International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June 2018 www.irjet.net p-ISSN: 2395-0072

DATA SECURITY USING ENCRYPTION ON MULTI-CLOUD

Pavan Kumar K[1] , Nikhil[1] , Pavan[1] , N D Mohankumar[1], Ramya Srikanteswara[2]

[1] Student B.E , Department of CS&E , Nitte Meenakshi Institute Of Technology, Bengaluru ,India
[2] Assistant Professor, Department of CS&E , Nitte Meenakshi Institute Of Technology, Bengaluru ,India

---

Abstract - *Adapting to the latest technological advancement is the only means for sustainability and growth for any organization in this era of fast growing business world. Cloud computing have proved to be a great boon for business development as it provides servers across the globe for storing data securely and performing computations on them. However security challenges still pose a great threat for using clouds especially in handling sensitive data. .The technique used here is of Encryption on multi-cloud computing. In this paper the method proposed makes use of the multi-cloud, encryption and key pairs matching concept which provides extra security to the data saved in cloud. This way of using multi-cloud provides extra security by saving the data in different clouds so that if any hacker tries to hack the cloud the hacker can't identify in which cloud the actual information or the data is saved. Making use of encryption also provides extra security by encrypting the folder or encrypting the information in the file before saving it to the cloud. If the hacker gets the correct information about the cloud and successfully hacks the data from the cloud the hacker can't decrypt the data as it is encrypted. The user is provided a private key which is mailed at the time of registering and another key is being provided by the trustee. The file or the information can be downloaded from the cloud only if the combination of these two keys is entered.*

***Key Words*: Encryption, Multi-cloud, User, Trustee, Admin, Secret key, Pseudonym key**

1. INTRODUCTION

Cloud computing is an emerging paradigm that provides computing, communication and storage resources as a service over a network. Communication resources often become a bottleneck in service provisioning for many cloud applications. Multi-cloud is the use of multiple cloud computing services in a single heterogeneous architecture. This also refers to the distribution of cloud assets, software, applications, etc. across several cloud-hosting environments. With a typical multi-cloud architecture utilizing two or more public clouds, a multi-cloud environment aims to eliminate the reliance on any single public cloud provider.

In this today's challenging world hacking is the fast growing technique which is spreading at a high speed and this spread of the technique needs to be stopped. This can only be stopped by increasing the security or by prevention. After hacking there will be no choice. The important data will be hacked, leaked and no other step or no other option will be there for a person that his/her data is being compromised. The important information is being leaked and this can cause many losses. These losses can be either loss of economy, privacy loss, loss of company's reputation or in some cases it can be loss of life. These factors encourage or motivate to research, to prevent the hackers from gaining the important or personal information.

The problem of hacking can only be prevented by making use of hacking prevention techniques. This can be done by many other techniques but the technique used here is of Encryption on multi-cloud computing. In this technique the file which is needed to be kept safe is being encrypted by an algorithm and this encrypted file is being uploaded to the cloud .When the file needs to be downloaded, two keys need to be provided and these two keys are generated by the person who uses the persons information to produce a 32 bit key which contains 32,000 characters. The other key is produced by the file uploaded and this key is given by the trustee to the user in a light weight device which can be pen drive or a disk or any other device. This way of encrypting the file and saving it to the cloud, provision of two keys at the time of downloading the file provides extra security to the file which is being uploaded and can't be hacked easily by the hacker.

2. RELATED BACKGROUND

In a Shared Cloud Environment like hospitals, the Centralized system might be used by different doctor say A and B working on rotational shifts. Here the user's medical records are sensitive data may be prone to risk. In these cases, user secret keys is easily stolen or used by an unauthorized party. Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares. In addition to a username/password, the user is also required to have a device to display a one-time password. Some systems may require the user to have a mobile phone while the one-time password will be sent to the mobile phone through SMS during the login process. First, the traditional account/password-based authentication is not privacy-preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems. Second, it is common to share a computer among different people. It may be easy for hackers to install some spyware to learn the login password from the web-browser.

3. PROPOSED METHOD

IRJET sample template format , Conclusion content comes here. Conclusion content comes here Conclusion content comes here Conclusion content comes here Conclusion content comes here Conclusion content comes here Conclusion content comes here Conclusion content comes here Conclusion content comes here Conclusion content comes here Conclusion content comes here Conclusion content comes here . Conclusion content comes here

In this paper, the proposed method, an encryption on multi cloud computing based two-factor access control protocol for web-based cloud computing services, using a lightweight security device is used to secure the data. An attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. The device has a few important properties like it can compute some lightweight algorithms, e.g. hashing and exponentiation and it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside.

The block diagram in Figure-1 shows the complete working architecture of the software. This architecture is based on the working of the software where several operations are performed from the authority to the user. The authority is the only person allowed to add the trustee and view the designations and department .He holds the information of the cloud in which data is being stored. Trustee can add the user and produce a private key which is being mailed to the user .

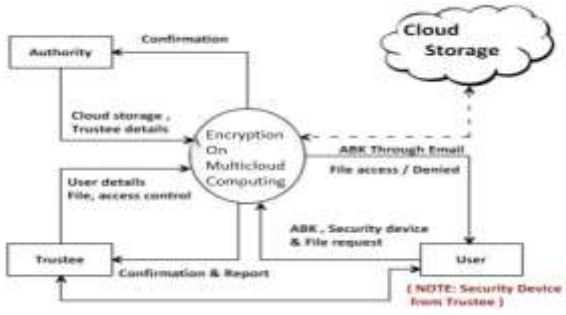

Fig 1: Block Diagram of Architecture

Trustee can upload a file, can provide the file access to the user and can also view the transactions that are being performed by the users. Trustee can also generate a pseudo key which has to be provided to the user to download a file. User can download the accessed file and can also change his profile details. All actions like uploading the file or downloading the file, when needed are being performed with the help of the cloud where the file is being uploaded and downloaded.

Advantages of the Proposed System are that the proposed protocol supports encryption access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved.

1. Domain Authority

Fig 2 Dataflow diagram of Authority

Domain Authority is a super user who creates the Data Trustee user and maintains the cloud servers' configurations. He has the rights to Add, Edit or Delete any number of Trustee. Once the Domain Authority has logged in he can perform the following functions.

- Cloud Storage: Used to update the data or used to add the data by the user to the cloud by all the other processes that are being used.
- Data Trustee: In this the trustee is being added by the admin and he is authorized for adding deleting or updating any information about the user.
- Key Generation: The key can be generated viewed and updated as per the changes of a user and this key can be updated time to time by the trustee.
- Department: The departments can only be viewed and these departments are used to provide access to the users.
- Designation: Apart from department, designations are also used to provide the access.
- Change Password: The password can be changed .It can be either user, trustee or admin .All the three are provided with the authority to change password.

2. Data Trustee

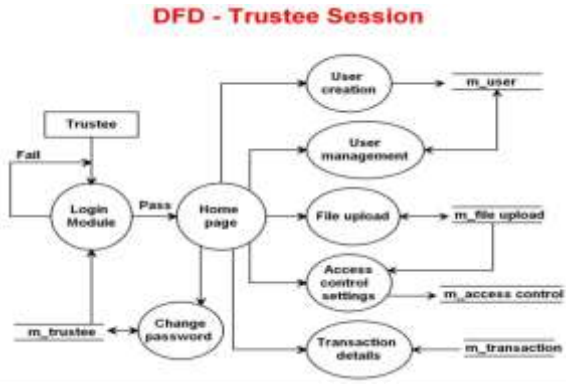

Fig 3 Dataflow diagram of Trustee

Trustee is a person who is authorized to store the files in cloud which in turn is accessed by the authorized Data Consumers. Trustees are like Liberian who can upload all the files in the system. Whenever the file is uploaded it will be encrypted by the system using Trustee Encryption Key. Trustee has to specify the Hierarchical Access Policy for each and every file. Access policies are set using Department Attribute and Designation Attribute. Trustee can create the Data Consumer and he has to send them Attribute based Decryption Key. Attribute based Decryption Key, contains the Trustee Decryption Key and Data Consumer Attribution Set (Department, Designation).Once the Trustee has logged in he has following functions.

- User Creation – (Data Consumer)
  - Fill the user details
  - Pick the Master Secret Key from DB
  - Generate Attribute Based Key (ABK) using MSK , Department & Designation of the user
  - Encrypt the ABK with DNA algorithm
  - Email the key to the user
  - Generate the Pseudonym Key from ABK using Hashing Technique(MD5)
  - Copy Pseudonym Key to lightweight security device & Send to respective user
- User Details (View, Delete)
- File Upload
  - File Selection
  - Encrypting using Private Key
  - Fetch Cloud Storage Configuration Details
  - Transfer the Encrypted file to cloud Storage
- Uploaded File Details (View, Delete)
- File Access Control Setting
- File Access Control Details (View, Delete)
- Transaction Details
- Change Password

3. Data Consumer

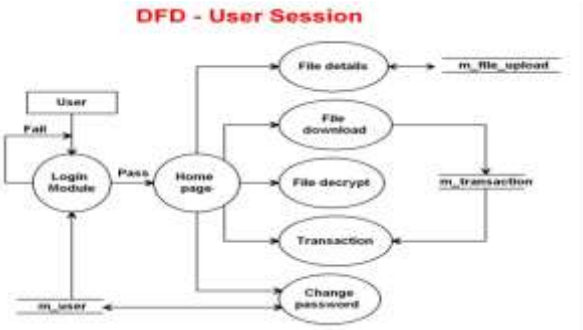

Fig 4 Dataflow diagram of User

Data Consumers are the data access users. Suppose Trustee is a college Liberian then data consumers are like students, lecturers and admin staff in a college. Data Consumer will receive their access key (Attributed based Decryption Key) from respective Trustee through email and lightweight security device. With the help of the access key they can download the files for which they have access. (Remember access control is set by data owner).Suppose the data consumer wants to download any file, first he has to select the file from the list and the system asks for the access key .After the system gets the access key it will separate the Attribute Set from the key and check for the access rights. If the user has the access he can download the encrypted file which in turn is decrypted using the decryption key and data is downloaded to the consumer local system. Once the Data Consumer logged in he has following functions.

- File Details (View)
- File Download
  - Select the file from the list
  - Select the Attribute based Key (ABK) file from the local system and Pseudonym Key from lightweight security device
  - Decrypt the Attribute based Key using DNA Decryption
  - Generate the Pseudonym(1) Key from ABK

- Fetch Pseudonym(2) from security device
- Compare Pseudonym(1) & Pseudonym(2) if Fail deny the file access
- Get the Attribute Values from decrypted ABK
- Check the Access Control with Attribute
- If Access Control pass download the file or deny the file access
- Enter the transaction record in the table

- File Decrypt
  - Select the file to be decrypted
  - Retrieve the Decryption Key from ABK
  - Decrypt the file
  - Download the file to user system
- Transaction
  - View the transaction of logged user

4. SIMULATION AND RESULTS

The proposed project uses Java (JDK), JSP, MySQL. Encryption on multi-cloud computing provides a high level of security to the persons who are using the software. Before the file is being saved in cloud it is encrypted .A few screen shots depicting the implementation are as shown below.

Authority Login

Fig 5 Authority Login Page

This snapshot gives a brief description about the Authority who can login to perform his actions of adding the trustee and can also change the activities related to the cloud. He is the one who is the main person performing the function of providing access to the trustee.

Authority Activities

Fig 6 Authority Activities

In this snapshot we can see the activities that can be performed by the authority. He is the one adding the trustee .He can only maintain or view the cloud details .He is the one who maintains the database. He is having the authority to only read the department and designations. He can only view these two factors.

Trustee Login:-

Fig 7 Trustee Login

The above is the login page which is given to the trustee and this authority of logging in is given by the authority or the admin who adds the trustee for further actions that is to be performed by the trustee.

Trustee Activities

Fig 8 Trustee Activities

The above snapshot shows the activities which can be performed by the trustee. The trustee maintains the records of all the users, can add the users. He has the authority to see the user details and can upload any file to the cloud. He can view details of the file, and can also provide the access to the user for the file .He can also view the access provided by him and has the record of all the transactions.

User Login

Fig 9 User Login

User is the one who is being added by the trustee and being provided with the secret key .This key reaches the user through his mail. And the other pseudo key is provided by the trustee to the user.

User activities

Fig 10 User Activities

User is the one who is using all the resources that are being allocated. He is the one downloading the file or he is uploading the private key and the pseudonym key to download the file. User can only see his transactions. Apart from this he can download the file , can also change his username ,can change his details apart from department and designation.

5. CONCLUSION

Cloud computing is a virtual host computer system that enables enterprises to buy, lease, sell, or distribute software and other digital resources over the internet as an on-demand service. The main concept of cloud is to make use of it in our day to day life, like saving any important file, photo, audio, video or any important information required by the user. But this way of saving the personal data or important folders to any cloud is not safe as only few steps are taken by the cloud to secure the personal data which is not a secure way to keep the data safe.

This paper presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, it is demonstrated that the construction is “feasible”. Future work can be to further improve the efficiency while keeping all other features of the system in place.

REFERENCES

[1] C. Wang Q. Wang K. Ren N. Cao W. Lou "Toward secure and dependable storage services in cloud computing" IEEE transactions on Services Computing vol. 5 no. 2 pp. 220-232 2012.

[2] S. Patil P. Vhatkar J. Gajwani "Towards secure and dependable storage services in cloud computing" Int. J. Innovative Res. Adv. Eng vol. 1 no. 9 pp. 57-64 2014.

[3] K. Hashizume D.G. Rosado E. Fernández-Medina E.B. Fernandez "An analysis of security issues for cloud computing" Journal of Internet Services and Applications vol. 4 no. 1 pp. 5 2013.

[4] M. García-Valls T. Cucinotta C. Lu "Challenges in real-time virtualization and predictable cloud computing" Journal of Systems Architecture vol. 60 no. 9 pp. 726-740 2014.

[5] M. Chase, S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption", *Proc. CCS*, pp. 121-130, Nov. 2009.

[6] D. Boneh, X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles", *Proc. EUROCRYPT*, pp. 223-238, May 2004

[7] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of network and computer applications*, vol. 34, no. 1, pp. 1-11, 2011

[8] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, "Toward secure and dependable storage services in cloud computing", *IEEE transactions on Services Computing*, vol. 5, no. 2, pp. 220-232, 2012.

[9] Philipp Junghanns B. Fabian T. Ermakova "Engineering of secure multi-cloud storage" Computers in Industry vol. 83 pp. 108-120 December 2016.

[10] Benjamin Fabian T. Ermakova P. Junghanns "Collaborative and secure sharing of healthcare data in multi-clouds" Information Systems vol. 48 pp. 132-150 2015