www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 11 November, 2014 Page No. 9374-9378

Implementation Aspects To Secure Criticaldatain Public Cloud Network Using Opnet Simulator

Kajal Singhai, Rajesh Kumar Chakrawarti
PGScholar,ComputerScienceEngineeringDeptShriVaishnavInstituteofTechnology&Science Indore,MadhyaPradeshkajalsinghaiswt@gmail.com
Reader,ComputerScienceEngineeringDeptShriVaishnavInstituteofTechnology&Science Indore,MadhyaPradeshrajesh_kr_chakra@yahoo.com

Abstract—Cloud Computingisafamousdaytodaybetween interestingapplicationsaccessbyinternetusers. Public Cloud allowgeneric publictoaccesstheseapplication,software and Platformatlowcostwithoutany SecurityMechanism, but insidethisdeployment Cloudsometimecriticaldatarequired privacyfromglobaluserand atnowonlyexistingfirewall mechanism usedtoprotectthecriticaldatafromattackers by creatingVirtualprivatenetworkwhichiscostlymechanism forshort period. This paper describes thePublic Cloud Networks,Criticaldata, existingmechanismand proposed Architecturewithimplementationtool.

Keywords—PublicCloudNetwork,CriticalData,Proposed Architecture,OPNET

I. INTRODUCTION

CloudComputingisbecomingincreasingly popularforits, lowercost,higherutilization,andbettermanagement, better usabilitywhich useremote servicesthrough network.Cloud computing isbeginningtotransform thewaycompanies involvewithcustomers, partnersandsupplierstoprovidesall necessary serviceontheirdemandovertheinternettoaccess cloudresources.Cloudstructureisstrongly basedonthe conceptof"LocationIndependence". Theuserisjustusinga system whichiscapableof usinganetworkthat connectittoa serverliesatsomeotherlocation. Usersdonotneedtostore dataontheirownsystemasalldataisstoredatremoteserver. Storing dataintheclouds eems tobequiteattractiveform of datamanagement.Oneofthemainadvantageofstoringdata incloudisunlimited access tothedatai.e.usercanretrieve theirstored datafrom theserveras andwhenrequiredwithno limitation.

Functioning ofpublic,privateandhybridcloudisnotmuch different,theremarkable factisusershastotrustathird-party and their valuable data are being kept with them through cloud.Therearefew questions associatedwithcloud computing thateveryoneasked,Canofferingservicesfroma CSPissecureandcompliant?So Security ofthestoragedataisaprimary concern incloud computing.Storagedatamustbesecureinsuchawaysothat itissafefrommalicious intruderandprohibitedusers.There arenopublically availablestandards specifictocloud computing security. So, in this paper, we propose the following standards for maintaining security in an unsafe cloudcomputingenvironment.

II. PUBLICCLOUD NETWORK

A public cloud is one based on the standardcloud computingmodel, in which a serviceprovider makes resources,suchasapplications andstorage,availabletothe general publicovertheInternet. Theterm"public" doesnot alwaysmeanfree,even though itcanbefreeorfairly inexpensivetouse.Apublic clouddoesnotmean thatauser's dataispublically visible,publiccloudvendorstypically provideanaccesscontrolmechanism fortheirusers.Public clouds provide anelastic,costeffectivemeans todeploy solutions. Publiccloudismadeupofseveralnodessituatedin deferentgeographic location.Examples of publicclouds includeAmazonElasticComputeCloud(EC2),IBM'sBlueCloud, SunCloud,GoogleAppEngine andWindowsAzure Services Platform.Themainbenefits ofusingapubliccloud serviceare:

A. Easy and inexpensive set-up because hardware, applicationandbandwidth costsarecoveredbythe provider.

B. Scalabilitytomeetneeds.

C. No wastedresourcesbecauseyoupayforwhatyouuse.

D.Opendatainitiatives.

E. Publicinformationrepositories.

F. Developing,pilotingandtestingnewapplicationsor solutionswhere.

G.Deepintegrationwithback-enddataofasensitiveor confidentialnatureisnotrequired

.

Thereareresharedinfrastructures andservicesingeneralcloud whichmaygiverisetonewsecurity issues.Thefollowing securitychallenges areyettobesolvedwheretheattackeror hacker needstobe hurdled:

- Theactualphysicalmachinewherethevirtualserver isrunning.
- Placingmaliciouscodeonthe physical machine.
- AttackonVM(VirtualMachine)fromotherVMs.
- DenialofService Attacks.

III. PUBLICCLOUDCONCERNS

Thisadoptionofpubliccloudwillincreaseheavily becauseof thehighdemandoncomputing resourcesinsearchengineor datawarehouses anddatamining. Thisdemandscomesfrom thelargeincreaseincomputing andmultimedia inevery day duties.However,cloudcomputing usersshould awareof security threatsthatcanoccurbecausecloudcomputing uses networks tograntaccesstotheresources required. Besidesits manypotentialbenefitsforsecurity andprivacy,publiccloud computingalsobringswith itpotentialareas ofconcern,when comparedwithcomputing environments foundintraditional datacenters.Someofthemorefundamental concerns include thefollowing:

Thereare somekeysecurityissuesandtheyareasdiscussed below:

A. Internet-facingServices

Publiccloudservices aredelivered overtheInternet,exposing boththeadministrative interfacesusedtoself-servicean accountandtheinterfacesforusersandapplications toaccess otheravailableservices.Applications anddatathatwere previously accessedfromtheconfinesanorganization's intranet, butmovedtothecloud,mustnowfaceincreased risk fromnetworkthreatsthatwerepreviously defendedagainstat theperimeteroftheorganization's intranetandfromnew threatsthattargetthe exposedinterfaces.Requiringremote Administrativeaccessasthesolemeanstomanagetheassets oftheorganization heldbythecloudprovideralsoincreases risk,comparedwithatraditional datacenter,where Administrativeaccess toplatformscan berestricted todirector internalconnections.

B. AccessIssue

Cloudcomputinghasthethreatofaccessing thesensitive and criticalinformation. Themanagement ofidentitiesand directory servicestoprovideaccesscontrol.Italsotakesinto accounttheassessment ofanenterprise's toconductcloud basedIdentityandAccessManagement(IAM).

C. PrivacyIssue

Privacy isthemainconcern tobeconsideredhere,andifthe cloudservices can'tprovidethelevelofprivacy itcanbe consideredasthemainsecuritythreat.Theseprivacyissues aremainlyirritatingacrossthe publicclouds,wheretheaccess tothecloudsisthroughthepublicdomains.

D.Availailityand Backup

In general most of the client software's and databases are maintained across theremote locationsacrosscloudcomputing. Iftherequired resourcesarenotavailableatpeaktimesandeven the backupfailingacrossthe clouds,thissituation definitelyleads to lots of securityissues.

E. DataProliferationIssue

Mostofthecloudserviceproviderssharetheinformation or data toagroupoforganizationsandthissituationleadstodataproliferatio nissues.Itwillbeveryeasyinpubliccloudto copythedatafrom differentdatacentersandthisfinallyleads tolotsofsecurity issues. Therearesomechanceswherethe originalcopy ofdatacanbedeletedduetomisuseofdata proliferation.

F. LackofControl

Enterprises mostly don'tknowwhere theirdataisphysically storedandwhichsecuritymechanisms areinplacetoprotect datai.e.whether thedataisencrypted ornotandifyes,which encryptionmethodisappliedalsoiftheconnection usedfor datatotravel inthecloudisencryptedandhow theencryption keysaremanaged(WindowSecurity,2010).

IV. EXISTING APPROCHTOSECURE ACCESSINGINPUBLIC CLOUDUSINGFIREWALL

Theproposedsystemwillattempt toprovidesecuredelivery of datatoandfrom the cloud. Oneoftheadopted technology istheVirtual PrivateNetwork (VPN). WithVPNprivateand securedsubnetworksinpubliccloudcanbeconstructed.

Thisprinciplehavebeenwidely appliedinwiredlocal-area network(LAN),remoteaccessnetworksand canbe also applied to wireless local-area network (WLAN). Furthermore, VPNusuallyimplementedwiththeaidofIP security (IPSec). Thiscanbeconsideredasthestandardway forVPNimplementation.TheIPSecandVPNhaverevised

andwellestablishedinthiswaytoprovidetherobustsecurity standardwithacceptable dataconfidentiality, authentication, andaccesscontrolregardlessofthetransmission medium. WhiletheVPNwouldsecureit,"asshowninFigure4.1

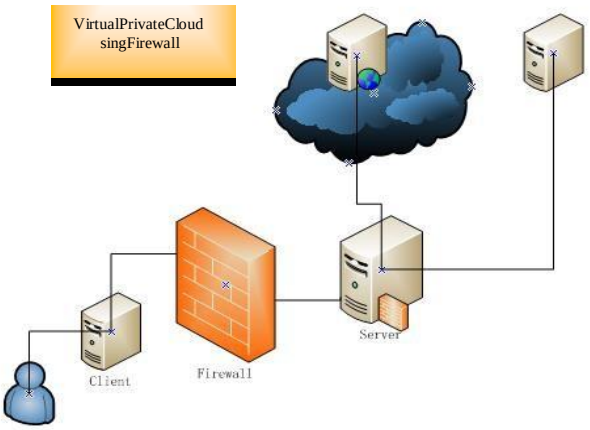

Fig4.1ExistingArchitecture

Firewallisusedinconjunction withVPN.Thefirewallisa packetfiltering thatstands between theinternalnetworkand theworldoutside. Thereasonfortheusageof firewalls with theVPNisbecausefirewallhavebeenemployed onlarge publicnetworksformanyyearsandareagreatstartingplace in thedevelopmentofasecuritystrategyandcloudcomputing canberegardedas publicnetwork.

V. PROBLEMIDENTIFIED

Cloudserviceprovidershavetoensurethattheirinfrastructure shouldbesecureandtheiruserpersonalinformation,dataand otherhardwareandsoftwareresources shouldbesecure enough. We considerin our research, Cloud users will requireddifferent security prospect,wherethey ensureasafe andprivileged accesstotheirdatawhich islocatedatthe remotelocationsinPublicCloud.Bytheserequirements, the security ofthecloudandthecorresponding policiesare designed usingdifferent proposed models having physical networkingcomponents (i.e.Firewall)whichiscostly mechanism.ButVirtualization makesCloudhostsandVM's muchprotectiveforaccessingofinformation anddata.The main advantagesof the virtualmachine implementation, wherealltherequiredDatacenteroperationsarenotphysical innature andagroup ofvirtual serversisused.Howeverthere aresomelimitationstothevirtualmachineconceptaswell andtheattacks onthevirtualdatacenter (VDC).TheCloud environment isdynamicinnatureandtheaccessing operation between theremoteVDC andtheuserarepronetofrequentupdates.Inthisprocessanyattacker canchangethereadand writeoperationsandthusa strictimplementationpolicyis required.

VI. PROPOSEDARCHITECHTURE

According tothecurrentsecurity system asshowninbelow givenfigure4.1,whichisusedthefollowing Firewall mechanismwithVPNincloudwhichprovidegreatsecurity butitisstillacostlymechanism whenwerequireprivacyof dataforvery shorttimeperiod andwhenthedata isalready existinpubliccloud.SoproposedarchitectureshownFig5.1

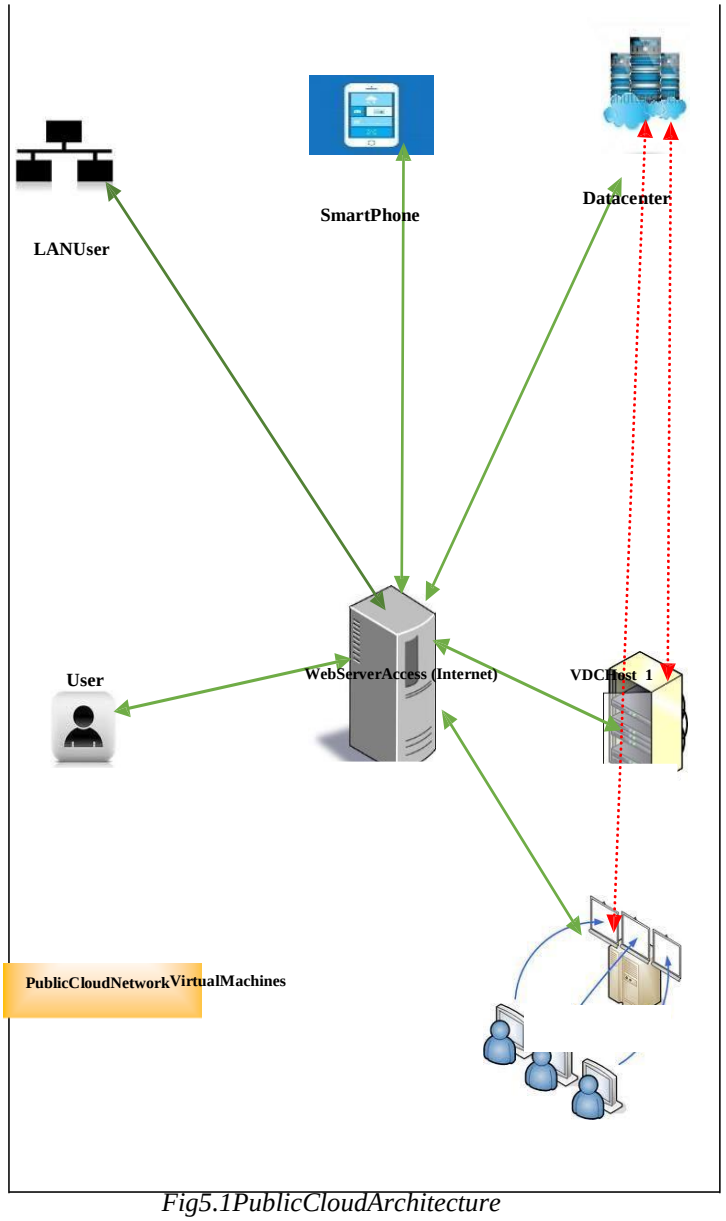

Fig5.1PublicCloudArchitecture

Thefig5.1shows Differenttype ofusershareacommon public cloudwherenormaluser,LANuser, Smart phone user theyalleasilygetaccessing toalldatacenterexistsinpublic cloudusingwebserveraccess.Datacenter alsoAccessusing WSA (thereareinsideonepubliccloudno.ofdatacenterare availableatdifferent locationandeachofthemhavingno.of hostaccordingtocapacityofdatacenter.Eachoftheavailable hosthaving virtualmachines)andthey allconnected through greenarrow.Theproposedinterfacing applytoparticularDC tospecific HostandHosttospecificuserusing IPAddress interfacing. Allspecific registered usercanaccessthatDCfor short period. Also Serverenable access and deny Configuration toallnodes.Whenenterprisehaving10to100 workstationdoesn'thireaprivatecloud,sotheirdataresides inpubliccloudbut thatdataalsorequired privacysometime theycan'taffordahardwaremechanismforshortperiodso this paperproposeda implementationaspectaboutcritical data privacy in proposed Architecture are simulated on OPNETtoolSimulator.

VII. OPNETSIMULATOR

OPNETisavastsoftware packagewithanextensivesetof featuresdesignedtosupportgeneralnetworkmodelingandto providespecificsupportforparticular typesofnetwork simulationprojects.OPNETprovidesaflexible,high-level programming languagewithextensivesupportfor communications anddistributedsystems.Thisenvironment allowsrealisticmodelingofallcommunications protocols, algorithms,andtransmissiontechnologies. OPNETsupports modelspecification withanumberoftoolsoreditorsthat capturethecharacteristics ofamodeledsystem'sbehavior. Becauseitisbased onasuiteofeditorsthataddress different aspects ofamodel,OPNETisabletofferspecific capabilities toaddressthediverseissuesencounteredin networksanddistributedsystems[4].

A. HierarchicalArchitecture

Topresentthemodel developer with anintuitiveinterface,the model-specificationeditors are organizedinan essentially hierarchicalfashion.Modelspecifications performedinthe ProjectEditorrelyonelementsspecifiedintheNodeEditor; in turn, whenworkinginthe Node Editor, the developer Makesuseofmodels definedintheProcess Editor.The remainingeditors are usedtodefine various data models; packetformateditor,linkmodeleditor,etc.[4] .
TheNetwork,Node,andProcessmodelingEnvironments are sometimesreferredtoasthemodelingdomainsofOPNET.

A. NetworkDomain

TheNetworkDomain'sroleistodefinethetopology ofa communication network. The communicatingentitiesare called*nodes.*Anetworkmodelmayuseofanynumberof nodemodels.Modelers candeveloptheirownlibrary of customizednodemodels, implementinganyfunctionalitythey require[4].

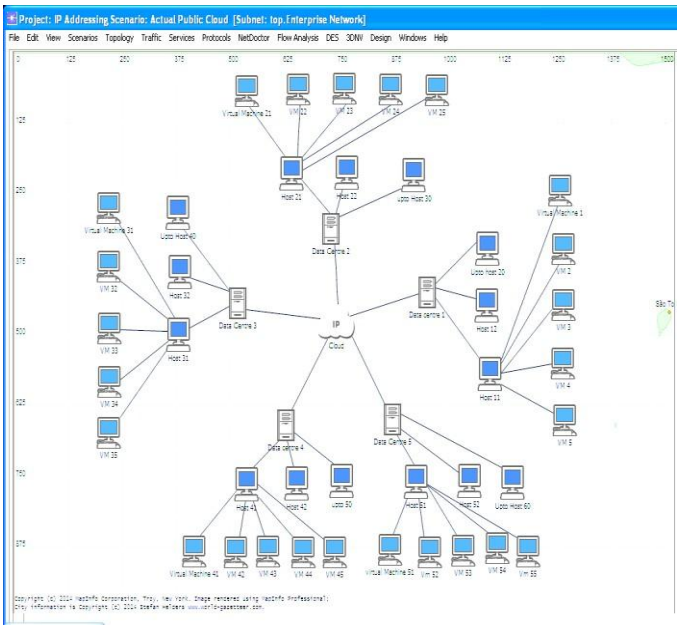

Fig6.1NetworkDomain

B. NodeDomain

The Node Domain provides for the modeling of communicationdevicesthatcanbedeployedand interconnected atthenetworklevel.Nodemodelsare developed intheNodeEditorandareexpressed intermsof smallerbuilding blockscalled*modules*. Somemodules Offer capabilitythat issubstantiallypredefinedand can only be configuredthroughasetofbuilt-in parameters. Theseinclude various transmittersand receivers allowing a node to be attachedtocommunicationlinksinthenetworkdomain.*[4]*.

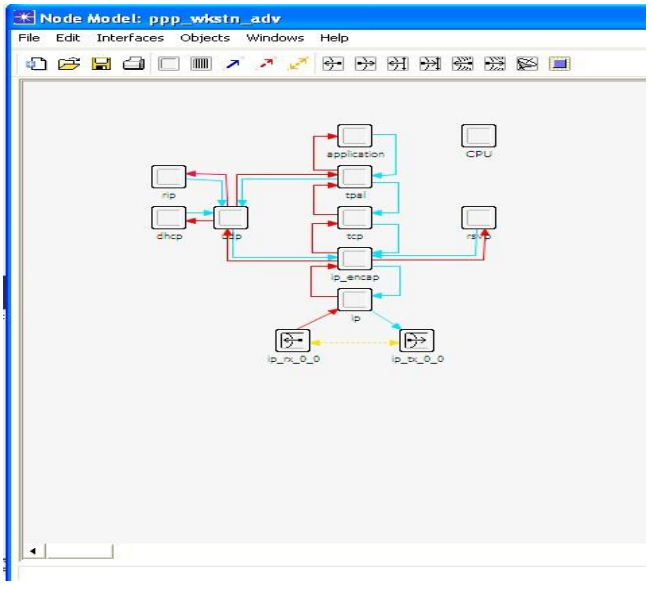

Fig6.2NodeDomain

C. ProcessDomain

Processmodels aredevelopedusingtheProcess Editor. Processor modules areuserprogrammableelements thatare keyelementsofcommunication nodes.ProcessesinOPNET aredesignedtorespondtointerrupts and/orinvocations. Interruptstypicallycorrespondto eventssuchas messages arriving,timersexpiring, resourcesbeingreleased, orstate changes inothermodules.Processes areextendedbya languagecalledProto-C.Proto-Cmodelsallow actionstobe specifiedatvarious pointsinthefinitestatemachine. Since Proto-Cisfocusedonmodeling protocols andalgorithms,it provides anextensive libraryofhighlevelcommand called KernelProcedures andthegeneralfacilitiesoftheCorC++ programminglanguage[4].

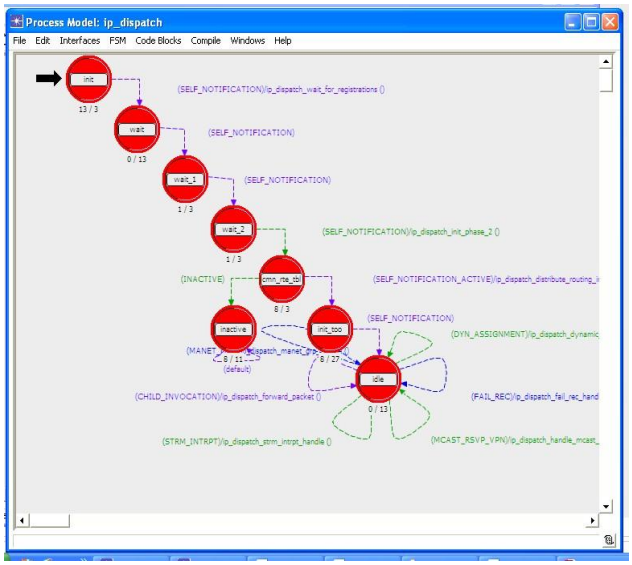

Fig6.3ProcessDomain

VIII. CONCLUSION

This paper describes publiccloudwhich isonebasedonthe standardcloudcomputingmodel,inwhichaserviceprovider Makesresources,suchas applicationsandstorage,availableto thegeneralpublicovertheInternet[3].Publiccloudismade upof severalnodessituatedindeferentgeographiclocation.In thisworkweimplementedandsimulation aspectoneofthe mostpracticalmethods inOPNETsimulatoranditworked properly. Wearealsoworking onasecureanduserfriendly methodtoimproveprivacyandaccessibility ofpubliccloud userbyavoidingFirewall.

IX. REFERENCES

[1]. ManeeshaSharma,HimaniBansal,AmitKumarSharma,"Cloud Computing:DifferentApproach&SecurityChallenge"InternationalJournal ofSoftComputingandEngineering (IJSCE)ISSN:2231-2307,Volume-2, Issue-1, March2012 421

[2]. SiddeeqY.Ameen,ShaymaWailNourildean,"FirewallandVPN Investigation onCloud Computing Performance"inIJCSES Vol.5, No.2, April2014.

[3]. M. Rouse,Public cloud,http://searchcloudcomputing,techtarget.com/definition/public-cloud,2012

[4] S. SaedRezaie, S. Amir Hoseini, H. Taheri, "Implementation of ExtensibleAuthenticationProtocol inOPNET Modeler"Departmentof Electrical Engineering,AmirkabirUniversity,Tehran,Iran.

[5] NehaUpadhyay,AjayKumar,"AFrameworkbasedonAuthentication andAuthorization toensure Secure DataStorage inCloud"International JournalofComputerApplications(0975– 8887)Volume 90–No 15, March 2014 .

[6] RichardChow,Philippe Golle,MarkusJakobsson,RyusukeMasuoka, JesusMolina,"ControllingDatainthe Cloud:Outsourcing Computation without OutsourcingControl".

[7] *KevinHamlen"*SecurityIssuesforCloudComputing"International JournalofInformationSecurityandPrivacy,4(2),39-51,April-June 2010.

[8] ChaoYANG,JianfengMA,XuewenDONG,"A New EvaluationModel forSecurity Protocols"Journalofcommunications,vol.6,no.6, September 2011

[9]MangalNathTiwari,KamalendraKumarGautam,Dr RakeshKumar Katare"AnalysisofPublicCloud LoadBalancing usingPartitioning MethodandGameTheory"Volume4,Issue2,February2014ISSN: 2277128X

[10] WindowsSecurity 2010