INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Data sharing using middle-key authentication

Vishnu Vardhan
vishnuvardhan2281@gmail.com
SRM Institute of Science and Technology, Chennai,
Tamil Nadu

Anish Ceppathi
anishceepathi@gmail.com
SRM Institute of Science and Technology, Chennai,
Tamil Nadu

Charu Nandhan
nandanreddymc@gmail.com
SRM Institute of Science and Technology, Chennai,
Tamil Nadu

Kamilwadsariya
kamilwadsariya83@gmail.com
SRM Institute of Science and Technology, Chennai,
Tamil Nadu

S. Jayakumar
jayakumar.s@rmp.srmuniv.ac.in
SRM Institute of Science and Technology, Chennai,
Tamil Nadu

ABSTRACT

The basic idea of the project is to share the data in the cloud. The dataset in the cloud storage is secured and more flexible to share the data with others. For that, we propose Key- Aggregate Cryptosystem which produces cipher text of a constant size such that decipherment rights are often assigned to them. By combining a collection of secret key, we will create a compact single key. By exploiting this compact key, we will send others very restricted secure storage. First, owner of the information sets up the general public system. Next Key information formula generates a public or master key. By exploiting this key, the user will convert plain text into cipher text. After that user can provide input as master secret key by an Extract function. It will manufacture output as mixture decipherment key. And this obtained secret key is safely sent to the receiver. Then the employment with the mixture key will decode the text of a cipher through the use of decode perform.

Keywords: *Plain text, Encrypt, Public key, Cipher text decrypt..*

1. INTRODUCTION

Cloud storage of data is become very popular. It is also used for purpose of core technology in online services these days. It may easy to create free accounts for sharing data in online and we can send the data up to 25GB through free services and if we want to send more data for that we need to pay extra money. These type of data we can access anywhere in the world. Now comes the most important part that is privacy where may unexpected privilege or third party user can access the data in a shared tendency. For that the A cryptographic schemes will resolve the problems in the shared tendency. Where the data user is not happy for storing the data in a virtual machine then he can choose the cryptographic solution with high security and theoretic assumptions are more desirable.

For example if a user is storing data and that data he might wants to send to his friends. But other friends also can view that data. These type of challenging problem is solved by cryptographic solution. The data will be in encrypted way only other user can see that data only by decrypting the file with a key that is used for encryption. Now Ajay wants to put all her photos in google drive he doesn't want anyone to see his photos so for that while uploading he encrypted all photos with a single key and uploaded in the drive. Now his other friend Vicky needs to see his photos so Ajay will share a key to Vicky and with that key he will see all his photos. The key system is two types it is present in AES (Advance Encrypted System) they are Symmetric and asymmetric. Here we are using symmetric method to encrypted data with the key. The size of a key will be a 16 bit key.

In AES we can use up to 256 key size and we are using only 16 bit length key. In symmetric the same is used for encryption and as well as decryption. But in asymmetric it is different key will be used for different purpose. So for easily purpose we are using symmetric method in data sharing in cloud storage.

2. EXISTING SYSTEM

In the old system of cloud storage the users will let their acquaintance read a set of their non-public footage. A firm could provide its staff access to some of its sensitive data. The drawback in this system is that we can't share encrypted knowledge effectively. After all the encrypted information will be transferred from the storage by the users, and then it will be rewritten, it is then sent to the others for the purpose of sharing, meanwhile the value of its time is lost in the cloud storage. The User have the need to access the sharing data rights to the other users so that the data from the servers can be accessed directly. Perhaps, finding a better and secured way to share remaining data in the cloud storage can't be a master key for a single class, but the combination of many similar keys gives the power to do so that decryption of cipher text classes is achieved. Here the cipher text key, the public key, the master/secret key and the aggregate key or of same size. In public system parameter a large cipher text class exist. But we only need a small portion of it is needed which can be fetched by demanding from cloud storage. Previous results could also be similar property that includes a constant-size decipherment key, however the categories ought to adapt to some per-defined hierarchal relationship. The work is versatile within the sense that this constraint is eliminated, that is, no special relation is needed between the categories.

3. PROPOSED SYSTEM

The proposed system of cloud storage make a decryption key as effective so that sense that the multiple ciher texts decryption is allowed by not increasing the size of it. Now we propose the public key encryption which is called key aggregate cryptosysytem(KAC) which users the AES algorithm. In this KAC the user encrypts the message under both the public key and a cipher text identifier known as class. That means the cipher texts area unit additionally classified into various types. The key possessor holds a master-secret key, which may be used to extract the secret keys for different categories. Here the key which is extracted can have an aggregate key which acts as a compact key.

A. AES (ADVANCED ENCRYPTED SYSTEM):

AES relies on a style principle referred to Substitutionlised permutated network which is quicker in each computer code and also hardware. not like its precursor, DES, AES won't be using a Feistel networking type. AES includes a mounted block of size 2^7 bits and it has a key of size 2^7, 192, or 2^8 bits, but Rijndael are often given with key sizes of multiples of thirty two bits, and has a minimum of 2^7 bits. The size of the block incorporates a most of 2^8 bits. AES works on a 4×4 column-row order matrix of bytes. Most of the AES calculations area unit drained on a finite field. The cipher of AES with a variety of repetitions and transformation rounds converts the plain input text into the cipher texts ultimate output .This process has many steps as well as one the coding key depends on one. A unit of reverse rounds are applied for the remodeling of the cipher text into first plain text mistreatment an equivalent cryptography key The Advanced cryptography customary (AES) specifies a FIPS- approved cryptological algorithmic rule which will be wont to shield electronic information. The AES algorithmic rule could be a isobilateral block cipher which will code (encipher) and rewrite (decipher) data. The process of encryption helps us to convert a piece of information in to different form called cipher text;the process of decryption helps us convert the cipher text in to the original form called as plain text. The AES formula can exploit scientific discipline keys of 2^7, 192, and 2^8 bits to encode and decipher knowledge in 2^7 bit blocks.

High-level description of the algorithm

1. Expansion of Key—by the victimization of cipher key the unit of round keys area is designed.
2. First Step
    1. Adding the Round Key— the spherical key is combined with the memory unit of each computer state by the successive rounds of bitwise XOR operations.

       1. Sub Bytes—it is a substitution step which is nonlinear and every memory unit in the computer can be replaced with the next one in row with operation.

       2. Shifting the Rows—here each and every row of the given state is transpositioned and shifted with the help of calculated steps.

       3. Combining the Columns—here the operation is done by combining the four bytes in the every column of the state.
3. Concluding step
    1. Sub Bytes
    2. Shifting the Rows

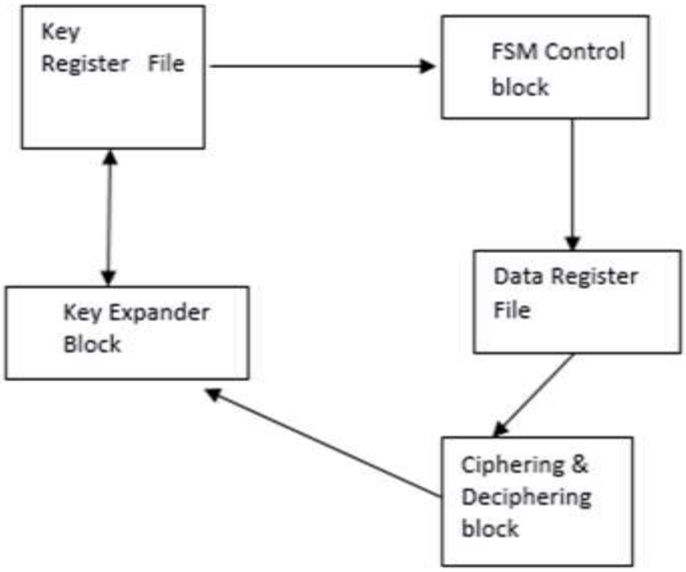

Figure 1: AES block diagram

B. MODULES:

- User -profile Registration
- User-profile Retraction
- Uploading and Deletion of a file
- Access and Traceability of a file

1. User-profile Registration:

For the process of user registration with the ID the manager of the cluster have to pick a category then the person can add the list of users in to the cluster lists which can be used in the part of traceability. When the registration is done the user will get a public key which can further be used for the process of cluster signature generating and also for coding of files.

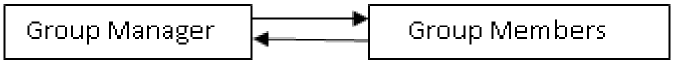

Figure 2: user registration diagram

2. User-profile Retraction:

User retraction can be done by the cluster manager through public accessible. Retraction list, supported that cluster members will write in code their knowledge files and make sure the secrecy against the retracted users. Cluster and updating the retraction list on a daily basis even though no one has been retracted within the day. Speaking differently words, the freshness of the retraction list on the present date will be verified by the others.

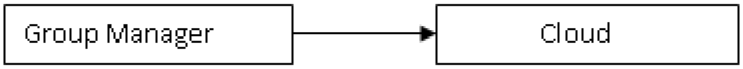

Figure 3: user revocation diagram

3. Uploading and Deletion of a File:

For the storage and the sharing of an information entering the cloud a gaggle participant obtains the retraction list through the cloud. During this process, the participant has to send the cluster ID group as if he is asking the cloud. The thoroughness of the retraction list which is received is supported. The files which are already in the cloud can often be deleted by person who manages the cluster or by the owner of the information.

4. Access and Traceability of a File:

For accessing the cloud, the user has to cypher a gaggle signature for his/her authentication. The utilized cluster signature theme will be considered a variant of the short cluster signature that inherits the inherent unforgeability property, anonymous authentication, and trailing happens, the cluster manager performs the tracing operation to spot the original identity of the information owner.

ADVANTAGES

- The delegation of decoding may be with efficiency enforced with the combination key that is simply of mounted size.
- Variety of cipher text categories is massive.
- It's straightforward to key management for cryptography and decoding**.**

C. USE CASE:

By the usage of case diagrams area unit behavioral figures will be showing a collection of set of performed actions that some system ought to or will be working together with the one or additional outer resource partcipants of the system. Every usecase ought to offer few noticeable and priceless results to the partcipants or the alternative actors of the system. Usecase diagrams area unit wiped out associate degree early part of a development project of a software package.

These categorical however is ought to be doable for the usage of ultimate system. Use cases ar a decent thanks to categorical the useful needs of a software package, they're intuitive and straightforward to grasp in order that they may be utilized in negotiations with non-programmers

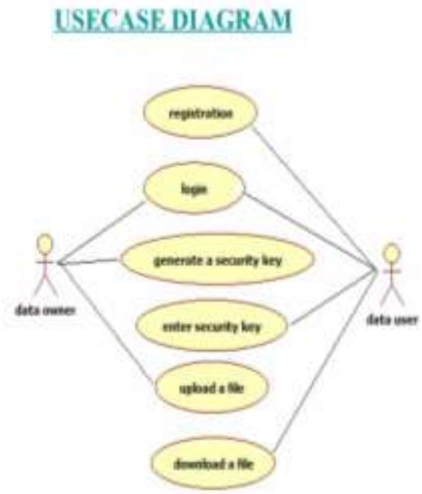

Figure 4: use case diagram

D. SYSTEM ARCHITECTURE

It shows the flow through a program from Associate in Nursing outlined begin purpose to Associate in Nursing finish purpose. Activity diagrams describe the progress behavior of a system. Activity diagrams are similar to state diagrams because activities are the state of doing something. The diagrams describe the state of activities by showing the sequence of activities performed. Activity figures indicate which are parallel or which can be conditional. The fundamental blocks in activity figures are activities, conditions are selections (branches), joints and transitions.

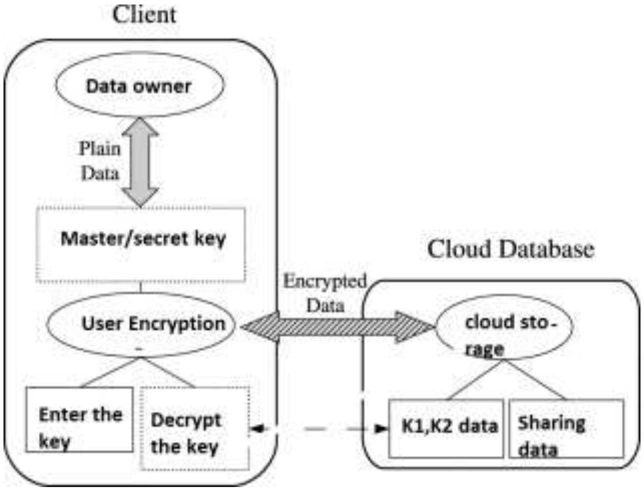

Figure 5: system architecture diagram

4. CONCLUSION

From this we tend to a style for the information sharing victimization middle key authentication in cloud storage. In mona a user is prepared to share the message with the other participant among the cluster but not showing his own identity in the cloud. In addition, island helps economic participant retraction and a new participant contribution. The economic participant retraction can be usually attained to by a public retraction list but not by changing the nonpublic keys of the remaining participants, and the new participants can easily decipher the files kept inside the cloud before they are actually participants. However the overheat storage, the computational encoding price square can be measured constant. In depth studies indicate that our planned theme will satisfy the mentioned security issues and will make sure the potency still. A cryptologic storage system by the name Plutus permits the sharing of secure file on the servers that are untrusted thus the owner of information also share file groups with the other participants by delivering corresponding safe deposit key. By dividing the files in to respective file groups and by encrypting each and every file group with the help of a novel file block key. And also this brings a lot of major distribution of keys over head for the file sharing in a large scale. However to boot this the key is hich is file blocked have to be updated and also it should be distributed another time for a user retraction.

5. REFERENCES

[1]S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, “SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment,” in Applied Cryptography and Network Security - ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.

[2] L. Hardesty, “Secure computers aren’t so secure,” MIT press, 2009, http://www.physorg.com/news176107396.htm.

[3] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “PrivacyPreserving Public Auditing for Secure Cloud Storage,” IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2013.

[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, “Storing Shared Data on the Cloud via Security-Mediator,” in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[5] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, “Dynamic Secure Cloud Storage with Provenance,” in Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.