A New Approach for Providing the Data Security and Secure Data Transfer in Cloud Computing

Manoj Prabhakar Darsi[#1], K.Suresh Joseph[*2], Dr. S.K.V.Jayakumar[#3]

[#1] *PG Scholar in department of CSE& Pondicherry University Puducherry, India.*

[*2] *Faculty in department of CSE & Pondicherry University Puducherry,India*

[#3] *Faculty in department of CSE & Pondicherry University Puducherry, India*

***Abstract*— Cloud computing is a emerging paradigm of computing in IT because of its performance ,low cost ,availability ,accessibility ,economy of scale, on-demand and other luxuries. Data is the most valuable of clients (or) company's asset; it must be protected with much vigilance than any other. Data Security in cloud is one of the big issue which acts as obstacle in the implementation of cloud computing. In this paper we propose a new method that can efficiently protect the data from begin to end. To protect data we use Advanced Encryption Standard (AES) to encrypt data in cloud and for secure transfer of data we use Secure Sockets Layer(SSL) this provider's communication security over the Internet.**

***Keywords*— Cloud computing, Data security, Internet, Advanced Encryption standard.**

I. INTRODUCTION

Cloud primarily refers to saving of user's data to an offsite storage system that is maintained by a cloud provider. This means instead of storing information on user computer's hard disk or other storage devices, client save it to a cloud database where internet provides the connection between user computer and the cloud provider database.

Cloud computing is the hottest topic of discussion in the IT & research world today. IT world is expecting profound miracles to happen with the intervention of cloud services in all spheres of business. It is a new utility computing model in which resources are pooled to provide everything as a service to many users as possible by sharing the available resources. Cloud computing is actually a combination of various traditional computing techniques like grid computing , distributed computing, virtualization , load balancing ,etc. It combines the functionalities of all these and is evolve as a new model on which everyone can rely for everything.

1. Cloud Service Provider (CSP): It is an entity, which manages Cloud Storage, has significant storage space to preserve the clients' data and high computation power.
2. Owner/Organization: Which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual Owner or company.
3. User: It is a unit, which is registered to the owner and uses the data of owner stored in the cloud. The user may be an owner itself.

The various security concerns and upcoming challenges are addressed in (Wilson and Daniel), 2003; Dimakakos et al., 2009) and also reviewed in terms of standards such as ITIL, PCI-DSS, and ISO-27001/27002. There are architectural security issues which are changing according to various architectural design functioning over cloud computing.
Since outsourcing is the main theme of cloud computing, there are main two concerns in this area:

- External attacker (any unauthorized person) can attack get to the critical data, user has no control over data
- Cloud service provider can breach the owner data is to be kept in his premises.

The proposed method for data security has been framed by bringing together various techniques and utilizing them to perform the task of data security in cloud.
The model uses encryption as the main fundamental protection scheme and data sent to cloud is in encrypted data form. Encryption is the conversion of data into encrypted form called a cipher text that cannot be easily understood by unauthorized person and can be decrypted by the authorized person having a valid decryption key.
In this computing model, owner sends the encrypted data to cloud where it is stored and then the data can be retrieved from the cloud by user, when they request. However, this

is achievable only after when they provides the authentication details to cloud and then search the data with help of keyword obtained from the owner.

II. PROBLEM STATEMENT

Data Security is a major issue in cloud computing environments. There are so many data security issues associated with cloud computing. Security is a major issue in any cloud computing , because it is essential to ensure that only authorized access is permitted and secure behavior is expected Hence we proposed a method to provide data security by using AES (Advanced Encryption Standard) and for secure transfer of data we used SSL (Secure Sockets Layer)this provide communication security over the Internet thus maintaining confidentiality of data.

III. RELATED WORK

The term cloud had already come into commercial use in the early 1990s to refer to large Asynchronous Transfer Mode networks. By 21st century, the term ‘‘cloud computing’’ had appeared, although major focus at this time was on Software as a Service (SaaS). In 1999, sales- force.com was established by Parker Harris,Marc Benioff. They applied many technologies of consumer web sites like Google and Yahoo! to business applications. They also provided the concept’s like ‘‘On demand’’ and ‘‘SaaS’’ with their real business and successful customers.

Cong Wang et al stated that security of data is a problem in cloud storage, which is essentially a distributed storage system. Juels et al. (2007) described a formal Proof of Retrievability (POR) model for ensuring the remote integrity of data. Their scheme combines spot-checking and error-correcting code to ensure both possession and recovery of data files on archive service systems.

Waters and Shacham (2008) built on this model and constructed a random linear function based Homomorphic Authentication. This enables lot of queries and requires less communication overhead.

Wang et al. (2009) described a homomorphism distributed verification scheme using Pseudorandom Data to verify the storage correctness of user data in the cloud. This scheme achieves the guaranty of data reliability, integrity and availability. However, this scheme also not providing complete protection to user’s data in cloud computing, since the pseudorandom data would not cover the entire information.

Sood et al. (2011) and Prasad al. (2011) discussed different security issues in computing. Prasad al. (2011) technique provides the new the authentication by 3-dimensional approaches. It provides data availability by surmounting many existing problem’s like denial of services and leakage of data etc. Additionally, it also provides flexibility and capability to meet the rising demand of today’s complex and network diverse. But in this model, the data stored is not in encrypted form and once the username and password is lost, the data can easily be retrieved by unauthorized user.

Lauter and Kamara (2010) worked over public cloud infra-structure and proposed a model which is well suited for preserving integrity with the help of cryptographic primitives. This technique is purely based on the cryptographic storage service. In their proposed procedure, when a user wants to send the data to other user, they first generate a secret key that encrypts the message. The secret key for decryption is stored on receivers’ system for decrypting the same message. They use the concept of encryption(with index) and tokens are generated with the knowledge of secret key. The searching technique is not efficient for encrypted the data. They discussed symmetric searchable encryption (SSE) and asymmetric searchable encryption (ASE). Both techniques are used to encrypted data searching but increase complexity and make the system cumbersome.

Wang al et. (2010) discussed the drawbacks of using ordinary encryption techniques and suggested that these techniques are not useful for cloud because for this user should have pre knowledge about the encrypted cloud storage data. Their model is based on symmetric searchable encryption method. They gave the design for existing cryptographic primitive and order preserving symmetric encryption (OPSE). Security analysis shows that the success rate for one to many mapping and for ranked keyword’s search. This model did not provide any information about the attacks on security, integrity and confidentiality. This model is not well suited for the security.

Popa al et. (2010) present’s Cloud Proof, a secure storage system for high security for the cloud. In this model users can detect violations of confidentiality, integrity, write serial ability and freshness. The model uses the cryptographic tools and engineering efforts to obtain an efficient and scalable system which allow users to detect and prove the cloud misbehaviour.

Cloud computing is a layered technology and the data in cloud computing has to go through different processing levels, so the security mechanism should be efficiently provided at each and every steps, i.e., from owner to cloud and cloud to user or back to owner. Data should not give a way to the attackers trying to retrieve or tamper with it and not even the cloud provider should be able to harm the data in any manner, because cloud service provider can’t be trusted with data sensitivity. Here by we can say’s that the proposed model has been designed by keeping all these things in mind and surely in comparison to prior works, provides the required measures to protect data in a very organized and efficient manner.

In this paper we are providing security to data by using AES data encryption algorithm and securely transfer of data by using SSL. It consist of two steps

1. ENCRYPTION:
   The data(owner) is encrypted with AES symmetric key encryption algorithm for providing data security.

2. SECURE DATA TRANSFER:

By using the SSL, we transfer the data securely from client to cloud provider, retrieve the data the data from cloud provider to client over the internet.

IV. PROPOSED MODEL

Proposed model has been structured to provides the complete security to the data in the entire process of cloud computing, be in transitit or in cloud. The proposed model divided into two phases, First Phase deals with the data encryption, and secure transfer data over internet. Second Phase deals with the data retrieval from cloud, includes the decryption process and double authentication process, one by owner/company and another by cloud service provider.

First Phase

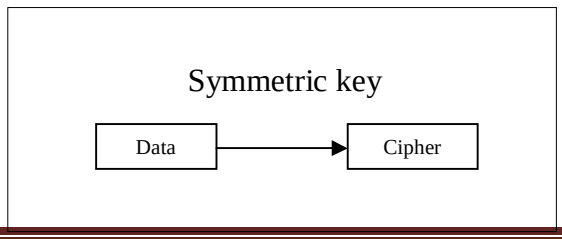
In phase deals with the encryption of data by using the AES data encryption as follows

1. Users: In this clients or user registered to the owner or organization for storing or retrieving of data, for this we provides the authentication process for checking valid user or not. If user is authenticated then provides the client id and decryption key for getting data from cloud. Sometimes user may be owner/company itself.

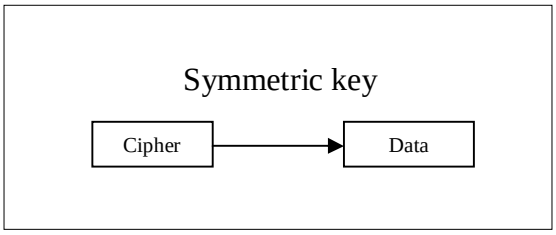
2. Owner : In this the data of owner or organization is encrypted by using data encryption algorithm, in this paper we are using AES-128 for encrypting the data.

Aes is an iterative and a symmetric key block cipher that uses three keys of 128, 192 and 256 bit. The Aes encryption and Aes decryption uses the block size of 128 bits. The maximum block size may be 256 bits, however the key size has no theoretically maximum. The AES decrypt method uses the same process to transform the cipher data back to the original data using the same Encryption key. The user simply need to select AES encrypt or AES decrypt and the encryptor can perform the the rest. It is one of the perfect cryptography algorithms to protect personal data. The encrypt AES tool converts the input plain text to cipher text in a number of repetitions based on the encryption key.The AES decrypt method use the same process to transform the cipher text to the original plain text using the same encryption key. AES has also been called Rijndael on its inventors Vincent Rijmen and Joan Daemen. It was issued by United States Government's National Institute of Standards and Technology in 1997. It is one of the strongest encryption methods that is very hard to break. The SSL is used to protect the data,when transfer from user to cloud, retrieve data from cloud to user over internet. It is being used to provide secure information online, banks financial transactions, e-commerce websites and other financial institutions.

ENCRYPTION PROCESS

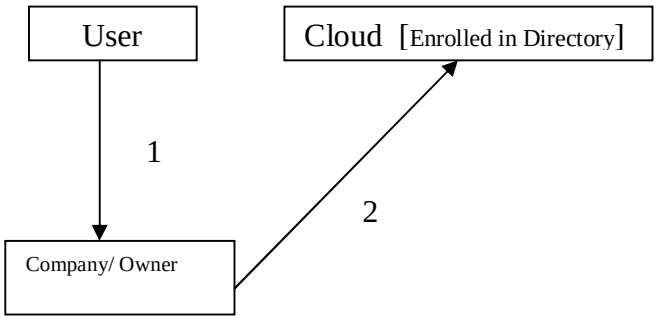


DECRYPTION PROCESS



Client or User Registration

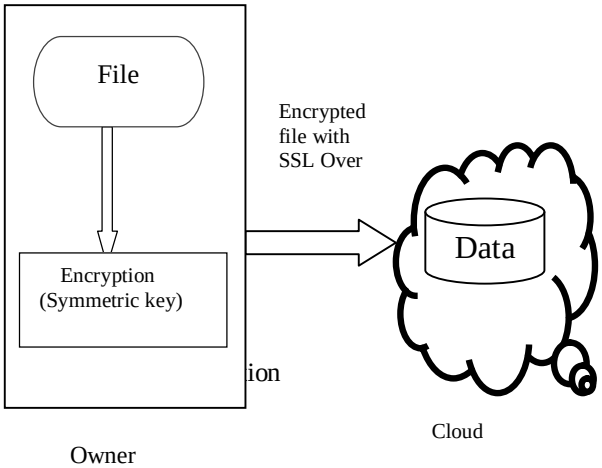
First the retrieval of data requires the user to register him with the owner/organization by getting a username and a password as shown in Figure. The user will register by providing username and password to Owner or Company, which will further forward the username to cloud to let it store the username into its directory.



1.Register to get username with password for authentication
2.Send username to cloud for storing in directory

Data stored in the cloud from owner to cloud: The data is encrypted and transferred to cloud as follows

The file is encrypted with AES and transferred with help of SSL over internet. And stored in cloud



1. Data owner encrypted data through AES algorithm technique as follows

A. Initialize State XOR Round Key are derived from the cipher key using

B. Initial Round

i. Add Round Key: Each byte of the state is combined with the round key using bitwise xor

C. For each of the Nr-1 Round than

i. Sub Bytes (State)

ii. Shift Row (State)

iii. Mix Columns (State)

iv. Add RoundKey (State)

D. Last Round than

SubBytes (State) ShiftRow (State)

i. Add Round Key (State)

ii. Output as encrypted data generates.

iii. Owner Send encrypted data to cloud coordinator.

iv. Cloud Service Provider is store the encrypted data.

High-Level Description of the Algorithm

a)The Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule

Initial Round

AddRoundKey—in this method each byte of the state is combined with the round key using bitwise xor

Sub Bytes –it is a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows –it is a transposition step where each row of the state is shifted cyclically a certain number of steps.

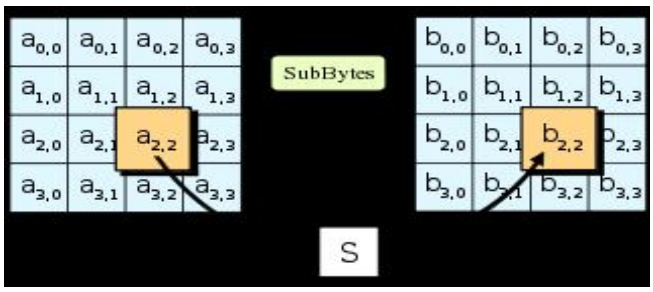
Mix Columns –in this a mixing operation is performed on the columns of the state, combining the four bytes in each column.

1. AddRoundKey

Final Round (no Mix Columns)

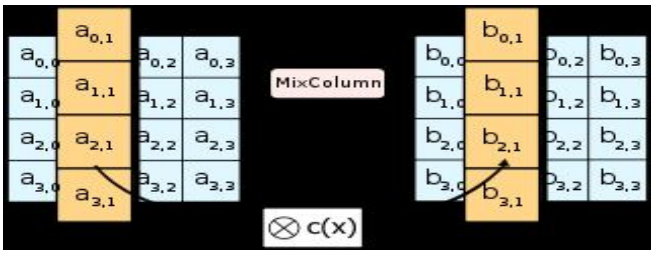
1. Sub Bytes
2. Shift Rows
3. AddRoundKey

In the Sub Bytes step, each byte in the array is updated using an 8-bit substitution box, the S-box. This operation provides the non-linearity in the cipher.



The Shift Rows step operates on the rows of the state, it periodically shifts the bytes in each row by a certain offset. For AES, the first row left is unchanged. Each byte of the second row is shift's one location to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively

In the Mix Columns step, the four bytes of each column's states are combined using an invertible linear transformation. The Mix Columns takes four bytes as input and four bytes as outputs, where each input byte affects all four output bytes. Together with Mix Columns, Shift Rows provides diffusion in the cipher data. During this operation, each column is multiplied by the known matrix that for the 128 bit key .



In the AddRoundKey function, the subkey is combined with the state of each round, a subkey is derived from the main key using Rijndael's key schedule, the subkey is the same size as the state. The subkeys are added by combining each byte of the state with their corresponding byte of the subkey by using bitwise XOR. AES (Rijndael) uses a key schedule to expand a short key into a number of separate the round keys. This is known as the Rijndael key schedule**.**

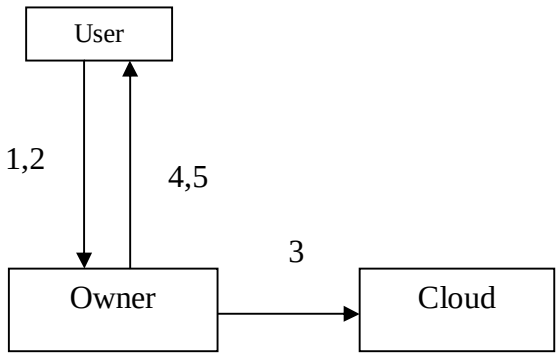
Cloud Service Provider

The CSP stores the data in encrypted form at cloud. The user can access the data by providing the users or owners details to cloud provider, to sote the data to cloud or for retrieval of data from cloud. The cloud service provider checks for authentication and if he is authenticated user then he can access the data.

Second Phase

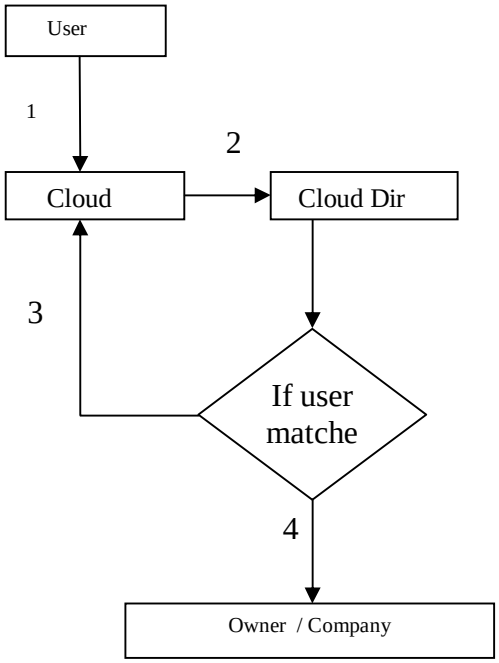
In this phase we describe the process of data retrieval from cloud(CSP). The client or user has to register for getting user id and password from the data owner or company. This phase consist of authentication followed by decryption method to retrieve the data from the cloud.

The following figure shows the process of the decryption of data from cloud by user or client.



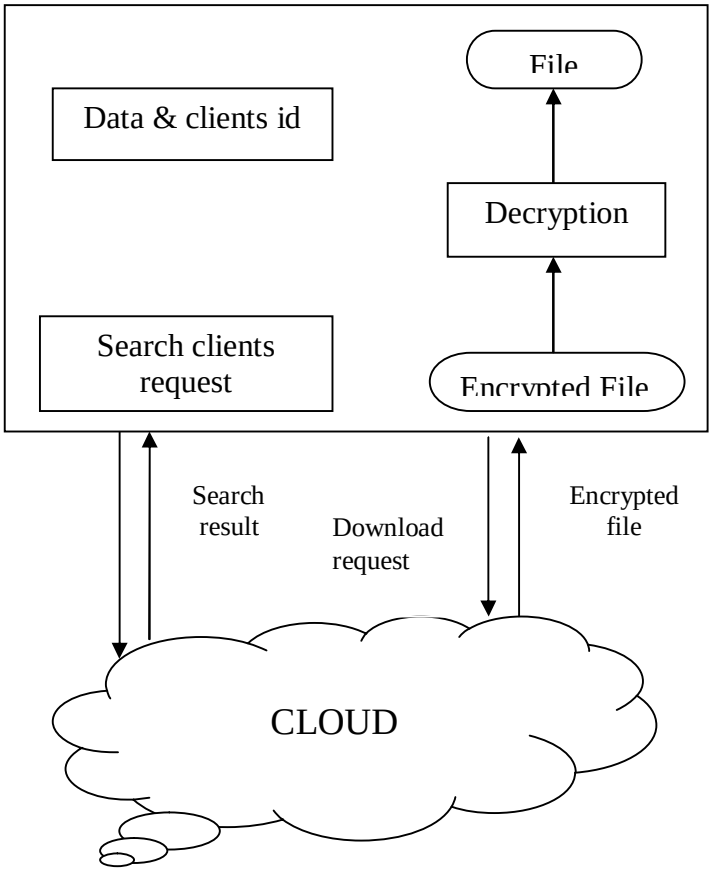
1. Sends password.
2. Answer security question.
3. Sends user id, owner details.
4. Request for data
5. Sends owner details.

User can access the cloud data as follows: The user sends request to cloud by sending user id and owner details. the cloud verifies the details of the user, checks for authenticated user or not ,if authenticated then it proceed to retrieve data from cloud.



1.Request to access data and sends userids,owner details.
2. Checks user id
3. Authentication message to user
4. Redirects to owner.

The below figure shows the authentication and request of data by user from the cloud. Sending data request to cloud and getting data from the cloud



V. SECURITY ANALYSIS

The analysis of the proposed model for security of data throughout the whole traversing into this cloud computing paradigm comes up with the following mentioned steps where data can be very vulnerable to threats like modification, data leakage, confidentiality and privacy of users etc. The proposed model is designed to tackle all the security issues very efficiently.

1. Loss of user identity and password

Authentication is major part in the cloud computing security structure. Thus, in case any user forget or by mistake reveals his user identity and password to any unauthorized persons, the data can be in danger. To protect entire data, we have added one more parameter, which is a must to clear in order to access the data from the cloud. Here the user has to answer a security question whose answer is known to the valid user only, so the unauthorized user will face disappointment only even after having the correct user identity and password. Moreover, attacker has to know the master key to decrypt the encrypted data received from the cloud.

2. Data tamper

The data is always under the threat of being tampered by any unauthorized person. As all the precautionary measures such as data encryption , keywords and AES encryption have been taken in the proposed model to not let anyone tamper the data. The encrypted data is transferred with the SSL over internet to cloud provider.The decryption also done with the same key thus AES provides more security to data, so it's difficult to guess the key.

3.Threat from cloud service provider

The cloud is the place where the data is stored after being transmitted by the owner or user. Suppose the data in cloud is safe from any third party, as the cloud provider will use strict measures to protect it. The cloud provider can turn against the owner. As the data is not in the control of user or owner , anything can be possible or cloud service provider can manage any leakage of data even by helping the rival parties. So, the cloud provider can't be trusted blindly. For this the best solution used in proposed model for data encryption stored in cloud. AES algorithm is used in the proposed model over the Internet. Using public key infrastructure, AES consists of a key which encrypts information and the same key used for which decrypts information, so that only the owners key can read it. 256-bit AES encryption encrypts the data in such a way that it is nearly impossible for an attacker to decrypt it by a brute force attack.

4.Brute force attack or exhaustive key search

The data while in transmission to cloud over an internet network can be attacked by various unauthorized interceptors. Since AES provides the encryption that prevents unauthorized persons from reading data while transferring to the cloud. It is not difficult to crack using today's computers which can crunch large number combinations quickly in order to determine every possible key in an effort known as a brute force attack.

5. Unauthorized Server

As the data needs to be transferred over a internet to the cloud, there are so many ways for an attacker can easily get into the internet based network and act as cloud provider to the owner of data, hence resulting into the loss of data.we are providing AES fro encryption the data and SSL for secure transfer over internet we can always registered with cloud provider only.

VI. CONCLUTION

The proposed model provides a way to protect the data in transit and at rest, check the data and authentication by following the best possible mechanisms. It also provides the data security by using AES algorithm, for secure data transfer from user or client to cloud, it uses the SSL. It also provides availability of data by surpassing many issues like data tamper, data leakage, data tamper and unauthorized access even from the cloud service provider. Proposed model achieves the reliability,availability and integrity of data traversing through user or owner to cloud and cloud to user. The user can retrieve data from cloud by providing the user details to cloud over internet.

VII. REFERENCES

1. Cong Wang, Qian Wang and Kui Ren. Ensuring Data Storage Security in Cloud computing‖ 978-1-4244-3876-1/2009 IEEE.

2. G. Jai Arul Jose Implementation of Data Security in Cloud Computing International Journal of P2P Network Trends and Technology- Volume1Issue1- 2011.

3. National Institute of Standards and Technology. "Request for Candidate Algorithm Nominations for the Advanced Encryption Standard." Federal Register, September 12, 1997.

4. Xiao Zhang Ensure Data Security in Cloud Storage 2011 International Conference on Network Computing and Information Security.

5.CloudSecurityAlliance. http://www.cloudsecurityalliance.org.

6. G. Jai Arul Jose, C. Sajeev, Research Scholar, Sathyabama University, Chennai, INDIA-―Implementation of Data Security in Cloud Computing‖ Aug Issue 2011.

7. http://www.cloudsecurity.org, accessed on April 10, 2009.

8.M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment.

9. Syam Kumar P, Subramanian R An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing International Journal of Computer Science Issues (2011) 261-273.

10.Sandeep K. Sood , A combined approach to ensure data security in cloud computing Journal of Network and Computer Applications 35 (2012) 1831–1838.