



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: VI Month of publication: June 2017

DOI:

www.ijraset.com

Call: ☎ 08813907089

E-mail ID: ijraset@gmail.com

Investigation of Cloud Computing Security Issue

Prabhleen Kaur Sohal¹, Sunil Saini²

¹Research Scholar, ²Assistant Professor, Department of Computer Science and Engineering, KITM kurukshetra India

Abstract: *This paper describes computing is to create a disciplined procedure of scattered resources with least expenditure in command to acquire great throughput and to throw a great problem with comfort. Cloud computing uses, some of the essentials like virtualization, interoperability, scalability, quality of service, fail over mechanism and the cloud delivery model. Clouds have layered structural design which fundamentally contains software as a service, platform as a service, infrastructure as a structure and hardware as a service. Cloud Modes are fundamentally public, private and hybrid. Cloud has some drawback too similar to low accountability taking rate and safety issues etc. Some other problems of the cloud contain load balancing, interoperability, scalable data storage.*

Index Terms: *Cloud Computing, SAAS, PAAS, EU*

I. INTRODUCTION

Cloud computing is a service oriented paradigm that offers “everything as a service” over internet i.e. platform, infrastructure (server space) and services can be shared [1]. Cloud Computing is a term used to illustrate both a platform and type of application. As a platform it provides, configures and reconfigures servers, where the servers can be physical machines or virtual machines. On the other hand, Cloud Computing [2] describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services.

It utilizes the techniques of virtualization and load balancing for increasing the cloud performance and complete utilization of resources. Other than these, it also makes use of technologies like distributed computing, networking, web services etc. Cloud computing is called ‘cloud’ since a cloud server can have any configuration and can be located anywhere in the world. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations e.g. online file storage, social networking sites, operating webmail and online business applications [3].

Clouds are basically virtualized data centers and applications offered as service on a subscription basis. Web based companies (Amazon, eBay), hardware vendors (HP, IBM), telecom providers (AT&T, Verizon), and software firms (Oracle/Sun) are investing huge amount of capital in establishing huge data centers. Cloud computing emphasizes on pay per use economic model means customers pay for services on pay-per-use (or pay as you go) basis as per their requirement. Cloud computing ensures performance needs through SLAs (Service Level Agreements) negotiated between customers and cloud providers by specifying the agreements on the QoS such as deadline constraints [4]. The use of cloud computing allows small and medium enterprises not to worry about buying, configuring, administering and maintaining their computing infrastructure.

II. CLOUD COMPUTING SECURITY CHALLENGES

These are the following security challenges which are faced in the environment [3]:

A. Multi-Tenancy

Cloud computing users share physical resources with others through common software virtualization layers. These shared environments introduce unique risks into a user’s resource stack. For example, the cloud consumer is completely unaware of a neighbor’s identity, security profile or intentions. The virtual machine running next to the consumer’s environment could be Malicious, looking to attack the other hypervisor tenants or sniff communications moving throughout the system. Because the cloud consumer’s data sits on common storage hardware, it could become compromised through lax access management or malicious attack.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Data Mobility and Control

Moving data from static physical servers onto virtual volumes makes it remarkably mobile, and data stored in the cloud can live anywhere in the virtual world. Storage administrators can easily reassign or replicate users' information across data centers to facilitate server maintenance, HA/DR or capacity planning, with little or no service interruption or notice to data owners. This creates a number of legal complications for cloud users. Legislation like the EU Privacy Act forbids data processing or storage of residents' data within foreign data centers. Careful controls must be applied to data in cloud computing environments to ensure cloud providers do not inadvertently break these rules by migrating geographically sensitive information across political boundaries.

C. Data Remanence

Although the recycling of storage resources is common practice in the cloud, no clear standard exists on how cloud service providers should recycle memory or disk space. In many cases, vacated hardware is simply re-purposed with little regard to secure hardware repurposing. The risk of a cloud tenant being able to gather pieces of the previous tenants' data is high when resources are not securely recycled. Resolving the issue of data remanence can frequently consume considerable negotiating time while establishing service agreements between an enterprise and a cloud service provider.

D. Data Privacy

The public nature of cloud computing poses significant implications to data privacy and confidentiality. Cloud data is often stored in plain text, and few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly. In fact, a recent report by the Cloud Security Alliance lists data loss and leakage as one of top security concerns in the cloud. Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impacts aside, loose data security practices also harm on a personal level. Lost or stolen medical records, credit card numbers or Bank information may cause emotional and financial ruin, the repercussions of which could take years to repair. Sensitive data stored within cloud environments must be safeguarded to protect its owners and subjects alike.

III. ATTRIBUTES OF CLOUD COMPUTING

What facilities can be used in the cloud?

Here are abundant facilities that can be brought through cloud computing, captivating benefit of the distributed cloud prototype. At this time, approximately short-lived similes of a limited of the greatest general cloud-based IT solutions:

A. Hosted Desktops

Hosted desktops eliminate the necessity for old-style desktop PCs in the organizational surroundings, and decrease the price of providing the facilities that you require. A hosted desktop appears and performs similar to a normal desktop PC; nonetheless the software and information consumers procedure are contained in faraway, extremely protected information focuses, somewhat on their personal machineries. Customers can merely contact their introduced desktops through an internet linking after, wherever in the sphere, by means of one or the other a present PC or laptop or, for determined cost competence, a particular expedient named a thin customer.

B. Hosted Email

By way of additional groups appearance aimed at a safe, consistent email explanation that will not price the world, they are progressively rotating to held Microsoft Exchange electronic mail strategies. By means of the universe's leading email stage, this facility occupancy administration together enormous and minor gain the welfares of exhausting MS Exchange interpretations deprived of obligating to capitalise in the expensive infrastructure. Electronic mail is stowed centrally on achieved provider, given that dismissal and debauched connectivity commencing some position. This permits customers to contact their email, schedule, associates and communal records by a diversity of income, counting Outlook, Outlook Mobile Access (OMA) and Outlook Web Access (OWA).

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. Hosted Telephony (VOIP)

VOIP (Voice over IP) is a resource of transporting handset requests and facilities through digital net communication. In relations of rudimentary practice and features, VOIP is no diverse to outdated telephony, and a VOIP-enabled handset the whole thing precisely similar to a 'common' one, nonetheless it has separated price compensations. A presented VOIP organization exchanges luxurious headset schemes, setting up, receivers, BT appearances and facts with a humble, cost-efficient substitute that is obtainable to custom on a regular contribution foundation. Characteristically, a pre-configured receiver fairly wants to be persevered in your broadband or workplace network to permit you to contact facility like voicemail, IVR and other.

D. Storage

Stowage is rising in attractiveness owing to the profits it delivers, like humble, price, that contact and elimination of the pressure of in-house conservation and organization. It is essentially the distribution of information stowage like a facility, since a third party supplier, through contact through the internet and promoting considered on volume castoff in a sure age (e.g. per month).

E. Dynamic Servers

Dynamic resources are the following age bracket of resources situation, substituting conservative idea of the devoted provider. A supplier alike ThinkGrid provides its clientele contact to servers that appear and sensation precisely alike a devoted resource, but these are fully expendable. User could straight regulate the quantity of manipulating capability and space you custom, significance user need not to fee on behalf of hardware user could not want. Characteristically, user could create modifications to user's forceful provider at some period, over the hover, deprived of the prices related with touching as of one provider to added.

IV. RELATED WORK

Du Ping et. al[3] in 2010 proposed defence System, a cloud founded structure called cloud based attack (CLAD) which turns on cloud infrastructures as a network facility to defend web service providers. Defence in contradiction of network level threat rest on the implementation environs of the cloud structure. On execution environment, it is favourable to run CLAD. The security challenges [4] for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security. Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage. These slides [5] tell us about security that it gracefully loses control while maintaining accountability even if operational responsibility falls upon 3rd parties. Also it tells us that the Provider and user security duties differ greatly between cloud models. This paper gives the 7 different security issues [50]. They are as follow: (1) privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications

V. RESEARCH METHODOLOGY

A. Cloudsim Toolkit

CloudSim is a Cloud computing modeling and simulation tool that was developed in the University of Melbourne, Australia. It is an experimental tool to conduct new research approaches. It supports the modeling and simulation of large scale Cloud computing environments, including data centers, computing nodes, Virtual machines, resource provisioning, and virtual machine provisioning, and power management [2]. CloudSim is a development toolkit for simulation of Cloud scenarios. CloudSim is not a framework as it does not provide a ready to use environment for execution of a complete scenario with a specific input. Instead, users of CloudSim have to develop the Cloud scenario it wishes to evaluate, define the required output, and provide the input parameters [3].

B. CloudAnalyst

CloudAnalyst was derived from CloudSim and extends some of its capabilities and features proposed [3]. CloudAnalyst separates the simulation experimentation exercise from a programming exercise. It also enables a modeler to repeatedly perform simulations and to conduct a series of simulation experiments with slight parameters variations in a quick and easy manner. CloudAnalyst can be applied to examining behavior of large scaled Internet application in a cloud environment.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. GreenCloud

GreenCloud is a CloudSim that have green cloud computing approach with confidently, painlessly, and successfully. In other words, GreenCloud is developed as an advanced packet level cloud network simulator with concentration on cloud communication. [3] GreenCloud extracts, aggregates and makes fine grained information about the energy consumed by computing and communication elements of the data center equipment such as computing servers, network switches and communication links available in an unprecedented fashion. Moreover, GreenCloud offers a thorough investigation of workload distributions. In particular, a special focus is devoted to accurately capture communication patterns of currently deployed and future data center architectures. In simple words, GreenCloud is the practice of designing, manufacturing, using and disposing computing resources with minimal environmental damage. The Green Cloud is a supercomputing project under active development at the University of Notre Dame.

D. GreenCloud Aim

- 1) To develop high-end computing systems such as Clusters, Data Centers, and Clouds that allocate resources to applications hosting Internet services to meet users' quality of service requirements
- 2) To minimize consumption of electric power by improving power management, dynamically managing and configuring power-aware ability of system devices.
- 3) To analyze energy efficiency and measure cloud performance

D. DCSim

Data Center Simulator is concentrated on virtualized data center which offers IaaS to Multiple tenants, in order to achieve a simulator to evaluate and develop data center management techniques. Data centers are becoming increasingly popular for the provisioning of computing resources. The cost and operational expenses of data centers have skyrocketed with the increase in computing capacity.

VI. CONCLUSION AND FUTURE SCOPE

In this paper [20], security issues for cloud computing, Big data, Map Reduce and Hadoop is discussed. The main focus is on security issues in cloud computing that are associated with big data. Big data applications are a great benefit to organizations, business, companies and many large scale and small scale industries. This paper gives the overview of data storage as well as security in cloud system. The main idea behind this report is to provide integrity to the cloud storage area.

REFERENCES

- [1]<http://searchservervirtualization.techtarget.com/definition/virtualization> (retrieved in Feb 2013)
- [2]<http://searchcloudcomputing.techtarget.com/definition/cloud-computing> (accessed in Feb 2013).
- [3] Ping u, Akihiro Nakao, "DDoS Defense as a Network Service". In International Conference on Network Operations and Management Symposium, pp.-894-897, IEEE, April 2010/
- [4] Monjur Ahmed and Mohammad Ashraf Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.
- [5] Randy Marchany , VA Tech IT Security, "Cloud Computing Security Issues", Virginia tech Invent the future Copyright marchany 2010.
- [6] Hisham A. Kholidy, Fabrizio Baiardi, "CIDS: A agenda for Interruption Detection in Cloud Systems". In Ninth International Conference on Information Technology-New Generation, pp. 379-385, October 2012
- [7] Sina Manavi, Sadra Mohammadalin, Nur Izura Udzir, Azizol Abdullah, "Ranked Protected Virtualization Model for Cloud". In the *Proceeding of the International Conference on Cyber Security, Cyber Warfare And Numerical Forensic (Cybersec2012)*, pp 219-224, IEEE, June 2012.
- [8] Dimitris Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues" , Future Generations Computer Systems , Volume 28, issue 3, March 2012, Pages 583-592.
- [9] Umer Khalid, Abdul Ghafoor, Misbah Irum and Muhammad Awais Shibli, "Cloud based Secure and Privacy Enhanced Authentication & Authorization Protocol", 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems - KES2013, Procedia Computer Science 22 (2013) 680 – 688.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)