REVOCABLE STOCKPILE IDENTITY BASED ENCRYPTION IN CLOUD COMPUTING FOR UNAISSILABLE DATA SHARING

[1]Mrs.P.Sunitha, [2]B.K.S.Brahmini, [2]T.Durga Bhavani, [2]P.Mounika, [2]A.Haswanth
[1]Assistant Professor (Ph.D), [2]Bachelor of Technology
[1]Computer Science & Engineering, [2]Computer Science & Engineering,
[1]Dhanekula Institute of Engineering and Technology, Ganguru, India

Abstract : Cloud Computing helps users by providing security to the data that is stored in cloud and allows the users to utilize its resources in a cost-effective manner. When a data provider uploads a file in the cloud then the file should be accessible only to the authorized users. We propose Identity Based Encryption so that it provides both the forward and backward security thus, making the data available only to the authorized users. By proposing Revocable Stockpile Identity Based Encryption we provide secrecy by allowing only non-revoked users to access the data at that current time period. The current time period is attached when the file is being uploaded to cloud and the download details of the file will be stored. The proposed scheme provides confidentiality and integrity of the data

I. INTRODUCTION

Now-a-days cybercrimes are increasing and the security for the data is being lost for the data to be in a secured form we need to cryptographically encrypt the data and store the encrypted data is difficult to understand and promotes data confidentiality. Cloud Computing provides confidentiality to the data and also stores the data in an encrypted format the decryption of the data by the unauthorized users is not possible and also thus promotes the data confidentiality. The data is available to users who have authorized access to the cloud.

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications and through any server. The use of hard disk drives and other storage devices will be minimized. The usage of cloud helps users to secure the files that are present in the cloud and one of the characteristic feature of the cloud is that it provides on demand service that means the services for which the user requests will be provided to the users .The data stored in the cloud will in the encrypted format and hence providing data confidentiality.

The primary motive of Revocable Stockpile Identity Based Encryption is that it allows the users to access the files that are made available in the cloud .It allows only the authorized users to access the data .The data is in encrypted form and the data will be available to the user only if the user provides valid secret key. The data provided by the data provider will be available to the authorized users and the current time period will be appended to the file that is being uploaded. This Revocable Stockpile Identity Based is used to provide both the forward and backward secrecy for the data.

II. EXISTED SYSTEM

In the previous approaches there was only selective security that means only a particular subset of data will be secured. There is no total security for the data and the data is shared for the authorized users that results in the loss of data and the confidentiality of the data is not achieved.

So, it makes the data available for every unauthorized user .This results in loss of confidentiality of data and whenever revocation is being done then the users who are not revoked at that time periodically received the secret keys from the key authority and that became a burden for the key authority for sending the keys every time for all the users

Disadvantages of existing system:

- Selective security
- Increased workload
- Loss of data

In order to overcome these disadvantages, we proposed a system called "Revocable Stockpile Identity Based Encryption in Cloud Computing for Unaissilable Data Sharing" which is discussed under this proposed approach.

III. PROPOSED SYSTEM

We in this proposed system “Revocable Stockpile Identity Based Encryption in Cloud Computing for Unaissilable Data Sharing " implemented a solution which overcomes the disadvantages of existing approach. The proposed system provides both the forward and backward security for the data .The users who have authorized access to the cloud can only access the data that is present in the cloud and thus promotes data confidentiality.

The proposed system can provide the security by making sure that the users who have registered at a particular time cannot access the previously present data and the users whose authorization is expired cannot access the data that is present in the cloud after his/her authorization is expired. By this way the data is secured in our proposed system

The proposed system will also provide data confidentiality by sending the secret keys for only those users who have requested for the key. The key authority sends the keys to only those users who have authorized access and who request for the key. This will also reduce the workload for the key authority.

Advantages:

- Provides both the forward and backward security
- Provides Data Confidentiality
- Reduced Workload

IV. IMPLEMENTATION

This system consists of the following modules:

- Data provider
- Key Authority
- User

Data Provider:

The data provider is responsible for uploading the files to the cloud. The data provider can update the files in the cloud

The various activities of data provider include:

- Signup
- Login
- Upload a file to cloud
- Uploaded file details
- File update
- Logout

Key Authority:

The Key Authority is responsible for sending the secret key to the users who request for the key

The various activities of key authority include:

- Login
- Data provider details
- User Details
- User Requests
- Download Details
- Logout

User:

The user is the one who access the files present in the cloud by seeking the secret key from the key authority

The activities of users include:

- Send request
- Download File
- Logout

Figure 1 provides flow of the "Revocable Stockpile Identity based Encryption in Cloud Computing for unaissilable data sharing ". Here in this architecture we have three actors data provider, key authority and user. First the data provider will login with the credentials and uploads a file into the cloud .The data provider will have all the information about the file. When user a logs in and if he/she need a particular file from the cloud then the user must request for the key .The user receives the secret key via email and the user can download the required file by using the secret key. The secret key generated will sent to the user from the key authority .The key authority is responsible to send the secret key to the user.

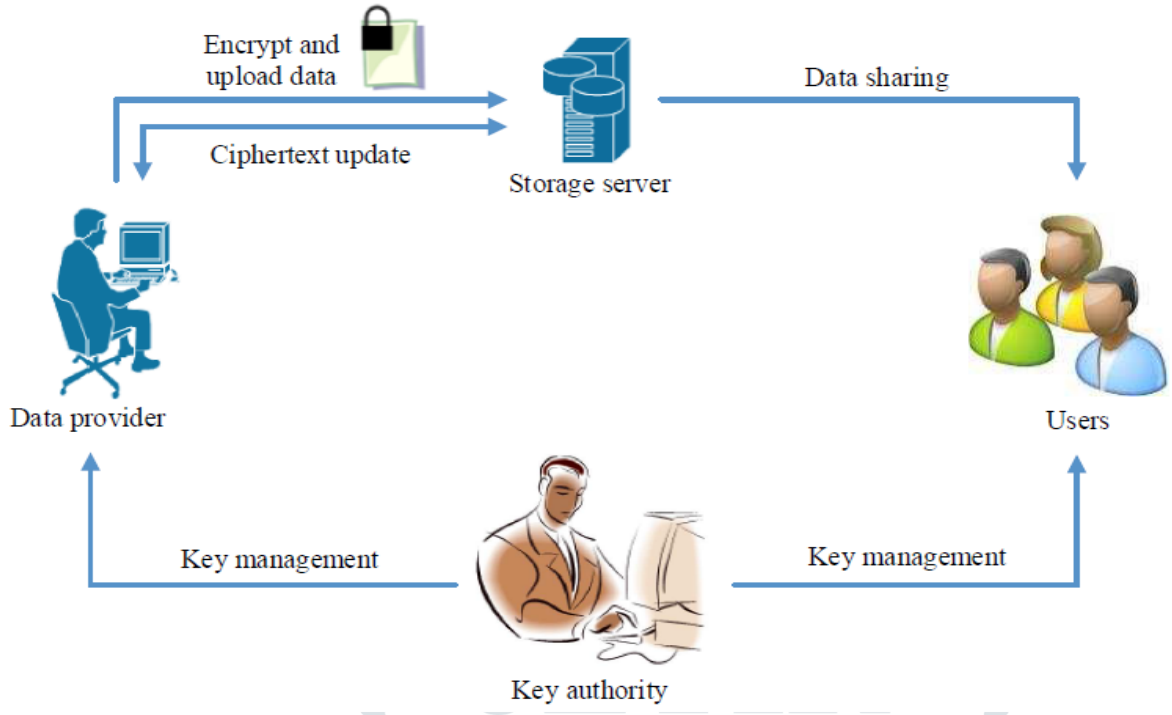

Fig.1 Flow of "Revocable Stockpile Identity Based Encryption"

The files uploaded by the data provider will be stored in the cloud in an encrypted format and a secret key is generated. The generated secret key will be shared to both the data provider and the key Authority. When a user want to access a particular file present in the cloud then he/she should request the key from the key authority. If the key given by the user is valid then only the user can download then file

The Advanced Encryption Standard (AES) algorithm is used for the encryption of data .The Advanced Encryption Standard (AES) Algorithm encrypts a 128 bit plain text block into 128 bit cipher text block using cipher key of either 128 bits, 192 bits or 256 bits. The different key lengths employed for AES are referred to: AES-128, AES-192 and AES-256. The AES Algorithm performs 10 rounds, 12 rounds and 14 rounds depending on the key length 128 bits, 192 bits and 256 bits respectively. Each round consists of 4 byte-oriented cryptographic transformations

- Byte Substitution
- Shift Rows
- Mix columns
- Add Round key

The Diffie Hellman Key Exchange algorithm was the first practical method for establishing a shared secret code over an open communication channel. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values. Calculation of Secret Key by User A

$$K = (Yb\ )\ Xa \bmod q$$

Calculation of Secret Key by User B

$$K = (Ya)\ Xb \bmod q$$

The algorithm itself is limited to the exchange of secret values. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.

V. CONCLUSION

Cloud Computing provides a great convenience for people. By using the Revocable Stockpile Identity Based Encryption we provide the data confidentiality and also both the forward and the backward security. The proposed Revocable Stockpile identity Based Encryption is proved to be adaptive and secure in the standard model. The comparison results prove to be feasible in terms of both the efficiency and functionality and also useful for the practical applications.

VI. REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50–55, 2008.

[2] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563, 2012.

[3] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.