Encryption, Attribute Based Encryption, Public Based Encryption	Efficiency, Availability	Existing jpeg images	Data Vulnerable to internal and external Threats
7.	Joseph K. Liu, Kaitai Liang and Willy Susilo	Two Factor Data Security Protection Mechanism for Cloud Storage System	IEEE Transactions on Computers ,Vol. 65, No. 6, 2016	Identity Based and Public Key Encryption	Efficiency, Security	Existing image documents	Confidentiality of the data is very less

8.	Sheren A.El-Booz,Gama l Attiya and Nawal El-Fishawy	A secure Cloud Storage System combinin g time- based one-time password and automatic blocker protocol	El-Booz et al. EURASHIP Journal on Informatio n Security, Vol. 13,2016	Time – based one time password, Automatic block protocol	Effectiveness, efficiency	Existing text documents	Less secure authentication
9.	Ashok Kumar Das and VangaOdelu	An Efficient Access Control Scheme in User Hierarch y based on Polynomial Interpolation and Hash Function	Internation al Journal of Communication Networks and Distributed Systems, Vol. 12, No. 2,2014	Practical solution for Dynamic Access Problems in a User Hierarchy	Security, Availabilit y	Associative arrays and dynamic sets	Less storage space

Table 1 Comparative Study on Existing Works

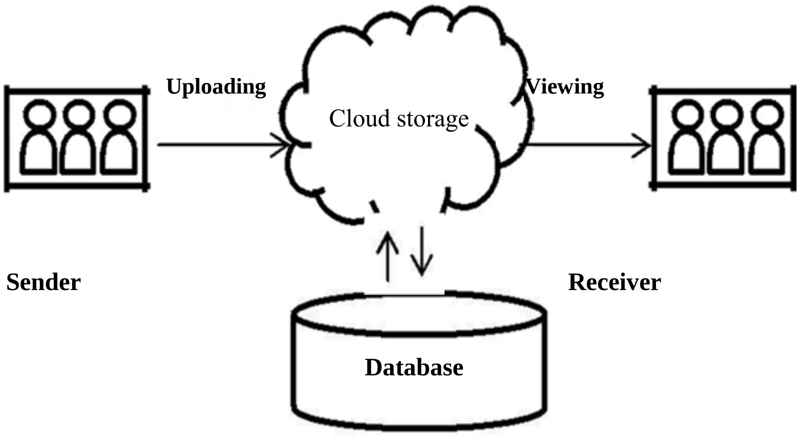


Figure 1 System Architecture

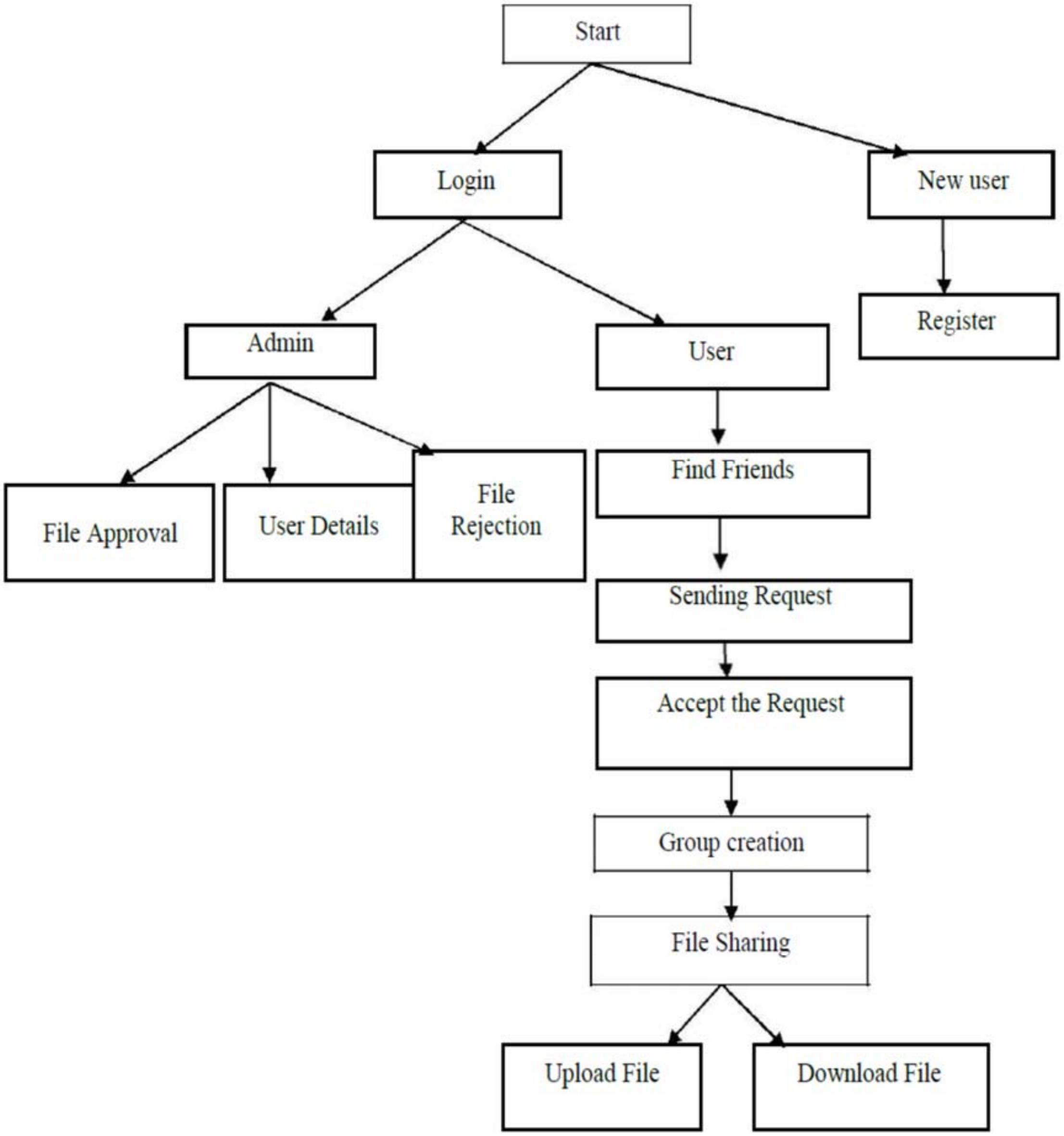


Figure 2 File Sharing in Social Networking

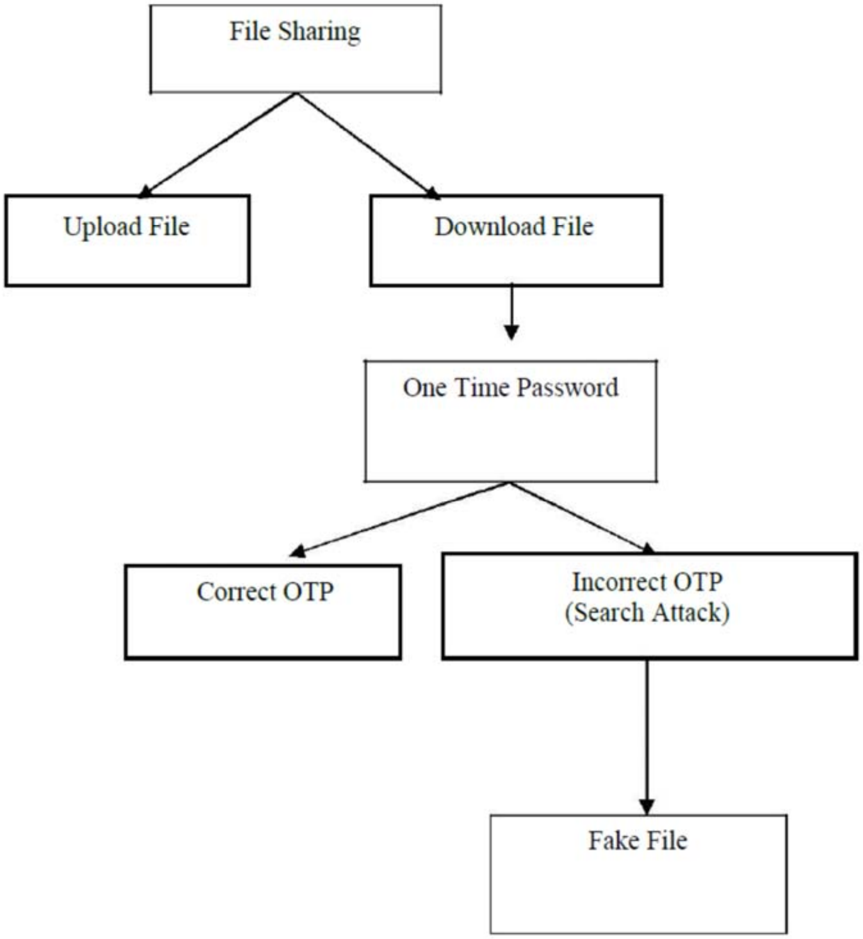
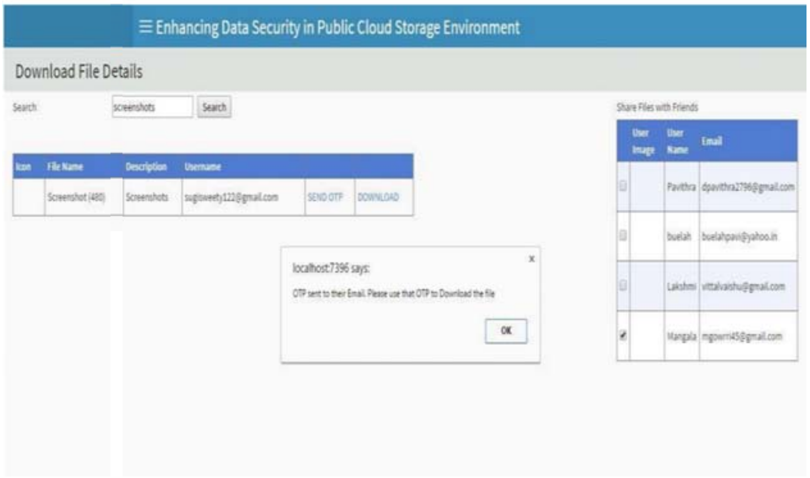


Figure 3 Flow Diagram for Incorrect OTP



☰ Enhancing Data Security in Public Cloud Storage Environment

Download File Details

Search: screenshots Search

Icon	File Name	Description	Username		
	Screenshot (480)	Screenshots	sugisweety122@gmail.com	SEND OTP	DOWNLOAD

localhost:7396 says:

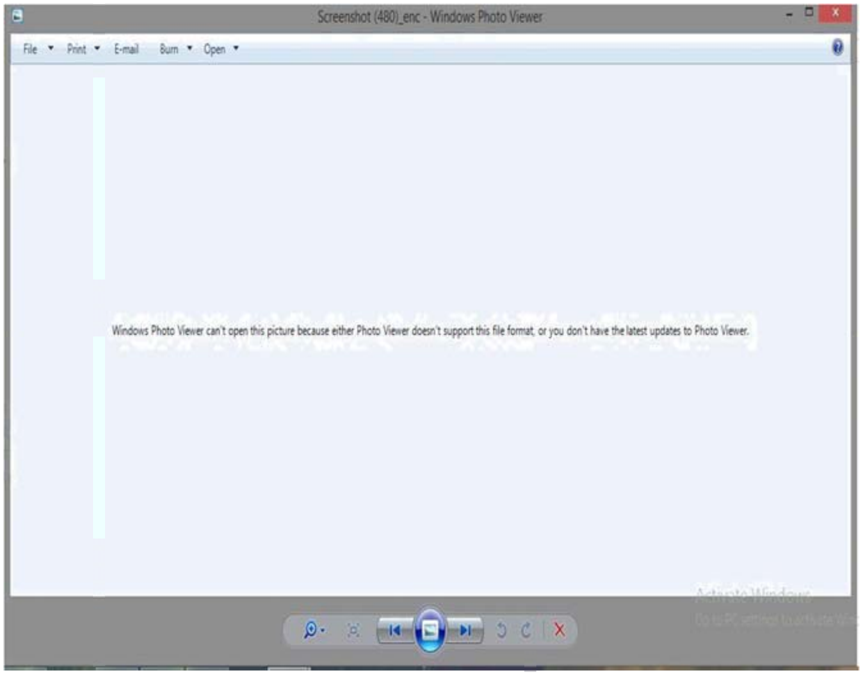
OTP sent to their Email. Please use that OTP to Download the file

OK

Share Files with Friends

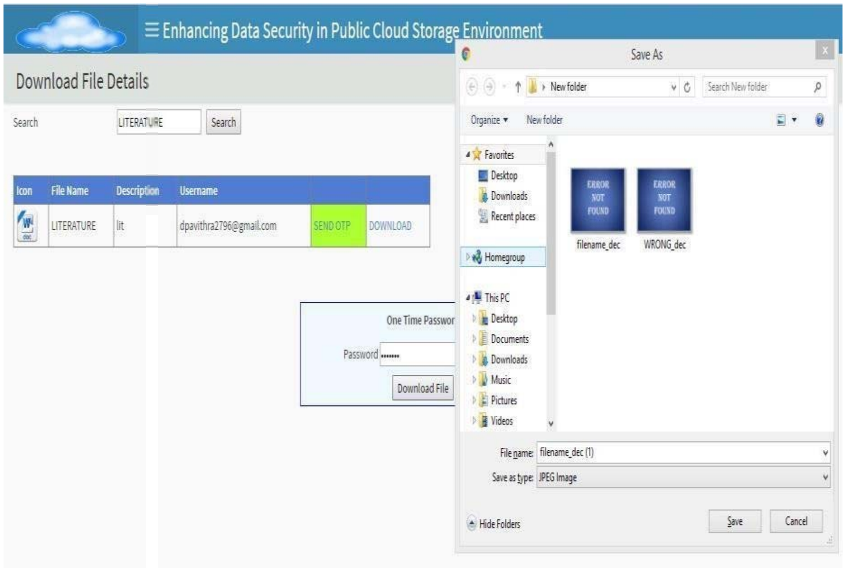
	User Image	User Name	Email
□		Pavithra	dpavithra2796@gmail.com
□		buelah	buelahpavi@yahoo.in
□		Lakshmi	vittalvaishu@gmail.com
☑		Mangala	mgowri45@gmail.com

Figure 4 File Sharing in Social Networking



Windows Photo Viewer can't open this picture because either Photo Viewer doesn't support this file format, or you don't have the latest updates to Photo Viewer.

Figure 5 Encrypted Format of JPEG File



Download File Details

Search LITERATURE Search

Icon	File Name	Description	Username		
	LITERATURE	lit	dpavithra2796@gmail.com	SEND OTP	DOWNLOAD

One Time Passwor

Password ••••••

Download File

File name: filename_dec (1)

Save as type: JPEG Image

Figure 6 Sample Fake File for Incorrect OTP

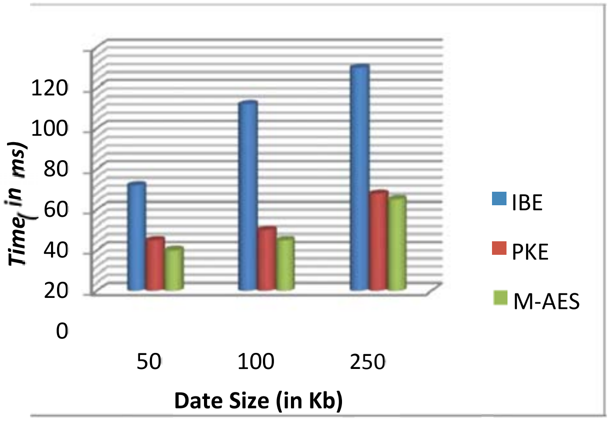


Figure 7 File Encryption Time

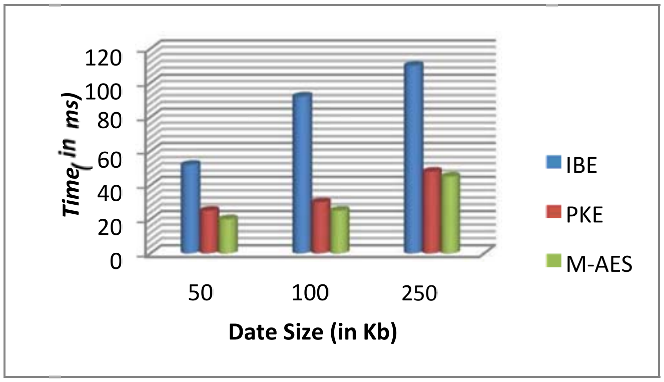


Figure 8 File Decryption Time

Security Parameters	**Confidentiality**	**Trustworthiness**	**Integrity**
IBE	Low	Medium	Low
PKE	Low	Medium	Medium
M-AES	Medium	High	High

Table 2 Measures of Security Parameters