International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Trustworthiness of Cloud Service Provider and Efficient Third Party Auditor in Cloud Computing using Access Control

K.Indhu, M.Gayathri, G.Annapoorani

Abstract: ***One of the advanced rising technology is Cloud computing. The storage of information could be a massive complication for bushed this world. the simplest associated quickest storage and retrieval of information is an economical answer for Cloud computing. The main issue in cloud computing is security. Present study developed model which helps the new user in comparing the different services provided by different Cloud Service Providers. It works on quality of service (QoS), which plays the vital role in the selection of best CSP. Before this study, many tools were developed, but they did not focus on Quality of Service (QoS). This model assists cloud customer in assessing cloud providers trustworthiness based on predefined trust attributes such as business factors, Quality of Services attributes and the 11 security control domains defined by the CSA. In this study, a mechanism is designed through which integrity of Third Party Auditor is checked with the help of access control. Security is the main concern for the development of the proposed system.***

Keywords: ***Quality of Service, infrastructure as a service, Platform as a service, Software as a service, Mandatory Access Control, Discretionary Access Control.***

I. INTRODUCTION

Cloud computing is a technology through which the required resources can be accessed on demand. It leads to technological shift in all aspects such as storage, computation, networks etc., it provides, elastic, on demand, pay-as-you-use services through internet. With the increase in the number of cloud service providers and users, there also arise many security concerns in the cloud. An access control model suitable for cloud environment is developed based on object relations. The method uses the object relations represented as authorization graph, along with the role assigned to the user for making an access control decision. Cloud can simply be defined as delivering services to the users on demand. J. Kaur and J. Singh et al, (2013) [6]

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
K.Indhu*, Student, Department of Information Technology,Sri Krishna Arts & Science College Coimbatore. -id: indhuk18mit008@skasc.ac.in;
M.Gayathri, Student, Department of Information Technology,Sri Krishna Arts & Science College Coimbatore. Mail-id:gayathrim18mit007@skasc.ac.in;
G.Annapoorani, Student, Department of Information Technology,Sri Krishna Arts & Science College Coimbatore. Mail-id:annapooranig18mit002@skasc.ac.in;

The major services provided by the cloud are Software as a service (Saas), Platform as a service (Paas), and infrastructure as a service (Iaas).IaaS provides various kinds of entities such as storage, networking, hardware etc as a service to the end users. With the advent of these cloud technologies the storage of user data moves from their personal desktop to the cloud systems.

The user is not aware about the location where his/her data would reside. In addition to this various other aspects of cloud computing demands new kind of access control mechanism. The requirements for access control of cloud vary much from a regular access control mechanism. Basic access control mechanism is the one which decides whether access permission can be granted to a user for accessing a resource. The general terminologies for referring to the user and the resource are subject and the object. The object can be any entity such as files, networks, devices like printers etc. The following Figure 1 represents the access control scenario, the subject requests permission for accessing an object. The subject is allowed to access the requested object only after the request is authorized by the Access control Mechanism.

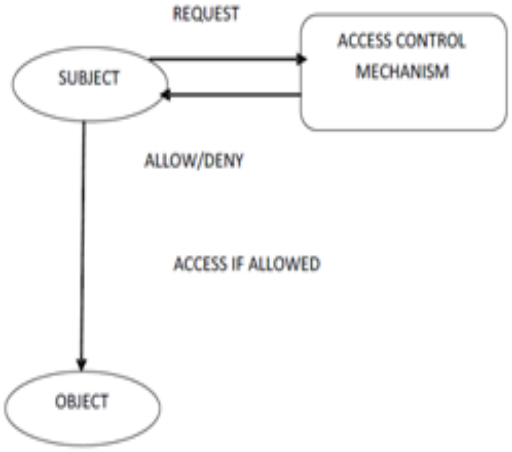

Figure 1 Basic model of access control mechanism

A. Bhagat and R.K. Sahu, [2013] The significance of the access control mechanism increases with the advent of new technologies such as cloud computing. The foremost reason for the requirement of new access control mechanisms with respect to the cloud environment is the nature of this environment. A simple example is the user is not aware about the location where his/her data resides. Another major characteristic of cloud that demands proper access control mechanism is its multitenancy, where a same resource is shared by multiple users.

The main types of access control are:

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role Based Access Control (RBAC)

Now we've got tons of techniques for access management in cloud computing. however these don't seem to be secured and economical. thanks to this downside, we tend to square measure attempt to propose a brand new secured and economical methodology for access management in cloud computing.

Mandatory access control (MAC): A security model within which access rights square measure regulated by a central authority supported multiple levels of security. usually utilized in government and military environments, classifications square measure appointed to system resources and therefore the package or security kernel, grants or denies access to those resource objects supported the knowledge security clearance of the user or device. as an example, Security increased UNIX system is associate implementation of macintosh on the UNIX system package.

Discretionary access control (DAC): An access management methodology during which house owners or directors of the protected system, information or resource set the policies process United Nations agency or what's approved to access the resource. several of those systems modify directors to limit the propagation of access rights. a typical criticism of DAC systems could be a lack of centralized management.

Role- based access control (RBAC): A wide used access management mechanism that restricts access to laptop resources supported people or teams with outlined business functions -- government level, engineer level one -- instead of the identities of individual users. The role-based security model depends on a fancy structure of role assignments, role authorizations and role permissions developed victimisation role engineering to control worker access to systems. RBAC systems will be accustomed enforce waterproof and DAC frameworks.

Rule-based access control: A security model within which the supervisor defines the principles that to manipulate access to resource objects. usually these rules area unit supported conditions, like time of day or location. it's not uncommon to use some style of each rule-based access management and role-based access management to enforce access policies and procedures.

Attribute-based access control (ABAC): A methodology that manages access rights by evaluating a group of rules, policies and relationships victimisation the attributes of users, systems and environmental conditions.

The rest of this paper is organized as follows. Section II provides the brief review of in cloud access control security. Section III provides the details various methodologies of proposed access control techniques. Section IV shows the Experimental results to evaluate the performance and comparison Section V includes conclusion of proposed system.

II. LITERATURE REVIEW

Many diverse factors such as integrity of data, data dynamics and data privacy affects the performance of a number of approaches in cloud data storage. Each and every approach has merits and demerits which make them suitable for different applications. K. Govinda,V.G. prasad and H.S. kumar [1] proposed a method in which RSA algorithm used for encryption and decryption which follow the process User and the TPA generate their own private key and public key with respect to the strong RSA algorithm. The public keys have been shared between them as the part of SLA or in some other ways. Then with respect to the protocol the message is encrypted as well as signed in a unique way. A. Mohta, R.K. Sahu and L.K. Awasthi [2] proposed Virtual Machine which uses RSA algorithm ,for client data/file encryption and decryptions.SHA 512 algorithm is also used which makes message digest and check the data integrity .The digital signature is used as an identity measure for client or data owner. Problem of integrity, unauthorized access, privacy and consistency are also solved in this proposed system. Watermark information is embedded into original image itself, and it is performed in the encryption process for making security on original information.

Cong Wang proposed public auditing [3] that allows TPA along with user to check the integrity of the outsourced data stored on cloud and Privacy Preserving allows TPA to do auditing without requesting for local copy of the data and cloud data privacy is maintained. T. Paigude and T.A. Chavan [4] proposed a system in which they used water marking process, to store the data or images in the cloud server by assigning the public key and this key and watermarking images are sent to third party and third party have complete authority to check the key and sent it to the server, and there TPA must have a public key whenever the data is retrieved. V. Vinaya and P. Sumathi [5] provide a scheme which checks data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. But this can be agreed upon by both the cloud and the customer and can be incorporated in the Service Level Agreement (SLA). They presented a model for secure integrity verification scheme and with data update protocol that dynamic data modification by introducing effective TPA. They addressed two main issues:-Data correctness and Public auditability. Data correctness means that there exists no cheating cloud server that can pass the TPA's audit without indeed storing user's data intact. Public auditability is to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

Hrushikesh , S. Patil and M. Pavaskar [8]proposed system in which they provide an OTP system at the user level. The OTP system will generate a verification code which the user needs to enter during registration. Further the code verified by the TPA and only after his approval the user registration will be completed .After that the uploading and downloading of files comes. While uploading the original data will be sent to the CSP and a copy of it would be sent to TPA for verification. After a simple yes/no message from the TPA the original file will be processed further for fragmentation and encryption by the CSP. T. Hemant at el.[9] proposed an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of user's data in the cloud. They rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability.

Due to this construction drastically reduces the communication and storage overhead as compared to the traditional replication – based file distribution techniques. By utilizing the homomorphism token with distributed verification of erasure-coded data, their scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, their scheme can almost guarantee the simultaneous localization of data errors, i.e. the identification of the misbehaving server(s).

K.Meenakshi and V.S.George [10], proposed a new system in which they are implementing the secure system namely privacy preserving auditing. In this system ,first the Data Owner will register with the Cloud Service Providers. During the registration phase the Public and Private will be generated for the Data Owner [11].The Data Owner have to provide their Private key while updating their data in the Cloud Server. Using Merkle Hash Tree Algorithm the Cloud Server split the data into batches. The Cloud Server will allow Third Party Auditor(TPA) to audit the data that was stored in the Cloud Server as requested by the user .The TPA will also audit multiple files. To support efficient handling of multiple auditing task , they further explore the technique of bilinear aggregate signature to extend their main result into a multi-user setting ,where TPA can perform multiple auditing tasks simultaneously. S. Rizvi, K. Karpinski, B. Kelly and T. Walker[12] proposed account, we propose a third party based validation and trust framework which facilitates the CSU in choosing the trustworthy CSP. The proposed model (1) allows the CSUs to provide their security preferences with the desired cloud services they are looking for, (2) provides a conceptual mechanism to validate the security controls and internal security policies of CSPs published in the STAR, and (3) maintains a database of CSPs along with their responses to CAIQ as well as the certificates issued by the certificate authorities. The proposed framework is divided into four modules around the TPA. First module shows the role of CSA in collecting the CAIQs from CSPs and maintaining them into STAR database.

III. SYSTEM DESIGN

In this model, we focus on Quality of Service. In the previous model , it is true that focus is given on the trust and transparency but they do work over the Quality of Service(QoS).QoS is varied according to the situation and needs of a work. Trust is very important for customers who are using various services of cloud service providers. Due to the vast diversity in the available cloud services, from the customer's point of view, it has become difficult to decide whose services they should use and what the basis for their selection should be. Adoption of cloud services is not easy for new adopters. So we need such a model which helps cloud service adopters in choosing best and most trustful Cloud Service Providers (CSPs).Having a trustworthiness profile for cloud providers is important because it will provide a reflection mechanism of the cloud provider's security profile that will reveal the strengths and weakness within the cloud providers.

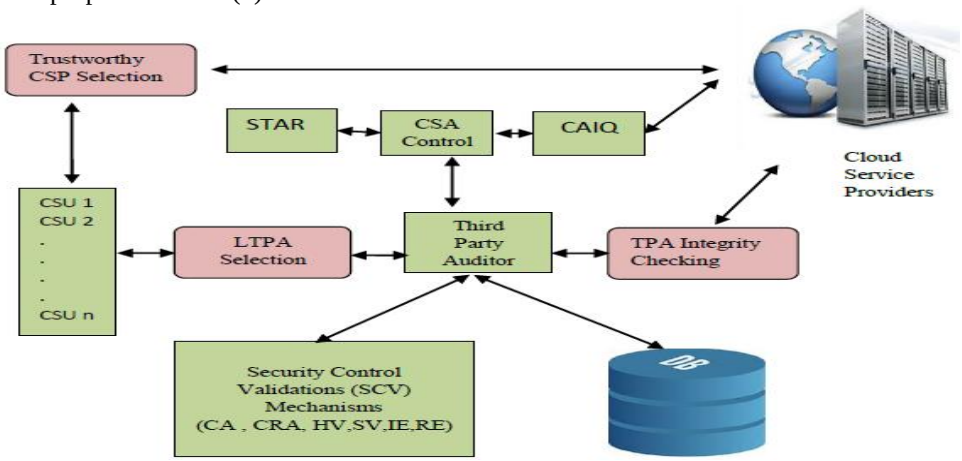

Figure 2 Proposed Models

First of all Cloud Service Provider (CSP) generated .In this section, the customer will select the number of CSPs that will be included in the comparative analysis study and it can be done by generating the number of CSPs using a random function. When the CSPs are generated they will be initialized with brief information related to the provider's cloud offering type. In this section, random data is generated for each CSP. The CSP is entitled to data that represent the CSP's trustworthiness. The trustworthiness data are expressed around factors which will help the customer to know the business and security history of the CSP, including includes years in business, membership, security and privacy breaches, outages and data losses. We also add Quality of Service parameters here for checking the trustworthiness of each CSP. After data is generated, it will go to next section. For trustworthiness, the evidence should be kept up-to-date.

3.1. Registration

To do any operation in cloud, the user and therefore the owner ought to register there. For registration the user and therefore the owner can send a registration request to the corresponding domain authority.

Then the domain authority verifies that's the new member receptive there terms and conditions. If they're able to settle for the terms and conditions, then the domain authority can forward that request to the trustworthy domain. Then the trustworthy authority can offer a permanent id to every of the house owners and users. Then they can set a countersign for them.

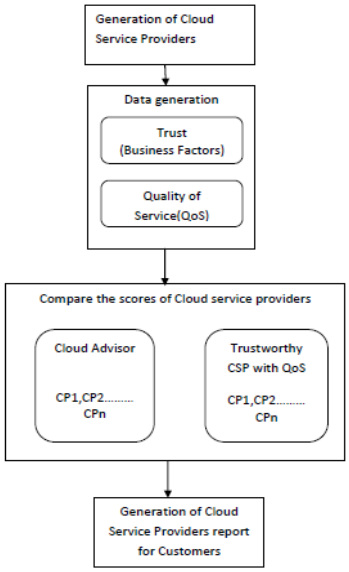

Figure 3 Trustworthy Cloud Service Provider with Quality of Services (QoS)

3.2. File Upload

To transfer a file, initial the info owner can write in code the file mistreatment his personal key and send it to succeeding higher level. that's domain authority. Then the domain authority can checks that the owner could be a registered one or not. If he's a registered owner, then the domain authority can forward that encrypted file to the trustworthy authority.

3.3. File Download

To transfer any file from the cloud, first the info user send an invitation to his corresponding domain authority. Then the domain authority can verify the user. If it's a legitimate user, then it'll forward that request to the sure authority. Then the trusted authority can forward this request to the corresponding information owner. Then the owner can check the attribute set of that user. If the user have a legitimate attribute set, then the owner send a key to the user. once the owner send a key to the user then the clock can begin tally. when a bound time amount, that key becomes associate degree invalid one. that the user ought to access the requested file inside that point limit.

3.4. File Deletion

Only the information owner will delete his file from the cloud. throughout the registration time of the information owner, the trustworthy authority can give associate degree id range to every of the info house owners. These id numbers are permanent for them. additionally every of them have a positive identification, that is not permanent. To delete a file, the info owner first send a request to his corresponding domain authority. This request contains the owner id and also the file name. Then the domain authority can raise positive identification to the owner. If the owner offers the proper positive identification, then the domain authority can forward the deletion request to the trustworthy authority. then the trustworthy authority can delete the file from cloud.

IV. RESULT AND DISCUSSION

In this section, we give simulated result of two frameworks. The main concern is cloud providers trustworthiness, result of Cloud Advisor and Trustworthy cloud service provider with QoS. Access management may be a method that's integrated into Associate in Nursing organization's IT atmosphere. It will involve identity and access management systems. These systems give access management code, a user information, and management tools for access management policies, auditing and social control. The goal of access management is to reduce the danger of unauthorized access to physical and logical systems. Access management could be a elementary element of security compliance programs that ensures security technology and access management policies area unit in situ to safeguard hint, like client knowledge. Most organizations have infrastructure and procedures that limit access to networks, laptop systems, applications, files and sensitive knowledge, like in person identifiable data and property. Access management systems area unit complicated and may be difficult to manage in dynamic IT environments that involve on-premises systems and cloud services. when some high-profile breaches, technology vendors have shifted far from single sign-on systems to unified access management, that offers access controls for on-premises and cloud environments.

Table 1 Uploading of various size of block of file on cloud server

File Size (KB)	Start Time	Finish Time	Status	Data Centre ID	WM ID	Time
50	0 0.1	0.29	Success	2	0	0.19
100	0 0.1	0.49	Success	2	0	0.39
150	0 0.1	0.89	Success	2	0	0.71
200	0 0.1	0.92	Success	2	0	0.82
250	0 0.1	1.1	Success	2	0	1.00
300	0 0.1	1.31	Success	2	0	1.21
350	0 0.1	1.49	Success	2	0	1.39
400	0 0.1	1.71	Success	2	0	1.61
450	0 0.1	1.89	Success	2	0	1.79
500	0 0.1	2.11	Success	2	0	2.01

It can be clearly seen from the Table 1 that proposed work increases the security on the cloud with its efficiency and control. The value of the security is greater than the existing approach. It may be possible that the computational overhead will increase but the security parameter is more serious issue w.r.t. these parameters on cloud. Table 1 and Figure 4 shows the uploading time and finishing time of file block on the cloud server. Uploading time increase as the size of file block increases but as explained earlier that security also enhanced because of different parameters which have been taken for accomplishing the same. This is true that there is no effect on computational cost but the integrity of third party auditor is increased, which direct leads to the security concern on cloud computing.

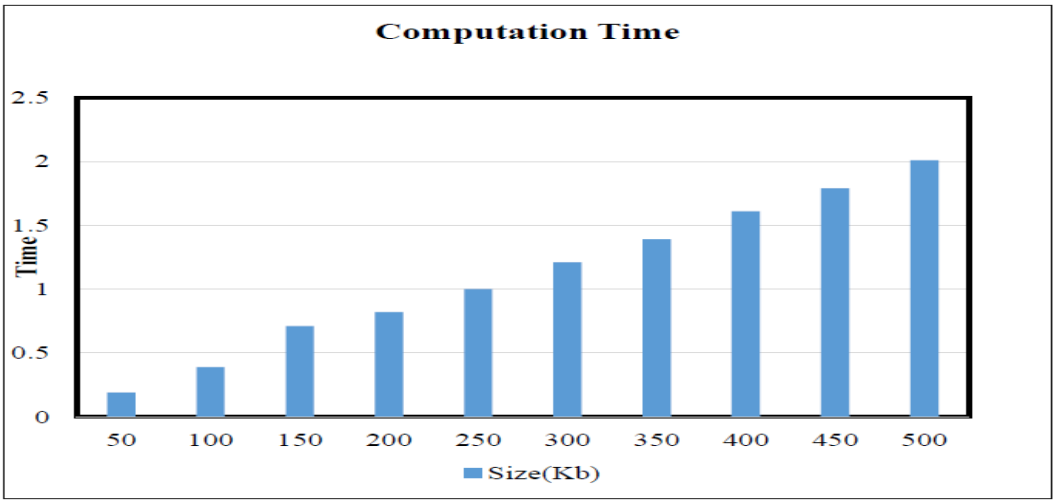

Figure 4 Computation time of uploading of various size of File block on Cloud Server

V. CONCLUSION

It is an extremely economical model for offer access management in cloud computing. It's in a very data structure and it employing a clock for providing cryptography key supported time. This model guarantee each security and access management in cloud computing. the most operations during this model area unit registration, file transfer, file transfer and file deletion. Present study a model has been developed which helps new users in comparing the different services provided by different cloud service providers. It works on quality of service (QoS), which play the vibrant role in the selection of best CSP. Before this study, many tools were developed, but they did not focus on Quality of Service (QoS). This model assists cloud customer in assessing cloud providers trustworthiness based on predefined trust attributes such as business factors, Quality of Services attributes and the 11 security control domains defined by the CSA.

REFERENCES

1. K. Govinda,V. Gurunathaprasad and H. Sathiskumar, "Third Party Auditing For Secure Data Storage in Cloud Through Digital Signature using RSA", International Journal of Advanced Scientific & Technical Research, vol. 4,pp. 525-530, 2012.
2. A. Mohta and L.K. Awasthi, "Cloud Data Security While Using Third Party Auditor", International Journal of Scientific & Engineering Research , vol. 3, pp. 1-4, 2012.
3. C. Wang, S.M. Chow, Q. Wang, K. Ren and W.Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE Transaction on Computer I, vol. 62,pp. 362-375, 2013.
4. T. Paigude and T.A. Chavan, "A Survey on Privacy Preserving Public Auditing for Data Storage Security", International Journal of Computer Trends & Techniques, vol. 4, pp. 412-418, 2013.
5. V. Vinaya and P. Sumathi, "Implementation of Effective Third Party Auditing for Data Security in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, 2013.
6. J. Kaur and J. Singh, "Monitoring Data Integrity while using TPA in Cloud Environment", Global Journal of Computer Science and Technology, vol. 2,pp. 19-23, 2013.
7. A. Bhagat and R.K. Sahu , " Using third party auditor for cloud data, security: A review", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, 2013.
8. H. Joshi, S. Patil and M. Pavaskar, "A Survey On Data Security & Accountability In Cloud", International Journal of Research in Advent Technology, vol. 2, pp. 331-338, 2014.
9. H.T. Dhole, P. C. Papade and S.B. Bhosle, "Ensuring Data Security using Cloud Computing", International Journal of Advance Research in Computer Science and Management Studies, vol. 2, pp.491-497, 2014.
10. K. Meenakshi and V.S. George, "Cloud Server Storage Security Using TPA", International Journal of Advanced Research in Computer Science & Technology, vol. 2, pp. 295-299, 2014.
11. C. Wang ,S.S.M. Chow, Q. Wang, K. Ren and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE, vol. 62,pp. 362-375, 2013.
12. S. Rizvi, K. Karpinski, B. Kelly and T. Walker, "Utilizing Third Party Auditing to Manage Trust in the Cloud", Procedia Computer Science, vol.61, pp.191-197,2015