I J C T A, 9(26) 2016, pp. 407-415

Anonymous Authentication of Data Stored using Attribute-Based Encryption and Digital Signature

M. Stalin[1] and R. Thamarai Selvi[2]

ABSTRACT

Cloud computing reaches huge growth in an Web-Based development and so privacy andsecurity are the most important issues. In this study proposed a new decentralized access control schemewith multiple KDC's for securing data stored in cloud. In proposed method, the cloud provides theunidentified authenticity of the user through Third party auditor. An implemented secure storage andaccess for creating a new file, modify the file and read the file in a cloud environment, a suitable encryptionmethod with key administration is applied before outsourcing the data. Secure access control byon condition that access to files with the policy-based access control using Attribute-Based Encryption (ABE)digital signature key schemescheme. Multiple KDC's for key management is provided to achieve the decentralized architecture. PrivateKey is the permutation of the member's credentials, so that high protection will be achieved. The protocol supportsmultiple read and writes arranged the data stored in the cloud.

Keywords: Cloud computing, Access control, authentication, digital signatures key, attribute-based encryption, cloud storage.

1. INTRODUCTION

In Web based social networking access control is very important and only valid user must be allowed to access and store personaldata, images and videos and all this data is stored in cloud. The goal is not just store the data strongly in cloud it is also important to make secure that anonymity of user is ensured. The situation like user wants to remark on object but does not want to be known. But the user wants the other user to know that he is a valid cloud member. In this study two protocols Attribute Based Encryptionand Attribute Based Signatureare used. ABE and ABS are combined to offer genuine access control without revealing the identity of the member.

The important offerings of this paper are distributed access control that is only approved users with valid attributes can have entree to information in cloud. The member who stores and modifies the data is verified. There are many KDCs for key organization because of this the structural design is decentralized. No two users can join together and verify themselves to access data if they are not valid. There is no access of data for users who have been revoked. The process of invalidation or withdrawal of manage by influence that is removal of license, name or position is revocation. The system is flexible to replay attack. There is maintain for multiple read and write operations on data in cloud. The costs are analogous to centralapproach and cloud performs the costly operations.

1 Research Scholar, Computer Science, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India.

2 Head and Assistant Professor, Computer Applications, Bishop Heber College, Tiruchirapalli,Tamil Nadu, India.

2. LITERATURE SURVEY

In [1] Patient-centric andfine-grained data access control in multi owner settings". A colossal measure of data is always archived in the cloud,and to a large extent of this is sensitive data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a fewright of entry strategy furthermore saved in the cloud. Clients are given sets of traits and corresponding keys. Just when themember have matching set of attributes, would they be able to decrypt the data saved in the cloud.

In [2] A.B. Lewko and B. Waters worked on In this proposed workusers could have zero or more number of attributes from every authority and did not require a trusted server. This proposedtechnique is collision resistant [8].

In [3] proposed scheme delegate the decryption job to a proxy Server, so that the user made computationon minimum resources like hand held devices. The benefit of using this is that the user significantly saves bandwidth,without raising the number of transmission.

In [4] Access control is likewise gaining imperativeness in social networking whereusers store their personal information, images films and shares them with selected group of users they belong. Access control inonline social networkinghave beenstudied.

In [5] gives confidentialitypreserveauthentic access control in cloud.Nevertheless, the researchers take a centralized technique where a 1 key distribution center disperses secretkeys and attributes to all clients. Inopportunely, a single KDC is not just a particular point of failure however troublesome touphold due to the vast no of customers that in a nature'sarea. This system uses a symmetric keyapproach and does not support authentication.

In [6]. On theother hand, the approach did not provide member verification. The other weakness was that a client can make and store documentation and different members can just read the record. Write access was not allowed to clients other than the originator.

In [7] scheme describes several Key Distribution Authorities (coordinated by a trusted authority) which hand out attributes and secret keys to members. Multi-authority Attribute Based Encryption protocol does not require a trusted authority, which way every member must have attributes from at all the KDCs. The benefit of using this technique is that it allows more number of attributes

3. PROPOSED WORK

3.1 Proposed System

The main contributions of this study are the following:

- Distributed access control of data stored in cloud so that only authorized members with valid attributes can access them.
- The identity of the member is protected from the cloud during authentication. The structural design is decentralized, meaning that there can be several KDCs for key management. The access control and authentication are both knowledge resistant, meaning that no two users can collude and access data or confirm themselves, if they are individually not authorized.
- Revoked users cannot access data after they have been revoke. The proposed system is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information.
- Authentication of users who store and modify their data on the cloud.

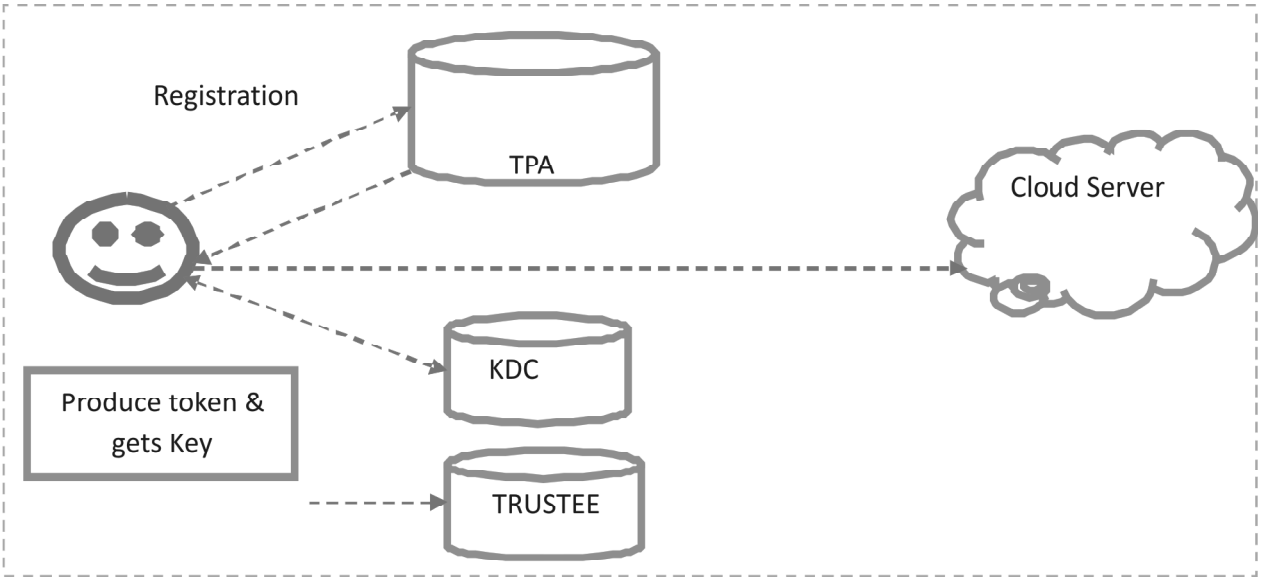

Figure 1: Decentralized Architecture

- The procedure supports multiple read and writes on the data stored in the cloud. The costs are comparable to the existing centralized approach, and the luxuriousoperation are mostly done by the cloud the identity of the user is protected from the cloud during authentication.

3.2 Proposed Approach Framework and Design

Propose Work

One restriction is that the cloud knows the access policy for every record stored in the cloud. In future, we would like to hide the attribute and access policy of a user.

Step: 1

Key Expansion: Using the key schedule of Rijndael, round keys are derived from the cipher key

Step: 2

Initial Round - AddRoundKey: Then using bitwise X OR every byte of the state is combined with the round key.

Step: 3

Rounds

(i) *Sub Bytes:* This is a non-linear substitution step where every byte is swap with another according to a lookup table

(ii) *Shift Rows:* In this transposition walk each row of the state is shifted at regular intervals a sure number of steps.

(iii) *Mix Columns:* A integrationprocess which operate on the columns of the state, combine the four bytes in eachcolumn.

(iv) Add Round Key

Step : 4

Final Round (no Mix Columns)

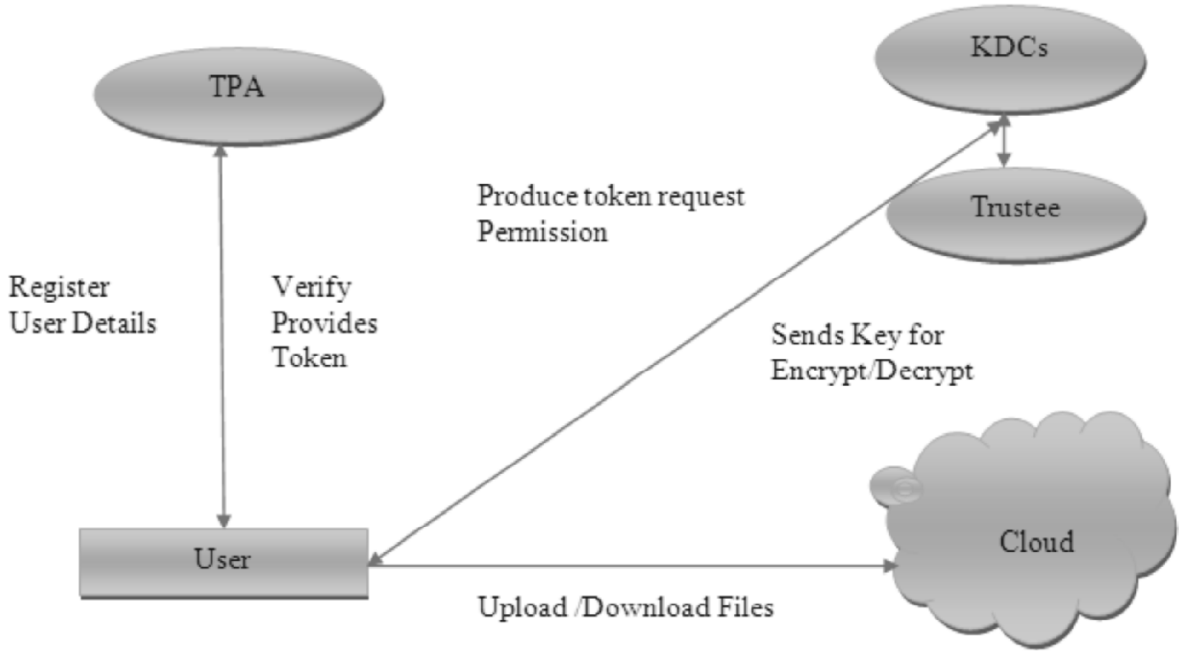

Figure 2: Flow of System

3.3 Process of Module

Client was authenticated with the username and secret code, which is provided by the user. Then the user was asked to answer two protection levels with his/her choice. Each security levels consist of 5 member selectable questions. The user may choose any one question from two protection levels. The private key for encrypt the file was generated with the mixture of username, password and the answers for the protection level questions. After generating the private key the member will apply for to the key administrator for the public key. The key manager will verify the policy Associated with the file. If the rule matches with the file name then same public key will be generated. Otherwise new public key will be generated. The client can revoke the policy and renew the policy due to the necessity.

In this study follow are the cryptographic keys to protect data files stored on the cloud

Public Key

It is a random generate binary key, generate and maintain by the Key administrator itself. mostly used for encryption and decryption.

Private Key

It is the arrangement of the username, password and two security question of member's choice. It is maintained by members itself. Used for encrypt / Decrypt the file.

Access key

It is associated with a policy. Private access key is maintain by the member. It is built on ABE. data access is of read or write.

3.3.1 Cloud member Creater, Writer, Reader Registration

This module is designed for new users who visit this thesis. The new user has to register with the proper details. This system requires a proper user authentication for accessing the features behind in this system.

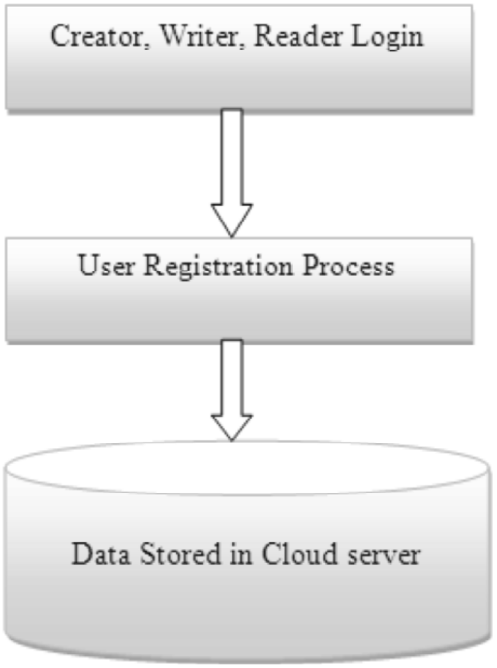

Figure 3: User Login Process

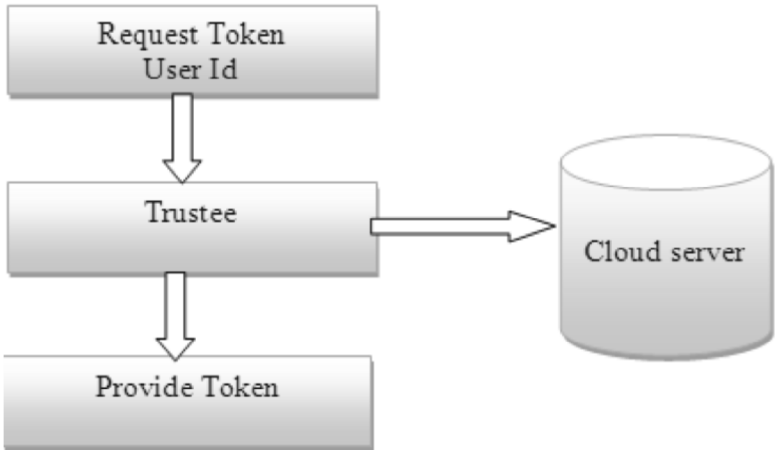

Figure 4: User Accessibility

For getting the rights to access the features users have to register their identity to this system. Once registered the system will provides the accessibility rights to the users to work in this system. This module is main module that is user can select the file type here then only the use can upload the files later. The selected file type only can be uploaded by the user.

3.3.2 Trustee and Key Distribution Centre

Users receive a token from the trustee, who is expected to be honest. A trustee can be someone like the centraladministration who manages public insurance numbers etc. On presenting her idlike health insurance number, the trustee gives her a token. There are multiple Key Distributor Controls (here 1), which can be scattered. Users on present the token to Key Distributor Control receive keys for encryption/decryption and signing. Secret keys given for decryption, keys for signing.

3.3.3 File Upload

The member made apply for to the key manager for the public key, which will be generated according to the policy associated with the file. special policies for files, public key also differs. But for same public key for same policy will be generated. Then the member generates a private key by combining the username, password and protectionidentification. Then the file is encrypted with the public key and private key and forwarded to the cloud.

FILE DOWNLOAD

The member can download the file after achievement of the authentication process. As the public key maintained by the key manager, the member request the key executive for public key. The authenticated client can get the public key. Then the member can decrypt the file with the public key and the private key. The member's credentials were stored in the member itself. All through download the file the cloud will authenticate the user whether the user is valid to download the file. But the cloud doesn't have any attribute or the details of the user.

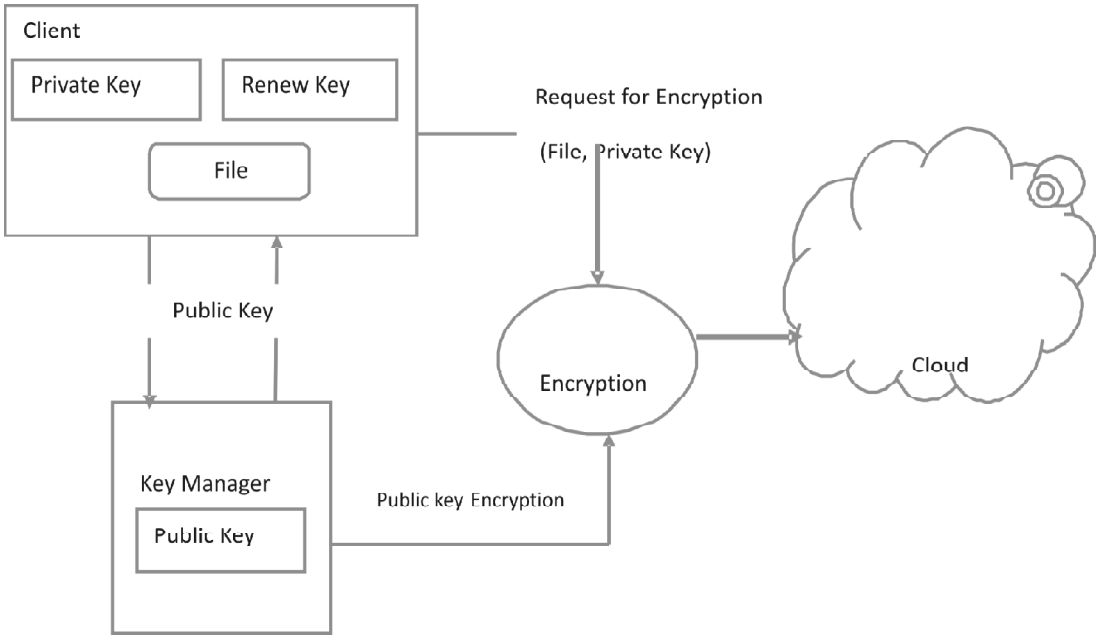

Figure 5: File uploading process.

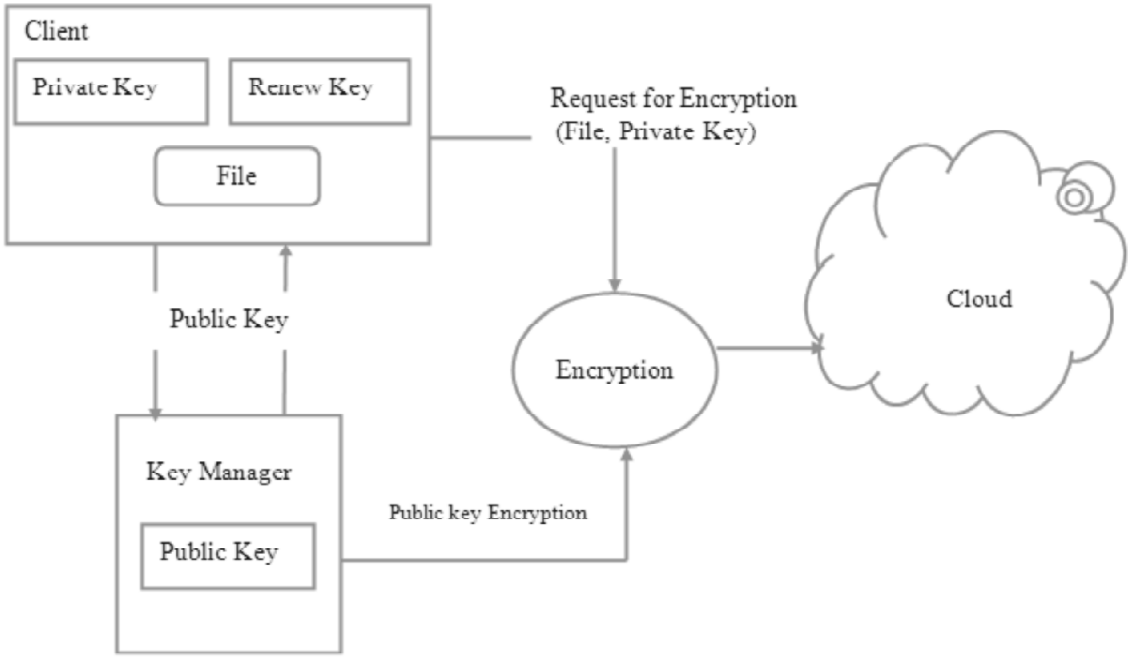

Figure 6: File downloading process

3.3.4 File Access Control

Capacity to limit and control the access to host systems and applications via communication links. To accomplish, access must be recognized or authenticated. After achieved the authentication process the users must associate with correct policies with the files.

3.3.5. Key Generation

Even such as working on SQLSERVER2005 database and ASP.NET for web applications we came across digital signature key. This message-digest algorithm takes as input a message of arbitrary measurement

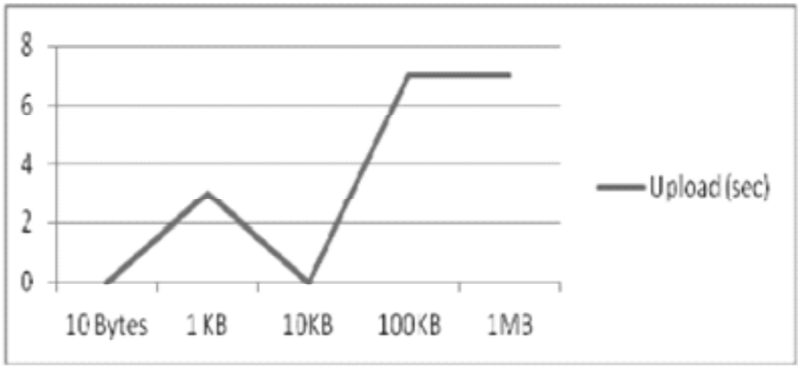

Figure 7: Graph showing time required for uploading the file on cloud

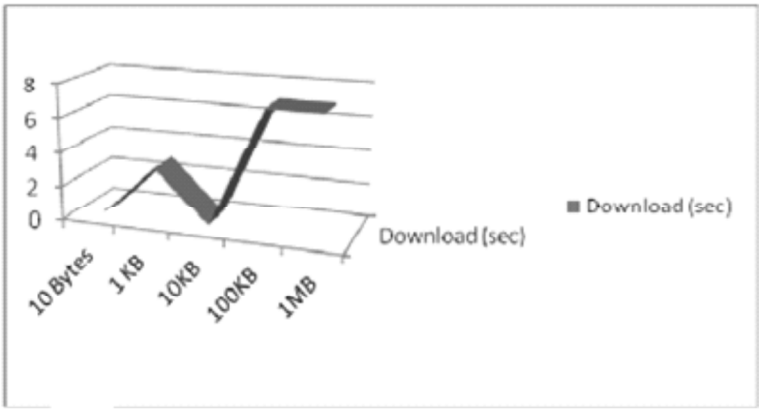

Figure 8: Graph showing time required for downloading the file on cloud

lengthwise and produce as output a 168-bit or "message-digest" of the input. The DEK algorithm is intended for digital signature key applications, where a huge file must be "compressed" in a protected manner before being encrypted with a secrete key under a public-key cryptosystem.

4. COMPARISON OF OUR SCHEME WITH EXISTING ACCESS CONTROL SCHEMES

Table 1
Analysis of time required for transaction on cloud

File Size	*Upload (Sec)*	*Download (Sec)*
10 Bytes	15	0
1 KB	17	3
10 KB	19	0
100 KMB	20	7
1 MB	22	7

5. EXPERIMENT AND RESULTS

The proposed method has been implemented using .NET Technology.A new decentralized access control scheme for secure data storing the clouds that supports unidentified authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the member's identity before storing data. The scheme also has the added feature of access manage in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, updating, and reading data

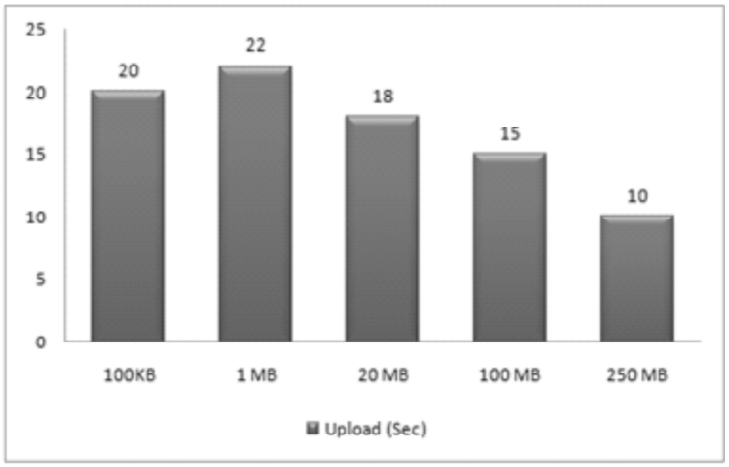

Chart 1: Graph showing time required foruploading the file on cloud

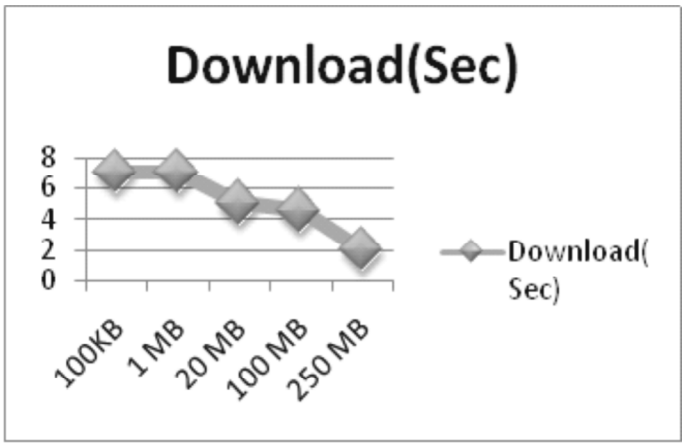

Chart 2 : Graph showing time required for downloading the file on cloud

stored in the cloud. Distributed access control of data stored in cloud so that only official users with legitimate attributes can access them. Authentication of users who store and change their data on the cloud. Theindividuality of the member is protected from the cloud during authentication.Moreover our verification and access control proposal is de-centralized, unlike other access control schemes designed for clouds which are centralized.

Table 2: Analysis of time required for transaction on cloud

File Size	*Upload (Sec)*	*Download (Sec)*
100KB	20	7
1 MB	22	7
20 MB	18	5
100 MB	15	4.5
250 MB	10	2

6. CONCLUSION

This paper presented a decentralized access control technique with anonymous authentication. This decentralized method provides member revocation and prevents replay attacks. Even though the cloud does not know the identity of the user who stores information, but it verifies the member's credentials. This paper made key distribution is done in a decentralized way. The authentication and accessing the Cloud is Robust,

Hence Overall Communication Storage are been developed by compare to the Centralized approaches. This thesis would promote a lot of research in the area of Anonymous Authentication.

REFERENCES

[1] M. Li. S. Yu. K. Ren. W. Lou., "Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings",*in Secure Comm*, 89–106, 2010.

[2] A.B. Lewko. B. Waters., "Decentralizing Attribute-Based Encryption", *Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT)*, 568-588, 2011.

[3] M. Green. S. Hohenberger. B. Waters., "Outsourcing the Decryption of ABECiphertexts", *Proc. USENIX Security Symp*, 2011.

[4] S. Jahid. P. Mittal. N. Borisov., "EASiER: Encryption-based access control in social networks with efficient revocation",*in ACM ASIACCS*, 2011.

[5] F. Zhao. T. Nishide. K. Sakurai., "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems",*in ISPEC, ser. Lecture Notes in Computer Science*, 83–97,2011.

[6] S. Ruj. A. Nayak. I. Stojmenovic. "DACC: Distributed access control in clouds," *in IEEE Trust Com*, 2011.

[7] Kan Yang. Xiaohua Jia. Kui Ren., "DAC-MACS: Effective Data Access Control for Multi- Authority Cloud Storage Systems", *IACR Cryptology ePrint Archive*, **419**, 2012.

[8] S. Ruj, M. Stojmenovic. A. Nayak., "Privacy Preserving Access Control with Authentication for Securing Data in Clouds",*Proc.IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing*, 556-563, 2012.

[9] C. Wang. Q. Wang. K. Ren. N. Cao. W. Lou., "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE Trans. Services Computing* **5(2)**, 220-232, 2012.

[10] J. Li, Q. Wang, C. Wang, N. Cao. K. Ren. W. Lou., "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing", *Proc. IEEE INFOCOM*, 441-445, 2010.

[11] D.R. Kuhn. E.J. Coyne. T.R. Weil., "Adding Attributes to Role- Based Access Control",*IEEE Computer*. **43(6)**, 79-81, 2010.

[12] M. Li. S. Yu. K. Ren. W. Lou., "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings",*Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm)*, 89-106, 2010.

[13] S. Yu. C. Wang. K. Ren. W. Lou., "Attribute Based Data Sharing with Attribute Revocation", *Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS)*, 261-270, 2010.

[14] G. Wang. Q. Liu. J. Wu., "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services", *Proc. 17th ACM Conf. Computer and Comm. Security (CCS)*, 735-737, 2010.

[15] F. Zhao. T. Nishide. K. Sakurai., "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems",*Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC)*, 83-97, 2011.

[16] S. Ruj. A. Nayak. I. Stojmenovic., "DACC: Distributed Access Control in Clouds",*Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2011.

[17] S. Kamar. K. Lauter., "Cryptographic Cloud Storage", *Proc. 14th Int'l Conf. Financial Cryptography and Data Security*, 136-149, 2010.

[18] H. Li. Y. Dai. L. Tian. H. Yang., "Identity-Based Authentication for Cloud Computing", *Proc. First Int'l Conf. Cloud Computing (CloudCom)*, 157-166, 2009.

[19] S. Jahid. P. Mittal. N. Borisov., "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation", *Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS)*, 2011.

[20] R.L. Rivest. A. Shamir. Y. Tauman., "How to Leak a Secret", *Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT)*, 552-565, 2001.