SURVEY ON THREE COMPONENTS OF CLOUD COMPUTING: SAFEKEEPING, EXPLORATION AND IMMINENT SCOPE

D.Saritha, *Asst. Professor, Dept. of BCA, Bon Secours College for Women, Thanjavur.*
E-mail:saridhana@gmail.com
K.Sumathi, *Asst. Professor, Dept. of BCA, Bon Secours College for Women, Thanjavur.*
E-mail:sumathikaruppaiyan2491@gmail.com

ABSTRACT

Cloud computing refers to the design that provides computing service through internet by pay as you go model in order to provide access to networks, storage, servers, services and applications, without tangibly procuring them. So it reduces consuming expenditure cost and time for organizations. Cloud computing is an utterly internet reliant expertise in which client data used to store and maintain the data in the cloud centers such as like Google, Amazon, Salesforce.com and Microsoft etc. Inadequate control over the data leads to the occurance of various security issues and threats such as data leakage, insecure interface, sharing of resources, data availability and Inside attacks. Some research challenges are there for adopting cloud computing, such as well managed service level agreement (SLA), privacy, interoperability and reliability. Now a days the enterprise is looking towards cloud computing to enhance their on-premises, transportation, but most cannot come up with the money for the risk of compromise the protection of their applications and data. This manuscript describes the what exactly the cloud computing is,cloud models and present security issues . In this manuscript, we present the factors which leads to the emergence of cloud computing, when compared to the traditional one.

Keywords: Cloud Computing, Networking, Security problem, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform.

I. INTRODUCTION

Cloud computing surfaces as a hot theme from 2007 due to its ability of offering dynamic IT infrastructures, QoS guaranteed computing backgrounds and configurable platform services. With web 2.0 has potential to change the face of Entire computing diligence and may signal of a return to the age of monopolization with data application and processing influences with the user having online utility interface. Amazon, Google, IBM is with the cloud computing revolution. This permits the originators to focus on the business value moderately on the starting budget. The clients of profit-making cloud provides the rent computing power (virtual machines) or storage space (virtual space) energetically, according to the needs of their business. With the achievement of this technology, users are allowed to access heavy applications via lightweight, portable devices such as mobile phones, PCs and PDAs.

Clouds are the new fashion in the progression of the distributed systems, the prototype of cloud being the grid. The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only an abstraction. It can be utilized as a service of an Internet with high scalability, higher material, quality of examination and high computing power. Cloud computing providers, transport common online business applications which are retrieved from servers through a web browser.

Top Cloud Data Security Issues: Gartner
From the cloud consumers' outlook, security is the major concern that obstructs the embracing of the cloud computing model because:
• Originalities outsource security administration to a third party that hosts their IT belongings (loss of control).
• Co-existence of assets of different leaseholders in the same location and using the same instance of the

service while is unacquainted of the gift of security controls used.
• The lack of security agreements in the SLAs between the cloud patrons and the cloud providers. • Hosting this set of valuable assets on publicly available infrastructure increases the possibility of assaults.In this paper, we analyze prevailingen counters and the issues involved in the cloud computing security problem. We have grouped these disputes into architecture-related disputes, service delivery model-related issues, cloud characteristic-related issues, and cloud stakeholder-related issues.

Enterprise role of IT in cloud computing

Cloud computing brings many advantages to companies. The pay-as-you-go business model adopted by cloud service providers enables companies of all sizes have access to very powerful resources and solutions without any capital expenditure. Furthermore, the easy scalability of cloud services allows companies to easily optimize their costs based on usage levels, instead of having to worry about peak demands.

The cloud has endorsed business to emphasis further on business, and less on the technology required to run it. Through outsourcing, there dimentary establishment to cloud providers, companies no longer have to anxiety about upgrading and upholding data centers and servers, parting that two companies who are focused entirely on the technology side of this issue. The same goes for cloud applications, which consent companies to worry more about using the software and less about maintaining it and keeping it updated. Furthermore, by moving infrastructure and applications to the cloud, companies set themselves up to take advantage of future economies of scale that will be on the side of cloud providers. For those concerns that adopt cloud technologies, these improvementsmalicious that the cloud is rapidly making IT sectorsantediluvian.

Security

The way that security control is implemented on Cloud computing is most of the times similar to those of traditional IT environments. But due to the distributed nature of the assets security risks vary depending on the kind of assets in use, how and who manages those assets, what are the control mechanisms used and where those are located and finally who consumes those assets.
Furthermore, earlier we mentioned that multi-tenancy. This means that a set of policies should be implementing how isolation of resources, billing, segmentation and so on is achieved is a secure and concise way.
In order to measure whether the security that a Cloud Provider (CP) offers is adequate we should take under consideration the maturity, effectiveness, and completeness of the risk-adjusted security controls that the CP implements. Security can be implemented at one or more levels. Those levels that cover just the Cloud infrastructure are: physical security, network security, system security and application security. Additionally, security can take place at a higher level, on people, duties and processes.
It is necessary at this point to have an understanding of the different security responsibilities that CPs and end users have. And also that sometimes even among different CPs the security responsibilities differ.

II. CLOUD SERVICE MODELS

Cloud service conveyance is separated among three architectural models and assorted imitative combinations. Three vital taxonomies are often referred to as the "SPI Model", where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively-defined.
· Infrastructure as a Service (IaaS): Here computing resources are conquered by the user, such as treating power, memory and stocking from an IaaS provider and the resources are used to condition and run their applications. IaaS has a low level of generalization as paralleled to PaaS that allows users to access the principal groundwork through the use of virtual machines. IaaS gives users more tractability than PaaS as it allows the user to situation any software stack on top of the operating system. However, tractability comes with a cost and users are blameable for modernizing and strengthening the operating system at the IaaS level. Amazon Web Services' EC2 and S37 are popular IaaS examples.
· Platform as a Service (PaaS): In here applications are established using a set of programming languages and tools that are buttressed by the PaaS provider. High level of abstraction is provided by PaaS that allows them to focus on developing their applications and not apprehensive about the principal infrastructure. Just like the SaaS model, users do not have control or access to the principal infrastructure being used to host their applications at the PaaS level. Google App Engine5 and Microsoft Azure6 are popular PaaS examples
· Software as a Service (SaaS): In SaaS, users humbly make use of a web-browser to access software that others have established and deal as a service over the web. At the SaaS level, users do not have control or access to the principal infrastructure being used to host the software. Salesforce's Customer Relationship Management software3 and

Google Docs4 are popular examples that use the SaaS model of cloud computing.

III. SECURITY ISSUES IN CLOUD COMPUTING

Cloud Deployments Mock-ups

In the cloud positioning reproduction, networking, platform, storeroom, and software transportation. Delivered as services that scale up or down contingent on the demand as depicted in figure 2.

The Cloud Computing model has three main placement models which are:

Private cloud

A private cloud is a new term that some purveyors have freshly used to describe the contributions that imitate cloud computing on private networks. It is set up within an administration's internal innovativeness data centre. In the private cloud, mountable resources and cybernetic applications provided by the cloud purveyor are assembled together and available for cloud users to segment and use. It differs from the public cloud in that all the cloud resources and applications are accomplished by the organization itself, similar to Intranet functionality. Consumption on the private cloud can be much more secure than that of the public cloud because of its specified internal acquaintance. Only the organization and nominated stakeholders may have access to operate on a specific Private cloud.

Public cloud

Public cloud pronounces cloud computing in the traditional conventional sense, whereby resources are enthusiastically provisioned on a fine-grained, self-service beginning over the Internet, via web applications/web services, from an off-site third-party wage-earner who shares resources and bills one fine-grained effectiveness computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is malleable enough to accommodate for prickles in mandate for cloud optimization. Public clouds are less secure than the other cloud models because it

Dwellingsasupplementaryencumbrance of ensuring all applications and data retrieved on the public cloud are not imperilled to nasty attacks.

Hybrid cloud

Hybrid cloud is a private cloud interconnected to one or supplementaryperipheral cloud services, centrally succeeded, provisioned as a single entity, and demarcated by a secure network . It provides cybernetic ITsolutionsthrough a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows countlessfestivities to access evidence over the Internet. It also has an open architecture that allows interfacing with other management systems. Hybrid cloud can describe the configuration conjoining a narrow device, such as a Plug computer with cloud services. It can also describe arrangements combining virtual and somatic, collocated assets -for example, a habitually actualized atmosphere that requires somatic servers, routers, or other hardware such as a network appliance acting as a firewall or junk strainer.

IV. CLOUD COMPUTINGCHALLENGES

The contemporary acceptance of cloud computing is supplementary with abundant experiments because users are still disbelieving about its faithfulness. Based on a survey piloted by IDC in 2008, the major experiments that thwart Cloud Computing from being embraced are renowned by the establishments are as follows:

A. Security: It is unblemished that the security dispute has frolicked the most imperative role in thwarting Cloud computing approval. Without doubt, putting your data, consecutively your software on someone else's hard disk using someone else's CPU appears overwhelming to many. Well-known security disputes such as data loss, phishing, botnet (running remotely on a collection of machines) carriagesombre threats to establishment's data and software. Moreover, the multi-tenancy model and the shared computing resources in cloud computing has familiarized new security experiments that necessitate novel performances to wrestle with. For example, hackers can use the Cloud to consolidate botnet as Cloud often provides more reliable infrastructure services at a comparatively cheaper expense for them to start an attack.

B. Costing Model: Cloud patrons must consider the trade-offmidstreckoning, communication, and amalgamation. While voyaging to the Cloud can emphatically reduce the infrastructure cost, it does elevate the cost of data communication, i.e. the cost of reassigning an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure) /community clouds. Intuitively, on ultimatum computing makes sense only for CPU rigorous jobs.

C. Charging Model: The mutable resource loch has made the cost investigation a lot more problematical than regular data epicenters, which often reckons their cost based on depletions on stagnant computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the fundamentalsomatic server. For SaaS, cloud breadwinners, the cost of developing multitenancy within their offering can be very significant. These include: re-design and restoration of the software that was initially used for single-tenancy, the cost of providing new features that allow for intensive customization, performance and security enrichment for concurrent user access, and dealing with densities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provision of multi-tenancy and the cost-savings yielded by multi-tenancy, such as condensed overhead through repayment, condensed number of on-site software licenses, etc. Therefore, a premeditated and the viable charging model for SaaS supplier is important for the lucrativeness and sustainability of SaaS cloud providers.

D. Service Level Agreement (SLA): Although cloud patrons do not have rheostat over the essential computing resources, they do need to safeguard the eminence, obtainability, trustworthiness, and enactment of these resources when consumers have voyaged their core business functions onto their commended cloud. In other confrontations, it is animated for patrons to obtain sureties from providers on service conveyance. Typically, these are provided through Service Level Agreements (SLAs) transferred between the providers and consumers. The very first issue is the characterization of SLA specifications in such a way that has an opposite level of granularity, namely the trade-off between poignancy and impenetrability, so that they can cover most of the consumer anticipations and is relatively simple to be partisan, substantiated, estimated, and obligatory by the resource apportionment mechanism on the cloud. In addition, different cloud assistances (IaaS, PaaS, and SaaS) will need to define different SLA Metaqualifications. This also raises a number of enactment problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA estimationstructure.

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result exposes that organizations still have security/privacy concerns in moving their data on to the Cloud. Presently, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are conservative in employing IaaS compared to SaaS. This is moderately because marginal functions are often outsourced to the Cloud, and core activities are kept in-house. The survey also shows that in three years' time, 31.5% of the organization will move their Storage Capacity to the cloud. However, this number is stagnant relatively low compared to Collaborative Applications (46.3%) at that time.

F. Cloud Interoperability Issue: Presently, each cloud offering takes the aforementioned peculiar technique taking place how cloud patrons/applications/users an intermingleby way of the cloud, prominent towards the "Hazy Cloud" happening. This relent lesslydeters the progress of cloud ecosystems by imposing vendor locking, which forbids the knack of users to select from alternative vendors/offering immediately in order to elevateproperties at poles apart stages surrounded business. More outstandingly, fashionable cloud APIs generatesappropriatechallenging to assimilate cloud services through an organization's specificprevailing legacy system (e.g. An on-premise data core for vastly interactive modelling applications in a pharmaceutical company). The key objective of interoperability is to recognize the unified fluid data across clouds and between cloud and local applications. Presently there occur a number of levels that interoperability remains crucial for cloud computing. First, to elevate the IT strength and computing resources, an organization frequentlyprerequisites to possess in-house IT resources and capabilities connected by their core know-howswhereas outsourcing marginal functions and activities (e.g. The human resource system) onto the cloud. Second, furthercommonly for the persistence of optimization, an organization may request to outsource a number of marginal functions to cloud services accessible by different vendors. Standardization acts asvirtuous key to report the interoperability issue. Still, cloud computing as impartial twitches to yield inedible, the interoperability predicament has not performed on the obstinate plan of major manufacturing cloud vendors.

V. CONCLUSION

Though Cloud computing is able to realize as a new experience which is set to transfigure the way we use the Internet, there is much to be vigilant around. There are voluminous innovative technologies sprouting at a rapid rate, each with technological innovations and with the impending of making human's lives tranquil. On the other hand, one be required to be very guarded to take into custody the security risks and challenges posed in utilizing these technologies. Cloud computing is no immunity.In this paper key security considerations and challenges which are currently facing in the Cloud computing are highlighted. Cloud computing has the potential to become a one to watch in promoting a protected, fundamental and cost-effectively viable IT solution in the opportunity.

VI. REFERENCES

[1] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDCeXchange<http: blogs.idc.com/ie/?p="730">

[2] J. Brodkin. (2008, Jun.). "Gartner: Seven cloud-computing security risks." Infoworld, Available: <http: www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page="0,1"> [Mar. 13, 2009].

</Http: ></http: >[3] Cloud Computing Use Case Discussion Group. "Cloud Computing Use Cases Version 3.0," 2010.

[4] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment

[5] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.

[6] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[7] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.

[8] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network ComputAppl doi:10.1016/j.jnca.2010.07.006. Jul., 2010.

[9] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[10] M. A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.

[11] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org.

[12] S. Arnold "Cloud computing and the issue of privacy." KM World, pp14-22.

[13] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.

[14] Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[15] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, Jun. 2009.

[16] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. "Business Models in the Service World." IT Professional, vol. 11, pp. 28-33, 2009.

[17] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues in Cloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.

[18] N. Leavitt. "Is Cloud Computing Really Ready for Prime Time?" Computer, vol. 42, pp. 1520.

[19] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore.

[20] C. Soghoian. "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era" The Berkman Center for Internet & Society Research Publication Series.