Journal of Computer Sciences and Applications, 2015, Vol. 3, No. 3, 73-78
Available online at http://pubs.sciepub.com/jcsa/3/3/3
© Science and Education Publishing
DOI:10.12691/jcsa-3-3-3

DecenCrypto Cloud: Decentralized Cryptography Technique for Secure Communication over the Clouds

Shyam Nandan Kumar*

M.Tech-Computer Science and Engineering, Lakshmi Narain College of Technology, Indore, India
*Corresponding author: shyamnandan.mec@gmail.com

Received May 12, 2015; Revised May 30, 2015; Accepted June 03, 2015

Abstract With the advent of the World Wide Web and the emergence of e-commerce applications and social networks, organizations across the Cloud, share a large amount of data day by day. Secure Data sharing is an important issue over the cloud environment. In order to enhance the security services, the paper proposes Decentralized Cryptography Technique for Secure Communication over the Clouds. In this paper, Cryptography Model for Secure Data Sharing over Cloud is presented first. Cryptography Management Approach is given to access the secure resource over cloud and then Algorithm Design Methodology is provided in decentralized manner. The paper also provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing.

Keywords: *cloud computing, data sharing, encryption, decryption, cloud security, cryptography, secure communication, data security, www*

Cite This Article: Shyam Nandan Kumar, "DecenCrypto Cloud: Decentralized Cryptography Technique for Secure Communication over the Clouds." *Journal of Computer Sciences and Applications*, vol. 3, no. 3 (2015): 73-78. doi: 10.12691/jcsa-3-3-3

1. Introduction

Cloud computing represents one of the magnificent shifts in information technology. It is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Cloud enhance collaboration, agility, scaling and availability, and provide the potential for cost reduction through optimized and efficient computing. Different from the existing technologies and computing approaches, cloud is defined with five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), ***SPI*** service models (Software as a Service (***SaaS***), Platform as a Service (***PaaS***), Infrastructure as a Service (***IaaS***)), and deployment models (Public, Private, Hybrid, Community). To satisfy the user requirements, Cloud Mining [14] can be done like: Service Mining, Deployment Mining, Architecture Mining and Workflow Mining.

Data Sharing and Accessing are gaining popularity recently. In enterprise settings, it is seen the rise in demand for data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology behind many online services for personal applications. With multiple users from different organizations contributing to data in the Cloud, the time and cost will be much less compared to having to manually exchange data. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking).

In 2009, Forrester Research Inc. [2] evaluated security and privacy practices of some of the leading cloud providers (such as Salesforce.com, Amazon, Google, and Microsoft) in three major aspects: Security and privacy, compliance, and legal and contractual issues. Cloud Security Alliance (***CSA***) [3] is gathering solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. The CSA has identified thirteen domains of concerns on cloud computing security [4].

There are two important challenges in secure outsourcing. First, the stored data must be protected against unauthorized access. Second, both the data and the access to data need to be protected from cloud storage service providers (e.g., cloud system administrators). In these scenarios, relying on password and other access control mechanisms is insufficient [15]. Cryptographic encryption mechanisms are typically employed. However, simply having encryption and decryption implemented in the cloud database systems is insufficient. In order to support both challenges, data should be encrypted first by users before it is outsourced to a remote cloud storage service and both data security and data access privacy should be protected such that cloud storage service providers have no abilities to decrypt the data, and when the user wants to search some parts of the whole data, the cloud storage system will provide the accessibility without knowing what the portion of the encrypted data returned to the user is about [5].

The challenges in privacy protection are sharing data while protecting personal information. The typical systems that require privacy protection are e-commerce systems [14] that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the Internet has become a growing concern. These concerns include whether personal information can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited collect, store, and possibly share personal information about users. The key to privacy protection in the cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements.

In this paper sections are organized as follows: Section II deals with security related issue for cloud. Section III reviews some related works. Section IV describes the proposed scheme. Section V discusses performance analysis of proposed methodology. Section VI concludes the paper and presents avenues for future work. References for this paper are given in section VII.

2. Security Issue for Cloud

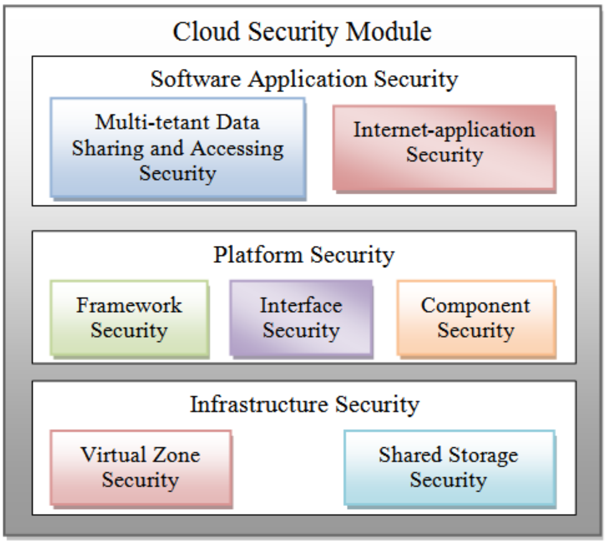

Figure 1. Cloud Security Model

Cloud security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The challenges of security in cloud computing environments can be categorized into network level, user authentication level, data level, and generic issues. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information. Based on Cloud Service Model, security issues can be categories as shown in Figure 1. The content of data security and privacy protection in cloud is similar to that of traditional data security and privacy protection. It is also involved in every stage of the data life cycle. But because of openness and multi-tenant characteristic of the cloud, the content of data security and privacy protection in cloud has its particularities [13].

2.1. Security Attacks

Since people are moving towards cloud computing, care must be taken against various types of attacks.

2.1.1. Active Attacks

An active attack attempts to alter system resources or affect their operation. It involves some modification of the data stream or the creation of a false stream. Types of active attacks:

- ***Modification of Messages***: some portion of a legitimate message is altered, or that messages are delayed or reordered.
- ***Denial of Service***: An entity may suppress all messages directed to a particular destination.
- ***Replay***: It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- ***Masquerade***: It takes place when one entity pretends to be a different entity.

2.1.2. Passive Attacks

This type of attacks includes observation or monitoring of communication. A passive attack attempts to learn or make use of information from the system but does not affect system resources. The goal of the opponent is to obtain information that is being transmitted. Types of passive attacks:

- ***Traffic Analysis***: The message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
- ***Release of Message Contents***: Read contents of message from sender to receiver.

2.2. Requirement of Data Sharing and Accessing over Cloud

The basic parameter for secure data sharing and accessing over the cloud includes Confidentiality, Authentication and Integrity of message or data. They prevent the message from active and passive attacks.

1) ***Confidentiality:*** Confidentiality is the protection of transmitted data from passive attacks. It preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, when a ***TCP*** connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. Confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals over the

clouds. A loss of confidentiality is the unauthorized disclosure of information.

2) ***Authentication**:* Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay). In many cases, there is a requirement that the authentication mechanism assures that purported identity of the sender is valid. It verity the integrity of message. For optimal authentication signing and verifying of message is need. Message authentication may also verify sequencing and timeliness. A digital signature is an authentication technique that also includes measures to counter repudiation by the source.

3) ***Integrity***: It guards against improper information modification or destruction. Data Integrity assures that information and programs are changed only in a specified and authorized manner. System Integrity assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. A loss of integrity is the unauthorized modification or destruction of information.

3. Related Work

In recent years, the research areas on secure data processing have gained more and more attention. There exist several expressive Attribute Based Encryption (ABE) [5] schemes where the decryption algorithm only requires a constant number of pairing computations. Recently, Green et al. proposed a remedy to this problem by introducing the notion of ABE with outsourced decryption, which largely eliminates the decryption overhead for users. Based on the existing ABE schemes, Green et al. also presented concrete ABE schemes with outsourced decryption.

Searchable encryption schemes are designed to solve security problems for remote cryptographic storage while enabling search for the expected contents corresponding to an encrypted keyword securely. Symmetric searchable encryption (SSE) scheme introduced in [6] is suitable for the setting where a party searching over the data is also the one who generates it. Such scenario is referred to as single writer and single reader (SW/SR).

Asymmetric searchable encryption (ASE) is designed for the scenario where a party searching over the data can be different from the party who generates it [7]. Such scenario is referred to as many writers and single reader (MW/SR). Since writers and readers can be different, ASE schemes are more suitable for the setting with a larger number of users. Both SSE and ASE protocols did not completely solve the problem that one can privately retrieve segments of encrypted data from remote databases. Since the database server can learn by passive logging with statistical inference which encrypted keyword matches the submitted search keyword and which encrypted document is retrieved.

Attribute-based encryption (ABE) [8,9] allows each cipher-text to be associated with an attribute, and the master-secret key holder can extract a secret key for a policy of these attributes so that a cipher-text can be decrypted by this key if its associated attribute conforms to the policy. For example, with the secret key for the policy (2 v 3 v 6 v 8), one can decrypt cipher-text tagged with class 2; 3; 6 or 8. However, the major concern in ABE is collusion-resistance but not the compactness of secret keys. Indeed, the size of the key often increases linearly with the number of attributes it encompasses, or the cipher-text-size is not constant.

To delegate the decryption power of some cipher-texts without sending the secret key to the delegates, a useful primitive is proxy re-encryption (PRE) [10]. A PRE scheme allows Alice to delegate to the server (proxy) the ability to convert the cipher-texts encrypted under her public-key into ones for Bob. PRE is well known to have numerous applications including cryptographic file system [11]. Nevertheless, Alice has to trust the proxy that it only converts cipher-texts according to her instruction, which is what we want to avoid at the first place. Even worse, if the proxy colludes with Bob, some form of Alice's secret key can be recovered which can decrypt Alice's (convertible) cipher-texts without Bob's further help. That also means that the transformation key of proxy should be well-protected. Using PRE just moves the secure key storage requirement from the delegates to the proxy. It is thus undesirable to let the proxy reside in the storage server. That will also be inconvenient since every decryption requires separate interaction with the proxy.

An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds [12] is proposed by Seung-Hyun Seo, Nabeel, M, Bertino, E. and Xiaoyu Ding. It deals with a mediated certificateless encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks. It was not a decentralized appoarch.

One of the main efficiency drawbacks of the most existing Encryption schemes is that decryption is expensive for resource-limited devices due to pairing operations, and the number of pairing operations required to decrypt a cipher-text grows with the complexity of the access policy. Also these existing schemes are given in centralized manner and not support multiple read and multiple write. Concurrent data sharing and accessing is other important issue with existing system.

In order to provide a secure communication over cloud, in the paper, inspired by above related work, a novel cryptography mechanism is proposed in decentralized manner.

4. The Proposed Scheme

In this section, Cryptography Model for Data Sharing over the Clouds is presented first. Cryptography Management Approach is given to access the secure resource over the clouds and then Algorithm Design Methodology is provided in decentralized manner.

As shown in Figure 2, the sender *A* uses the public key of receiver B (or some set of rules) associated with access policy and attribute, to encrypt the plaintext message *M*. Encrypted message is also known as cipher text. Now the ciphertext *C* is sent to the receiver using the cloud. The receiver applies own private key (or ruleset) to decrypt the cipher text *C* and recover the plaintext message *M*. A user in the system should be able to decrypt if their attributes (possibly issued by multiple authorities) satisfy the policy specified by the ciphertext. Because pair of keys is required, this approach is also called ***asymmetric cryptography*** *[13]*. Asymmetric encryption can be used for ***confidentiality, authentication***, or both.

For handling the fault tolerance, there should be several *Key Distribution Centre* (***KDC***) located at multiple servers over the cloud. User receives a token from the service provider, who is assumed to be honest. A service provider can be someone like the government agency who manages user's identity. On presenting the identity (government issued photo based id), the service provider gives a token. There are multiple KDCs, which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing as shown in Fig. 2. Cryptography Model is designed to allow multiple and independent clients to connect directly to the untrusted cloud for concurrent access the cloud database.

A user in the system with a global user identity *u* will collect private keys for attributes *i* that it has from different authorities. When receiver B wants to read some data stored in the cloud, it tries to decrypt it using the secret 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. Data security not only involves the encryption of the data, but also ensures that appropriate policies are enforced for data sharing.

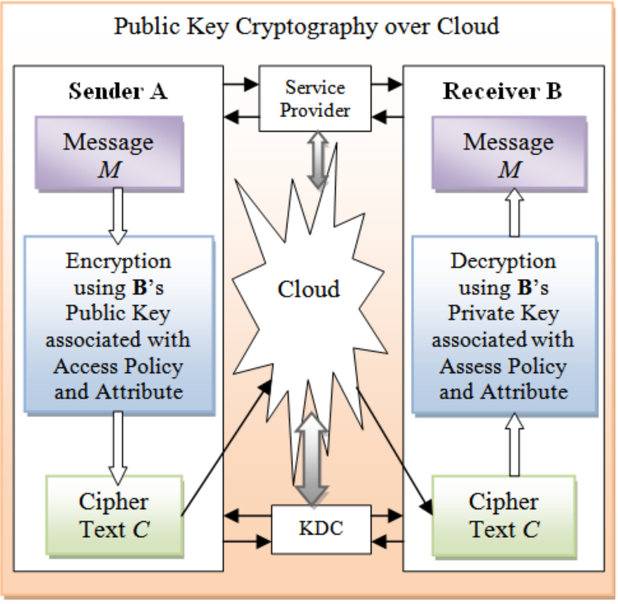
Public Key Cryptography over Cloud
Sender A
Message M
Encryption using B's Public Key associated with Access Policy and Attribute
Cipher Text C
Service Provider
Cloud
KDC
Receiver B
Message M
Decryption using B's Private Key associated with Assess Policy and Attribute
Cipher Text C

Figure 2. Cryptography Model for Secure Data Sharing over Cloud

4.1. Cryptography Management Approach

1) ***Encryption and Key Management:*** Encryption provides data protection while key management enables access to protected data. It is strongly recommended to encrypt data in transit over networks, at rest, and on backup media. In particular, data encryption at rest (e.g., for long-term archival storage) can avoid the risk of malicious cloud service providers or malicious multi-tenants abuse. At the same time, secure key stores (including key backup and recoverability) and access to key stores must be securely implemented since improper (or access to) key storage could lead to the compromise of all encrypted data. Key management is anything you do with a key except encryption and decryption and covers the creation/deletion of keys, activation/deactivation of keys, transportation of keys, storage of keys and so on. Most Cloud service provider's provide basic key encryption schemes for protecting data or may leave it to the user to encrypt their own data. Both encryption and key management are very important to help secure applications and data stored in the Cloud.

2) ***Identity and Access Management:*** Secure management of identity and access control is a critical factor to prevent account and service hijacking. It is strongly recommended to prohibit sharing of account credentials, to leverage strong (multi-factor) authentication if possible, and to consider delegated authentication and managing trust across all types of cloud services. Access control is a security features that control how users and systems communicate and interact with one another. Access means flow of information between subject and object. Subject is an active entity that requests access to an object or the data in an object whereas object is a passive entity that contains information.

4.2. Design Methodology

4.2.1. Assumptions

For a given group generator G_G, the following distribution is defined: G = (n = $n_1n_2n_3$, G, G_T, e), $\leftarrow^R G_G$, $g1\leftarrow^R G_{n1}$, $g2 \leftarrow^R G_{n2}$, $g3\leftarrow^R G_{n3}$, a,b,c,d$\leftarrow^R$ Zn, U = (G, g1,g2,g3,$g1^a$,$g1^b g3^b$,$g1^c$,$g1^{ac}g3^d$), T1 = $e(g1,g1)^{abc}$, T2 $\leftarrow^R$ G_T

Now an algorithm A can be break as:

$$M = C_0 / \mathrm{e}\left(g_1, g_1\right)^s \tag{1}$$

It can be say that GG satisfy the assumption if $I_{GG,A(\lambda)}$ is a negligible function of λ for any polynomial time algorithm A.

4.2.2. Mathematical Background

System is constructed using [5], composite order bilinear groups. Consider bilinear pairings on elliptic curves. If *G* and G_T are the cyclic groups of order $n = n_1n_2n_3$, which are generated from a group generator G_G. G_G takes input as Security Parameter λ and yield the output (*n*, *G*, G_T, e) which is the description of bilinear groups. Mapping is define as $G \text{ X } G \to G_T$, which satisfy the following properties:

a) Bilinear, For all $\beta,\gamma \in Z_n$*, and R, L* ∈ *G*

$$\mathrm{e}\left(R^{\beta}, L^{\gamma}\right) = \mathrm{e}\left(R, L\right)^{\beta\gamma} \tag{2}$$

b) Non-degenerate,

$$g \in G, \mathrm{e}\left(g, g\right) \neq 1 \tag{3}$$

4.2.3. Formats of Access Policies

An access structure (***monotonic access structure***) is a collection A_s of non-empty subset of communication parties say {p1, p2, ….pN}. Now A_s is consider as authorized sets and the sets not in A_s are known as unauthorized sets. Collection A_s is monotone if for all X, Y: if X belong to A_s and A_s is the subset of Y then Y belongs to $A_{s.}$ In Linear Secret-Sharing Schemes (***LSSS***), Consider $D = \{x \mid r(x) \in A_s\}$. then the vector (1, 0,…….0) is in the span of rows of access matrix A indexed by D and there exist constant $\{w_x \in Z_p\}_{x \in D.}$

4.2.4. Construction of Design Code

Proposed Cryptography model as shown in Figure 1, supports these five design code algorithms:

a) *Global Initialization*: It is given as ***Init*(λ) → *Gp***. Consider a bilinear group G of order $n = n_1 n_2 n_{3.}$ Also g_1 is the generator $Gp_{1.}$ For mapping global user identity u to G, it used Secure Hash Function-512. It takes Security Parameter λ as input and yields the output as Global Parameter G_p. Its output value, Global Parameter is used for secure communication during authority permission, encryption process, key generation phase and decryption module.

b) Authority Setup: It is given as ***f(Gp) → PK, SK***. It takes input as Global Parameter and yield public key and secret key as output, for each attribute i belonging to authority/service provider. Consider ${}^{\alpha}{}_{i}$, $y_i \in Z_n$. For all i, it computes:

$$PK = \left\{ \mathrm{e}(g_1, g_1)^{\alpha i}, g_1{}^{yi} \right\}, SK = \left\{ {}^{\alpha}{}_{i}\ , y_i \right\} \tag{4}$$

c) *Encryption process*: The Encryption function is given as ***Encrypt(M, (A, r), G_p, {PK}) → C***. It takes input as Message M, Access Policy(an n X l access matrix A with r mapping its rows to attributes), Global Parameter G_p and the Public key PK using Equation (4). After the encryption process, which occurs at sender side, we get cipher text C. It chooses a random $s \in Z_n$ and a random vector $v \in Z_n{}^l$ with s as its first entity. Consider $\lambda_x = A_x.v$, where A_x is row x of matrix A. Also consider random vector $w \in Z_n{}^l$ with 0 as its first entity. If $w_x = A_x.w$, $R_x \in Z_n$, and $t = {}^{\alpha Rx}{}_{r(x)}$ Compute the cipher text for all x as follows:

$$\begin{aligned} C &= e(g_1, g_1)^s \\ C_{1,x} &= \left(\mathrm{e}(g_1, g_1)^{\lambda x}\, \mathrm{e}(g_1, g_1)^t \right) \\ C_{2,x} &= g_1{}^{Rx} \\ C_{3,x} &= g_1{}^{wx} g_1{}^{Rx} y_{r(x)} \end{aligned} \tag{5}$$

d) *Key Generation and Distribution:* The Key Generation function is given as ***KeyGen(u, i, SK, G_p) → K_{i,u}***. It takes input as Global user identity, Attribute value, Secret Key SK using Equation (4) and Global Parameter. This function yields the output as Private Key $K_{i,u.}$ It is used for the decrypting the cipher text. Key will be generated for the Global User u with attribute i, which is associated with the service provider, as follow:

$$K_{i,u} = g_1{}^{\alpha i} \mathrm{H}(u)^{yi} \tag{6}$$

e) *Decryption:* The Decryption Function is given as ***Decrypt*(*C*,{*K_{i,u}*}, *G_p*) → *M*.** It takes input as Cipher text C, Generated Private Key $K_{i,u}$ for Receiver B using Equation (6) and Global Parameter. After Decryption we get message M in plain text. Since the ciphertext is encrypted under an access matrix (A, r). During decryption phase first H(u) is computed. If the decryptor has the secret keys $\{K_{r(x),\, u}\}$for a subset of rows A_x of A such that (1,0,……. 0) is in the span of these rows, then the decryptor proceeds as follows. For each such x, using Equation (5) the decryptor computes:

$$\begin{aligned} &\left(\mathrm{e}(g_1, g_1)^{\lambda \mathrm{x}}\, \mathrm{e}(\mathrm{H}(u), g_1)^{wx} \right) \\ &= C_{1,x}.\mathrm{e}(\mathrm{H}(u), C_{3,x}) / \mathrm{e}(\mathrm{K}_{r(x),u}, C_{2,x}) \end{aligned} \tag{7}$$

The decryptor then chooses constants $C_x \in Z_n$ such that $\sum_x c_x A_x$ = (1, 0,……, 0). Now using Equation (7) compute:

$$\mathrm{e}(g_1, g_1)^{\mathrm{s}} = \Pi x \left(\mathrm{e}(g_1, g_1)^{\lambda \mathrm{x}}\, \mathrm{e}(\mathrm{H}(u), g_1)^{wx} \right)^{cx} \tag{8}$$

After that message M can be obtained using Equation (8) as:

$$M = C_0 / \mathrm{e}(g_1, g_1)^{\mathrm{s}} \tag{9}$$

5. Performance Analysis

5.1. Computational Complexity

The Sender needs to encrypt the message. During encryption one pairing e(g, g) is calculated. Encryption takes 2 exponentiations to calculate each of $C_{1,x}$. So this requires $2mE_n$ time, where m is the number of attributes. User needs to calculate 3 exponentiation to calculate $C_{2,x}$ and $C_{3,x}$. So time taken for encryption is $(3m + 1)E_0 + 2mE_n + \tau P$, where τP is the time taken to perform one pairing operation in e and E_i is the exponentiation in group G_i

5.2. Comparison with Existing Scheme

The existing schemes given in [5-11], either work in centralize manner or support single read and single write which degrades the service over cloud and restrict concurrent access. While the proposed methodology, in this paper, supports multiple read and multiple write. Also it is a decentralized approach, meaning that there can be several KDCs for key management, which allows concurrent access on the resource and data sharing. Since in the proposed approach KDCs are distributed across the cloud, so it helps in fault tolerance in case a KDC failure. Proposed methodology is collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized.

Equation (8) holds due to $\lambda_x = A_x.v$ and $w_x = A_x.w$, where A_x is row x of matrix A. Also *v.(1,0,…….,0) = x and w.(1,0,……., 0) = 0*. For an invalid user, there does not exists attributes corresponding to rows x, such that $\sum_x c_x A_x$ = (1, 0,……, 0). Therefore $\mathrm{e}(g_1, g_1)^{\mathrm{s}}$ cannot be calculated. Hence unauthorized person unable to decrypt the message M, which is calculated using $\mathrm{e}(g_1, g_1)^{\mathrm{s}}$ as shown in Equation (9).

In this proposed technique, two or more users cannot collude and gain access to data that they are not individually supposed to access because to decrypt the message M, e(g_1, g_1)^s is essential. Also for e(g_1, g_1)^s, e(H(u), g_1)^{wx})^{cx} should be calculated as shown in Equation (8). For the different users, the value of e(H(u), g_1)^{wx})^{cx} will be different. Hence proposed methodology is collusion resistant and able to revoke the unauthorized user.

Also KDC generates different key for different users. Private Key $K_{i,u.}$ is used for the decrypting the cipher text. Key will be generated for the Global User *u* with attribute *i*, which is associated with the service provider, as shown in Equation (6). Hence, message confidentiality is achieved by proper cryptography encryption.

6. Conclusion and Future Work

Due to the fast growth of science and technology, world are moving towards Cloud Computing. Requirement of data sharing is increasing day by day over the cloud. Secure data sharing is one of the most important concerns over the cloud. To provide optimal service, the paper proposed Decentralized Cryptography Technique for Secure Communication over the Clouds. Due to the multiple KDCs, which are distributed across the cloud servers, the presented methodology supports concurrent access and sharing the data over the clouds. Multiple read and multiple write feature is supported in this proposed technique. Confidentiality of message is achieved. Collusion resistant property is also supported. Cloud related security issues are also discussed.

To achieve optimal message authentication, message signing and verification is needed. In future work can be done on Advance Algorithm for key distribution and management, security and privacy protection of *Big Data* with confidentiality, authentication and integrity over the Cloud.

References

[1] G. Peter Mell, and Tim Grance, “The NIST Definition of Cloud Computing,” Version 15, 10-7-09, http://www.wheresmyserver.co.nz/storage/media/faq-iles/cloud-def-v15.pdf.

[2] “Cloud Security Front and Center. Forrester Research”. 2009-11-18. http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html.

[3] “Cloud Security Alliance”. http://www.cloudsecurityalliance.org.

[4] “Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing”, V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.

[5] Shyam Nandan Kumar, “Cryptography during Data Sharing and Accessing Over Cloud.” International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1 (2015): 12-18.

[6] D. X. Song, D. Wagner, A. Perrig. “Practical techniques for searches on encrypted data”. Proceedings of the IEEE Symposium on Security and Privacy, 2000, pp. 44-55.

[7] D. Boneh, G. D. Crescenzo, R. Ostrovsky, G. Persiano. “Public key encryption with keyword search. Advances in Cryptology”-EUROCRYPT'04, 2004, LNCS 3027, Springer, pp. 506-522.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,” in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS ’06). ACM, 2006, pp. 89-98.

[9] M. Chase and S. S. M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” in ACM Conference on Computer and Communications Security, 2009, pp. 121-130.

[10] M. S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, “Efficient Unidirectional Proxy Re-Encryption,” in Progress in Cryptology - AFRICACRYPT 2010, ser. LNCS, vol. 6055. Springer, 2010, pp. 316-332.

[11] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1-30, 2006.

[12] Seung-Hyun Seo, Nabeel, M, Bertino, E. and Xiaoyu Ding, “An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds” IEEE Transactions on Knowledge and Data Engineering, Volume:26 , Issue: 9, pp. 2107-2119, 05 August 2013.

[13] Shyam Nandan Kumar, “Review on Network Security and Cryptography.” International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1 (2015): 1-11.

[14] Shyam Nandan Kumar, “World towards Advance Web Mining: A Review.” American Journal of Systems and Software, vol. 3, no. 2 (2015): 44-61.

[15] Shyam Nandan Kumar, “Technique for Security of Multimedia using Neural Network,” Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp. 1-7. Sep-2014.