ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(S7), 220–227, April 2015* DOI: 10.17485/ijst/2015/v8iS7/71223

Secure Authentication and Access System for Cloud Computing Auditing Services Using Associated Digital Certificate

R. Manjusha[1*] and R. Ramachandran[2]

[1]Department of Information Technology, Sathyabama University, Chennai, India; manjushaphd14@gmail.com
[2]Department of ECE, Director (Research), Sri Venkateshwara College of Engineering

Abstract

Cloud computing helps in transforming the traditional internet computing paradigm and IT industry. Since many Cloud Service Providers (CSPs) are untrusted, the confidentiality, integrity, and privacy of the enterprise information must be protected by some mechanisms. In this paper, we proposed a new framework to enhance secure data storage, fine grained access and preserve data from unknown users or intruders in enterprise cloud. In the proposed mechanism data is encrypted under the set of user attributes and privilege access rights. The Associated Digital Certificate (ADC) is generated for secure, authenticated and fine grained access from cloud. The proposed framework extended the research towards user revocation and integrity check by data owner. Thus, the analysis of our newly approached scheme is provably secure and efficient in enterprise cloud than other existing scheme.

Keywords: Access Control, Associated Digital Certificate (ADC), Cloud Computing, Security

1. Introduction

Cloud Computing has been intended as the next generation structure of Information Technology (IT) enterprise, due to its huge list of exceptional advantages in the IT history such as ubiquitous network access, on demand self-service, rapid resource elasticity, utilization based pricing, location independent resource pooling and transference of threat. Cloud Computing is transforming the nature of how businesses utilizing IT[1,2]. The essential feature of this model shifting is that data is being outsourced or centralized into the Cloud. From users' viewpoint, including both IT enterprises and individuals, storing data remotely into the cloud in anon-demand manner brings attractive benefits such as autonomous geographical locations, relief of the problem for storage management, universal data access and avoidance of capital expenditure on software, hardware and individual maintenances, etc. While Cloud Computing sorts these advantages more interesting than ever, it also brings challenging and new security extortions towards users' outsourced data.

Subsequently, to completely ensure to the save the cloud users' computation resources and data security, it is significance to facilitate public auditability for cloud information storage so that the user may depend on a verifier, who has ability and capacities that the user do not, to audit the outsourced information when is required. In light of the audit result, verifier could public an audit report, which would not just help users to assess the risk of their subscribed cloud information services, additionally be advantageous for the cloud service provider to enhance their cloud based service platform. A digital certificate is the mix of a statements and a digital signature.

The Cloud Service Providers (CSP) have the data outsourcing, distinct administrative entities is actually relinquishing user's dynamic control over their data. As a

*Author for correspondence

result, the perfection of the data about information in the cloud is being place at risk due to the following causes. The infrastructures under the cloud are more reliable and powerful than personal computing devices, but they have to face the wide range of both external and internal risk for data integrity. There exist a few inspirations for cloud service providers to act unfaithfully towards the cloud user with respect to the status of their outsourced data. Include cloud service providers, for financial reasons; recovering storage data etc. Accessing to the cloud services from a service provider, security and privacy will play a vital roll. Security model must have three types of guarantees such as confidentiality, availability and integrity. The number of users improves the probability of cyber crime. Based on the above issues the proposed system is designed so that the security, user revocation and fine grain access to a user is achieved. The system is constructed with the owner of the data, Trusted Third Party, Internal trusted party and Cloud Service Providers (CSP). The rest of the paper as follow: Section 2 summarizes the related work for cloud computing security. In section 3, summarizes the problem statement about cloud computing in section 4, framework is proposed which is designed to solve the security problem of cloud computing. Section 5 provides the module description of proposed framework. Section 6 shows the performance analysis of proposed work and conclusion and future scope are presented in section 7.

2. Related Work

Cloud computing includes components from grid computing, autonomic computing and utility computing, into an innovative deployment structured model. This quick move towards the clouds has fuelled concerns on a discriminating issue for the accomplishment of information systems, communication and data security[3]. From a security point of view, various unchartered dangers and difficulties have been acquainted from this migration with the clouds, crumbling a great part of the viability of traditional protection mechanisms. Firstly to assess cloud security by recognizing one of a kind security prerequisites and furthermore to endeavour to present a feasible result that wipes out these potential threats a Trusted Third Party (TTP), tasked with guaranteeing particular security qualities inside a cloud environment. The result calls upon cryptography, particularly. Open Key Infrastructure working together with Single Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP), to guarantee the integrity authentication, and confidentiality of involved communications and data.

Cloud computing is the newest technologies in IT field which causes a few stresses for producers and its consumers because of its novelty. The security and privacy aspects and trust are the primary concerns[4]. It makes an imperative obstacle for utilizing by the users. To assess a few elements, for example, security for the acceptance of cloud computing. Highlighted imagine about security underlining for the maintenance of security and trust in tolerating the cloud computing.

As per the user' request cloud computing gives resources, applications as a service by means of the Internet. It can make utilization of computing resources with high speed and at minimal costs[5,6]. It can furnish user with a scope of service, infrastructure and storage of a lot of information, including important information. Regardless of the abilities of the cloud computing, there is an inquiry check on its security. Along these lines, security has turned into a standout amongst the most critical issues in the cloud computing. The idea of the cloud computing, its qualities, models and additionally the different security dangers that threaten the cloud computing

The security of the data can be preserved by encrypting the data[7]. In Fuzzy identity based encryption, user whose attributes match defined on a set overlap distance metric can decrypt a message encrypted with the same identity. KP-ABE, where each attribute private key is associated with an access structure that specifies which type of cipher text the key is able to decrypt and this supported only the monotonic structure[8]. CP-ABE was introduced by Bethencourt et al, a user's private key is associated with a set of attributes and an encrypted cipher text will specify an access policy over attributes[9]. A model where the access structure of the cipher text in CP-ABE is hidden from the decryptor[10].

The access rights have to be provided in order to prevent intrusion several researches were done. The Privilege Management Infrastructure (PMI) must be taken into consideration[11]. Digital signature can be used to verify the identity of the user. They are several types of certificates which provide the access rights. Public key certificates are used to prove the identity and they were first implemented International Telecommunication Union and International Organization for Standardization published the X.509 standard which has been adopted by IETF (International Engineering Task Force). Later, [12] proved public key certificates tend to collide.

An attribute certificate or authorisation certificate links attributes to the user. Attribute certificate can offer role based privilege management but the identity of the user is not verified. It suggested that the attributes can be bind with the identity in order to verify the identification of the holder of the certificate[13]. Based on the recent works, the proposed model is constructed as two step model. The delegation of keys and certificates are done by trusted third party. The authorisation is achieved by Distributed Attribute-Based Encryption (DABE) and access control is provided by ADC[14,15].

Even though, the cloud storage has attained the advantages like personnel maintenance, cost expensive on personnel maintenance, provides scalability, less storage cost, the maintenance of the stored data in a secure manner is difficult activity. Hence, Rajathi and Saravanan[16] had an insight discussion about the methods for cloud storage, algorithms, and their challenges during real time implementation, advantages and disadvantages. And Rajakumari and Nalini[17] suggested a new innovative approach implemented to decrease the data storage cost within the cloud. This approach actually collects the data and converts it into a horizontal layout form which decreases the size of the data to be stored in the cloud.

In cloud computing services, Distributed Denial of Service (DDoS) is an attack which damages the cloud service's availability. Thus Sharif, Amirgholipour, Alirezanejad, Aski and Ghiami[18] designed a model for this attack and a simulation is conducted for this cloud system which results that the cloud system may damage due to this attack. To resolve this, various solutions were proposed and suggested honey pots and load balancing to prevent from this attack. Virtualization is a vital technique for the maintaining the resource pool from which needed resources is run on the various heterogeneous applications by different virtual machines. Pal and Pattnaik[19] presents different categorization of virtualization, their working principle and features. Anjaneyulu and Sanyasirao[20] introduce a method to generate a grouped key distribution among four different persons which is possible using polynomials over non-commutative division semirings. This methodology can be broaden to 'n' persons with the same procedures.

3. Problem Description

Cloud computing service providers offer their services based on two essential models such as Service model and Deployment Model. In service model contain three types of services such as Infrastructure as a Service (IAAS), Platform As A Service (PAAS), Software As A Service (SAAS). In Deployment model have been identified different types of architecture such as public, private, hybrid and community models. Figure 1 shown as typical architecture of cloud computing system. Cloud computing essential characteristics are broad network access, rapid elasticity, measured service and on demand self service. These essential services play vital role in cloud computing environment but still it has a major security issues such as trust, confidentiality and privacy, integrity, availability. The cloud computing issues that had been identified in a central server is employed for not only processing and receiving user requests in the front, but it is also responsible for the enterprise information must be handled in secure way very important feature.

In this proposed approach considers the major problem of cloud computing is cloud data storage service and security about the data. This service included four types of different entities such as Data Owner (DO), end user, Cloud Service Provider (CSP) to provide data storage service and computation resources, Trusted Third Party (TTP) who has capabilities and expertise that cloud users doest not have and it is trusted to consider the cloud storage service reliability of the user upon request and Internal Trusted Party (ITP) for certifying the storage integrity of the outsourced data, though planning to retain their data private from Third Party Auditor (TPA), as this approach used to increase the data security to include user private key and Associated Digital Certificate (ADC). ADC provides security authorizations of both data encryption and identification of user data in cloud computing environment.

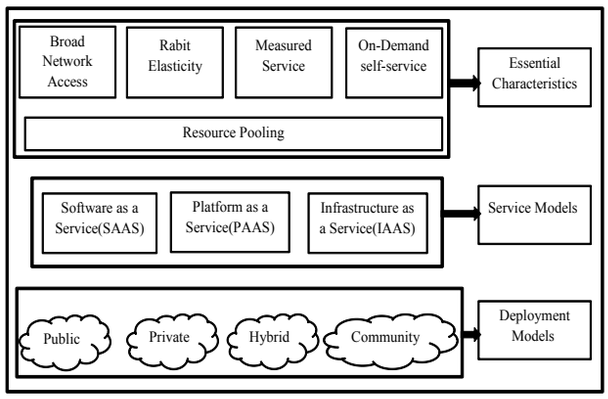

Figure 1. Cloud computing architecture.

4. System Description

4.1 System Models

Figure 2 demonstrate the proposed framework for cloud security utilizing Associated Digital certificates. In this framework assume that the system is composed of the following component, the Data Owner, end user, Cloud Service Provider (CSP), Trusted Third party (TTP), Internal Trusted Party (ITP), Associated Digital Certificate (ADC). To access data files shared by the data owner or users for quickness, download data files from Cloud Servers. The CSP operates a wide number of servers to provide services, the trusted third party generates private key to the users. Internal trusted party provides the digital certificates and sends the certificate list along with the privileges to the CSP. The data owner is the owner of the data files.

4.2 Security Models

In this proposed work, cloud Servers will follow system is general, but try to find as much secure data as possible based on their Dynamic Attribute Based Encryption (DABE) and Associated Digital Certificate (ADC). Specially, expect cloud servers are interested in file information and user access privilege about information than other secret data. Communication between the data owner or user and cloud server are secured under proposed system. Users try to access files either outside or within the space of their access privileges. To accomplish this goal, authorized or registered user may work on own data independently and to storing information in cloud means it have TTP Keygen, delete, encrypt, and decrypt, delegation of certificates options.

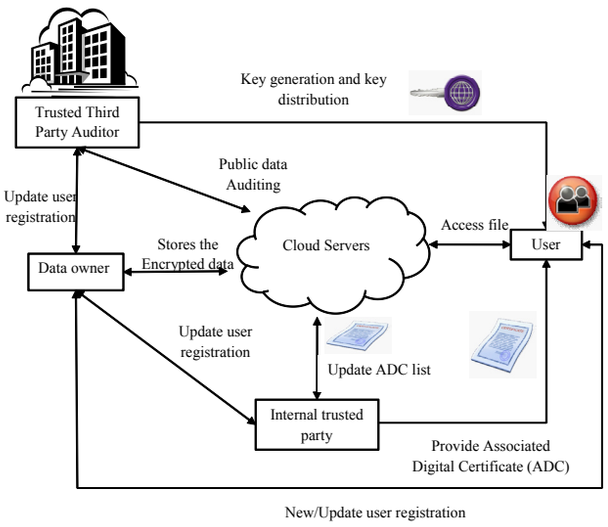

Figure 2. Proposed framework for cloud security utilizing associated digital certificates.

4.3 Design Goals

Main design goal is to achieve fine grained access control on files stored by cloud computing system. Specially, need to enable the data owner to enforce a distinctive access structure on every user, which exactly design at the data files that the user is allowed to access. In additional, the proposed system should be able to achieve security goals such as user auditing and support basic processes such as modification, insertion, deletion, verification and the user contribution as a common one to many communication frame work is require. These enterprise objective should be achieved efficiently and that the system is scalable.

5. Module Description

5.1 Third Party Auditor (TPA)

TPA performs reviews for multiple users efficiently and simultaneously. To securely introduce a Third Party Auditor (TPA) achieve two important prerequisite, first one is TPA should be able to efficiently audit the cloud information storage without applying the neighbourhood duplicate of information, and present no extra online load to the cloud user. Second one is the third party auditing system should be obtain the user data privacy. In this proposed framework, particularly utilizing the general private key based authentication to achieve the privacy and public cloud data auditing system, which meets all the above prerequisite method. It will help to achieve efficient handling of the multiple auditing tasks, the method of combined signature to extend the main result into setting the multiple users. The TPA can simultaneously achieve various auditing tasks. Extended security indicates the proposed scheme is secure and highly efficient.

5.2 Data Dynamics Module

Supporting data dynamics for private and public risk of auditing is additionally it will be perform the key generation and key distribution is paramount importance. Presently indicate how the fundamental method could be expand upon the present work to help data dynamics, including fundamental operations of TTPKeygen, delete, encrypt, and decrypt, delegation of certificates.

Data dynamics implies after user store their information at the remote server; they can dynamically elevating their information at later times.

5.3 Internal Trusted Party (ITP)

When the user needs to access a file it sends a request to the Cloud Service Provider (CSP). ITP is responsible for generating Associated Digital Certificate (ADC) and certificate list distributed to the cloud server and the enterprise users along with the creator's signatures are transmitted over authenticated and trusted enterptise users. In the proposed model, the security and access rights are highly improved by using the DABE and ADC. In case of the enterprise scenario, the file must be accessed only by the desired privileged users and it must be secured from internal as well as external attacks.

A security parameter, k will denotes the size of the groups and also define the coefficient $\Delta_{i,S}$ *for* $i \in \mathbb{Z}_p$ and set S, element in $\mathbb{Z}_p : \Delta_i S(x) = \prod_{j \in S, j \neq i} \frac{x-i}{i-j}$. Additionally apply the Hash function $H : \{0,1\}^* \rightarrow \mathbb{G}_0$

Setup: The algorithm setup will choose a group $\mathbb{G}_0$ of prime order p with generator g and select two random exponents $a, \beta \in \mathbb{Z}_p$. The TTP gives the public key to all the registered users. The published as a Public Key (PK) is

$$PK = \mathbb{G}_0, g, h = g^B, f = g^{1/\beta}, e(g,g)^a \quad (1)$$

Where (MK) β, g^a is the master key and f is utilized only for delegation.

Encrypt: encryption algorithm have three parameters which is Public key (PK), encrypted message M and an access structure $\mathbb{A}$ over the attributes and produce a cipher text CT, the access structure able to decrypt the message. Assume the cipher text implicitly contains $\mathbb{A}$.

$$CT = \mathbb{A}, C = Me(g,g)^{as}, C = h^s \quad (2)$$

TTPKeygen: The key generation will take a set of attributes as S, input as Master Key (MK), output as private key is Secret Key (SK).

$$SK = \left(D = g^{(a+r)/\beta}, \forall \in S : D_j = g^r H(j)^{rj}, D_j = g^{rj}\right) \quad (3)$$

Delegate: The delegation takes in a Secret Key (SK) which used for S of attributes and S' is as another set of attributes such as $S' \in S$. The secret key is of the form $SK = (D, \forall_j \in S : D_j, D_j^1)$ and select the random values such as $r^{\sim}$ and $r_{\sim k} \forall k \in S'$. It will be used for create new Secret Key (SK)

$$SK = D^{\sim} = Df^r, \forall k \in S^{\sim} : D_k = D_k g^r H(K)^{rk}, D_k^{\sim} = D^{\sim} k g^{rk} \quad (4)$$

The new Secret Key (SK) is a secret key of set of S attributes. Delegated key is equal to one user received directly from the Internal Trusted Party.

Decrypt: specifies decryption technique as a recursive algorithm. For every description present the simplest form such as the input as a Secret Key (SK) and set of attributes is S. The set is define as $\tilde{S} \subseteq S$ and a decryption output may be secret key is $\tilde{S}K$ and the set of attributes $\tilde{S}$.

$$CT^{\sim} = (T, C^{\sim}, C, \forall y \in Y : C^y, C'_y) \quad (5)$$

Delete

The deletion of keys is added in order to support the dynamic nature of the attribute and to prevent the internal attack of the user. When the attributes of the user changes (if the user moves to different department) the new secret key has to be provided. Hence the user requests for new key to the DO and DO invoke TTP. The existing old key of user is deleted with the help of the master key by the TTP and TTPKeygen is automatically invoked. The secret key of the user can also be deleted if the data owner orders the TTP. The steps for deleting and providing a new key are as follows:

Step 1: User requests a new secret key

Step 2: The existing old secret key of the user is deleted by the TTP.

Step 3: The new secret key is created based on the new attributes given by the user during registration to the data owner. The TTP verifies the attributes before delegating the new key.

5.4 Certificate Delegation

The ADC is designed on the basis of the identity and attribute certificate. The ITP provides the ADC to the users, based on the Data Owner (DO) list. The ADC is formed by combining the identity and attribute certificate information. The identity certificate consists the information of the public key along with the user detail. The attribute information in the file consists of role and group. Roles are defined in an organisation (Eg. manager, project lead, Team member). Each role is given a set of privileges

in order to perform a task. Each user can be assigned to one or more roles. The group refers to the department of the user (IT, Sales, Marketing). Each certificate also has expiry date of months or days.

When user request a file, the CSP checks the public key of the user in the ADC and checks for the TTP information in the ADC, if found correct, moves on to the role attribute in the ADC and checks if the role is allowed to perform this action. By removing the role from the original role holder ADC, his privileges are automatically removed. The role attribute given in the attribute list shows the privilege based on that, the access to a data file is given. The group shows the department of the particular certificate holder.

The ITP provides digital signature after verification of the user's details. As the identity information is verified by the DO and the public key is provided by the TTP the server can trust the correctness of the ADC. The certificate is to be frequently verified by the CSP by referring to the ITP certificate list stored in the CSP. The ADC consists of Serial number in order to uniquely identify the certificate, the user name and public key of the user, the algorithm used to create the Digital signature, ID of the ITP, The date the certificate from which the certificate is valid. The expiration date of the ADC, Key-Usage in the cloud, sequence of attributes being bound to the user (Roles attribute, Group attribute).

The user in order to use a secured file, as to have the secret key, public key and the digital certificate. The user provides the ADC to the CSP. The CSP checks for the validity, data of the ADC and provides access. If the file is downloaded to the user local disk, the user uses its secret key in order to decrypt the Cipher Text (CT). If the access policy of e is satisfied by the secret key the file is decrypted.

5.5 Revocation of the Certificates

Refreshing certificates after a certain period of time can prevent attacks. In few cases the ITP may detect a malicious activity by a user and it can immediately revoke the certificate. The Certificate Revocation List (CRL) is provided periodically by the ITP to the CSP.

There are two different states of revocation mentioned in the CRL such as the revoked certificate and hold certificate. Revoked certificate is irreversibly revoked certificate. When the ITP detects any malicious activity or if the user certificate is lost the certificate is permanently revoked. Hold certificate is temporarily invalid due to the security measures and can be valid after a short span of time. In case of any mistake in the certificate revocation the ITP provides the user a new certificate. The ITP also acts as certificate verifier it verifies the validity and confidentiality of the certificate. If a CSP orders to verify a certificate the ITP verifies the certificate and provides an update.

6. Performance Analysis

The model is designed with a CSP, a data owner, TTP, ITP and five users. The user requests are processed on a daily basis by the data owner. The model is designed on an enterprise managed by the data owner. The experiments were directed on a 4GB main memory, 64-bit machine, a 2.4GHz Intel 4 core CPU (only one core is active), and 8MB L2 cache memory.

The proposed system utilizing Associated Digital Certificate (ADC) is compared with two different existing algorithms which are Date-constraint Hierarchical Key (DCHK), Public Auditability and Data Dynamics system (PADD). Computational complexity of different key derivation algorithm is shown in Figure 3.

From Figure 3 it is observed that the key values, the proposed key derivation time is minimum then existing approach which is better than of other two existing schemes. Moreover, if the number of files to be retrieved by a user increases, then the computation time progressively increases. However, proposed system remains less than with the other two existing methods.

The attribute certificate consists of the details of the attribute. The ADC is a combination of attribute and identity information. In case of the attribute certificate,

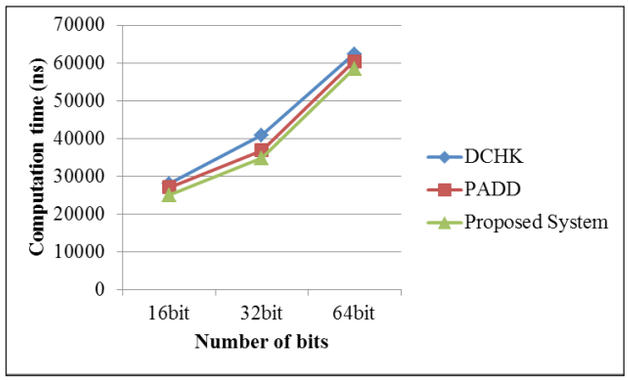

Figure 3. Computation complexities of key derivation algorithms.

the identity of the user has to be verified at the time of access. In case of the adc both attribute and identity are verified when the certificate is delegate, hence a secure access is provided. The ADC provides a access to a file quicker than the AC. The Figure 4 illustrates the comparison of access time between the ADC and AC.

The Figure 5 illustrates the comparison of Encoding time and different file size. Figure 5 it is observed that the proposed method utilizing a minimum encoding time to compared with other existing methods.

7. Conclusion

The proposed approach security performance is based on authentication and authorisation which is used for Distributed Attribute-Based Encryption (DABE) and Associated Digital certificates (ADC) were formed by combining the certificates which verified the identity of the user. The effective revocation was achieved by revocation of the certificate and by dynamic revocation of keys. It provides confidentiality, robustness of data and data forwarding utilizing of encoding method. It is very flexible for the number of cloud storage servers. The research can be further improved by the attention to other parameters such as performance, cost and other factors .The read and write access rights for the user is considered in our upcoming research. The research can also extend in studying linking of certificates using chained signatures.

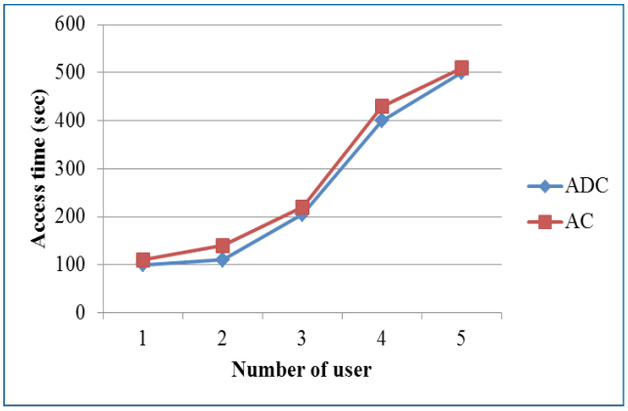

Figure 4. Access time vs number of users.

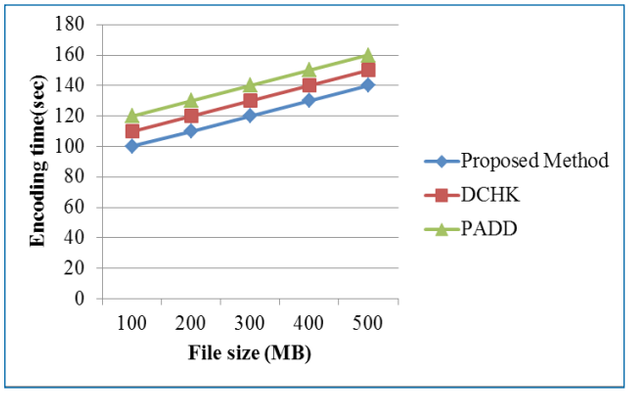

Figure 5. Encoding time vs File size.

8. References

1. Tidigol N, Lokesh TP, Kumar YPT. Effective cloud service management through volunteer computing. IJCSIT. 2013; 4(1):175–7.
2. Chaitanya NS, Ramachandram S, Sruthi P. Secure communications using GDC in cloud computing. International Research Journal of Computer Science Engineering and Applications. 2012; 1(3).
3. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generat Comput Syst. 2012; 28(3):583–92.
4. Gharehchopogh FS, Hashemi S. Security Challenges in cloud computing with more emphasis on trust and privacy. International Journal of Scientific & Technology Research. 2012; 1(6):2277–8616.
5. Al-Attab BS, Fadewar HS. Security issues and challenges in cloud computing. IJESE. 2014; 2(7):2319–6378.
6. Chaturvedi K, Mishra J, Bisen D. A recent review on cloud computing and trust. International Conference on Cloud, Big Data and Trust; 2013. p. 13–5.
7. Tian M, Huang L, Yang W. Security analysis of a fuzzy identity-based encryption scheme. J Circ Syst Comput. 2014; 23(3):1793–6454.
8. Liu X, Ma J, Xiong J, Liu G. Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data. International Journal of Network Security. 2014; 16(4):351–7.
9. Wang Y. Lattice ciphertext policy attribute-based encryption in the standard model. International Journal of Network Security. 2014; 16(4):358–65.
10. Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures. International Conference on Applied Cryptography and Network Security. 2008; 5037:111–29.
11. Stevens M, Lenstra A, de Weger B. Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities. International Conference on Advances in Cryptology. 2007; 4515:1–22.
12. Kim J-M, Moon J-K. Secure authentication system for hybrid cloud service in mobile communication environments. International Journal of Distributed Sensor Networks. 2014; Article ID 828092, 7 pages.

13. Saroha V, Malik A, Pahal M. The enormous certificate: digital signature certificate. Int J Adv Res Comput Sci Software Eng. 2013; 3:6.
14. Aarthika S. Securely managing the personal health records using attribute based encryption in cloud computing. International Journal of Innovative Research in Computer and Communication Engineering. 2014; 2(Special Issue 1).
15. Sasikala S, Bhuvaneswari R. Establising virtualized cloud computing using hypegear disk I/O Model. International Journal of Inventions in Computer Science and Engineering. 2014 May; 1(4):2348–3539.
16. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013 Apr; 6(4):4396–01.
17. Rajakumari SB, Nalini C. An efficient cost model for data storage with horizontal layout in the cloud. Indian Journal of Science and Technology. 2014 Mar; l 7(3S):45–6.
18. Sharif AM, Amirgholipour SK, Alirezanejad M, Aski BS, Ghiami M. Availability challenge of cloud system under DDOS attack. Indian Journal of Science and Technology. 2012 Jun; 5(6):2933–337.
19. Pal AS, Pattnaik BPK. Classification of virtualization environment for cloud computing. Indian Journal of Science and Technology. 2013 Jan; 6(1):3965–71.
20. Anjaneyulu GSGN, Sanyasirao A. Distributed group key management protocol over non-commutative division semirings. Indian Journal of Science and Technology. 2014 Jun; 7(6):871–6.