Secure Data Storage in Cloud by Decentralized Access Control

Pooja N. Narve
PG Student
M.B.E.S. College of engineering, Ambajogai, Maharashtra, India

B.M. Patil, PhD
Professor
M.B.E.S. College of engineering, Ambajogai, Maharashtra, India

ABSTRACT
Cloud computing is recently developed new emerging technology for complex systems with massive-scale services sharing among numerous users, where user can rent the storage and computing resources of server provided by a company. Users only require a terminal, a smart phone or tablet connected to the internet. Cloud can store huge amount of data, so the mobile users do not have to carry their data. Therefore, security of data, privacy of user and authentication of both users and services is a significant issue for the trust and security of cloud computing. In order to achieve safe storage, we proposed a secure cloud storage scheme providing access to the data using RSA public- key encryption algorithm and digital signature scheme. In this scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Access control feature is also added by which only a valid users are able to decrypt the stored information. This scheme also prevents replay attack and supports creation, modification, and reading data stored in cloud. Time based user Revocation scheme is also used. Also we compared performance of our system with the 3DES system on the basis of encryption and decryption of data.

Keywords
Cloud computing, Access control, User revocation.

1. INTRODUCTION
Cloud computing is a collection of scalable resources and computing infrastructure which provides services to users with the "pay only for use" strategy [6]. Cloud computing provides three types of service models:

Software-as-a-service provides clients to access the software application running on cloud only paying for it they don't have to store the software [11].

Platform-as-a-service, the provider delivers to user a platform including all the systems and environments comprising software development life cycle viz. testing, deploying, required tools and applications. The user does not have any control over network, servers, operating system and storage but it can manage and control the deployed application and hosting environments configurations [11].

Infrastructure-as-a-service, the provider delivers to user the infrastructure over the internet. With this model, the user is able to deploy and run various software including system or application software. The user has the ability to provision computing power, storage, networks. The consumers have control over operating systems, deployed applications, storage and partial control over network [11].

Cloud computing offers various services through internet. The important service is data storage. It isn't wrong to say that storing personal and sensitive data in cloud is became a trend now. But as the use of new technology increases the concern about the security and privacy of the data is also increase in the mind of the users. So they want such a system which not only secure their data but also maintain the privacy of the user who is storing the data in the cloud [14].

As all the existing systems has a centralized access control method except ABE using system. They are using only one KDC which distribute the keys and stores the data in cloud. But when the KDC fails whole system fails so it is beneficial to use more than one KDC by which the system works in a decentralized way.

1.1 Problem statement
The current work reflects on the problem statement as:

"To provide safe and fast access to cloud for an authorized user without revealing his identity but the user wants the other user to know that he is a valid user. The problems of access control, authentication, and privacy protection are solved."

The above problem statement is divided into sub problems as below:

- Entering the users having attributes as the validation period.
- Encrypt the data file using RSA Encryption and Signature technique.
- Checking the validation period of the user.
- Data file is stored in the cloud securely.
- User decrypt file and make the modification.

1.2 Contribution
New contributions to this work are:

[1] More than one KDCs used so that it becomes decentralized.

[2] RSA encryption-decryption and digital signature cryptosystem is used.

[3] User revocation is done i.e, only non-revoked user can access cloud.

[4] Data uploading, downloading and modification is supported.

1.3 Organization
This paper is organized as follows: Section 2 represents related work or existing secure data storage techniques. Section 3 represents proposed system RSA-DS architecture. Section 4 represents system design that is functional modules implemented. Section 5 represents algorithm. Section 6 represents results. Finally we concluded at section 7.

2. RELATED WORK

This section gives a brief review about the existing systems for secure storage of data in cloud.

Sahai and B. Waters [1] proposed a new Identity-Based Encryption (IBE) scheme that is called as Fuzzy Identity-Based Encryption. A Fuzzy IBE private key was identity by ω whereas the cipher text encrypted is identified by ω'. It identities ω and ω' are close to each other as measured by the "set overlap" distance metrics. It used to apply the Encryption by obtaining the biometric input as identifier which inherently will have some noise each time they are sampled. Thus it is used for a type of application that "attribute-based encryption".

Goyal et al [2], worked on "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data" .In this system the sender has an authorization to encrypt information. A revoked attributes and keys of users cannot write again to stale information. The attribute authority receives attributes and secret keys from the receiver and he/she is able to decrypt information if it has matching attributes. It performs distribution of audit log information and screen out encryption.

Bethencourt et al [3] proposed distributed system the user can access the data only if the data consist of credential or attributes. Only way of enforcing such data in Cloud can be performed through the trusted server to store the data and accessing the cloud. Here the complex access control on the encrypted data is performed in which the Cipher text policy Attribute-Based Encryption is used. By using this scheme the storage data can be kept confidential even when the storage is untrusted, and this method secures against the collusion attack. This system attributes are used to describe a user's credentials and a party encrypting data determines a policy for who can decrypt. Thus this method uses the Role Based access Control (RBAC).

M. Chase [4] proposed identity based encryption the user use the identity to search the data whereas in attribute based encryption involves attribute to search the data. Sahai and water introduced a single authority attribute encryption scheme and left the question whether the multiple authorities allowed distributing system. This scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number *dk* and a set of attributes. Thus this scheme tolerates an arbitrary number of corrupt authorities.

Maji et al [8], worked on "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance". This technique ensures anonymous user authentication ABSs were introduced. This was also a centralized approach. The user significantly saves decryption time, without raising the number of transmissions.

Maji et al [9], worked on "Attribute-Based Signatures," This method takes a decentralized approach and provides authentication without disclosing the identity of the users. It also provides security against a malicious attribute authority.

Ruj et al [10] proposed a data storage and access in which the multiple encrypted copies of data can be avoided. The main novelty of this system is producing the key distribution centers where one or more KDCs distribute keys to data owners and users. KDC provide access to particular fields in all records. Single keys separates the data and the data owners, using this technique the user own the data by having the attribute it had, and this can be retrieved only if the attribute matches the data. The Author apply the attribute based encryption (ABE) based on bilinear pairings on elliptic curves. This scheme is collusion secure in which two users cannot together decode any data, that no one has individual right to access. DACC also supports revocation of users, without re-distributing keys to all the users of cloud services. This system results in lower communication, computation and storage overheads, compared to existing models and schemes.

3. PROPOSED SYSTEM

The architecture of the proposed system is described below:
According to the proposed system, there are three following users, a creator, a reader, and a writer. Creator first get himself registered to cloud. Then it asks for public and private key to KDC. KDC generates multiple keys and distribute it among users. Creator take key and encrypt the file using RSA encryption algorithm it converts message into ciphertext. The ciphertext C with a signature c is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read the message in the cloud sends C. That the user has attributes matching with the access policy, it can be decrypted and get back the original message.

Write also proceeds in the similar way as file creation. By designating the verification of the data to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypting and using the keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

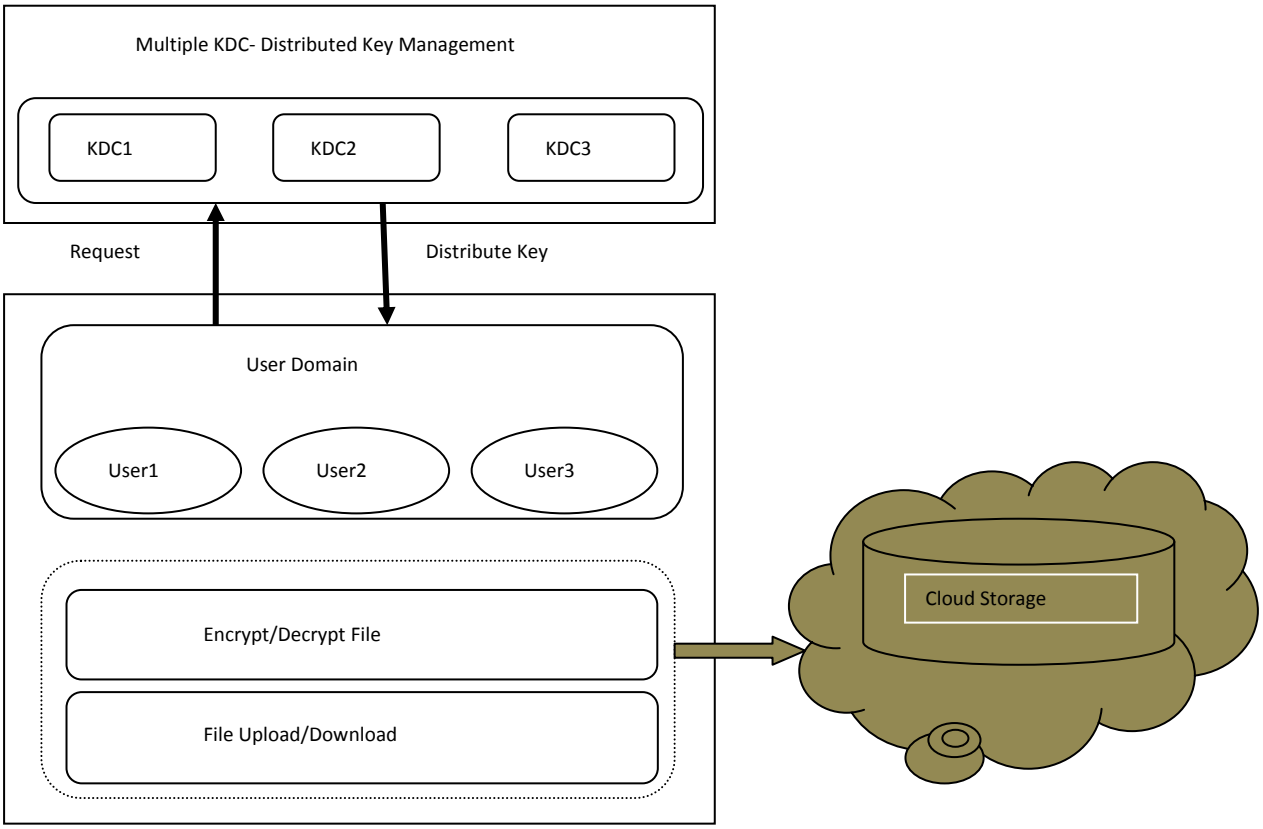


Fig 1: System architecture of proposed system

4. SYSTEM DESIGN

In this system six modules are implemented:

4.1 Key Management:

Following cryptographic keys are used to protect data files stored on the cloud:

4.1.1 Public Key

The Public key is a random generated binary key, generated and maintained by the Key manager itself.

4.1.2 Private Key

It is the combination of the username, password and two security question of user's choice.

4.2 File Encryption/Decryption

In existing system Attribute-based encryption method is used for encryption and decryption. Here RSA algorithm is used for encryption and decryption. RSA algorithm is most commonly used public-key algorithm. The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the e^{th} power modulo n:

$$C = ENCRYPT(M) = M^e \bmod n \quad \text{.....(1)}$$

The input M is the message; the output C is the resulting cipher text. The decryption operation is exponentiation to the d^{th} power modulo n:

$$M = DECRYPT(C) = C^d \bmod n \quad \text{.....(2)}$$

4.3 Signature

Digital signatures are one of the most important inventions of modern cryptography. Digital signatures should be such that each user should be able to verify signatures of other users, but that should give him/her no information how to sign a message on behind of other users. The main difference from a handwritten signature is that digital signature of a message is intimately connected with the message, and for different messages is different, whereas the handwritten signature is adjoined to the message and always looks the same. An RSA digital signature key pair consists of an RSA private key, which is used to compute a digital signature, and an RSA public key, which is used to verify a digital signature.

4.4 File upload

The client made request to the key manager for the public key, which will be generated according to the policy associated with the file. Then the file is encrypted with the public key and private key and forwarded to the cloud.

4.5 File download

The client can download the file after completion of the authentication process. As the public key maintained by the key manager, the client request the key manager for public

key. The authenticated client can get the public key. Then the client can decrypt the file with the public key and the private key. During 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 attributes or the details of the user.

4.6 File modification

Until now no one was able to perform modification or updating in a file stored in a cloud. So this project gives the facility to modify the content of the file. For that firstly there is need the private keys to download the file from the cloud then after decrypting the file it is possible to update the content of the file securely.

5. ALGORITHM

The algorithm to develop this project is given below:

Step 1: User should register in the cloud first with username, id and cloud subscription limit.

Step 2: User request for connection to key generation centre.

Step 3: Key generation center generate the group of keys.

Step 4: Key Distribution Centre distribute the keys among users.

Step 5: User upload the data file and forward it for Digital signature.

Step 6: After signing file the content of the file are Encrypted using public key and file stored in the cloud.

Step 7: Second user login with the help of username and id.

Step 8: Checking of second user if it is revoked or non-revoked is done on the basis of cloud subscription limit.

Step 9: If the user is non-revoked then it request cloud for downloading the file.

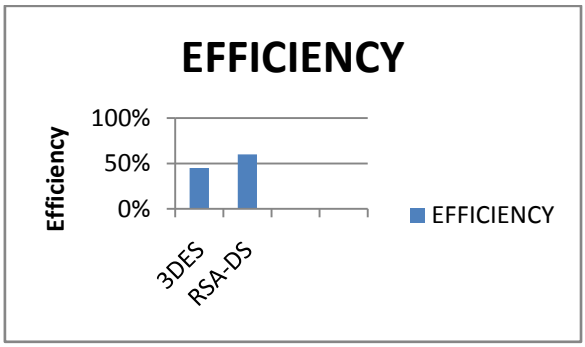
Step 10: Cloud check the validity and give permission to download the file.

Step 11: Cloud start the process and the file is decrypted using private key and open for user to read or modify.

6. RESULTS

RSA algorithm for encryption of data unlike other existing systems which uses attribute based encryption. The disadvantages of using attribute based encryption are that, there aren't a lot of deployments as it is still new, and the full benefit can be obtained only after deploying sufficient infrastructure. Vendors are still playing with the right implementation of the right protocols. The major advantage of using RSA algorithm is that it uses Public Key encryption. This means that your text will be encrypted with someone's Public Key (which everyone knows about). However, only the person it is intended for can read it, by using their private key (which only they know about). Attempting to use the Public Key to decrypt the message would not work. RSA can also be used to "sign" a message, meaning that the recipient can verify that it was sent by the person they think it was sent by.

The efficiency of the system can be analyzed in terms of performance of encryption and decryption algorithm. The performance of the proposed system is compared with a 3DES.Graph 1 shows that the performance of the proposed system is too much higher than existing one.



Graph 1: Performance evaluation graph

The following table shows the comparison between existing system and proposed system by analyzing various parameters such as distribution of keys, access policies and authentication.

Table 1. Table comparing Proposed system with other existing system

Scheme	Approach	Authentication	Read /write Aces s
Secure and Efficient Access to Outsourced Data	Centralized	No Authentication	1-W-M-R
Attribute Based Data Sharing with Attribute Revocation	Centralized	No Authentication	1-W-M-R
DACC: Distributed Access Control in Clouds	Decentralized	No Authentication	1-W-M-R
Outsourcing the Decryption of ABE Ciphertexts	Centralized	No Authentication	1-W-M-R
Realizing Fine-Grained	Centralized	Authentication	M-W-

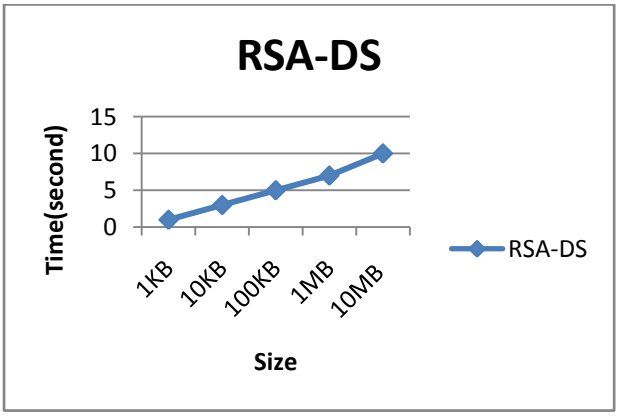
and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems			M-R
Proposed System	Decentralized	Authentication	M-W-M-R

In the single key distribution environment, the public key of all the users is maintained by the single KDC. The single KDC is responsible for all the encryption and decryption. Hence the load on the center is too much too handle such a large amount of key as the users of cloud are increasing day by day. Hence the burden of one KDC is divided into more than one KDC. As the one KDC is the single point of failure may breakdown the transaction hence the keys are distributed all over the KDCs.

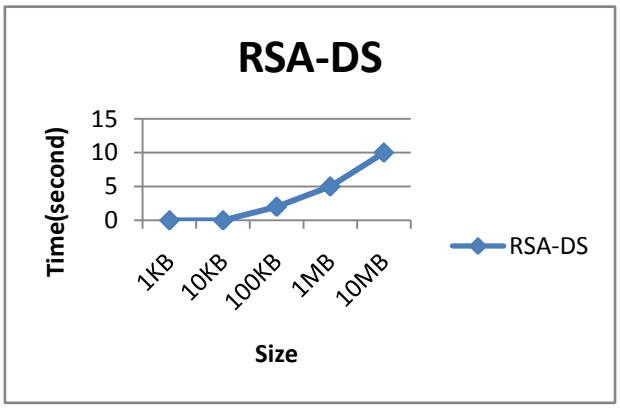
The Authentication is to verify the user among the various users. Only Authorized user can access the data. The authentication process exceeds authorization. The authentication can be providing by obtaining the username and id. According to the credentials that are received by the user can get verified uniquely.

The user can decide that which user can access his data, and which user can only read the data or can modify it and write back. There are 2 types of access policies, the only read policy permits user to only read the file and can only downloads the file. User can't make any changes through it. 1-W-M-R means that only one user can write while many users can read. M-W-M-R means that many users can write and read.

The following graph shows the time required for file with different sizes to upload and download from the cloud using RSA-DS proposed system.



Graph 2: Uploading Data file to cloud



Graph 3: Downloading data from cloud

7. CONCLUSION AND FUTURE SCOPE

This paper puts the light on the security, privacy and storage issues in cloud by the means of services, existing systems and their disadvantages, access control methods and authentication methods.

So the decentralized access control scheme with more than one KDCs is implemented. Also without using ABE algorithm here used the RSA cryptosystem which is public key encryption technique. This system provides user revocation based on the cloud subscription limit of the user. It also prevents replay attacks. It also does uploading, downloading and modification in data present in cloud.

As a future research direction, this technique can be implemented in real cloud environment and also designing more efficient algorithm which can hide attributes and access policy of the user is possible.

8. REFERENCES

[1] Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89- 98, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[4] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

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

[6] Ch. M Siva Rama Krishna and G. John Samuel, "Decentralized access control with Anonymous authentication of data stored in cloud,"IJMETMR, vol.2,issue no. 8, pp. 2052-2060, 2015.

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

[8] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion- Resistance," IACR Cryptology ePrint Archive, 2008.

[9] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376- 392, 2011.

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

[11] L. Ertaul, S. Singhal and G. Saldamli, "Security challenges in cloud computing," Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009.

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

[13] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.

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

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

[16] F. Zhao, T. Nishide, and 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), pp. 83-97, 2011.

[17] Sushmita Ruj, Member, Ieee, Milos Stojmenovic, Member, Ieee, And Amiya Nayak," Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds" Ieee Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

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