Security Issues and Data Management in Cloud Computing

T.P.Sarachandrika[#1], Dasari Kiran Kumar[#2],P.Jayasankar[#3],B. Sunil Kumar[#4]

[#1]*Working as Asst. Professor in Sri venkateswara College of Engineering,*[#2] *working as Asst Professor in Vignana Bharathi Institute of Technology,*[#3]*working as Associate Test Architect in Alliance Global Services,*[#4]*working as Asst Professor in Jawaharlal Nehru Institute of Technology*

Abstract: Cloud computing placed IT to higher and new limits by providing the market environment data storage and capacity with flexible and scalable and processing power to reach the demand and supply while reducing the capital expenditure . The cost of the successful implementation of the cloud computing is to efficiently manage the security in the cloud computing applications. Security awareness and anxiety arises as soon as application starts running over the officially assigned firewall and move closer towards the public domain. The main purpose of the paper is to provide an overall security view of cloud computing. The main aim is to highlight the security concerns that should properly addresses and managed to realize the full feasible of cloud computing. Some important issues like Gartner's list on cloud security and cloud threats will be discussed in this paper.

Keywords – Cloud computing, security, hybrid cloud, public cloud, private cloud.

1.INTRODUCTION

Today's successful technologies highly depends on its quality that brings out an effect of the world's standard, and difficult of use by the end users and most important is its degree of data or information security and control over the information. Cloud computing is a very new and emerging information technology that changes the way IT architectural solutions are put forward by means of moving towards the theme of virtualization: of data storage, networks and software[2-3].

In a survey done by the International Data Corporation group the majority of results point to employing cloud computing is a low cost and successful working environment option to users[1]. It also shows that cloud computing is a best for individuals who are attempt to find quick solution for startups such as developers and research projects and ecommerce business man. Cloud computing help in keeping IT budget to bare minimum. It is best for development and testing purpose and cloud computing is the easiest solution to test potential proof without investing too much capital. Cloud computing can deliver a vast array of IT capabilities in real time using many types of resources such as hardware, software, virtual storage once entered to a cloud. Prioritized applications use cloud computing while other applications which are critical maintains resources as per normal. This process is for cost saving while maintaining security and control within an organization.

Service oriented architecture looks like a cloud computing, so it examines every computing component and it is not limited to distributed computing, grid computing, utility computing, on-demand, open source, peer to peer. It is a further step for grid to utility model. In down grading the potential security trust issues and also stick to governance issues that are facing cloud computing ,a compulsory control measure is to make sure that a concrete cloud computing service level agreement was kept in place and maintained when dealing with outsourced suppliers and specialized cloud dealers. Because of the situation and demand of prominent cloud technologies there is assured degree of inexperience when dealing with cloud security. At present cloud computing clients have to trust the third party cloud providers on many fronts, particularly on the availability of cloud service and data security. Consequently the SLA forms an complete part of a clients first line of defense. Then SLA have become the hermit legal understanding between the service provides and client.

The paper is framed as follows: Sec II brings out the different types of cloud models together with its security implications, here cloud models are also known as deployment models. Sec III deals with cloud computing architectural delivery designs with security understanding. Sec IV that explains cloud computing tracking of security constraints .Sec V belongs to information on how to manage the data while providing security requirements that are used to cloud computing. Sec VI provides the conclusion for security issues and management of data in cloud computing.

II. DIFFERENT TYPES OF CLOUD MODELS

In accommodating a most secure cloud computing solution is to take an important decision to decide which type of cloud to be selected and implemented .At present there are four types of cloud models those are named as public, private, hybrid, community cloud. These models along with their security conclusions will be discussed. With this paper dealers are referred as cloud providers or companies concentrating in providing a tailor made cloud solution. These items have established cloud infrastructure containing virtual servers for storage needed processing power. Organizations are items containing business managers, executives and end users, going into a agreement with cloud dealers to use the cloud capabilities for their personal and private use.

II (a). Public cloud:

In a simple words public cloud means, it can be approached by any users with an internet connection and access to the cloud space. It is also called as traditional cloud computing where resources are dynamically provisioned on a fine grained self service basis over the internet or via or from off-site third party provider who bills on a fine grained basis [5]. It is generally based on pay-per-use model, means how much you need you have to pay for that and have to use. These public clouds are less secure than that of remaining models because it places an extra stress in providing all the applications and data accessed on public cloud are not subjected to malevolent attacks. Hence trust and privacy are common in handling public clouds with SLA at its core. A prerequisite management considerations which to answered with in the SLA contracts the sample security controls are put in place. There is a common for cloud dealer and client is to agree in sharing combined responsibilities in cloud check and testing in their own systems. Here we have other option that is every party is divided individually and working with cloud computing security with their own used borderlines.

II (b). Private cloud:

A private cloud is founded for a selected group or organization and gives permission only to that group [6]. It is easy to coordinate with security, regulatory requirements and provides more undertaking control and command over distribution and use. Here in public cloud users have to pay the bill for their usage but in private money is charged per GB usage along with bandwidth transfer fees. Here resources and applications are managed and maintained by the organization itself which is same as intranet functionality. When compared to public cloud private cloud is more secure in usage due to its internal exposure. Private cloud is only accessed by the organization and designated persons.

II (c). Hybrid cloud:

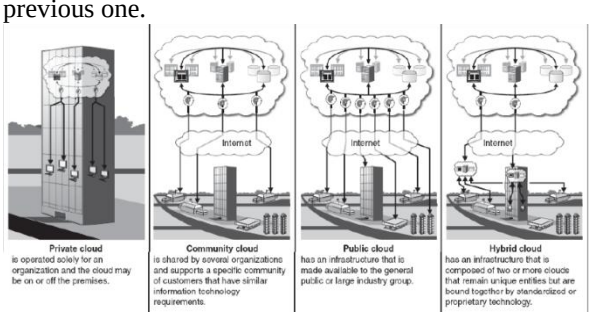
A hybrid cloud is designed with a combination of two clouds, where the clouds included are a mixture of public, private, or community. Here it is linked to one or more external services supplied as a single unit and enclosed by a secure network. It provides high secure on data and applications and gives permissions to other users to use the information over the internet. The hybrid cloud has an architecture which gives permission to interface with management systems [7]. Hybrid clouds can be considered an intermediate stage as enterprises prepare to move most of their workloads to public clouds.

II (d). Community cloud:

A community cloud is shared among two or more organizations that have similar cloud requirements[8]. Cloud infrastructure that is shared by so many organizations and supports a specific community such as healthcare, that has shared concerns around mission, policy and compliance considerations.

To anatomize the cloud deployment model networking, plat forming, storage and software infrastructure are provided as services that scale up or

down depending on the demand. Finalizing which cloud to deploy, business managers have to assess the whole security conditions in design point of view, considering the information security differences of each cloud implementation model referred in previous one.



III. CLOUD COMPUTING DELIVERY MODELS

According to the cloud deployment models, the future security regarding that business administration must undo relates to different cloud delivery models. Because of the pay-per-use models or public cloud model that appropriate to cloud delivery models, the level of information security is controlled towards adhering to industries level of quality and lawmaking towards stakeholders. The architectural design models are grouped according to three types of models, they are namely Infrastructure as a service, software as a service, platform as a service.

III (a): Infrastructure as a Service (IaaS)

An Infrastructure as a Service agreement, as the name states, deals first with computational infrastructure. In an IaaS contract, the users who subscribed completely, outsources the storage and resources like hardware and software that they need, it is a pay-per-use fee. This facility very highly reduces the demand for huge initial investment in computing hardware like networking devices, servers, processing power. These clients gives permissions to various degrees of monetary and functional flexibility that are not developed in internal data centers, the reason is computing resources can increase or release the degree more quickly with minimum cost than in internal data center[11]. The qualifications and components of IaaS are utility computing service and billing model, automation of administrative tasks, dynamic scaling, desktop virtualization, policy based services, internet connectivity.

III(b) Software as a Service (SaaS)

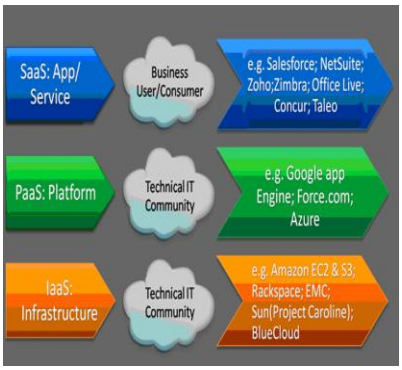
Software as a Service (SaaS) is a software distribution model where applications are acts as a host by a vendor or service provider and made available to customers over a network, typically the Internet [10]. Software as a Service is becoming an increasingly predominating delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) full grown and new evolutionary approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two little different delivery models for SaaS. The hosted application management (hosted AM) model is similar to Application Service Providers: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution[10]. Benefits of the SaaS model include: easier administration, automatic updates and patch management, compatibility: All users will have the same version of software, easier collaboration, global accessibility.

The conventional model of software distribution, in which software is purchased and installed on personal computers, is sometimes referred to as software as a product.

III(c) Platform as a Service (PaaS)

Platform as a Service (PaaS) is a way to hire hardware, operating systems, storage and network capacity over the Internet [9]. The service delivery model gives permission to the customers to rent virtualized servers and associated services for running presently using applications or developing and testing new applications. Software distribution model in which hosted software applications are available to customers over the Internet. PaaS provides many advantages for developers. With PaaS we can change and upgrade the features of operating system frequently. Geographically distributed

development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be minimized by the use of infrastructure services from a single seller rather than maintaining multiple hardware facilities that frequently perform duplicate functions or suffer from incompatibility problems. Overall cost can also be minimized by integration of programming development efforts. On the otherside, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly develop



Merging the three types with delivery models we get holistic cloud picture, having connectivity devices combined with information security themes. Virtualized physical resources, infrastructures , and also virtualized middleware platform and other business applications are provided and buy as services in cloud. All cloud dealers and clients have to maintain cloud computing security in all interactions.

IV . TRACKING OF SECURITY ISSUES

There are many issues in cloud computing:

- Network Availability: The worth of cloud computing is only known when your network connections and bandwidth meet your minimum needs. The cloud computing is accessible whenever you want it. If not, the importances are no different than a denial-of-service attack.
- Cloud Provider Viability: Because cloud providers are comparatively new to the business, there are questions about their development and commitment. This concern depens when a provider needs tenants to use proprietary interfaces, leading to tenant lock-in.
- Disaster Recovery and Business Continuity: Tenants and users needs confidence that their operations and services will move on if the cloud provider's production environment is subject to a disaster.
- Security Incidents: The provider must notify tenants and users of any security break. Tenants or users may need provider support to answer to audit or assessment findings. Also, a provider may not provide sufficient support to tenants or users for resolving investigations.
- Transparency: When a cloud provider doesn't reveal details of its own internal policy or technology, tenants or users must believe the provider's security claims. Tenants and users may still need some transparency by providers as to how they manage and maintain cloud security, privacy and security incidents.
- Loss of Physical Control: Because tenants and users physically lose their control over their data and applications, this gives rise to a range of concerns:
  - Data Privacy: With public or community clouds, data may not remain in the same system, raising multiple legal concerns.
  - Data Control: Data could be coming in to the provider in much number of ways with some data belonging to some others. A tenant administrator has finite control scope and accountability within a public Infrastructure as a Service implementation, and even less with a Platform as a Service. Tenants required having confidence on their provider that they will offer appropriate control, while finding the need to adapt their expectations for how much control is reasonable within these models.
  - New Risks and Vulnerabilities: There is an anxiety that cloud computing brings new classes of risks and vulnerabilities. There are hypothetical new risks, but the actual exploits will mostly be a function of a provider's execution. All software, hardware and networking equipment are subject to

unearthing new vulnerabilities. By performing layered security and well-conceived operational processes, you can protect a cloud from common attacks, even if some of its components are inherently vulnerable.

- Legal and Regulatory Compliance: It may be difficult to use public clouds if your data is subject to legal limitations or regulatory agreement. You can expect providers to develop and certify cloud infrastructures to address the wants of regulated markets. Accomplishing certification may be challenging due to the more non-technical factors, including the present state of general cloud knowledge. As best practices for cloud computing encompass greater scope, this concern should fade.

V. DATA MANAGEMENT SECURITY

Data management security means storage service providers will collect user's information as little as possible and should ensure that the data will not be allowed to be seen by any third party without the user's agreement. In Cloud computing substructure, sharing of physical resources brings crisis to data security and privacy, and they can no longer depend on a physical machine or network boundary. What's more, users get worry about the transparency of data storage location. For most businesses, data security and data protection is the biggest impediment for developing of cloud computing technology on applications that having sensitive or confidential data. As we all know that, data encryption is a fundamental measure to ensure data security. But many applications need data processing in the cloud, and then they need to decrypt the data, the best contract system and management system is basic to the protection of data security. In conventional service protocols, user can treat the control right of location of the data storage with the service provider, thus the data transmission regulations which management approach should be provided. However, as to cloud computing, data can be moved to anywhere in the world and also distribute enterprise's data at different locations, the betterment of freedom degree will guide the processing procedure not to conform with many of the world's regulations on data storage and transfer [15]. So, Cloud computing service providers should advance the development of new data management regulations in order to adjust to the development of cloud computing. Another problem is that data management needs to consider substitution or deactivation of service provider. Once the cooperation agreement expires, as the user may disable a service, what way will the data stored in the cloud return back to its owner? In general, cloud computing provides large storage capacity and special format, if copy back to the user exactly, it is impossible to user to restore itself, even has nowhere to store. The solution is to use products of another service provider, and then they will deal with data smooth panning. In present days major cloud computing service providers, such as Microsoft, Google, Amazon all have relative form of data storage and system, how to ensure the smooth panning of data between these service providers also need to be considered. Though the data in multiple cloud computing platforms can be sent from one place to another place smoothly, effective means are required to ensure the effective ruination of data in the original service provider after the expiration of the agreement. Here all the above-mentioned problems have been resolved; users will also take the dependability of cloud computing platform into account. Most today's cloud computing platforms declared that their reliability reached 99.9% [16], but even failure rate of 0.001% for a user may be fatal, so third-party backup among service providers is necessary, that is, the data is backed up to a provider that does not in the same network, same area or even same country, to obtain fixed services that is separate from equipment failures, natural disaster, and even regional policies. Once a error occurs, the cloud computing service providers should have a set of possibly plans to be able to regain from disaster quickly and efficiently. Seeing that data management security of cloud computing is getting more and more concerns that may give birth to a new data security insurance. Users can buy insurance from insurance company for its software and data, and at the time of an accident, the insurance companies will pay for it which can minimize the risk of users and cloud computing service providers. Therefore, when selecting, the user should primarily choose service providers with good reputation, powerful technology and economic strength. Of course, this may cause jungle situation in cloud computing industry.

Some other security issues are, with the progressive promotion of the application, any private information in the facilities of the cloud computing may be found on any equipment. In order to preserve the user's data from reveal, a person named Siani Pearson put some advanced design principles in design process of cloud computing services to secure that user's message and business information would not revealed out. It Transmit and store user's information as little as possible. After systematic analysis, the cloud computing applications will gather and store the most necessary information only.

Security measures will be followed to prevent unauthorized access, copying, using or modifying personal information. Firstly, it is needed to allow the user to control the most critical an important personal information. Secondly, it is available to manage personal information by a trusted third party. Users have the right to select the use of personal information and user have right to select the choice. Make clear and limit the purpose of use of data. Personal information must be used and taken care by the person with identification for special purpose and owner of information should be mentioned before using. Establish feedback mechanism to ensure that safety tips and detailed measures of the service will be given to the user timely. It can increase the security of user's data after introducing the above principles. The network speed and standards sometimes cannot meet the requirements of cloud computing services of users, so, many applications try to reach the target through a local cache data, such as Drop box based on Amazon S3-based [14]. Local data cache will poses a threat to data security, although will not go so far as to lose or corrupt data, reveal of personal information still worth noticing. In general, a service provider will specify that the data security issues provided by local cache should be entirely taken care by the user, but the author believes that this is an irresponsible shirking. The local cache is a method to improve the users experience, and it is one part of the system design. So, service providers should protect the cached data from revealing as much as possible by using technical means or otherwise. Now, some service providers begin to set user authentication and encryption for cached data.

VI. CONCLUSION

In the promoting of cloud computing services, the issue of data security is one of the most important problems to be solved. Today's network construction, safety products, and encryption protocol have been protected the safety of data transmission basically; Data storage security can be solved through technical means in the design stage of cloud services, such as redundancy, parity, user authentication and access control; Data management security contains many aspects, the first is to advance the relevant laws and regulations as early as possible, and the second is consistent with data between cloud computing service providers to secure that users can smoothly pan data, and service providers should develop a rapid and effective disaster recovery mechanisms to secure the availability of the data. At present, in a less period of time, the cloud computing cannot completely replace traditional computing. It is still not being fully accepted that to manage data by a third party, especially for large enterprises and government departments. In order to take full advantages of cloud computing characteristics, some large enterprises with strong economic and technological strength have begun to try to establish their own cloud computing platforms.

REFERENCES.

[1]. Gens F, 2009,' New IDC IT Cloud Services Survey: Top Benefits and Challenges', IDC exchange, viewed 18 February 2010, from <http://blogs.idc.com/ie/?p=730>.

[2]. Leavitt N, 2009, 'Is Cloud Computing Really Ready for Prime Time?', Computer, Vol. 42, pp. 15-20, 2009.

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

[4]. Josh Ames blog.appcore.com/blog/bid/167543/Types-of-Cloud-Computing-Private-Public-and-Hybrid-Clouds in 2012.

[5]. A Platform Computing Whitepaper, 'Enterprise Cloud Computing: Transforming IT', Platform Computing, pp6, viewed 13 March 2010.

[6]. Dooley B, 2010, 'Architectural Requirements Of The Hybrid Cloud', Information Management Online, viewed 10 February 2010, from <http://www.information-management.com/news/hybrid-cloudarchitectural- requirements-10017152-1.html>.

[7] Global Netoptex Incorporated , 2009, Demystifying the cloud. Important opportunities, crucial choices, http://www.gni.com, pp 4-14, viewed 13 December 2009.

[8]. The basics of cloud computing by Alexa Huth and James Cebula.

[9].searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS.

[10].searchcloudcomputing.techtarget.com/definition/Software-as-a-Service-SaaS.

[11].searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS.

[12]. Brodkin J, 2008, 'Gartner: Seven cloud-computing security risks', Infoworld, viewed 13 March 2009, from www.infoworld.com/d/security-central/gartner-seven-cloudcomputing- security-risks-853?page=0,1.

[13] ISO. ISO 7498-2:1989. Information processing systems-Open Systems Interconnection.

[14]. Dropbox www.dropbox.com,2011.1..

[15] "Cloud computing and outsourcing data safety analysis and suggestionshttp://datacenter.ctocio.com.cn/Cloud%20Computing/249/8990749.shtml,2009.7.

[16] "Amazon Simple Storage Service," http://aws.amazon.com/s3 2011.1.

[17] HBase, http://hbase.apache.org/,2011.1.

Author Details:

Author -1

Mrs. T.P.Sarachandrika, M.Tech (CSE) from Acharya Nagarjuna University. I am presently working as Assistant Professor in Department of Computer Science & Engineering in Sri Venkateswara College of Engineering - Tirupathi. I am having 5 years of teaching experience. My interested subjects are Operating Systems, Computer Organization, Software Engineering and Data Base Management Systems.

Mail Id: sarachandrika@gmail.com

Author -2

Dasari.Kiran Kumar M.Tech from ANU Guntur, completed M.C.A from KU, Warangal,. I am presently working as Assistant Professor in Department of Computer Science Engineering in Vignana Bharathi Institute of Technology, Ghatkesar, Aushapur, Hyderabad. I am having 5years of Teaching Experience. My interested subjects are Software Engineering, Data mining, Web services, Web Technologies, Java, C, and C++.....

kiran_cgp@yahoo.com

Author -3

Mr. P.Jayasankar, M.Tech (CSE) from Acharya Nagarjuna University. I am presently working as Associate Test Architect in Alliance Global Services in Hyderabad. I am having 8 years of experience as a Test Lead. My interested subjects are Embedded Systems, Computer Networks, Network Security, Operating Systems and Computer Organization.

Mail Id:pandurusankar@yahoo.com

Author -4

Mr. B. Sunil Kumar working as Assistant Professor in Department of Computer Science & Engineering in Jawaharlal Nehru Institute of Technology, I am having 3years of Teaching Experience. My interested subjects are Web Technologies, Web services, Mobile computing, cloud computing, Computer Networks, Operating System, Computer Organisation, Java, C, and C++

Mail id: sunilkumar0060@gmail.com

,