International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Secure Login, Data Sharing and Recovery on Cloud

Hitesh Dharmadhikari[1], Kisan Chauhan[2], Pranav Das[3], Sachin Desai[4]

Department of Computer Science, Mumbai University, Mumbai, 400709, India

Guide and Professor, Department of Computer Science, Mumbai University, Mumbai, 400709, India

Abstract: ***In our proposed project, the users can share their files (like PDF, Audio, Video, etc.) over the internet through cloud to other users. The user will have two options while sharing the file: Public and Private. In 'Public', user can publically share the file with TPU and they can view the same file multiple times, while in 'Private', the TPU has to request for having the access to the file only once, and after the one-time access the shared file will get deleted automatically. Also, before the file is shared, it will be safely stored in the user's cloud space. Thus, the secondary memory of the user's device will not be utilized for saving of the file data. The particular cloud will be secured by using two-layer encryption approach to secure data sharing in cloud computing. Encryption technique which we will be using is Improved AES algorithm. Seed block recovery algorithm is used to recovery any lost/deleted data from the cloud. It is the most efficient algorithm available till date with the efficiency of 95%. Seed Block uses logical operations to recover the lost data.***

Keywords: OTP login, Improved AES algorithm, Seed block algorithm

1. Introduction

In day-to-day communication, people still use portable storage devices as their primary mode of data sharing. In cloud storage, security of our data and giving access permission to only authorized user is a big issue. If data gets deleted/lost by any reason then it is not convenient to recognize the traitor behind the data deletion. Data recovery in portable devices and cloud storage is much difficult.

This Project provides some new features and advantages and it will mostly attract the people who are actually interested in trying new methods of data sharing through cloud. The future of our project is that we can host it on the cloud provided by third party cloud providers, so that the storage space on the user's device won't be utilized. The project will be more efficient, secured and integrated on private cloud server. Also, new features can be added in it as the time goes by.

2. Related Work

[1]In this paper author have described basic concept of OTP and showed us what methods can be used to generate OTP their proposed idea is to enhance the security level of One Time Password by Encrypting it and logging the user by forwarding the encrypted OTP with Password to the system. It increases the security level of the system.

[2]In this paper author has described aboutOne-Time Passwords (OTP) that can provide complete protection of the login-time authentication mechanism against replay attacks. In this paper, we propose TSOTP: a new effective simple OTP method that generates a unique passcode for each use. The calculation uses both time stamps and sequence numbers. A two-factor authentication prototype for mobile phones using this method has been developed and has been used in practice for a year.

[3]In this paper author has described about passwords and their vulnerabilities and also described about password cracking and showed us advantages of normal password over (OTP).

[4]In this article authors has described about improved AES algorithm In order to overcome the drawback of typical expansion algorithm whose key is easily attacked by Square, an improved AES algorithm is proposed. In this algorithm, the double S-box model, the only non-linear structure, is employed to increase the diffusivity of data.

[5]In this paper authors has described about AES algorithm in this paper authors has shown how AES algorithm is executed step by step and shown us efficiency of AES algorithm.

[6]In this paper authors has described about recovery of data from server by creating backup and getting recovery using seedblock algorithm.

[7]In this paper authors has described about the basic steps has are taking place in seedblock algorithm and showed us how data is getting recovered from remote storage location.

3. Secure Login and Data Sharing Methodology

Registration: In this module each user registers his user details for using files. Only registered user can able to login in cloud server.
Record/Create: This module allows the user to record or create a short live video or a file.

Upload: In this module user upload a block of files in the cloud with encryption by using his secret key. This ensures the files to be protected from unauthorized user.

View file: In this module the user can view or watch the file that is sent to him by other user.

Request: In this module, the user at the other end can request the sender to give him permission to watch the

confidential video or access to the file that he sent one more time.

Download: This module allows the user to download the file using his secret key to decrypt the downloaded data of blocked user and verify the data and re-upload the block of file into cloud server with encryption .This ensure the files to be protected from unauthorized user and once viewed files it will be deleted from account.

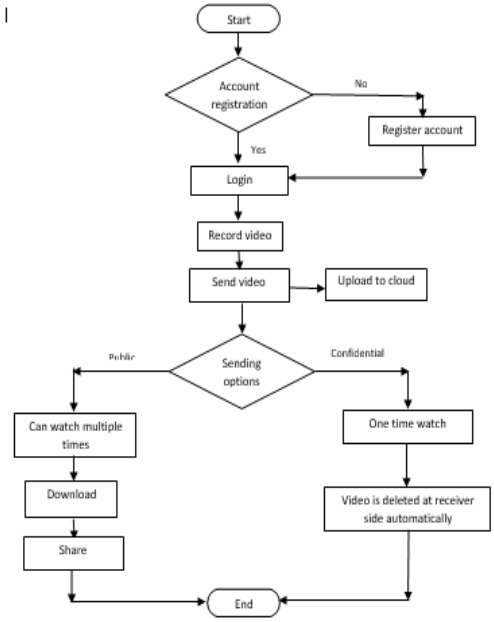


Figure: Flowchart for Cloud data access and Sharing

4. Improved Advanced Encryption Standard (IAES)

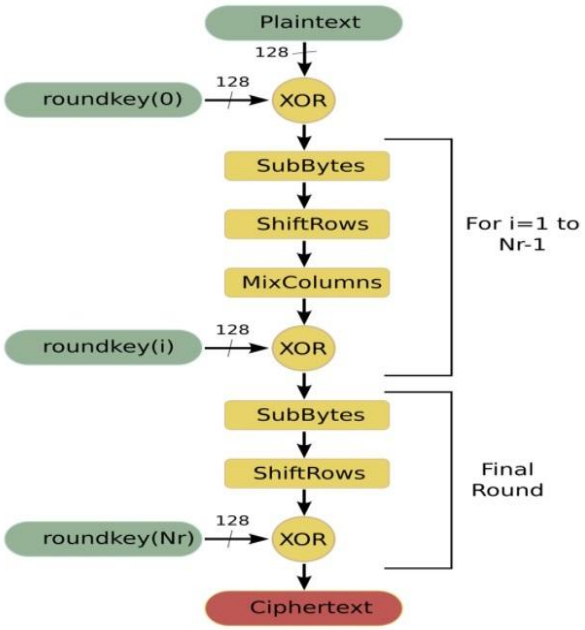
The **Advanced Encryption Standard** algorithm is a symmetric key cryptographic algorithm published by National Institute for Standards and Technology (NIST) in December 2001. The algorithm was proposed by Rijndael , hence it is also known as Rijndael encryption algorithm. AES is a popular replacement of DES algorithm.

Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. In this case the entire data block is processed in parallel during each round using substitutions and permutations. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key.

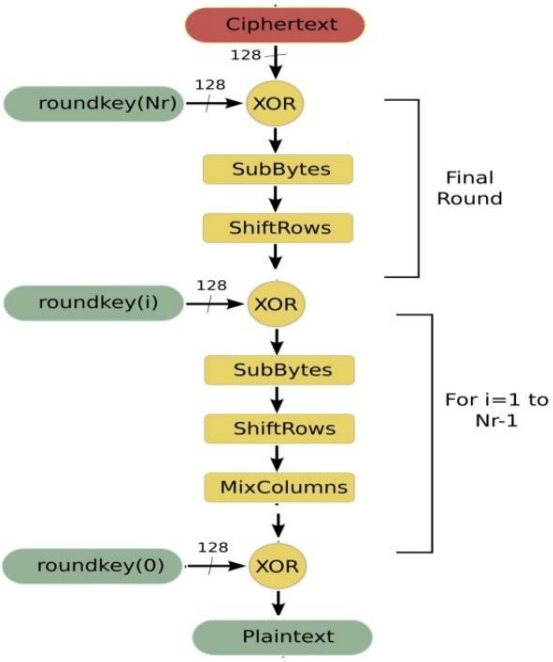
The input is a single 128 bit block both for decryption and encryption and is known as the in matrix. This block is copied into a state array which is modified at each stage of the algorithm and then copied to an output. Both the plaintext and key are depicted as a 128 bit square matrix of bytes. This key is then expanded into an array of key schedule words (the w matrix). It must be noted that the ordering of bytes within the in matrix is by column.

STEPS for AES Encryption:	*STEPS for AES Decryption:*
Substitute bytes	Inverse Shift rows
Shift rows	Inverse Substitute bytes
Mix Columns	Inverse Add Round Key
Add Round Key	Inverse Mix Columns

5. Flowchart for Encryption



6. Flowchart for Decryption



Substitute Bytes

This stage (known as SubBytes) is simply a table lookup using a 16×16 matrix of byte values called an s-box. This matrix consists of all the possible combinations of an 8 bit sequence (2 8 = 16 × 16 = 256). However, the s-box is not just a random permutation of these values and there is a well defined method for creating the S-box tables.

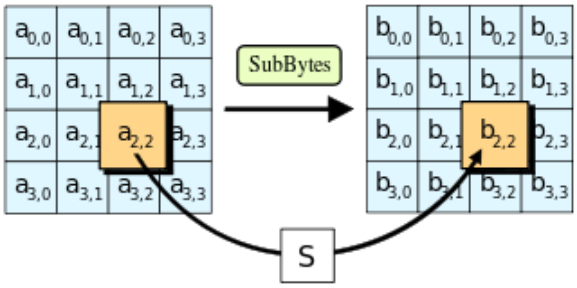


Figure: General SubByte transformation

ShiftRows:

This stage (known as ShiftRows) is shown in figure below. It works as follow:

- The first row of state is not altered.
- The second row is shifted 1 bytes to the left in a circular manner.
- The third row is shifted 2 bytes to the left in a circular manner.
- The fourth row is shifted 3 bytes to the left in a circular manner.

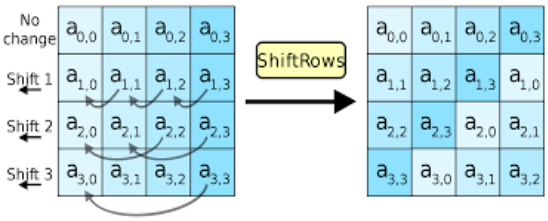


Figure: Shift Rows

Mix Columns

This stage (known as MixColumn) is basically a substitution but it makes use of arithmetic. Each column is operated on individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column. The transformation can be determined by the following matrix multiplication on state.

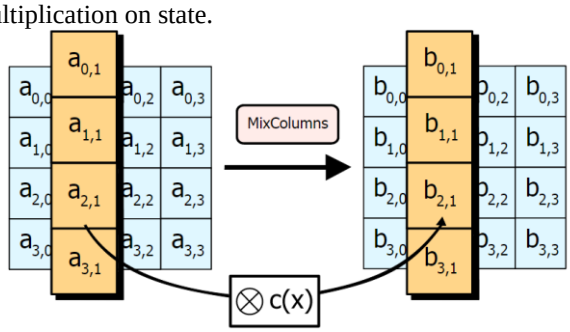


Figure:

AddRoundKey

In this stage (known as AddRoundKey) the 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a columnwise operation between the 4 bytes of a state column and one word of the round key. This transformation is as simple as possible which helps in efficiency but it also effects every bit of state.

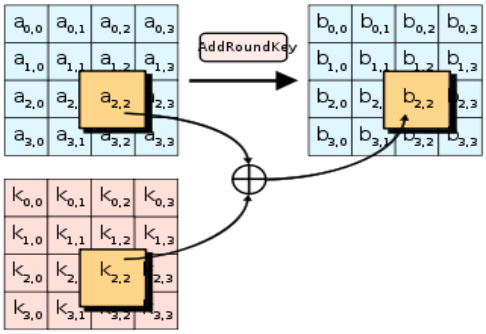


Figure: Add Round Key

Improvement in AES:

IAES is slightly advanced then AES, because the IAES support the key expansion concept. While Encryption, we perform Add Round Key operation in every round, while performing this operation in IAES algorithm we extend the length of the key so to enhance the quality of Encryption. Thus, IAES algorithm enhance the quality of encryption and makes the data more secure for transmission.

7. One Time Password Concept

OTP stands for one time password as the name suggests one time password are used in banking transactions and for account login of any type it is also called as disposable password. Opt working is such that it generates different password for different sessions, if user is starting a session and opt concept is use then for login or any transaction only one password is generated and can be use only one time and as session expires it cannot be used again and for new session new password is generated. It is not convenient to remember different password for different services opt will be easy to use. One time password can be anything random numbers or alphabets which will be selected by server using different method.

There are different terms related with opt concept such as:

How are one-time passwords generated?

If a one-time password is going to give you access to a computer system, the disposable password you hold in your hand obviously has to match the password the computer has in its memory, just like a conventional password. The only trouble is, the password has got to change every time you use it. This means there has to be some form of synchronization that allows both you and the computer system to use the same, ever-changing password, without the computer having to transmit it to you each time by some insecure method such as email. You can see how this would work with a cellphone-based system: the computer system would generate the one-time password, send it to you in an SMS text message, and then allow you a certain time period to type it in before the password expired. A mail-based system works in essentially the same way, but the password would have to be valid for longer to allow for delays in transit OTP generation algorithms typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash

functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time).

Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).

How to send password through user?

There are different methods to do it such as we can send password to users' phone by using GPRS API. Another method which is easy is sending OTP through mail by taking users email id on login page and sending OTP on that, but there is a disadvantage that if user email account is operated by any unauthorized person then password will fall prey to another person and system will be unsecured.

8. Seed Block Algorithm

The algorithm concerns about the simplicity of backup and recovery process. Seed Block Algorithm uses logical operations to recover the lost data or deleted data. The further working is explained below with the algorithm and an example.

For e.g.: We having two data files A and B. A(OR)B produces X .When A file may be destroy or delete and we want that file so can be retrieve by using X-OR of file X and B i.e. A=X (XOR) B.
The main objective of this algorithm is for smart recovery of data which is lost or deleted from the cloud storage.

Why Seed Block Algorithm?
- Efficiency of Seed block algorithm is 95%.
- Requires very less time to recover data compare to other recovery algorithm.
- Smart recovery because it uses logical operations like OR and XOR.

Seed block Algorithm:
Step 1: Convert the Login id of the user to binary say A.
Step 2: Convert the saved data file to binary say B.
Step 2: Perform the OR operation between A and B and save the result as C.
Step 3: To recover the lost data (B), perform XOR operation between A and C.
Step 4: Download the lost file from the backup server.

Explanation:
In Step 1, the login id which the user uses to login in his cloud space is converted to binary using Convert to binary module. In Step 2, convert the saved file id to binary. After this, name both the binary files as A and B. Then, perform the OR operation between A and B and save the result as C in the system. Later, we will use C to recover the lost data.

Suppose, an third party user, gets the access to our cloud space and he deletes our saved file. After this, our job is to get back our lost file. For this purpose, we perform logical operation i.e. XOR between A and C to recover the binary id of B. In Step 4, we recover the binary id and plot our file and download it from the backup server. Thus, we recovered our lost file using smart recovery technique.

Example: Say, A=1000 and B= 0100. After performing OR operation, we get, C= 1100. Then, XOR operation between A and C gives 0100, which is B.

9. Conclusion

We have designed an application which deals with few of the obsolete features of data sharing and thus making the security and sharing over the internet more trustworthy. By using our application, one can capture a video or can create a file and send it over the internet to their contact list. Our architecture provides two modes of video sharing (i.e. public and confidential) by which the sender can feel absolutely secure about the file he/she shares. Also the video or document file is stored in an encrypted format in the cloud and can be retrieved any time by the user who created the file. Our future work includes the implementation of this application in a larger scale using by actually using cloud services from third party cloud providers, and also enhance the application by adding more features

References

[1] Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology. Ms.E.Kalaikavitha M.C.A., M.Phil.,Mrs. Juliana gnanaselvi M.Sc., M.Phil., Ph.D Asst. Professor, Dept. of Information Technology. Rathinam College of Arts AndScience College. Coimbatore
[2] 2013 International Conference on Electronic Engineering and Computer Science A new One-time Password Method Yun Huang, Zheng Huang, Haoran Zhao, Xuejia Lai
[3] A Survey on One Time Password Mirza TanzilaMaqsood Pooja Shinde SRTM University, Department of CSE, M. S.Bidve Engineering College, Latur, Maharashtra, India SRTM University, Department of CSE, M.S. Bidve Engineering College, Latur, Maharashtra, India
[4] An Improved AES Key Expansion Algorithm Junjie Yan* and Feng Chen School of Information Science and Technology, University of Science and Technology of China, Hefei, Anhui, 230027, China *Corresponding author
[5] Efficient Implementation of AES algorithm RituPahal , Vikas Kumar SGI Samalkha, Haryana, India.
[6] Seed Block Algorithm: Remote Smart DataBackup Technique for Cloud Computing Kailas Pophale,PriyankaPatil,RahulShelake,SwapnilSapkalDepartment of Computer Engineering Sinhgad Institute of Technology, Lonavala, Maharashtra,India

[7] Seed block algorithm: a remote smart data back-up technique for cloud computing. Vijayalaxmi V Kadlimatti,RameshKumar H KM.Tech Student, Assistant Professor, Dept. of Computer Science and Engineering, STJIT, Ranebennur, Karnataka, India.