International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.2., 2016
(Mar-Apr)

REVIEW ARTICLE

ISSN: 2321-7758

A SURVEY ABOUT CLOUD COMPUTING AND ITS ISSUES

SHELGIN.S[1], SURUTHI.M[2]

[1,2]PG Scholar : Department of Computer Science and Engineering
Valliammai Engineering College
Chennai, India

ABSTRACT

In this paper the various cloud computing issues related to security are analyzed which are observed during the information processing in cloud computing. Cloud computing is an associate degree architecture for providing computing service via the net on demand and pay per use access to a pool of shared resources specifically networks, storage, servers, services and applications, while not physically getting them. Cloud computing has fashioned the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is quickly moving towards cloud based design. If security isn't strong and consistent, the flexibleness and benefits that cloud computing must supply can have very little credibleness. Restricted management over the information might incur varied security problems and threats that embody data outflow, insecure interface, sharing of resources, knowledge avails and within attacks. Here are varied analysis challenges are there for adopting cloud computing, such as well managed service level agreement (SLA), privacy, ability and dependableness. This paper outlines the analysis of what is cloud computing, the assorted cloud models and therefore the main security risks and problems that are presently available among the cloud computing business. This analysis paper additionally analyzes the key analysis and challenges that present in cloud computing and offers best practices to service suppliers furthermore as enterprises hoping to leverage cloud service to boost their bottom line during economic climate.

Keywords—Cloud Security, Cloud Architecture, Data Protection, Security Issues, Cloud Platform.

INTRODUCTION

The cloud computing infrastructure is the rapidly developing environment. Cloud Computing is a distributed design that centralizes server resources on an ascendable platform therefore to give an on demand computing resources and services. Cloud service providers (CSP's) supply cloud platforms for his or her customers to use and make their internet services effectively being used with a high speed broadband to access the net. CSPs and ISPs (Internet Service Providers) each supply service to the client. Cloud computing could be a model that allows convenient, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications that may be speedily provisioned and discharged with lowest management effort or service provider's interaction. Generally, cloud suppliers supply 3 sorts of services, i.e. package as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There square measure numerous reasons for organizations to maneuver towards IT solutions that embrace cloud computing as they're simply needed to purchase the resources on consumption basis. Additionally, organizations will simply meet the meet the requirements of speedily ever-changing markets to confirm that they're perpetually on the vanguard for his or her customers[1]. Cloud computing appeared as a business necessity, being animated by the concept of simply victimization the infrastructure while not managing it. Though at first this concept was giftsolely within the educational space, recently, it absolutely was reversed into the trade by corporations like Microsoft, Amazon, Google, Yahoo and salesforce.com. This makes it attainable for brand spanking new startups to enter the market easier, since the value of the infrastructure is greatly diminished. This permits developers to focus on the business worth rather on the beginning budget. With the exploit of this technology, users will access serious applications via lightweight transportable devices like mobile phones, PCs and PDAs.

Fig. 1. Cloud Infrastructure

The fig 1 shows the cloud computing architecture in an simple way.Clouds square measure the new trend within the evolution of the distributed systems, the forerunner of cloud being the grid. The user doesn't need data or regulate the infrastructure of clouds; it provides solely abstraction. It is used as a service of an online with high measurability, higher output, quality of service and high computing power. Cloud computing suppliers deliver common on-line business applications that square measure accessed from servers through application program[2]. These provides the subsequent 3 sensitive states or eventualities that area unit of specific concern intervals the operational context of cloud computing:

- The transmission of private sensitive knowledge to the cloud server,
- The transmission of knowledge from the cloud server for clients' computers and
- The storage of clients' personal knowledge in cloud servers that area unit, remote server not owned by the shoppers.

Cloud computing is a fully web dependent technology wherever consumer information is hold on and maintain within the knowledge center of a cloud supplier like Google, Amazon, Salesforce.com and Microsoft etc.

Ease of Use

Different models of cloud computing

Generally, cloud services can be divided into three categories as follows.

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

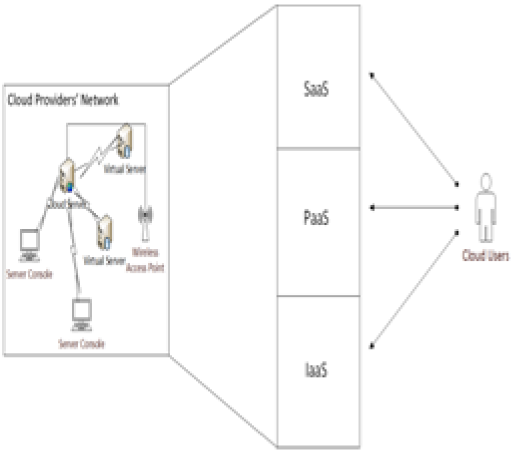

Fig. 2. Cloud Service Models

Fig 2 shows the cloud service models in such a way that the technical details, arrangements and management of the cloud service providers' network is always available to the cloud users. From the top of the cloud user, the service from the supplier comes within the type of SaaS, PaaS or IaaS wherever the cloud user has no intention or worry concerning what goes on within the internal arrangement of the cloud service providers' network.

Software-as-a-Service (SaaS): SaaS is often represented as a method by that Application Service provider (ASP) offers completely different software system applications over the web. This makes the client to get rid of installing and operating the application on own laptop and conjointly eliminates the tremendous load of software system maintenance; Continued operation, safeguarding and support [3]. SaaS Merchandiser heedfully takes responsibility for deploying and managing the IT infrastructure and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.)needed to run and manage the total answer. SaaS options an entire application offered as a service on demand. Samples of SaaS include the following.

- Salesforce.com,
- Google Apps.

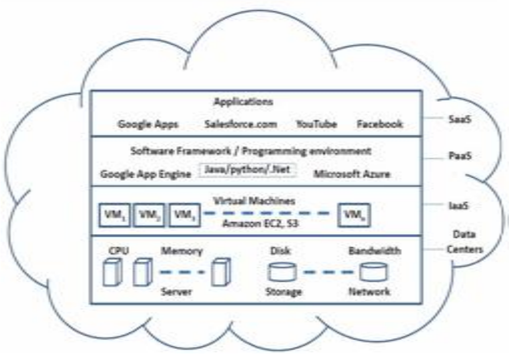

Fig. 3. High Level View of Cloud Computing Architecture

Platform as a Service (PaaS)

The PaaS is that the delivery of a computing platform and resolution stack as a service while not software system downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration so as to implement and check cloud applications. The user doesn't manage the infrastructure (including network, servers, operating systems and storage), whoever he controls deployed applications and possibly their configurations. The following are the examples of PaaS.

- Force.com
- Google App Engine
- Microsoft Azure.

Infrastructure as a Service (IaaS):

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to create resources like servers, network and storage a lot of promptly accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and therefore the capability of adding new instrumentality in an exceedingly straightforward and clear manner. In general, the user doesn't manage the underlying hardware within the cloud infrastructure, however, he controls the operating systems, storage and deployed applications. The service supplier owns the instrumentality and is liable for housing, running and maintaining it. The client generally pays on a per-use basis. Examples of IaaS includes the following.

Amazon Elastic Cloud Computing (EC2)

- Amazon S3, GoGrid.

Cloud computing entities

Cloud suppliers and customers are the two main entities within the business market. But, service brokers and resellers are the service level entities within the Cloud world.

Cloud Provider

Includes net service suppliers, telecommunication corporations, and enormous business method outsourcers that give either the media (Internet connections) or infrastructure (hosted information centers) that change customers to access cloud services. Service suppliers may additionally embody systems integrators that build and support information centers, hosting non-public clouds and that they supply totally different services (e.g., SaaS, PaaS, IaaS, and etc.) to the customers, the service brokers or resellers [6].

Cloud Service Brokers: Includes technology consultants, business skilled service organizations, registered brokers and agents, and influences that facilitate, guide customers within the choice of cloud computing solutions. Service brokers consider the negotiation of the relationships between customers and suppliers while not owning or managing the entire Cloud infrastructure. Moreover, they add further services on high of a Cloud provider's infrastructure to form up the user's Cloud setting.

Cloud Resellers: Cloud resellers will become a vital issue of the cloud market. Once, the cloud suppliers can expand their business across continents. Cloud suppliers might opt for native IT practice corporations or brokers of their existing merchandise during an explicit region.

Cloud Consumers: Cloud consumers finish users belong to the class of Cloud shoppers. However, additionally Cloud service brokers and resellers will belong to the present resellers will belong to the present class as presently as their customers of another cloud supplier, broker or reseller. Within the next section, key advantages of and doable threats and risks for Cloud Computing area unit listed [7].

III. CLOUD COMPUTING SECURITY ARCHITECTURE

Security in cloud computing is particularly an important issue owing to the very fact that the devices won't to offer services don't belong to the users themselves. The users don't have any management of, nor any information about, what might happen to their knowledge. This is often an excellent concern in cases once users have valuable and private data keep in an exceedingly cloud computing service. Users won't compromise their privacy, therefore cloud computing service suppliers should make sure that the customers' data is safe. This, however, is changing into progressively difficult as a result of a security developments square measure created, there continuously appears to be somebody to work out how to disable the protection and cash in on user data. A number of the vital parts of Service supplier Layer square measure SLA Monitor, Metering, Accounting, Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management. A number of the protection problems associated with Service supplier Layer square measure Identity, Infrastructure, Privacy, knowledge transmission, folks and Identity, Audit and Compliance, Cloud integrity and Binding problems. The variety of the vital parts of Virtual Machine Layer, creates a variety of virtual machines and a number of operating systems and its watching. A number of the protection problems associated with Virtual Machine Layer square measure VM Sprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legal and Regularity problems, Identity and Access management a number of the vital parts of information Center (Infrastructure) Layer contain the Servers, CPU's, memory, and storage, and is henceforward usually denoted as Infrastructure-as-a-Service (IaaS). A number of the protection problems associated with knowledge Center Layer square measure secure knowledge at rest, Physical Security: Network and Server. Figure 2 shows the cloud computing architecture with a high level view of security.

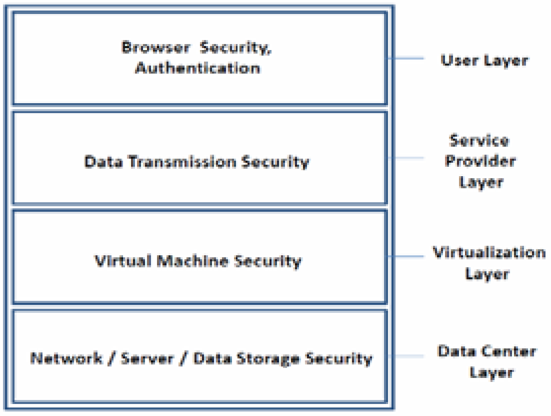
Browser Security, Authentication
Data Transmission Security
Virtual Machine Security
Network / Server / Data Storage Security
User Layer
Service Provider Layer
Virtualization Layer
Data Center Layer

Fig. 4. Secured Architecture

Some of the organizations are specializing in security problems within the cloud computing. The Cloud Security Alliance may be a non-profit organization shaped to push the utilization of best practices for providing security assurance at intervals Cloud Computing, and supply education on the uses of the cloud computing to assist secure all different types of computing.

IV. KEY ISSUES IN CLOUD COMPUTING

Cloud computing consists of applications, platforms and infrastructure segments. Every section performs totally different operations and offers different merchandise for businesses and people round the world. The business application includes the software system as a Service (SaaS), Utility Computing, net Services, Platform as a Service (PaaS), Managed Service suppliers (MSP), Service Commerce and web Integration. There are various security problems for cloud computing because it encompasses several technologies together with networks, databases, in operation systems, virtualization, resource planning, group action management, load equalization, concurrency management and memory management. Therefore, security problems for several of those systems and technologies are applicable to cloud computing. For instance, the network that interconnects the systems in an exceedingly cloud must be secure and mapping the virtual machines to the physical machines must be disbursed firmly. Information security involves encrypting the information likewise as guaranteeing that applicable policies are implemented for data sharing. The given below are the varied security considerations in an exceedingly cloud computing atmosphere.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security

Access to Servers & Applications: In ancient data centers, administrative access to servers is controlled and restricted to direct or on-premise connections that isn't the case of cloud information centers. In cloud computing, administrative access should be conducted via the net, increasing exposure and risk. It's very necessary to limit body access to information and monitor this access to keep up visibility of changes in system management. Information access issue is principally associated with security policies provided to the users whereas accessing the info. In an exceedingly typical situation, a little concern will use a cloud provided by another supplier for winding up its business processes. Some organization can have its own security policies supported that every worker will have access to a selected set of information. The safety policies could entitle some issues whereby a number of the staff doesn't seem to be given access to certain quantity of information. These security policies should be adhered by the cloud to avoid intrusion of information by unauthorized users [9].

Data Transmission: Encryption techniques the unit area used for information in transmission. To produce the privacy protection for information the client desires it to victimization authentication and integrity and isn't changed in transmission. SSL/TLS protocols unit area used here. In Cloud surroundings most of the information isn't encrypted within the interval. However the information, for any application, the information should be unencrypted. During an absolutely homomorphy cryptography theme advance in cryptography, that permits information to be processed while not being decrypted. To produce the confidentiality and integrity of data-in-transmission to and from the cloud supplier by victimization access controls like authorization, authentication, auditing for victimization resources, and make sure the handiness of the Internet-facing resources at cloud supplier. Man-in-the-middle attacks is science attack is administered once associate degree aggressor will place themselves within the communication's path between the users. Here, there's the likelihood that they'll interrupt and alter communications.

Virtual Machine Security: Virtualization is one among the most parts of a cloud. Virtual machines area unit dynamic i.e it will quickly be reverted to previous instances, paused and restarted, comparatively simply. Guaranteeing that completely different instances running on a similar physical machine area unit isolated from one another may be a major task of virtualization. They will even be without delay cloned and seamlessly touched between physical servers. This dynamic nature and potential for VM sprawl makes it tough to attain and maintain consistent security. Vulnerabilities or configuration errors could also be inadvertently propagated. Also, it's tough to keep up Associate in Nursing auditable record of the protection state of a virtual machine at any given purpose in time. Full Virtualization and Para Virtualization area unit 2 styles of virtualization in a very cloud computing paradigm. Fully virtualization, entire hardware design is replicated nearly. However, in para-virtualization, Associate in Nursing OS is changed so it will be run at the same time with different operating systems. VMM (Virtual Machine Monitor), may be a software package layer that abstracts the physical resources utilized by the multiple virtual machines. The VMM provides a virtual processor and different virtualized versions of system devices like I/O devices, storage, memory, etc. several bugs are found altogether common VMMs that permit escaping from Virtual machine.

Network Security: Networks area unit classified into many varieties like shared and non-shared, public or non-public, little space or massive space networks and every of them have a variety of security threats to take care of. Issues related to the network level security comprise of DNS attacks, soul attacks, issue of reused information science address, etc. that area unit explained in details as follows.

A Domain Name Server (DNS) server performs the interpretation of a site name to AN information science address. Since the domain names area unit a lot of easier to recollect. Hence, the DNS server area unit required. However, there is a unit cases, once having referred to as the server by name, the user has been routed to another evil cloud rather than the one he asked for and therefore victimization information science address isn't continually possible. Though victimization DNS security measures like: name System Security Extensions (DNSSEC) reduces the consequences of DNS threats, however still there are a unit cases, once these security measures persuade be inadequate once the trail between a sender and a receiver gets rerouted through some evil affiliation. It should happen that even in the end the DNS security measures are a unit taken, still the route designated between the sender and receiver cause security issues.

Sniffer attacks area unit launched by applications which will capture packets flowing in a very network and if the information that's being transferred through these packets isn't encrypted, it often browses and there are a unit possibilities that very important data flowing across the network are often derived or captured. A soul program, through the NIC (Network Interface Card) ensures that the data/traffic joined two different systems on the network conjointly gets recorded. It is often achieved by putting the NIC in promiscuous mode and in promiscuous mode, it will track all knowledge, flowing on an equivalent network. A malicious sniffing observation platform supported creative person (address resolution protocol) and RTT (round trip time) are often wanting to detect a sniffing system running on a network [11]. Reused information science address issue is an enormous network security concern. Once a selected user moves out of a network, then the IP address related to him (earlier) is assigned to a replacement user. This general risks the protection of the new user as there's a precise delay between the amendment of AN information science address in DNS and also the clearing of that address in DNS caches. And hence, we are able to say that generally, although the previous information science address is being assigned to a replacement user still the possibilities of accessing the information by another user aren't negligible because the address still exists within the DNS cache and also the data happiness to a selected user might become accessible to another user violating the privacy of the first user [12].

Data Security: For general user it's quite straightforward to seek out the doable storage on the fact that gives the service of cloud computing. To realize the service of cloud computing, the foremost common utilized communication protocol is a machine-readable hypertext Transfer Protocol (HTTP). So as to assure knowledge} security and data integrity, machine-readable text Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) area unit the foremost common adoption. During an ancient on-premise application readying model, the sensitive knowledge of every enterprise continues to reside at intervals the enterprise boundary and is subject to its physical, logical and personnel security and access management policies. However, in cloud computing, the enterprise knowledge is kept outside the enterprise boundary, at the Service supplier finish. Consequently, the service supplier should adopt extra security checks to confirm knowledge security and forestall breaches thanks to security vulnerabilities within the application or through malicious workers. This involves the utilization of robust coding techniques for knowledge security and fine-grained authorization to regulate access to knowledge. Cloud service suppliers like Amazon, the Elastic reckon Cloud (EC2) directors don't have access to client instances and can't log into the Guest OS. EC2 directors with a business would like area unit needed to use their individual cryptographically robust Secure Shell (SSH) keys to achieve access to a bunch. All such access area unit logged and habitually audited. Whereas the information at rest in easy Storage Service (S3) isn't encrypted by default, users will write in code their knowledge before it's uploaded to Amazon S3, so it's not accessed or tampered with by any unauthorized party [13].

CONCLUSION

One of the biggest security worries with the cloud computing model is the sharing of resources. Cloud service providers need to inform their customers about the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues and research challenges in cloud computing. Data security is a major issue for Cloud Computing. There are several other security challenges, including security aspects of network and virtualization. This paper has highlighted all these issues of cloud computing. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the cloud architecture. As the development of cloud computing technology is still at an early stage, we hope our work will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

REFERENCES

[1]. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2]. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[3]. R. L Grossman, “The Case for Cloud Computing,” IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[4]. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[5]. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6]. Pring et al., “Forecast: Sizing the cloud; understanding the opportunities in cloud services,” Gartner Inc., Tech. Rep. G00166525, March 2009.

[7]. Aman Bakshi, Yogesh B. Dujodwala, “Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine,” ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[8]. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE

SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[9]. K. Hwang, S Kulkarni and Y. Hu, “Cloud security with virtualized defence and Reputation-based Trust management,” Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695-3929 -4.

[10]. R. Gellman, “Privacy in the clouds: Risks to privacy and confidentiality from cloud computing,” The World Privacy Forum,2009.http://www.worldprivacyforum.org/pdf/WPF_Cloud_ Privacy_Report.pdf.

[11]. Ohlman, B., Eriksson, A., Rembarz, R. (2009) What Networking of Information Can Do for Cloud Computing. The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Groningen, The Netherlands, June 29 - July 1, 2009

[12]. L.J. Zhang and Qun Zhou, “CCOA: Cloud Computing Open Architecture,” ICWS 2009: IEEE International Conference on Web Services, pp. 607 616. July 2009.

[13]. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O’ Reilly Media, USA, 2009.

[14]. Ronald L. Krutz, Russell Dean Vines “Cloud SecurityA Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, Inc.,2010

[15]. K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment,” IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[16]. Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, “Cloud Computing: Distributed Internet Computing for IT and Scientific Research,” IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.

[17]. A.Williamson, “Comparing cloud computing providers,” Cloud Comp. J., vol. 2, no. 3, pp. 3–5, 2009.