A Secure Document Distribution System in Distributed Network

Rohit. R. Nikam[1], Vaibhav. P. Badhe[2], Satyam. V. Gondhale[3], Ashish. S. Bedmutha[4], Ashwini. D. Sonawane[5], Jayshri. A. Gaikwad[6]

[1] Assistant Prof, Information Technology, Sanjivani COE, Maharashtra, India.
[2]Student, Information Technology, Sanjivani COE, Maharashtra, India.
[3]Student, Information Technology, Sanjivani COE, Maharashtra, India.
[4]Student, Information Technology, Sanjivani COE, Maharashtra, India.
[5]Student, Information Technology, Sanjivani COE, Maharashtra, India.
[6]Student, Information Technology, Sanjivani COE, Maharashtra, India.

ABSTRACT

In this paper, we propose the system which helps the person to share the document securely to different people present in the group at the same time. In group there is no centralized initialization for user of other people present in group. For security of document we are encrypting the document by using AES algorithm and by dividing in two parts and then stored remotely in cloud .We have mainly used group key agreement technique in which a user is only aware of his neighbours while the connectivity graph is arbitrary and Diffie-Hellman key exchange protocol where the key is actually calculated and not shared over the network. Cloud is platform which is not full secure for storing the documents, using this technique the document on the cloud are securely stored and also share to the user who goes through authentication process and gets the required document. Techniques mentioned above helps the user to share document securely.

Keyword: - *Group Key Agreement, Diffie- Hellman, Encryption, Decryption, Distributed System.*

1. INTRODUCTION

The Distributed system have changed the way of communication between the two machine, it provides with different features such as availability of resources at anytime we require, it also reduces the workload of the single machine and provide synchronization. For securing the document encryption is the one of the best solution, which ensure that the document which is send across the network is received to the authenticated user without leak of information to any of the unauthenticated person. AES symmetric block cipher which is much faster than the DES. AES uses 128bit key for encryption and same for the decryption. AES uses 10 rounds for 128-bit key. AES is high speed algorithm and requires low RAM. To increase the security the encrypted document is converted into byte array and the byte array is divided into two parts and then stored on cloud.

Cloud is consider as the best service provider, the services provided by the cloud mainly consist of 1.Software as a Service (SAAS) 2.Platform as a Service (PAAS) 3.Infrastructure as a Service (IAAS) by using the cloud services we have access to our data 24X7 at any place we want. It also provide us with many features such as security, availability, pay as you use, and storing our encrypted file is providing more security as compare to having just encryption. Group key agreement is also one of the issue where the user of the group have to agree to one key for all the members of the group, but it is not the secure to share the to the new user of the group without authenticating him, to solve this problem we use the active algorithm for solving the group key agreement problem. In the group key agreement the user is aware of only the person who is his neighbour.

Sharing key of the encrypted document without providing any type of security leads to compromise of message which we don’t want to happen, to avoid this we use the Diffie-Hellman key exchange protocol for sharing the key, in this algorithm actually key is not transferred over the network to the user, but is calculate. Above all the mentioned technology helps us to share the document in the distributed system.

2. LITERATURE SURVEY

Key pre-distribution system is non-interactive group key agreement. The problem with this system is that as the size of the group is increased the size of key get increased respective to group. The major problem is if key get leaked cannot be recovered

There is need to scale up the hardware and software resources as we outsource the data in cloud. The more the sensitive data we outsource the more the security risk is to protect the data. To address these data security challenges, the author [3] propose an efficient data encryption to encrypt sensitive data before sending to the cloud server. This is achieved by exploiting the block level data encryption using 256 bit symmetric key with rotation. In addition, data users can reconstruct the requested data from cloud server using shared secret key. An improvement based on attack analysis is proposed [2]. The is data transmitted at various stages of the protocol, the improved protocol can resist various passive and active attacks

The multimedia data in multimedia sensing are high-volume, Real-time, dynamic and heterogeneous. To maintain the confidentiality of multimedia data is really difficult. The different solution and the result of proposed system are mentioned. [5] A general-purpose lightweight speed tunable video encryption scheme is introduced. Key exchange protocols are a core building block for secure communication. They allow participants to establish a shared symmetric key, which can in turn be used with primitives such as symmetric encryption or message authentication codes, for secure communication. Most key exchange protocols are designed for two participants.

2.1. Existing System

The existing system consist only of sharing the documents and there are no security provided, due to which the information present in document may get compromise. There is also no efficient algorithm for group key agreement and there is centralized initialized admin in present system.

2.2 .Proposed System

To overcome the drawbacks of previous system or applications, we proposed an application which will provide with the all type of security to the document and the efficient for user to join the group without any centralized initialized admin.

3. SYSTEM ARCHITECTURE

The combination of different technology help this application to work efficiently, securely, and error free. The below fig 2.1 describe the architecture of the current architecture of the proposed system. The sign in and login is provided for the purpose so as the authenticated user will be entering the system. The person may act as both entity i.e. user and publisher, the role of user is that it is able to join the group and access the document present in group and send request to the cloud for download the document. The publisher upload the document in the specific group, after getting the permission of the cloud the document uploaded by the publisher is visible to all the group member. To provide security the encryption algorithm is used, which looks after the authentication of document and prevent the leak of the content present in the document and then the file is divided into two parts and stored in the two different database on the cloud.

Dividing the encrypted document into two parts decreases the risk of compromising of the message present in document, the divided document is stored in distributed database, even if the hacker gets the one part of file he could not decrypt without the second part.

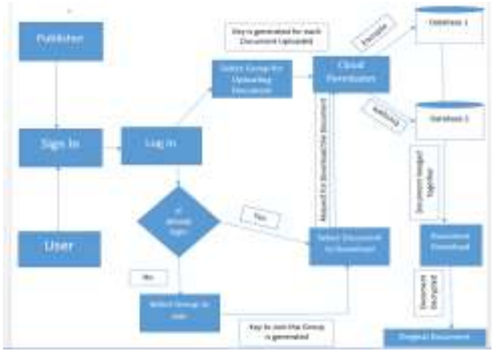

Fig 1: System Architecture

Downloading of the document can be done by the user if he have the key, which will be provided to user on his registered mail while registering. For comparison of key send to the email and the key entered by the user at the time of document download by using the Diffie-Hellman key exchange protocol**.**

4. WORKING

4.1 PUBLISHER

The entity of the project are publisher, cloud admin, user. The working of the project starts with the publisher sign in. Publisher need to fill the details like name, email, phone no, password. Later the publisher needs to login for uploading the document. While uploading the document publisher needs to specify the group in which he wants to publish the document. As soon the user click on the submit button the file will be uploaded. . To provide the security to the document, document will be encrypted with the help of AES (Advanced Encryption Standard) algorithm using 128 bit key.

The encrypted document is inserted into the array of the blob type and the array is divided into two parts, consider that if the file is of 10Mb then it will be divided as 5Mb each and then stored on two different database. In our system we will have different category of groups based on commonality. After uploading the document it will not be visible to user till the Cloud admin accept it.

The key generated during encryption is mailed to user which will be used further for decryption and download of document. To prevent the compromise of document a new functionality we have implemented which adds more security to document. The uploaded document will be stored in cloud on different database instances using MySQL and Oracle. The half part of document will be stored in one instance in MySQL database. The remaining part will be stored on another instance using Oracle database. If any part get compromise from any instance the Hacker will not be able to recover the whole document.

4.2 USER

To download the documents from a particular group user need to be added in the group. The concept of Group Key Agreement is used for joining the group. Group key agreement is the way by which a new is added into a group without knowing anyone in the group by using key agreement. User will Sign in and fill all login details. While login, when he selects the group through which he wants to download the document he will be prompted to enter the key which he will receive through mail. The key will be calculated by using the Diffie-Hellman key sharing algorithm. After entering the key, the user will be considered as the authenticated user of the group. To download the document user will need to log in. After login uploaded documents present in group will be visible to user if and only if it is accepted by cloud admin.

Once the document is selected for download the document which is stored on two different database will merge together and the file will be download. To decrypt the download file once again user will receive the mail in which there is key. Using the key in standalone application the user can decrypt the document.

4.3 CLOUD ADMIN

The cloud admin have the authority to accept the document from the user and make it visible to the user for download the document. If the cloud admin does not accepts the document then the document is not prepared for download.

5. RESULTS

The web application is developed on the java platform where client have web application from which the user can share document in secure way over the internet. The document is encrypted stored on two different databases on cloud and after downloading file and decrypting it we get the document in the same format when it was encrypted. As Every System has its own benefits and limitations our system also has them. The first advantage about our system is that we can share the document having any of the file type, i.e.docx, .pptx, .pdf, .txt.

The security provided to the document is also one of the advantage of our system. Only the application development is not enough is should execute its task in minimum time on any of the system, so our application provides with the ability to encrypt, decrypt and store data with fast execution *Table 4.1* shows the result. Some of the disadvantage of the system are the time consumption as the size of document increases the time required for encryption of document increases and for now the system is developed for sharing only the documents. Furthermore development will lead this project to send the message or any packet securely over the internet.

Table 1: Result

Type of File	File Size before Encryption	Size in MySQL	Size in Oracle	Time Taken to Store	File size after Decryption
Word File	5 Mb	2.5 Mb	2.5 Mb	10sec	5 Mb
Pdf	7 Mb	3.5 Mb	3.5 Mb	15sec	7 Mb
Text File	2 Mb	1 Mb	1 Mb	5sec	2 Mb
Audio File	2 Mb	1 Mb	1 Mb	20sec	2 Mb
Image File	500 Kb	250 Kb	250 Kb	15sec	500 Kb
Video File	5 Mb	2.5 Mb	2.5 Mb	60 sec	5 Mb
.Exe File	200 Kb	100 Kb	100 Kb	25 sec	200 Kb

6. CONCLUSION

In this paper we conclude that the combination of different technology can result in development of the best web based application for sharing the document. We studied about the group key agreement technique and also the Diffie-Hellman key exchange protocol for sharing key. The developed application demonstrate the ability of the sharing any type of document. And the best application ever developed. The same application is used for security of images.

At present we are using 128-bit key encryption technique for the purpose of encryption and decryption of document which has 10 rounds for each of process. So we can increase the key size to 192-bit or 256-bit which will have 12 and 14 rounds respectively for increasing security.

7. REFERENCES

[1]Shaquan Jiang, “Group Key Agreement with Local Connectivity”, IEEE Transection on Dependable and Secure Computing, vol.13,no3,May/June 2016.

[2]Kangwen Hu, Jingfeng Xue, Changzhen Hu, Rui Ma, and Zhejiang L., “An Improved ID-Based Group Key Agreement Protocol”, TSINGHUA SCIENCE AND TECHNOLOGY ISSN 1007-0214 01/13 pp421-428 Volume 19, Number 5, October 2014.

[3], Prakash G L, Dr. Inder Singh, “Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System”,2014.

[4] Chen Xiao1, Lifeng Wang2, Zhu Jie1, Tiemeng Chen, “ A Multi-level Intelligent Selective Encryption Control Model for Multimedia Big Data Security in Sensing System with Resource Constraints”, 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing.

[5] Benedikt Schmidt, Ralf Sasse, Cas Cremers, David Basin, “Automated Verification of Group Key Agreement Protocols”, Benedikt Schmidt. Under license to IEEE, 2014.

[6] Keke Gai, Meikang Qiu, Hui Zhao, Jian Xiong, “Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing”, IEEE 3rd International Conference on Cyber Security and Cloud Computing, 2016.