PROTECTED CLOUD COMPUTING

Ms.Apsarunnisa[1]., Mr.Rony Preetam[2]
1,2 Assistant Professor, Department Of CSE.,
(✉apsarunnisa06@gmail.Com, ✉ronyjcpreetam @gmail.Com)
1,2 Malla Reddy College Of Engineering For Women., Maisammaguda., Medchal., Ts, India

Abstract—Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In thecloud, th, data is transferred among the serverand client. Highspeed is the important issue in networking.Cloud security is the current discussion in the IT world. This research paper helps in securing the data withoutaffecting the network layers and protecting the data from unauthorized entries into the server, the data is securedin server based on users' choice of security method so that data is given high secure priority. Cloud Computinghas been fancied as the next generation architecture of IT Enterprise. In contrast to traditional solutions,
wheretheITservicesareunderproperphysical,logicalandpersonnelcontrols,CloudComputingmovestheapplication software and databases to the large data centres, where the management of the data and services maynot be fully trustworthy. This unique attribute, however, poses many new security challenges which have notbeen well understood. In this article, we focus on cloud data storage and transmission security,which hasalways been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, wepropose an effective and flexible distributed scheme with two salient features, opposing to its predecessors.[1]Cloudstorageenablesusersto remotely storetheirdataandenjoy theon-demand highquality cloudapplications without the burden of local hardware and software management. This article explores the barriersandsolutionstoprovidingatrustworthycloudcomputingenvironment**.**

Keywords-Cloud,PrivateCloud,Security, SecuredataTransmission**.**

I. INTRODUCTION

Cloud computing is a recent trending in IT that where computing and data storage is done in data centres ratherthan personal portable PC's. It refers to applications delivered as services overthe internet as well as to thecloud infrastructure – namely the hardware and system software in data centresthat provide this service. Thesharing of resources reduces the cost to individuals. The best definition for Cloud is defined in [9] as large poolof easily accessible and virtualized resources which can be dynamically reconfigured to adjust a variable load,allowing also for optimum scale utilization. Several trends are opening up the era of Cloud Computing, which isan Internet-based development and use of computer technology. The key driving forces behind cloud computingis the omnipresence of broadband and wireless networking, falling storage costs, and progressive improvementsin Internet computing software. The main technical supporting of cloud computing infrastructures and servicesinclude virtualization, service-oriented software, grid computing technologies, management of large facilities,and power efficiency. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) andAmazon Elastic Compute Cloud (EC2) [1] are both well-known examples. While these internet-based onlineservicesdoprovidehugeamountsofstoragespaceandcustomizablecomputingresources,thiscomputing

platform shift, however, is eliminating the responsibility of local machines for data maintenance at the sametime. As a result, users are at the mercy of their cloud service providers for the availability and integrity of theirdata. Recent downtime of Amazon's S3 is such an example [2]. From the perspective of data security, which hasalways been an important aspect of quality of service, Cloud Computing inevitably poses new challengingsecurity threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of datasecurity protection cannot be directly adopted due to the users' loss control of data under Cloud Computing.Considering various kinds of data for each user stored in the cloud and the demand of long term continuousassurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes evenmorechallenging. Secondly,CloudComputingisnotjustathirdpartydatawarehouse.

The rest of the paper is organized as follows. Section II introduces the system model section IIIintroduce adversary model, section IV introduce our design goal. In Section V security architecture. Then weprovide Security data transmission in Section VII.Finally, Section VIII gives the concluding remark of thewholepaper.

Figure1- generalstructureofclod computing

II. SystemModel

In[1] and [2] Representative network architecture for cloud data storage is illustrated in Figure 2. Threedifferentnetworkentities canbeidentifiedasfollows:

- User:users,whohavedatatobestoredinthecloudandrelyonthecloudfordatacomputation,consistofbothindividualconsumersandorganizations.
- CloudService Provider(CSP):aCSP,who has significantresources andexpertise inbuildingandmanaging distributed cloud storageservers,ownsandoperatesliveCloud Computingsystems.
- ThirdPartyAuditor(TPA):anoptionalTPA,whohasexpertiseandcapabilitiesthatusersmaynothave,istrusted toassess andexposeriskofcloudstorageservicesonbehalfoftheusers uponrequest.

In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running inasimultaneous,cooperatedand distributedmanner.Data redundancy canbe employedwithtechnique oferasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance.Thereafter,forapplicationpurposes,theuserinteractswiththecloudserversviaCSPtoaccessorretrievehis

data. In some cases, the user may need to perform block level operations on his data. The most general forms ofthese operations we are considering are blockupdate, delete, insert and append. Inourmodel, we assume thatthe point-to-point communication channels between each cloud server and the user is authenticated and reliable,which can be achieved in practice with little overhead. Note that we don't address the issue of data privacy inthispaper,asinCloudComputing,dataprivacyandstorageisorthogonaltotheproblemwestudyhere.

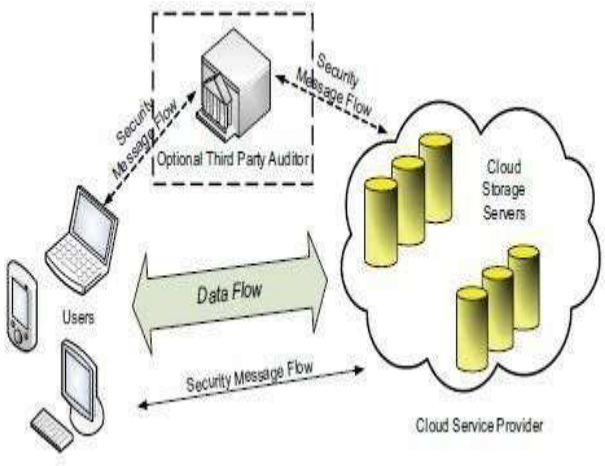

Figure2–clouddatastoragearchitecture.

III. AdversaryModel

Securitythreatsfacedbyclouddatastoragecancomefromtwodifferentsources.Ontheonehand,aCSPcanbe self-interested, un-trusted and possibly malicious. Not only does it desire to move data that has not been or israrely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a datalossincidentduetomanagementerrors,convolutedfailuresandsoon.Ontheotherhand,theremayalsoexistan economically motivated adversary, who has the capability to compromise a number of cloud data storageservers in different time intervals and Specifically, we consider two types of adversary with different levels ofcapability in this paper: *Weak Adversary*: The adversary is interested in corrupting the user's data files stored onindividual servers. Once a server is comprised, an adversary can pollute the original data files by modifying orintroducing its ownfraudulent data to prevent the original data from being retrievedby the user.*StrongAdversary*: This is the worst case scenario, in which we assume that the adversary can compromise all thestorage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact,thisis equivalenttothecasewhereallservers arecolludingtogethertohideadataloss orcorruptionincident.

IV. DesignGoals

To ensure the security and dependability for cloud data storage under the aforementioned adversary model, weaimtodesignefficientmechanismsfordynamicdataverification and operationandachievethefollowinggoals:

(1) Storage correctness: to ensure users that their data are indeed stored appropriately and kept intact all the timeinthecloud.
(2) Fastlocalizationofdataerror:toeffectivelylocatethemalfunctioningserverwhendatacorruptionhasbeendetected.
(3) Dynamicdatasupport:tomaintainthesamelevelofstoragecorrectnessassuranceevenifusersmodify,deleteorappendtheirdatafilesinthecloud.
(4) Dependability:to enhancedataavailability againstByzantinefailures,maliciousdatamodificationandservercolludingattacks,i.e.minimizingtheeffectbroughtby dataerrors orserverfailures.
(5) Lightweight:toenableuserstoperformstoragecorrectnesschecks with minimumoverhead.

V. SecurityArchitectures

The above discussion is on certain review literature by many research people on different aspects of security.The aspects went on describing the problems and threats in related to security in cloud. The literature in detailexplains about the issues like security for data, virtualization security and prescribed format of SLA etc. Thereare many research people have keen interest in designing certain security architectures help for secure cloudcomputing. The following are described below: Gary Anthes [14] has described the various security researchworks in cloud are discussed. He brought forward the research works done in popular companies like IBM, HP,and Microsoft. **T**here are many security risks involved in cloud computing, and also some good solutions arealsobeendesignedbytheresearcherswhicharepointedbelow.

1) Researchers at HP laboratories are prototyping cells as a service to automate security management incloud. A cell is single administrative domainusing security policies containing virtual machines,storagevolumesacrossphysicalmachines

2) IBM research people doing virtual machine introspection which puts security inside protected VMrunning on same machine. This employs number of protective methods listing the kernel functions. Itcanmakereduceofrunningvirusscannersonsystem.

3) Microsoft research described about cryptographic cloud storage where the data is secured by user byencryptingformatsuchthattheprovidercannotgetwhatthedataispresent.

Flavio Lombardi and Roberto Di Pietro has discussed [15] about a secure virtualization technique for ensuringsecurity at hypervisor level. In a general system at base OS level, there is a problem like a user at one guest OSmay interact with other Guest OS, which may lead to data loss if they are any attackers. So the new proposalACPS(AdvancedCloudProtectionSystem)wasintroduced.Thiswillmaintainsecuritybypreventingunneces sary logins into the other guest OS by weak passwords or weak SSH. Cong Wang [5] has proposed theirwork on Data Storage security with respect to Quality of service. They have proposed approach which checkswhethertheirdatahas beenattackedoranyintegritylossis doneornotoverthecloud.

VI. High-levelCloudArchitecture

We provide and architectural view of the security issues to be addressed in cloud computing environment forprovidingsecurityforthecustomer.WehavedefinedfourlayersbasedoncloudcomputingservicescategorizationTh ecloudcomputingcategorizationbasedonservicesasSoftware-as-a-Service(SaaS),Platform- as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). This section elaborates the four layersshowninfigure1andmappingthedifferentsecurityissuesineachlayer.

SomeoftheimportantcomponentsofUserlayerareCloudApplications,Programming,ToolsandEnvironments. Some of the popular examples for these applications are B2B, Face Book, MySpace, Enterprise,ISV,Scientific,CDNs,Web2.0Interfaces,Aneka,Mashups,MapReduce,Hadoop,Dryad,Workflows,Libr aries, and Scripting. Some of the security issues related to the user layer are Security as a Service, BrowserSecurity,andAuthenticationaselaboratedinnextsections.

SomeoftheimportantcomponentsofServiceProviderLayerareSLAMonitor,Metering,Accounting,Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, andPolicyManagement.

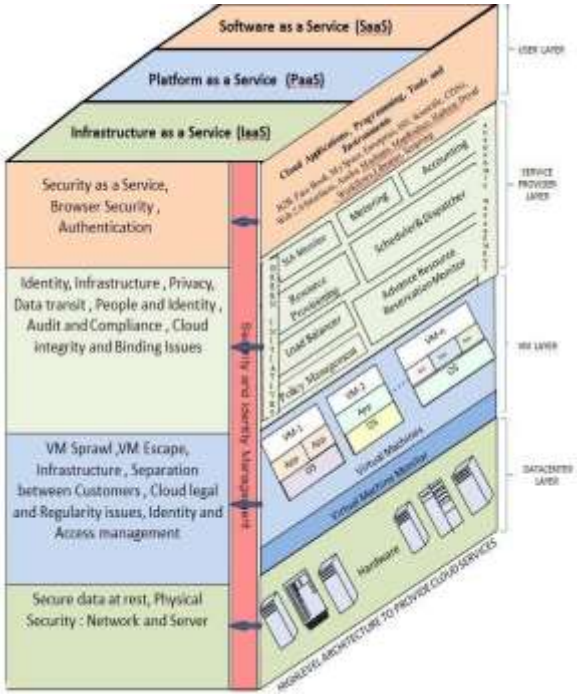

Figure 3:SecurityArchitectureofCloudComputing

Someofthesecurity issuesrelatedtoServiceProviderLayerareIdentity,Infrastructure,Privacy,Datatransmission,PeopleandIdentity,AuditandCompliance,CloudintegrityandBindingIssues.

Some of the important components of Virtual Machine Layer create number of virtual machines and number ofoperating systems and its monitoring. Some of the security issues related to Virtual Machine Layer are VMSprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legal and Regularity issues, IdentityandAccessmanagement

Some of the important components of Data Center (Infrastructure) Layer contains the Servers, CPU's, memory,andstorage, andishenceforthtypicallydenotedasInfrastructure-as-a-Service(IaaS).

VII. EndUserSecurityIssues

End Users need to access resources within the cloud and may bear in mind of access agreements like acceptableuse or conflict of interest. The client organization have some mechanism to find vulnerable code or protocols atentry points like servers, firewalls, or mobile devices and upload patches on the native systems as soon as theyare found. The cloud should secure from any user with malicious intent that will conceive to gain access toinformationorpackupaservice.

Security-as-a-service

In Cloud environment the security provided by customers using cloud services and the cloud service providers(CSPs).Security-as- a-service is a security provided*as* cloud services and it can provided in two methods: Infirstmethod anyone canchanging theirdelivery methods to include cloudservicescomprises establishedinformationsecurityvendors.

The second method Cloud Service Providers are providing security only as a cloud service with informationsecurity companies. Almost all the security companies, anti-malware vendors involved in the delivery of SaaSwithregardtoemailfilteringandsoon.

BrowserSecurity

In a Cloud environment, remote servers are used for computation. The client nodes are used for input/outputoperationsonly,andforauthorizationandauthenticationofinformationtotheCloud.AstandardWebbrows eris platform in-dependent client software useful for all users throughout the world. This can be categorized intodifferent types: Software-as-a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryptionandhostauthentication

The Legacy Same Origin Policy is the insertion of scripting languages into Web pages for access rights forscripts. In is to allow access read or write operations the same *origin* on content, to disallow but from thedifferent origin any access on content. Origin means a "the same application", it can be defined with domainname, protocol, port in a web. But some problems with the SOP, but it could be solved with "origin" definition.In the case of WWW it's not working properly. Security requirements for to protect both data during transport,andtoauthenticatetheserver'sdomainnameinWebapplicationsisTLS.

Attacks on Browser-based Cloud Authentication are one of the security problem withbrowser-based protocolsin Cloud Computing and it is not capable to generate cryptographically valid XML tokens. So, it can possiblewith a trusted third party. Login is not possible at a server due to the fewer credentials in browser, So HTTPforward it to the Passport loginserver. Afterentering username and password from user, thenthe Passportserver convert this authentication into a Kerberos token, it can redirected to the requesting server from otherHTTP redirect. Kerberos tokens are not clear to the browser is the security problem with Passport, and itprotectedbytheSOP. Butanyattackercanaccess thosetokensthenheaccessesallservicesofthevictim.

Secure Browser-based Authentication is the situation is not suggested, but we can perform for better results bycombined SOP and TLS for secure FIM protocols. In Cloud Computing by using TLS Browser Enhancementsare very limited in an authenticationcenter.It is notpossible forXML Signature, the browsercanbe addedmany Web Service functionalities by simply loading an appropriate JavaScript library during runtime. So, thebrowsersecurityAPIcanbeaddingtheenhancementsXMLEncryptionandXMLSignature.

Authentication

In the cloud environment, the primary basis for access control is user authentication and access control are moreimportant than ever since the cloud and all of its data are accessible to all over the Internet. Trusted PlatformModule(TPM)isawidely availableandstrongerauthenticationthanusernameandpasswords.TrustedComputing Groups (TCG's) is IF -MAP standard about authorized users and other security issue in real-timecommunication between the cloud provider and the customer. When a user is reassigned or fired, the customer'suniqueness management system can report the cloud provider in real-time so that the user's cloud access can berevoked or modified within seconds. In cloud any fired user is logged, they can be immediately disconnected.Trusted Computing enables authentication of client nodes and other devices for improving the security in cloudcomputing.Thefrequentlytargetedattackisauthenticationinhostedandvirtualservices.Thesecuremechanismsar eusedtotheauthenticationprocessforfrequenttargetofattackersby differentwaystoauthenticateusersbasedondifferentinformationknowbytheuser.

VIII. Securityframeworkforserver-client network

The Fig 3 is the design architecture where a new security layer is designed for private cloud. The new securityframework is present in between session layer and transport layer such that it is transparent to application layerand the lower layers. So whenever a data is transferred by the client it is first secured by certain authenticationprotocols andsavedattheserverend.

With this, the data will be stored in a secured way at server end. Those who want to download application userlevel so that the data will be secured and transferred where there is need to disturb any lower layers of thenetwork.

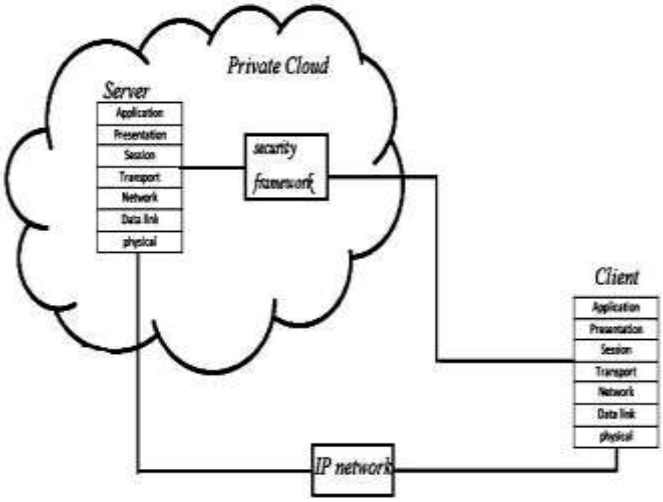

Figure4–highlevel design

IX. DESIGN OFTHESYSTEM

- SecurityFrameworkModel

The detailed design of the framework is in the below Architecture Figure 4. The nodes which are connected toserverwillbeconnected tothesecuritylayer.WhenanApplication userwantstosenddatatoprivatecloud,

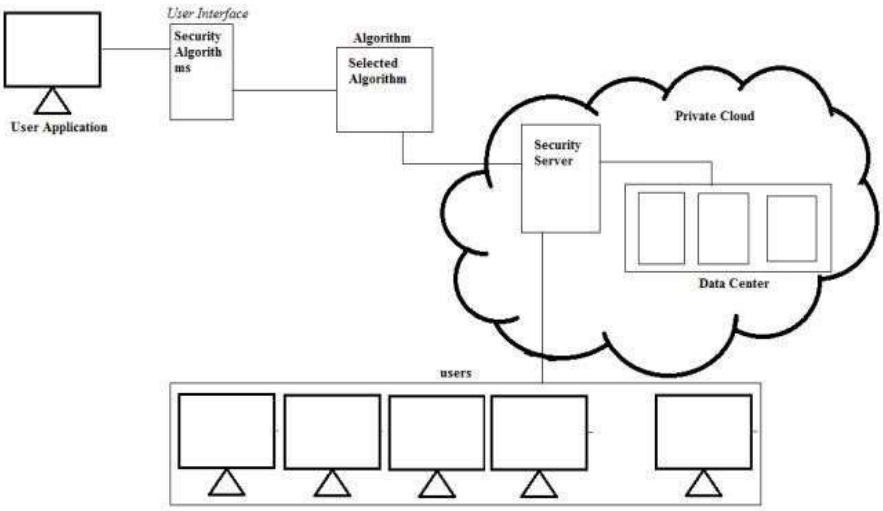

Figure5–systemarchitecture

Security Algorithm based on the privacy level of the document, if he needs more security there must be a strongsecurityalgorithmtobeselected.Thesecurityserverwillsecurethedocumentandsaveitindatabase.

Here all the systems which belong to that network are connected to the same architecture. When any other userwishes to select any document from the data center, he is required to be connected to the same security server togettheoriginaldocument. Thishelpsinsecurityandprivacyofthedocuments.

- Processatsender

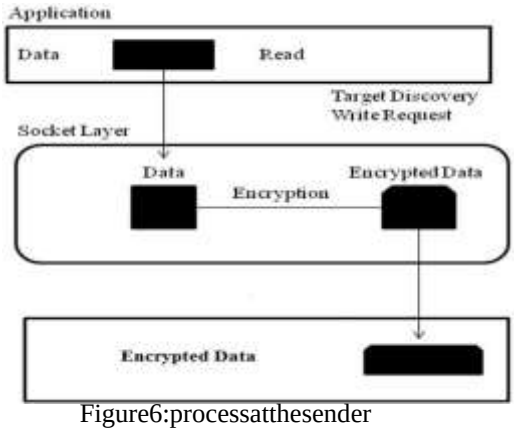

Figure6:processatthesender

The data at the initiator end (client) will all set his data. He encrypts the data by selecting the appropriateapproach from the interface and sends it to the server end. As shown in the above figure, at the client end thedata is read, ready to send data. At socket layer, before sending it to the remote end the data will beencryptedfor each byte and send encrypted data. The data is carried by the protocol to process the other commands whichhappens in a network. The data will be secured at the sender end by the security framework which helps insecuredatatransfer.

- Processatreceiverend

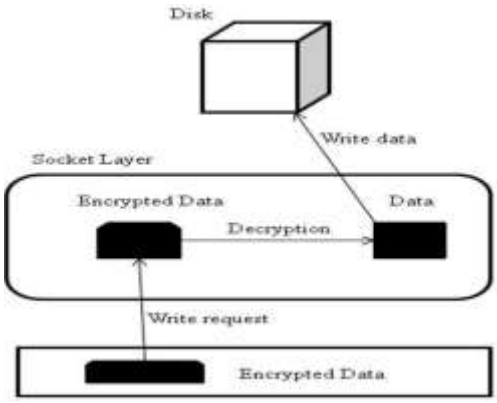

Fig7:processatthereceiver

Atthereceiverendwhenthedataisreceived,thedatawillbedecryptedandwrittenonthedisk.Thedatawillbe decrypted by the security approach used at encryption end. This is again worked above transport layer justwhere the packets arrive at end application. As before the write request is given by the protocols, the securityframework decrypts the data and saves on to the disk. In the similar way when the client requests a file fromserverthe same process as mentioned will be happened. This will make sure that data is secure overthenetwork.Wecanhaveconfidentialityandintegritychecksatthereceiverend.

X. Conclusion

In this paper, we investigated the problem of data security in cloud data storage and data transmission, which isessentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, weproposedaneffectiveandflexibledistributedscheme.ourschemeachievestheintegrationofstoragecorrectness insurance and data error localization. In the data transmission proposed, method transferred data isencryptedintheupper-layerontopofthetransportlayerinsteadofusingIPSecorSSL.Thus,theschemefor

the performance improvement can be applied without modifying the implementation of IP layer, and efficientsecure communications by pre-processing of encryption in the upper-layer are realized. We have used fileuploading as service as web application, the security is applied over to the data at the background using theencryption algorithms like AES, Triple DES and DES. Through detailed security and performance analysis, weshow that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack,andevenservercolludingattacks.

Webelieve thatdatastorage security inCloud Computing,an areafullof challenges and of paramountimportance, is still in its infancy now, and many research problems are yet to be identified. Adding secure cloudstorage using the proposed cryptographic solution and with a searchable encryption technique for the files to beaccessed, it will work as a better approach to the user to ensure security of data. The cloud security usingcryptography is already in use for secure data storage which can be enhanced for secure data transmission andstorage. An interesting question in this model is if we can construct a scheme to achieve both public verifiabilityand storage correctness assurance of dynamic data. Besides, along with our research on dynamic cloud datastorage,wealsoplantoinvestigatetheproblemoffine-graineddataerrorlocalization.

REFERENCES

[1] Cong Wang, QianWangKuiRen, Ning Cao, and Wenjing Lou Toward Secure and Dependable StorageServicesin CloudComputingIEEEtransactionsonservices computing,vol.5,no.2,april-june2012

[2] QianWang,CongWang,KuiRen,WenjingLouJinLiEnablingPublicAuditabilityandDataDynamicsfor Storage Security in Cloud Computing IEEE transactions on parallel and distributedsystems,vol.22,no.5, may2011

[3] Boris Tomas1and BojanVuksic2 Peerto PeerDistributed Storage and Computing Cloud SystemInternationalconferenceon informationtechnologyinterfaces,June25-28,2012,cavtat,croatia

[4] SecurityandPrivacyChallengesinCloudComputingEnvironmentsco-publishedbytheIEEEcomputerandreliabilityieeeNovember/December2010

[5] Subashini S, Kavitha V.,A survey on security issues in service delivery models of cloud computing,JournalofNetworkandComputerApplications(2011)vol.34Issue1, January2011pp.1-11.

[6] Balachander R.K, Ramakrishna P, A. Rakshit,Cloud Security Issues, IEEE International ConferenceonServicesComputing(2010),pp. 517-5.