Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Facet in Cloud Computing

Suresh Kumar R G *

Assistant Professor, Department of Computer Science
Rajiv Gandhi College of Engineering and Technology

Abstract*—The concept of cloud computing is a very vast concept which is very efficient and effective security services. The cloud computing and data methodology retrieval is a conceptual one of the based most technology which is used widely now a day. But in data privacy protection control challenging research work in cloud computing, because of users secrete data which is to be stored by user. An enterprise usually store data in internal storage and then tries to protect the data from other outside source. They also provide authentication at certain specific level. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. This paper mainly proposes the core concept of secured cloud computing. It suggests the cloud computing based on separate encryption and decryption services from the storage service. Due to this increasing demand for more clouds there is an ever growing threat of security becoming a major issue. This paper shall look at ways in which security threats can be a danger to cloud computing and how they can be avoided.

***Keywords*— SaaS, PaaS, IaaS, Security, threats**

I. Introduction

The US National Institute of Standards and Technology (NIST) define cloud computing as "a model for user convenience, on- demand network access contribute the computing resources (e.g. networks, storage, applications, servers, and services) that can be rapidly implemented with minimal management effort or service provider interference" Cloud computing can also be defined as it is a new service, which are the collection of technologies and a means of supporting the use of large scale Internet services for the remote applications with good quality of service (QoS) levels [4]. Cloud computing is has many technologies such as Saas i.e. "Software as a Service", Paas i.e. "Platform as a Service", IaaS i.e. Infrastructure as a Service". Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. Examples of such nodes include end user computers, data centers, and Cloud Services. We term such a network of nodes as a Cloud. Cloud service delivery is divided among three archetypal models and various derivative combinations. The infrastructure (as a Service), respectively defined.

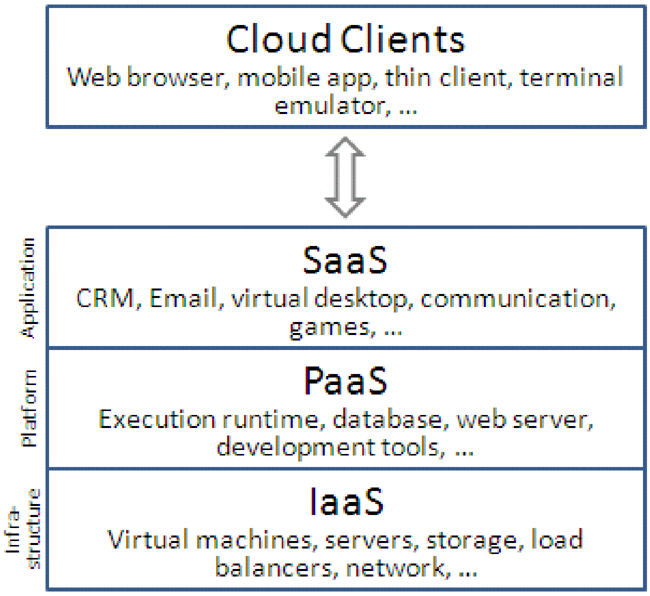
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Figure 1.0 Cloud Service Model

II. CLOUD SERVICE MODELS (4)

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email) Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider(e.g., configurations) Cloud Infrastructure as a Service (IaaS):The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.(e.g., host fire walls)

III. CLOUD DEPLOYMENT MODELS (4)

Regardless of the service model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud services, with derivative variations that address specific requirements are depicted

Public Cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Private Cloud: The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off premises.

Community Cloud: The cloud infrastructure is shared by concerns (e.g., mission, security several organizations and supports a specific community requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may present on-premises or off-premises.

Hybrid Cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

IV. CLOUD SECURITY

Cloud computing and web services run on a network structure so they are open to network type attacks. One of these attacks is the distributed denial of service attacks. If a user could hijack a server then the hacker could stop the web services from functioning and demand a ransom to put the services back online. To stop these attacks the use of syn cookies and limiting users connected to a server all help stop a DDOS attack. Another such attack is the man in the middle attack. If the secure sockets layer (SSL) is incorrectly configured then client and server authentication may not behave as expected therefore leading to man in the middle attacks. It is clear that the security issue has played the most important role in hindering Cloud computing. Without doubt, putting your data, running your software at someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, and botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with.

Service Provider Security Issues - The public cloud computing surroundings offered by the cloud supplier and make sure that a cloud computing resolution satisfies organizational security and privacy needs. The cloud supplier to provision the safety controls necessary to safeguard the these organization's controls information and applications, information and additionally the proof provided regarding the effectiveness of migrating organizational functions into the cloud.

- Identity and access management
- Identity and Access Management (lAM)

(lAM) features are Authorization, Authentication, and Auditing (AAA) of users accessing cloud services. In any organization "trust boundary" is mostly static and is monitored and controlled for applications which are deployed within the organization's perimeter. In a private data center, it managed the trust boundary encompasses the network, systems, and applications. And it is secured via network security controls including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication.

Privacy - Privacy is the one of the Security issue in cloud computing. Personal information regulations vary across the world and number of restrictions placed by number of countries whether it stored outside of the country. For a cloud service provider, in every jurisdiction a single level of service that is acceptable. Based on contractual commitments data can store within specific countries for privacy regulations, but this is difficult to verify. In case of Private and confidential customer's data rising for the consequences and potential costs of mistakes for companies that handle. But professionals develop the security services and the cloud service privacy practices. An effective assessment strategy must cover data protection, compliance, privacy, identity management, secure operations, and other related security and legal Issues.

Securing Data in Transmission - Encryption techniques are used for data in transmission to provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time, but to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider.

User Identity - In Organizations, only authorized users across their enterprise and access to the data and tools that they require, when they require them, and all unauthorized users are blocked for access. In Cloud environments support a large enterprise and various communities of users, so these controls are more critical. Clouds begin a new level of privileged users working for the cloud provider is administrators. And an important requirement is privileged user monitoring, including logging activities. This monitoring should include background checking and physical monitoring.

Audit and Compliance - An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements Classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail. In traditional out sourcing relationships plays an important role for audit and compliance. In Cloud dynamic nature, increase the importance of these functions in platform as-a service (PaaS), infrastructure-as-a-service (laaS), and software-as -a-service (SaaS) environments.

V. INFRASTRUCTURE SECURITY ISSUES [1]

Cloud suppliers provide security-related services to a good vary of client types; the security equipped to the foremost demanding clients is additionally created on the market to those with the smallest amount stringent necessities. Whereas Infrastructure Security Solutions and product are often simply deployed, they need to a part of an entire and secure design to be effective.

Securing Data-Storage - In Cloud computing environment data protection as the most important security issue. In this issue, it concerns include the way in which data is accessed and stored, audit requirements, compliance notification requirements , issues involving the cost of data breaches, and damage to brand value. In the cloud storage infrastructure, regulated and sensitive data needs to be properly segregated. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact. Software encryption is less secure and slower because the encryption key can be copied off the machine without detection.

Network and Server - Server-Side Protection: Virtual servers and applications, very like their non-virtual counterparts, have to be compelled to be secured in IaaS clouds, each physically and logically. Example, virtual firewalls are often used to isolate teams of virtual machines from different hosted teams, like production systems from development systems or development systems from different cloud-resident systems. Rigorously managing virtual machine pictures is additionally vital to avoid accidentally deploying pictures underneath development or containing vulnerabilities. Preventing holes or leaks between the composed infrastructures could be a major concern with hybrid clouds, as a result of will increase in complexity and diffusion of responsibilities. The supply of the hybrid cloud, computed because the product of the supply levels for the part clouds, also can be a concern; if the % availability of anyone part drops, the availability suffers proportionately. In cloud environment, purchasers want to form certain that every one tenant domains are properly isolated that no probability exists for data or transactions to leak from one tenant domain into successive.

VI. END USER SECURITY ISSUES [1]

End Users need to access resources within the cloud and may bear in mind of access agreements like acceptable use or conflict of interest. The client organization have some mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native systems as soon as they are found.

Security-as-a- service - In Cloud environment the security provided by customers using cloud services and the cloud service providers (CSPs).Security-as-a-service is a security provided as cloud services and it can provide in two methods: In first method anyone can changing their delivery methods to include cloud services comprises established information security vendors. The second method Cloud Service Providers are providing security only as a cloud service with information security companies.

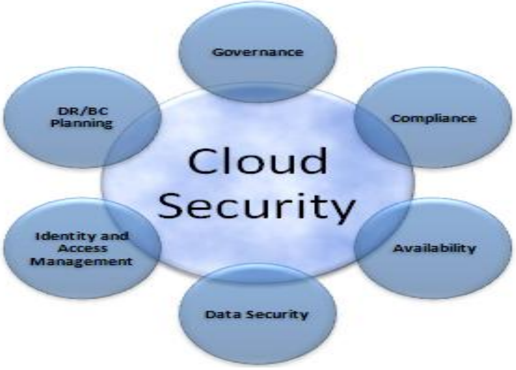

Figure 2 Various Point of View of Cloud Security [7]

Browser Security - In a Cloud environment, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud. A standard Web browser is platform in-dependent client software useful for all users throughout the world. This can be categorized into different types: Software as- a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication.

Authentication - In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted Platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG's) is IF-MAP standard about authorized users and other security issue in real-time communication between the cloud provider and the customer. Other such risks which are marked as high risk in cloud security are

Loss of Governance: in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defenses.

Lock-In: there is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled.

Data Protection: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g. between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g.,SAS70 certification. Data flowing from the Internet is filled with mal ware and packets intended to lure users into unknowing participation in criminal activities.

VII. LIMITATIONS OF CLOUD COMPUTING [2]

Data losses / leakage - Cloud computing efforts to control the security of the data is not very better; accordingly API access control and key generation, storage and management deficiencies may result in data leakage, and also may lack the important data destruction policy. Leakage, and causes lack the vital- data destruction policy.

Difficult to assess the reliability of suppliers - Cloud computing service provider of background checks on staff strength may be related to corporate efforts which is then actually used to control data access which is different from many suppliers in this circumstances, but not enough, companies need to Evaluation of suppliers and propose to prove that how to filter the program staff.

Authentication mechanisms are not so strong [6] - In cloud, huge data, applications and resources are collected and cloud computing is very weak authentication mechanism, and then the attacker can easily obtain the client user account and log in the virtual machine.

VIII. CONCLUSION

In this paper, we explored the security issues at various levels of cloud computing service architecture. Security of customer information is a major requirement for any services offered by any cloud computing. We investigated ongoing security issues in Software-as-a-service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). Cloud computing systems challenge is assessing and managing risk. In the system lifecycle, risks that are identified should be rigorously balanced against the protection and privacy controls out there and therefore the expected edges from their utilization. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted.

REFERENCES

[1] "Security Architecture of Cloud Computing", V.KRISHNA REDDY 1, Dr. L.S.S.REDDY, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9 September 2011.

[2] 'The Effective and Efficient Security Services for Cloud Computing ",Sambhaji Sarode, Deepali Giri, Khushbu Chopde, International lournal of Computer Applications (0975 - 8887) Volume 34- No.9, November 2011

[3] "Cloud Computing Security" Danish Jamil Hassan Zaki, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4 April 2011

[4] Peter Mell, and Tim Grance, "Draft NIST Working Definition of Cloud Computing," 2009

[5] http://csrc.nist.gov/ groups/SNS/cloud-computing

[6] "Cloud Computing Security Issues and Challenges", Kuyoro S. 0.Ibikunle F., Awodele O.

[7] Catteddu D. 2010 Cloud Computing. [Online] Available from: http://w. enisa. europa. eu/ act/rm/files/deliverables /c1oud-computing risk- assessment [Accessed 26th April 2010]

[8] http://adventuresinsecurity.comlblognp=67

[9] http://www.maintec.comlblog/find-your-way-to-securecloud-part-2