E-ISSN: 2395-1702 P-ISSN: 2395-0382
Volume 02- Issue 12-, pp-36-48

Research Paper Open Access

A SURVEY ON SECURITY ISSUES IN DISTRIBUTED CLOUD COMPUTING.

Sharmila.P[1], Dr.Danapaquiame.N[2], Mr.Rajadurai.R[3]

M. Tech Student, Associate professor, Assistant professor
Department of Computer Science & Engineering,
Sri Manakula Vinayagar Engineering College,
Sharmiksd93@gmail.com,n.danapaquiame@gmail.com,king8153@gmail.com.

Abstract:

Distributed computing is an approach to expand the limit or include capacities progressively without putting resources into new foundation, preparing new work force, or authorizing new programming. It amplifies Information Technology's (IT) existing capacities. In the most recent couple of years, distributed computing has developed from being a promising business idea to one of the quickly developing fragments of the IT business. Yet, as more data on people and organizations are put in the cloud, concerns are starting to become about exactly how safe a domain it is. In spite of all the build-up encompassing the cloud, undertaking clients are still hesitant to convey their business in the cloud. Security is one of the real issues which decreases the development of distributed computing and entanglements with information protection and information insurance keep on plaguing the market. The approach of a propelled model ought not to consult with the required functionalities and capacities display in the present model. Another model focusing at enhancing elements of a current model must not hazard or debilitate other essential elements of the present model. The design of cloud postures such a danger to the security of the current advances when sent in a cloud domain. Cloud benefit clients should be cautious in comprehension the dangers of information breaks in this new environment. In this paper, a study of the distinctive security hazards that represent a danger to the cloud is exhibited. This paper is a study more particular to the distinctive security issues that has exuded because of the way of the administration conveyance models of a distributed computing framework.

Introduction:

Today Small and Medium Business (SMB) organizations are progressively understanding that just by taking advantage of the cloud they can increase quick access to best business applications or definitely support their foundation assets, all at irrelevant cost. Gartner (Jay Heiser, 2009) characterizes distributed computing (Stanojevi et al., 2008; Vaquero et al., 2009; Weiss, 2007; Why man, 2008; Boss et al., 2009) as "a style of registering where enormously versatile IT-empowered abilities are conveyed 'as an administration' to outside clients utilizing Internet advances". Cloud suppliers right now appreciate a significant open door in the commercial centre. The suppliers must guarantee that they get the security perspectives ideal, for they are the ones who will bear the duty if things turn out badly. The cloud offers a few

advantages like quick organization, pay-for-utilize, bring down costs, adaptability, fast provisioning, fast versatility, omnipresent system get to, more prominent strength, hypervisor protection against system assaults, minimal effort fiasco recuperation and information stockpiling arrangements, on-request security controls, ongoing detection of framework altering and fast re-constitution of administrations. While the cloud offers these focal points, until a portion of the dangers are better comprehended, a large number of the real players will be enticed to keep down (Viega, 2009). As per a late IDCI review, 74% of IT officials and CIO's referred to security as the top test keeping their reception of the cloud administrations demonstrate (Clavister, 2009). Investigators' assess that inside the following five years, the worldwide market for distributed computing will develop to $95 billion and that 12% of the overall programming business sector will move to the cloud in that period.

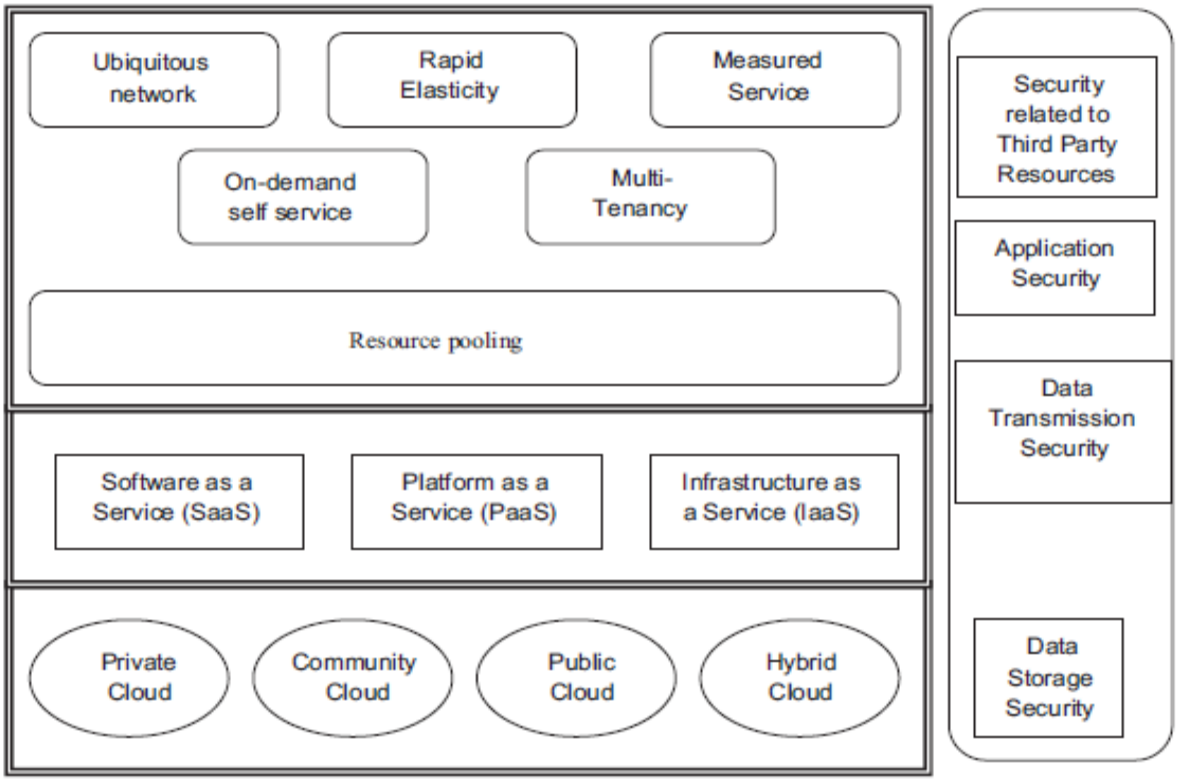

Fig. 1. Complexity of security in cloud environment.

To understand this gigantic potential, business must address the security questions raised by this new processing model (BNA, 2009). Distributed computing moves the application programming and databases to the substantial server farms, where the administration of the information and administrations are not reliable. This one of a kind quality, notwithstanding, postures numerous new security challenges (Cong Wang et al., 2009). These difficulties incorporate however not restricted to openness vulnerabilities, virtualization vulnerabilities, web application vulnerabilities, for example, SQL (Structured Query Language) infusion and

cross-webpage scripting, physical get to issues, protection and control issues emerging from outsiders having physical control of information, issues identified with personality and accreditation administration, issues identified with information confirmation, altering, honesty, classification, information misfortune and robbery, issues identified with validation of the respondent gadget or gadgets and IP caricaturing. In spite of the fact that distributed computing is focused to give better utilization of assets utilizing virtualization procedures and to take up a great part of the work stack from the customer, it is loaded with security dangers (Seccombe et al., 2009). The many-sided quality of security dangers in a total cloud environment.

Related work:

Distributed computing uses three conveyance models by which distinctive sorts of administrations are conveyed to the end client. The three conveyance models are the SaaS, PaaS and IaaS which give foundation assets, application stage and programming as administrations to the shopper. These administration models likewise put an alternate level of security prerequisite in the cloud environment. IaaS is the establishment of all cloud administrations, with PaaS based upon it and SaaS thus based upon it. Generally as abilities are acquired, so are the data security issues and dangers. There are noteworthy exchange offs to every model in the terms of incorporated components, unpredictability versus extensibility and security. On the off chance that the cloud benefit supplier deals with just the security at the lower part of the security engineering, the purchasers turn out to be more in charge of actualizing and dealing with the security abilities.

A late study by Cloud Security Alliance (CSA) and IEEE demonstrates that endeavors crosswise over segments are energetic to embrace distributed computing however that security are required both to quicken cloud selection on a wide scale and to react to administrative drivers. It additionally points of interest that distributed computing is moldings the eventual fate of IT however the nonattendance of a consistence domain is having sensational effect on distributed computing development. Associations utilizing distributed computing as an administration framework, basically jump at the chance to analyse the security and classification issues for their business basic heartless applications.

The automated data placement for geo-distributed cloud services Applications make use of Volley by logging data to the Cosmos distributed storage system. The administrator must also supply some inputs, such as a cost and capacity model for the data centres. The Volley sys-tem frequently runs new analysis jobs over these logs, and computes migration decisions. Application-specific jobs then feed these migration decisions into application-specific data migration mechanisms. We focus on improving latency to users and not bandwidth to users. Incorporating band-width would require both specifying a desired latency. But bandwidth trade off and a model for bandwidth between arbitrary points in the Internet. Network aware resource allocation in distributed clouds. The cloud automation software computes a

placement of VMs for the user request. The output contains a mapping of VMs to the physical Resources. To perform its assignment function, the cloud automation software interacts with the network management system (NMS) and the local cloud management system (CMS) in the data centres. NMS provides a view of the current network between the data centres. Not Support all resources at mobiles. Towards predictable data canter networks. In a distributed cloud environment, datacenters are placed at multiple geographic locations. The first step in servicing a user request is selection of the right datacenters to place the VMs. A single datacenter may not have enough capacity to host all the VMs of the user. Even if there is enough capacity a data center, the user may not want to have all the VMs hosted in one data center. Results compared to random approach and greedy algorithm. Reduce the possibility of tasks running on distant pairs of virtual machines which will lead to large communication. Faster and simpler algorithms for multi-commodity flow and other fractional packing problems. Reduce the possibility of tasks running on distant pairs of virtual machines which will lead to large communication latencies and hence delay overall completion times for the user request. Further, using a simple pricing model, we find that the abstractions can reduce tenant costs by up to 74% .while maintaining provider revenue neutrality. Distributed data placement to minimize communication costs via graph partitioning. In the second setting, we implemented our own distributed query processor on the top of multiple MySQL instances running on a cluster where predicate evaluations are pushed on to the individual nodes and data is shipped to a single node for perform the final steps. For fault tolerance, load balancing and availability, these systems usually keep several copies of each data item. Query span directly impacts the total communication that must be performed to execute a query. This is clearly a concern in distributed setups. We formally define the problem that we study, and draw connections to some closely related prior work on graph algorithms. However, ensuring the security of corporate information in the ""cloud"" is troublesome, if not unthinkable, as they give distinctive administrations like SaaS, PaaS, and IaaS. Every administration has its own security issues (Kandukuri et al., 2009). SaaS is a product sending model where applications are remotely facilitated by the application or administration supplier and made accessible to clients on request, over the Internet.PaaS is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development lifecycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the ‘‘view’’ of the developers. The dark side of PaaS is that, these advantages itself can be helpful for a hacker to leverage the PaaS cloud infrastructure for malware command and control and go behind IaaS applications. IaaS completely changes the way developers deploy their applications. Instead of spending big with their own data centres or managed hosting companies or collocation services and then hiring operations staff to

get it going, they can just go to Amazon Web Services or one of the other IaaS providers, get a virtual server running in minutes and pay only for the resources they use. With cloud brokers like Right scale, enStratus, etc., they could easily grow big without worrying about things like scaling and additional security. In short, IaaS and other associated services have enabled start-up and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but ‘‘out of the box’’ IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.In a SaaS model of a cloud environment, the consumers use the applications provided by the SaaS and process their business data. But in this scenario, the customer does not know where the data is getting stored. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in much enterprise architecture (Softlayer, 2009). For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there’s also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing reliability to the customer on the location of the data of the consumer.

Data integrity is one of the most critical elements in any system. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications. In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manger. Each application in the distributed system should be able to participate in the global transaction via a resource manager. This can be achieved using a 2-phase commit protocol as per XA standard.The following key security elements should be carefully considered part of the SaaS application development and deployment process: Data security, Network security, Data locality, Data integrity, Data segregation, Data access, Authentication and authorization.

Data security:

In a traditional on premise application deployment model, the touchy data of each enterprise continue store side within the undertaking boundary and is subject to its physical, logical and work force security and access control policies. However, in the SaaS model, the enterprise data is stored outside the enterprise limit, at the Saa Svendorend. Consequently, the SaaSvendor must adopted additional security checks to ensure data security and anticipate breaches

due to security vulner abilities in the application on the other hand through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data.

In cloud vendors such as Amazon, the Elastic Compute Cloud (EC2) administrators don'tha veaccess to customer instances what's more, cannot login to the GuestOS.EC2Administratorswitha business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain accesstoahost.All. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, clients can encrypt their data before it is uploaded toAmazonS3,so that it is not accessed or tampered with by any unauthorized party. Malignant users can exploit weaknesses in the data security demonstrate to gaining authorized access to data.

Data locality:

In a Saa Smodelofa cloud environment, the consumers use the applications provided by the SaaSand process their business data. Be that as it may, in this scenario, the customer does not know where the datais getting stored.In many accesses, this can be anissue.Dueto consistence and data privacy laws in various countries, locality of information is of most import ancient many enterprise architecture (Softlayer, 2009). Forexample, inmany EUandSouthAmerica nations, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of nearby laws, there's also the question of whose jurisdiction the data falls under when an investigation occurs. A secure SaaSmodel must be capable of providing reliability to the customer on the area of the data of the consumer.

In a SaaS model of a cloud environment, the consumers use the applications provided by the SaaS and process their business data. Be that as it may, in this scenario, the customer does not know where the data is getting stored.Inmanyacases,thiscanbeanissue.Dueto consistence and data privacy laws in various countries, locality of information is of utmost import an ceinmanyenterprisearchitecture (Soft layer, 2009). For example, in many EUandSouthAmerica nations, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of neighborhood laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaSmodel must becapableofprovidingreliabilitytothecustome ronthe area of the data of the consumer. Not yet mature and don't many vendors have implemented these. Generally SaaS vendors expose their web services APIs without any bolster for transactions. Also, each SaaS application may have diverse levels of availability and SLA(service-level agreement), which further complicates management of transactions and data respectability across multiple SaaS applications. The lack of integrity controls at the data level (or in the case of existing

Integrity controls, by passing the application logic to get to the data base directly) could result in profound problems. Engineer's and develops presented to approach this danger cautiously, making sure they don't compromise databases 'integrity in their zealot move to cloud computing.

Data segregation

Multi-tenure is one of the major characteristics of cloud figuring. A saresult of multi tenancy multiple users can store their data using the applications provided by SaaS. In such a circumstance, data of various users will reside at the same location. Interruption of data of one user by another becomes possible.inthis environment. This intrusion can be done thre by hacking through the loopholes in the application or by injecting client code in to the SaaS system. A client can write a masked code and infuse in to the application. If the application executes this code without verification, then there is a high potential of intrusion into other's data. A SaaS model should therefore ensure clear limit for accuser's data. The boundary must been sure not just at the physical level but also at the application level. The benefit should be intelligent enough to segregate the data from diverse clients. A malicious user can use application vulnerabilities to hand-create parameters that by pass security checks and access sensitive information of other tenants.

Information access issue is mainly related to security policies given to the users while accessing the data. In atypical situation, a small business organization can use a cloud provided by some thre provider for carrying out its business processes. This organization will have it so insecurity policies based on which each Employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of information. These security policies must be adhere by the cloud to stay away from intrusion of data by un authorized users (Blaze etal., 1999; KormannndRubin, 2000; Bowersetal., 2008). The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization. The model must also be able to give organization a boundary within the cloud because multiple organization will be deploying their business processes within a single cloud environment.

Data confidentiality issue:

The definition alb orders of cloud computing are much debated today. Cloud computing involves the sharing or storage by users of their own information on remote servers owned cooperated by others and accesses through the Internet or other connections. Cloud computing services exist in many variations, including data capacity sites, video sites, tax preparations it's, personal heal thre cord websites and many more. The entire content so fuser's capacity device may be stored with a single cloud provider or with numerous cloud providers. Whenever an individual, a business, a government agency, or any other entity's hares information in the cloud, privacy or confidentiality questionsarise.Some of the discoveries related to the confidentiality issues are:

1. Cloud computing has significant implications for the privacy of an individual information as well as for the confidentiality of business and government al information.

2. A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud supplier.

3.For some types of information and some categories of cloud registering users, privacy and confidentiality rights, obligations, and

status may change when a user discloses information to a cloud provider.

4. Disclosure and remotes to rage may have adverse consequences for the legal status of protections for personal or business data.

5. The location of information in the cloud may have significant impacts on the privacy and confidentiality protections of data and on the privacy obligations of those who handle or store the information.

6. Information in the cloud may have more than one legal area at the same time with differing legal consequences.

7. Laws could oblige cloud provider to examine user records for prove of criminal activity and other matters.

8. Legal uncertainties make it difficult to assess the status of data in the cloud as well as the privacy and confidentiality protections available to users.

Webapplicationsecurity SaaS is software deployedovertheinternetand/orisdeployed to runbehindafirewallinlocalareanetworkorpersonal PC. ThekeycharacteristicsincludeNetwork basedaccess to, andmanagementof,commerciallyavailablesoftwareand overseeing activitiesfromcentrallocationsratherthanat each client's site,enablingcustomerstoaccessapplication remotely viatheWeb.SaaSapplicationdevelopmentmay usevarious sorts of softwarecomponentsandframeworks.These tools can diminish time-marketandthecostofconvertingatraditionalon - preface softwareproductorbuildinganddeployingane wSaaS arrangement. Examplesincludecomponentsforsubscription management, gridcomputingsoftware,webapplicationframeworksand finish SaaSplatformproducts.One of the "must-have'' necessities foraSaaSapplicationisthatithastobeusedand overseen overtheweb(inabrowser)(Michal Zalewski, 2009).

Thesoftwarewhichisprovidedasaserviceresidesinthecloud without tyingupwiththeactualusers.Thisallowsimprovising the softwarewithoutinconveniencingtheuser. Securityholesin the webapplicationsthuscreateavulnerabilitytotheSaaS application. Inthisscenario,thevulnerabilitycanpotentially have impeding impactonallofthecustomersusingthecloud.The challenge withSaaSsecurityisnotanydifferentthanwithany different webapplicationtechnology,howeveroneofthe problems is that traditionalnetworksecuritysolutionssuchasnetwork firewalls, networkintrusiondetectionandprevention systems (IDS&IPS),donatedequitablyaddresstheproblem.Web applications introducenewsecurityriskthatcannoteffectivelybe defendedagainstatthenetworklevel,anddorequire application leveldefences.

Databreaches:

Since datafromvarioususersandbusinessorganizationslie together inacloudenvironment,breachingintothecloud environment willpotentiallyattackthedataofalltheusers.Th

us the cloudbecomesahighvaluetarget(Bernard Golden, 2009; Kaufman, 2009). IntheVerizonBusinessbreachreportblog(Russ Cooper, 2008) ithasbeenstatedthatexternalcriminalspouseth e most prominent threat(73%),butachievetheleastimpact(30,00 0 traded off records),resultinginaPseudoRiskScoreof 67,500. Insidereposetheleastthreat(18%),andachievet he most prominent impact(375,000compromisedrecords),resulti ngina Pseudo RiskScoreof67,500.Partnersaremiddleinboth (73.39% also, 187,500)resultinginaPseudoRiskScoreof73,1 25.Though SaaS advocatesclaimthatSaaSproviderscanprovide better security tocustomers'datathanbyconventionalmeans,I nsiders still haveaccesstothedatabutitisjustthattheyareacc essingit in adifferentway. Insidersdonothavedirectaccesstodatabases, however, itdoesn't reducetheriskofinsiderbreacheswhic hcanbe a huge impactonthesecurity.TheSaaSproviders'empl oyees have accesstoalotmoreinformationandasingleincid entcould uncover informationfrommanycustomers.SaaSprovid ersmustbe agreeable withPCIDSS(PaymentCardIndustry—Data Security Guidelines) (PCI DSS,2009) inordertohostmerchantsthatmust go along withPCIDSS.

Table 1
Security challenges in identity management [IdM] and sign-on process.

IdM and SSO model	Advantages	Disadvantages	Security challenges
Independent IdM stack	• Easy to implement • No separate integration with enterprise directory	• The users need to remember separate credentials for each SaaS application	• The IdM stack should be highly configurable to facilitate compliance with enterprise policies; e.g., password strength, etc.
Credential synchroniza-tion	• Users do not need to remember multiple passwords	• Requires integration with enterprise directory • Has higher security risk value due to transmissions of user credentials outside enterprise perimeter	• The SaaS vendor needs to ensure security of the credentials during transit and storage and prevent their leakage
Federated IdM	• Users do not need to remember multiple passwords • No separate integration with enterprise directory • Low security risk value as compared to credential synch	• Relatively more complex to implement	• The SaaS vendor and tenants need to ensure that proper trust relationships and validations are established to ensure secure federation of user identities

SecurityissuesinIaaS:

WithIaaSthedeveloperhasbettercontrol over the securityas long asthereisnosecurityholeinthevirtualizationma

nager. Likewise, thoughinthevirtualmachinesmightbeabletoaddress these issuesbutinpracticethereareplentyofsecurityproblems (Attanasio, 1973;Gajeketal.,2007). Theotherfactoristhe unwavering quality ofthedatathatisstoredwithintheprovider's equipment. Duetothegrowingvirtualizationof'everything' in data society,retainingthe ultimate controloverdatato the ownerofdataregardlessofitsphysicallocation willbecomea theme ofutmostinterest.Toachievemaximumtrustandsecurity on acloudresource,severaltechniqueswouldhave tobeapplied (Descher etal.,2009).

The securityresponsibilitiesofboththeproviderand theshopper greatlydifferbetweencloudservicemodels.Amazon's Flexible ComputeCloud(EC2)(Amazon, 2010) infrastructureasa benefit offering,asanexample,includesvendorresponsibilityfor security uptothehypervisor,meaningtheycanonlyaddress security controlssuchasphysicalsecurity,environmental security, andvirtualizationsecurity.Theconsumer,inturn,is capable forthesecuritycontrolsthatrelatetotheITsystem counting theOS,applicationsanddata(Seccombe etal.,2009).

SecurityissuesinPaaS:

In PaaS,theprovidermightgivesomecontroltothe peopleto fabricate applicationsontopoftheplatform.Butanysecurity below the applicationlevelsuchashostandnetworkintrusion counteractive action willstillbeinthescopeoftheproviderandthe supplier hastofferstrongassurancesthatthedataremains out of reach betweenapplications.PaaSisintendedtoenable engineers tobuildtheirownapplicationsontopofthe platform.

As areresulttittendstobemoreextensiblethanSaaS, attheexpense of client readyfeatures.Thistradeofextendstosecurity highlights andcapabilities,wherethebuilt-in capabilitiesareless finish, butthereIsmoreflexibility to layer on additional security. Applications sufficientlycomplextoleverageanEnterprise Benefit Bus(ESB)needtosecuretheESBdirectly,leveraginga convention suchasWebService(WS)Security(Oracle, 2009). The capacity tosegment ESBsisnotavailableinPaaSenvironments. Measurements shouldbeinplacetoassesstheeffectivenessofthe application securityprograms.Amongthedirectapplication,security specificmetricsavailablearevulnerabilityscoresand fixcoverage.Thesemetricscanindicatethequality of application coding.Attentionshouldbepaidtohowmalicious performers reacttonewcloudapplicationarchitecturesthat obscure application componentsfromtheirscrutiny.Hackers arelikely to assault visiblecode,includingbutnotlimitedtocoderunningin client

context.Theyarelikelytoattacktheinfrastructureand perform extensiveblackboxtesting.Thevulnerabilities ofcloud are notonlyassociatedwiththewebapplicationsbut also vulnerabilities associatedwiththemachine-to-machineService- Arranged Architecture(SOA)applications,whichareincreasingly being deployedinthecloud.

Currentsecuritysolutions:

There areseveralresearchworkshappening inthearea of cloud security.Severalgroupsandorganizationareinretested in creating securitysolutionsandstandardsforthecloud.The Cloud SecurityAlliance(CSA)isgatheringsolutionproviders,non- benefits andindividualtoenterintodiscussionaboutthecurrent furthermore, futurebestpracticesforinformationassuranceinthecloud ("Cloud SecurityAlliance(CSA)—security bestpracticesforcloud figuring," 2009(Cloud SecurityAlliance,2010a,2010b)). The Cloud Standardswebsiteiscollectingandcoordinating information about cloud relatedstandardsunderdevelopmentbythe bunches.
TheOpenWebApplicationSecurityProject(OWASP) keeps up listoftopvulnerabilitiestocloud-basedorSaaSmodels which isupdatedasthethreatlandscapechanges("OWASP", 2010).
TheOpenGridForumpublishesdocumentstocontaining security andinfrastructuralspecificationsandinformationfor lattice computingdevelopersandresearchers ("Open GridForum", 2010).

Conclusion :

As describedinthepaper, though there are extreme advantages inusingacloud-basedsystem,thereareyetmanypractical issues whichhavetobesolved.Cloudcomputingisa troublesome technologywithprofoundimplicationsnotonly for Web servicesbutalsofortheITsectorasawhole.Still, several exceptional issuesexist,particularlyrelatedtoservice-level assertions (SLA),securityandprivacy, andpowerefficiency.Asport rayed inthepaper,currentlysecurityhaslotoflooseends which scarestopotentialusers.Untilapropersecurity module isnotinplace,potentialuserswillnotbeabletoleverage the advantagesofthistechnology.Thissecuritymoduleshould cook toalltheissuesarisingfromalldirectionsofthecloud.Every component inthecloudshouldbe analysedatthemacroandmicro level andanintegratedsolutionmustbedesignedanddeployed in thecloudtoattractandenthral thepotentialconsumers.Until at that point, cloudenvironmentwillremaincloudy An integratedsecuritymodeltargetingdifferentlevelsof security ofdataforatypicalcloudinfrastructureisunder explore.
Thismodelismeanttobemoredynamicandlocalized in nature.Myresearchquestionswillcentreonapplicationand information securityoverthecloud,andintendtodevelopafr amework by whichthesecuritymethodologyvariesdynamicallyfromone exchange/communicationtoanother.Oneofthepiecesofthe structure

mightbefocusedonprovidingdatasecuritybystoring also, accessingdatabasedonmetadatainformation.Thiswould be morelikestoringrelateddataindifferentlocationsbasedon the meta-datainformationwhichwouldmakeinformation significant ifamaliciousintentuserrecoversit.Keepingthis as a coreconceptdoing researchonaframeworkwhichwould be practical.Anotherpieceoftheframeworkwouldbe providing 'Security asaService'totheapplicationsbyprovidingsecurityas a solitary multi-tierbasedontheapplication'srequirement also, additiontoit,thetiersareenabledtochangedynamically making thesecuritysystem-lesspredictable.Thisresearch is based ontheconceptualizationofthecloudsecuritybasedonreal world securitysystemwhereinsecuritydependsonthenecessity andassetvalueofanindividualororganization.

References

1. Amazon.AmazonElasticComputeCloud(EC2),2010 /http://www.amazon.com ec2/S [accessed: 10December2009].
2. AttanasioCR.Virtualmachinesanddatasecurity.In:Proceedingsoftheworkshopon virtualcomputersystems.NewYork,NY,USA: ACM;1973.p.206–9.
3. AugerR.SQLInjection,2009 /http://projects.webappsec.org/SQL-InjectionS [accessed on:15February2010].
4. BastaA,HaltonW.Computersecurityandpenetrationtesting.DelmarCengageLearning 2007.
5. BernardGolden.Definingprivateclouds,2009/ http://www.cio.com/article/492695/Defining_Private_Clouds_Part_OneS [accessed on:11January2010].
6. BerreAJ,RomanD,LandreE,HeuvelWVD,SkarLA,UdnaesM,etal.Towardsbestpracticesindesigningforthecloud.In:Proceedingsofthe24thACMSIGPLAN conferencecompanionononobjectorientedprogrammingsystemslanguages Andapplications,Orlando,Florida,USA,2009, p.697–8.
7. BlazeM,FeigenbaumJ,loannidisJ,KeromytisAD.Theroleoftrustmanagementindistributedsystemssecurity,secureInternetprogramming,issuesformobileand distributedobjects.Berlin:Springer-Verlag;1999.p.185–210.
8. BNA.Privacy&securitylawreport,8PVLR10, 03/09/2009.Copyright2009byThe
9. Bureau ofNationalAffairs,Inc.(800-372-1033),2009 /http://www.bna.comS[accessed on:2November2009].
10. Boss G,MalladiP,QuanD,LegregniL,HallH.Cloud computing,2009,p.4/http://www.ibm.com/developerswork/websphere/zones/hipods/library.htmlS[accessedon:18October2009].