International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# Achieving Data Confidentiality and Authentication in Cloud Computing

**Abhilash S Nath[1], Reshna T[2]**

[1]PG Scholar, Department of Computer Science & Engineering, Malabar Institute of Technology Anjarakandy, Kannur (Dt), Kerala

[2]Faculty, Department of Computer Science & Engineering, Malabar Institute of Technology, Anjarakandy, Kannur (Dt), Kerala

**Abstract:** ***The Data sharing is one of the important property in cloud computing. Today our IT industry is developing huge amount of data.it is so difficult to store a large amount of data. Its also expensive and it's not easy to secure those documents which are personal or confidential. Cloud computing is such a technology that help us to maintain this large amount of data in a distributed manner in a network. It's a technology that is rapidly progressing in today's world. The huge building for the servers are becoming imaginary when this technology came. But the security loop holes has given a impact to this technology. It's not easy to handle a data in a unsecure channel .we need some data confidentiality and integrity in our systems. We must also take care the security also meet the expenses of the company in a desired wish. We want a more better encryption schemes used in cloud for data confidentiality one is such that using of a constant size aggregate key where release a constant-size aggregate key for required choices of ciphertext set in cloud s, but the other encrypted files which remain outside should be set confidential. In authentication where users authenticate using a two factor technology where password and a secret number play a role. This technology of using a password and a number for recovery and not lose of personal data for user for authentication even after a failure of Kerberos protocol. This gives user a trust and a thrust to cloud security.***

**Keywords:** Data confidentiality, Authentication, Key-aggregation, Encryption, Decryption

## 1. Introduction

It is like a "resource pool", which can provide the cost-effective and on-demand services to meet the needs by outsourcing data. Cloud computing is defined as both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. Amount of requirement for new resources and storage requirement for terabyte of data generated dailylife. Cloud Computing provides on demand resources as services to client. Cloud is better in scalability, flexibility and platform independent. Cloud computing reduces this whole complexity as organizations need not to own all these resource.

The emerging of cloud computing allows companies to focus more on their core business and brings perceived economic and operational benefits. However, it is an attractive model, it faces many challenges, where the security issues are the most important. cloud security issues can be classified into four categories 1)authentication 2) data integrity 3) data confidentiality and 4)access control mechanisms. Within these challenges that would prop-up great concerns from users when they store sensitive information on cloud servers. The issues arises from the realization that cloud servers are usually handled by commercial providers which are very likely to be outside of the some trusted domain of the users. Confidentiality of data against cloud service providers is frequently desired when users outsource data for storage in the cloud. In daily application systems, data confidentiality is not only a privacy issue, but also of law concerns. The other thing is authentication that must be resolved in Cloud computing environment as soon as possible. The data owner and the servers storing the data are in the entrusted domain, where the servers are fully trusted as an reference monitor responsible for defining and adding access control agenda. By understanding and noticing the main issues and proposing a secure and scalable fine-grained data access control scheme for cloud computing. In this paper is proposed strategy is literally based on the observation that, in daily application scenarios each data file can be associated with a set of attributes which are meaningful in the context of interest. The access structure of user can be defined as a logical expression over these attributes to reflect the scope of data files that the user is allowed to access. As the mathematical or logical expression can express of any required filesets, detailed fine-grainedness of data access control is achieved. compelling observance on these access structures, defining a public key component for each attribute. The difficulty of encryption is just related the number of attributes related to the data file, and is free to the number of users in the system and data file creation/deletion and new user grant operations just affect current file/user without involving system-wide data file update or re-keying.

User authentication is the paramount requirement for cloud computing that restricts illegal access of cloud server is been proposed cloud computing contains three main sides 1) a data owner 2)a user 3) cloud service provider. The Kerberos authentication protocol is to provide reliable authentication over open and insecure networks where communications between the hosts belonging to it may be intercepted. The efficiency and limitation with Kerberos ,it assumes that each user is trusted but is using an un-trusted host on an un-trusted network. Its primary goal is to prevent unencrypted passwords from being sent across that network. However, if anyone else than the proper user has access to the one host that issues tickets used for authentication called the key distribution center (KDC) the entire Kerberos authentication system is at risk. This will reduce the security of Kerberos authentication model. For preventing these all limitations a

new approach should be provided and we focus on the remote user authentication between the user and cloud server. In many circumstances, the weakest link is the password used to get access cloud applications. The reason is the password is often easy to guess and hack. To help to fight any human weakness to the security part, many security-related services are implementing a technology called two-factor authentication. By just other than using just one password for login to a website, users couple a password with a secondary authentication mechanism the two-factor authentication, even if hackers hack password, they'll need physical access to your secondary authentication mechanism in order to access your cloud-based data . To true of our knowledge, paper is the first that simultaneously achieves scalability and data confidentiality for data access control in cloud computing. Main focus and attention is to authenticate a client before accessing service. Username , passwords checking is not enough for a cloud computing like distributed and shared environment. This saves to secure data without much attention on data encryption techniques when an authenticated user is accessing the data.

## 2. Related Work

The Identification based cloud computing security model have been worked out by different researchers But only identifying the actual user does not all the time prevent data hacking or data intruding in the database of cloud environment. The flaw in this system is that it does not ensure security in whole cloud computing platform. Research related to ensuring security in whole cloud computing environments was already done in anonymous structures and modified. Advanced encryption standard based encryption file system is used in some of these models. Because these type of models keep the key and encrypted file in one storage server(database).A successful harmful threat or intended attack in the server may open the whole information files for the expert in hacking, which is not desirable.

Some other models and secured architectures are proposed for ensuring security in cloud computing environment. Although these models ensures secured communication between users and servers, but they do not secure by encrypting the uploaded information. For best security ensuring process, the uploaded information needs to be encrypted so that none can know about the information and its location. At recent times different types of security is used for cloud computing environment are also being researched. Exiting work relates on shared cryptographic file systems" and "access control of data

Shucheng Yu et. al in the work Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing[1] that KP-ABE is a public key cryptography primitive for one-to-many communications. In this paper, KP-ABE, data are related with attributes for each of which a public key component is defined. The encrypting component relates different set of attributes to the message by encrypting it with the corresponding public key components. Every user is assigned an access structure(login) which is usually defined as an access tree over data attributes, i.e, interior nodes(Hierarchical form) of the access tree(login form) are threshold gates and leaf nodes are associated with attributes. Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a ciphertext encrypted under Alice's public key into another ciphertext that can be opened by Bob's private key without seeing the underlying plaintext.

Plutus as a cryptographic file system to secure file storage on entrusted servers. Plutus groups a set of files with similar sharing attributes as a file-group and associates each file-group with a symmetric lockbox-key.its is not suitable for the case of fine-grained access control in which the number of possible "file-groups" could be huge.

Atienese a secure distributed storage scheme based on proxy re-encryption. The data owner encrypts blocks of content with symmetric content keys. The content keys are all encrypted with a master public key, which can only be decrypted by the master private key kept by the data owner. Main issue with this scheme is that collusion between a malicious server and any single malicious user would expose decryption keys of all the encrypted data.

Cheng-Kang Chu et.al in their work" Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage"[2] proposed KAC make a decryption key more powerful in the sense that it allows decryption of multiple ciphertexts, without increasing its size.

ShubhaBharill et.al in their work "A Secure Key for Cloud using Threshold Cryptography Kerberos" that A problem of data security in cloud service provider and also proposed an effective and flexible distributed scheme with explicit dynamic data support, including Kerberos authentication service and third party to authenticate the user in the cloud server . Proposed two approach, Kerberos and MIKEY to provide authenticated transport of group keys in environments that deploy Kerberos for authentication

RuiJiang , "Advanced Secure User Authentication Framework for Cloud Computing",in his work proposed a method called two factor technology which is dicussed in proposed method.

The new policy for preserving was proposed as for authenticated access control scheme for securing data in clouds in which the cloud verifies the authenticity of the user without knowing the user's identity before storing information and added feature of access control in which only valid users are able to decrypt the stored information.

Designed and implemented an optimized infrastructure for secure authentication and authorization in Cloud Environment using SSO (Single Sign-On) for authenticate once and gain access of multiple resources to reduce number of login and password in heterogeneous environment and to attain advantage in security and efficiency.
In 1981, Lamport proposed a remote user authentication system, in which, the server stores the hash value of the user's password for the later verification. However, in 2000, Hwang et al figured that if the password table was in an understandable terms,then whole system could be wrong. Then they proposed a new remote user authentication

scheme using smartcards. The idea was based on the El Gamal's public cryptosystem and did not require a system to maintain a password table for verifying the legitimacy of the login user. But this scheme was not able to resist impersonate attack. A legitimate user could impersonate other valid user to use his ID and PW without knowing the secret key. In 2002, Chien et al proposed an efficient password based remote user authentication scheme, and claimed that their scheme had the merits of providing mutual authentication, no verification table, freely choosing password, and involving only few hashing operations. In 2004, Ku–Chen pointed out that Chien et al.'s scheme was vulnerable to a reflection attack insider attack and was not reparable. Choudhury et al presented a user authentication frame for cloud computing.

They proposed a new idea to apply remote user authentication with smartcard to cloud computing. They claimed their scheme verified user authenticity using two-step verification, which was based on password, smartcard and out of band authentication. However, security analysis, the scheme exists extremely serious attacks such as the masquerading attack, the OOB (out of band) attack, and the password change flaw. Analyzed the vulnerability and attacks existing in Choudhury et al's protocol. Kerberos protocol and some remote user authentication schemes such as Ku-Chen's scheme and Chen's scheme being used for data authentication.

## 3. Problem Identification

In Data Confidentiality enforcing policies that cloud provides for efficiency and economy in case of KP-ABE is not desirable, Attribute-based encryption (ABE) keeps each CT to be associated with an a random attribute number, and the main secret key user can get a secret key for a policy of these attributes so that a ciphertext can be decrypted by this key if its associated attribute conform to the policy. Eg: with the secret key for the policy (1 , 8 , 4 , 2), one can decrypt ciphertext tagged with class above mentioned(1,8,4,2). But, the major concern in ABE is resistance in collusion but not the compactness of secret keys. Interestingly, the size of the key often increases gradually with the number of attributes it passes or encompass, or the ciphertext-size is not constant. Keeping Data confidentiality against cloud servers and increase of ciphertext keys (size) this is in case of key policy based are some of other.

Kerberos is a complex and not a fully good algorithm for trust .To validate the optimal final values of the given parameters of the reputation model and evaluate the performance of the system. Data Storage Security in Cloud Computing is still in its infancy now and research problems are yet to be identified. Improve the efficiency of the algorithm the designated verifiers can concurrently handle multiple sessions from different users' verifying requests. Cloud server can activate and allocate resources are in need, when changes made, updating the workspace elements, and shift workloads to improve efficiency without having to worry about creating new infrastructures . The unnecessary login of user can reduce scalabilty or overhead for cloud servers verifying each time. Authenticating a client to server must be look into user as trusted user but this is not done by Kerberos protocol

### 3.1 Proposed Model

This approach proposed by Cheng-Kang Chu et.al in their work" Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage"[2], that a data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen. Messages can be encrypted via Encrypt by anyone who also decides what ciphertext class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of ciphertext classes via Extract. The keys which are generated are passed to members securely (via secure e-mails or secure devices) Finally, any user with an aggregate key can decrypt any ciphertext provided that the cipher text's class is contained in the aggregate key via Decrypt. A key- aggregate encryption scheme consist of five polynomial-time algorithms as follows.

### 3.2 Algorithm

Setup(1; n): executed by the data owner to setup an account on an untrusted server.whileinputing a some parameter x and the number of ciphertext classes m (i.e., class index should be an integer between or bounded by x and m), it outputs the public system parameter y, which is released from the input of the other algorithms for brevity.

KeyGen: it is run by the data owner to generate a public/main-secret key pair (p, msk).
Encrypt(p, i,m):it is executed by anyone who wants to encrypt data. while input a public-key p, an symbol i denoting the ciphertext class, and a message m, it executes a value or a ciphertext C.

Extract(msk; S): it is executed by the data owner for delegating the decrypting power for a certain set of ciphertext classes to a delegatee. While inputing the main secret key msk and a set Ss of values of index corresponding to different classes, it executes an the aggregate key for set Ss denoted by KS.
Decrypt(KS; S; i; C): executed by a delegatee who received an aggregate key KS generated by Extract.whileinputing KS, the set Ss, an value i denoting the ciphertext class the ciphertext C.

KP-ABE is a public key cryptography primitive for one-to-many transfer of messages. KP-ABE, data are related with attributes for each of which a public key component is defined.

Attribute-based encryption (ABE) makes each ciphertext to be related with an attribute, and the main-secret key holder can get a secret key for a policy of these attributes so that a ciphertext can be decrypted by this key if its associated attribute conforms to the policy. For example, with the secret key for the policy , one can decrypt cipher text

Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a ciphertext

encrypted under Alice's public key into another ciphertext that can be opened by Bob's private key without seeing the underlying plaintext. More formally, a PRE scheme allows the proxy, given the proxy re-encryption key rk a<->b, to translate ciphertexts under public key pka into ciphertexts under public key pkb and vise versa.

PRE just moves the secure key storage requirement from the members to the proxy. It is thus not a desirable to make the proxy inside the database server.

Shucheng Yu et. al in the work "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud ComputingData"[1] proposed that confidentiality is also achieved since Cloud Servers are not able to learn the plaintext of any data file in our construction. Decreasing the computation overhead and increasing scalability on Cloud Servers and thus saving the data owner's payment on this platform, the idea of the lazy re-encryption technique and allow Cloud Servers to "aggregate" computation tasks of multiple system operations.

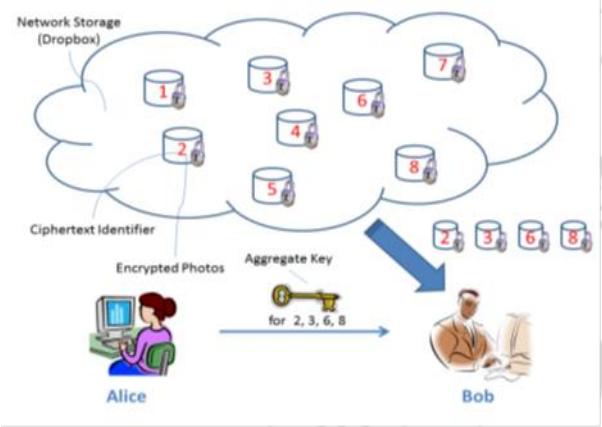
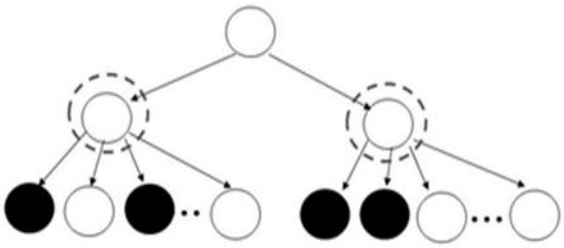



**Figure 3.1:** Key-Aggregate Cryptosystem

We achieve "local aggregation", which means the secret keys under the same branch can always be aggregated. We must use a four sided tree for the bottom level just for better illustration of our main feature. The advantage is still on our hands secure and preserved when compared with 4-sided trees in hierarchical method, in which latter the person who is decrypting the message, the decryption power for all 4 classes (if the key for their parent class is delegated) or the number of keys will be the same as the number of classes. Correctness is not much more difficult to see:



The reality of getting constant-size aggregate key and constant-size ciphertext simultaneously comes from the linear-size system . The main idea to inspiration is to reduce the secure storage and this is a trade-off between two kinds of storage. The random parameter can be placed in unauthorized local storage or in a storage provided by the provider company.it can also be attained on demand, and cannot be attained all the time.

### 3.3 Authentication Strategy

Kerberos is used for providing authentication for a client who want to access the applications stored at server side. Some another reasons for using Kerberos is, in Kerberos user password will not pass over the network, never stored in any form on the client machine and it never be stored in unencrypted form and mutual authentication.The understanding of authenticity for the user and cloud server to each other is known as Mutual authentication. Authentication Server issues a ticket granting ticket to users. User sends their user name to server. Server responds with TGT encrypted with the password given by the user. The password is entered by user on client-if correct the TGT is successfully decrypted.

Logically different from the AS but may reside on the same server. User contacts when a network service is desired. Service ticket request is encrypted with session key provided by the in the TGT, not user's password. TGS authenticates tickets and issues a ticket for the resources as well as the encryption key to use with communication with the service.

Client sends resource ticket and authentication server to the service encrypted with sever key or the client . The client or server will both verify and issues a valid return message i.e with a modified version of timestamp in the authenticator encrypted with client/service key. views message- if timestamp is modified correctly the service is genuine and ready to process request.

Since all authentication process is controlled and monitored by a centralized Key Distribution Centre(KDC),verification of this authentication will allow an attacker to impersonate any user by getting the knowledge about the key. So we use Threshold Cryptography algorithm to divide Ticket Granting Server into multiple parts to allow multiparty authentication, the meaning of above is that one cannot hack or decrypt the key until the predefined numbers of parts of TGS are not available. The second reason for making Threshold Cryptography(TC) algorithm is to provide more availability to the TGS. In a simple Kerberos authentication if TGS got deactivated due to any reason, then all the system get affected and the whole procedure of authentication get shut down. To avoid this type of system failure in this paper we are proposing a Threshold Cryptography algorithm which will divide our TGS into n parts and at least k parts are need to make an useful information. Here k is always smaller than n. Using threshold cryptography is to provide more security to the key used by secret share scheme. In this scheme data D is divided into n pieces and knowledge of some pieces k is enables to derive secret data D. knowledge of any pieces k-1 makes secret data D completely undetermined. Such a scheme is called a (k, n) threshold scheme. This scheme is easily computable when it has necessary data available. This is a safe and convenience method to provide security to key.

Threshold Cryptography algorithm, is applied at TGS. Through this algorithm instead of single TGS, multiple TGS

(n) have been used where at-least k number of parts are needed to decrypt the master key (where k< n). Client sends a request for master key to k number of TGS. If k number of TGS reply ,then the client can get the required master key otherwise client will send the request to TGS[ k+1] and wait for reply. This process will continue until at-least k no. of TGS will not reply. After getting the master key client can request the required service form the service provider.

The server either rejects the ticket or accepts it and performs the service. The master key granted to client can only be decrypted by the cloud server with the secret key shared between the cloud server and TGS. Client or anybody else will never be able to decrypt the master ticket. Since the ticket client has received from the TGS is time-stamped , it allows client to make additional request using the same ticket within a certain time period (typically, 8 hours) without need to prove authentication again.

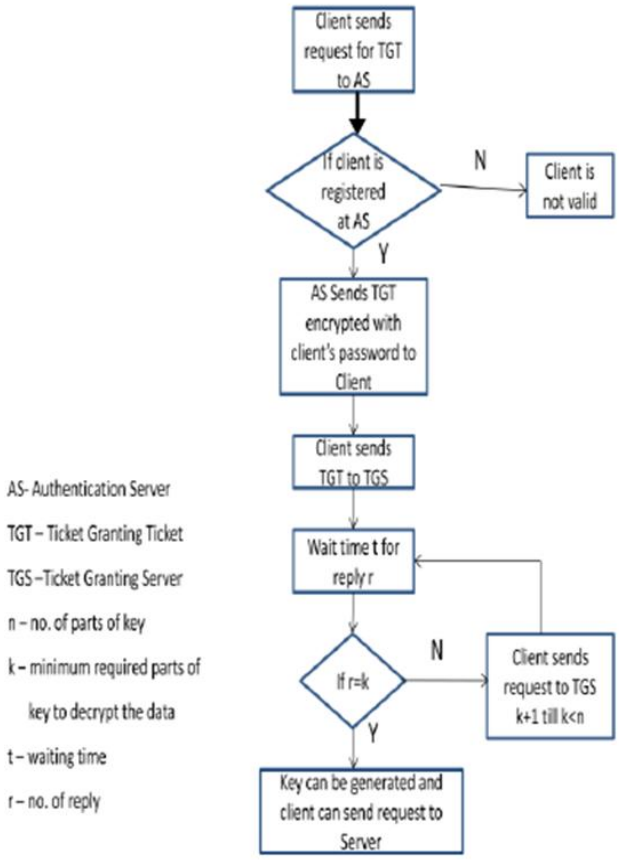



**Figure 3.2:** Authentication Strategy

Applying the two-factor authentication technology, which consists of the user password PW and the secret random number x, to propose an advanced secure authentication protocol which can provide mutual authentication, identity management, session key agreement between the user and the cloud server, and the demanded user password change without sending one time key.

The attacks mainly happens on the login and registration a new algorithm was proposed how this is solved.

### 3.4 Phases of Two Factor Technology

In my second phase of my project is authentication part. Kerberos is used for providing authentication for a client who want to access the applications stored at server side.

Authentication Server issues a ticket granting ticket to users. User sends their user name to server. Server responds with TGT encrypted with user's password. User enters password on client-if correct the TGT(ticket Granting Server) is successfully decrypted. TGS authenticates tickets and issues a ticket for the resources as well as the encryption key to use with communication. Server verifies both and issues a return message with a modified version of timestamp.

In authentication server part applying 2-factor technology ( contain a user password and a secret random number).it is using of smart card for authentication. There are 3 phases
1) Registration phase
2) Login phase
3) Authentication phase.

This technology helps during a failure in Kerberos protocol in authentication server part. The random number which is stored is passed to cloud server during registration phase which also contains the user registration details. The secret number is used as an tool for recovering after any failure in cloud server. This help ticket granting server to provide ticket without a password as this number is used to identify the user without any problem.

## 4. Advantages/ Disadvantages

Advantages;
1) Scalability improving
2) Data confidentiality and authentication improvance

Disadvantages;

Expensive for good encryption algorithms

## 5. Future Scope

In Future it can be upgraded with verifiable and recoverable. The ABE with verifiable provides us to verify the data whether it is modified or not. We can add different encryption schemes in this paper for enhancing the encryption

## 6. Conclusion

The proposed system helps to maintain a constant size key i.e. aggregate key which helps the data safe and secure in cloud. Protect users' data privacy is a central question of cloud storage. The help of using technical tools, cryptographic techniques are getting more versatile and often involve multiple keys for a single application. In this, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. The person can get the constant aggregate key from any class no matter from this, the receiver can always get an constant aggregate key

same size. The approach is more flexible than hierarchical key assignment

## References

[1] Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou, "Achieving secure, scalable, fine grained access in cloud computing," IEEE cloud Computing, Dept. of ECE, Worcester Polytechnic Institute, Email: {yscheng, wjlou}@ece.wpi.edu , Dec. 2012.
[2] Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," IEEE , Sept. 2014.
[3] ShubhaBharill, T. Hamsapriya and Praveen Lalwani , "A Secure Key for Cloud using Threshold Cryptography in Kerberos," IJCA Trans. Cloud computing, vol. 79, no. 7, pp. 09785-8887, Oct 2013.
[4] Kawser WazedNafi, TonnyShekhaKar, SayedAnisulHoque, Dr. M. M. A Hashem4], "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture," IJACSA Trans. Cloud Computing, Vol. 3, No. 10, 2012.
[5] Rui Jiang , "Advanced Secure User Authentication Framework for Cloud Computing", IJSIS Trans. Cloud computing, Vol. 6, No. 4,Sept 2013