DataSecurity in Cloud Storage using Cyber Technique – An Overview

[1]M. Joseph Rajakumar, [2]S.ManjuPriya

Abstract

This paper contributes towards effecting the security technique to protect data stored in cloud environment. The cloud computing is to make the business activities more potential and useful to the end user at all times when it is required. In this scenario, the services those are available as a resource in the cloud has to be protected from the unauthorized access. In this paper, the existing security techniques in protecting data stored under cloud is analyzed and reviewed those security aspects and suggested better security solutions in the cloud environment. Enterprises are striving to reduce their computing cost through the means of virtualization. Cloud computing offers better computing cost model through potential utilization and reduced infrastructure cost and administration. Cloud computing is suitable for medium and small sized enterprises with respect to cost and security.

Keywords : Cloud Computing, SaaS, PaaS, IaaS, Virtualization, Cloud Storage, Cloud Security, CSP(Cloud service provider), SLA(Service Level Agreement).

[1]Research Scholar, Karpagam University Coimbatore, Tamilnadu

[2]Associate Professor, Department of Computer Science, Karpagam University, Coimbatore.

Introduction

Cloud computing provides many benefits such as low cost, high performance and delivery of variety of services. Cloud computing policies are necessary to ensure that the cloud computing resources are not misused by the unauthorized access. The policies such as user accounts access, storage-access, data manipulations and confidential data access that are laid by the company must be followed by the employees of an organization strictly and any violation to it may jeopardize the security of the business activities. Solutions to various cloud security issues vary, from cryptography, particularly public keyinfrastructure (PKI), to use of multiple cloud providers, standardization of APIs, and improving virtual machine support and legal support [1].

Cloud computing security has been referred to as a sub domain of computer network and information security in a broader aspect. Security has been designed to safeguard organizations policies and technologies. Controls are deployed to protect company's data, applications and frame work of security protocols. Cloud computing is an emerging model where users can gain access to their applications from anywhere through their connected devices. A simplified user interface makes the infrastructure supporting the applications transparent to users. The applications reside in massively-

scalable data centers where compute resources can be dynamically provisioned and shared to achieve significant economies of scale.

In this paper, security policies to be adhered by the organization to secure their data have been reviewed. The employees of a company should not reveal their login credential to others outside the organization. Service Level agreement must be laid between the cloud service provider and cloud service consumer. The laws and regulations related to accessing the financial data must be followed.

Characteristics of Cloud Computing

- **On-demand self-service**: The consumer can provision multiple computing capabilities as needed. The provisioning can be entirely online.
- **Broad network access**: The services are available over the network and access is supported through multiple platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling**: The cloud service provider computing resources are pooled to serve multiple consumers at the same time, the consumers can be from anywhere in the world. Examples of resources include storage, processing, memory, and network bandwidth.
- **Scalability**: Cloud resources can be easily provisioned and released. It may appear to the consumerthat the resources available for provisioning to be unlimited and can be appropriated in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer.

Service Models of Cloud Computing

The service models of cloud computing is as shown in figure1.

- **Software as a Service (SaaS)**: This model offers the state agency the facility to use the Cloud service provider's applications running on a cloud infrastructure. The software applications are accessible online via a web interface or via desktop application. The consumer has no control over the underlying hardware configuration.
- **Platform as a Service (PaaS)**: This model offers the state agency the facility to deploy or install onto the cloud infrastructure a state agency-created or acquired application with the condition that the application is created using programming languages, libraries, services, and tools supported by the cloud service provider. The consumer has no control over the underlying hardware configuration, storage, network, operating system or management layers.

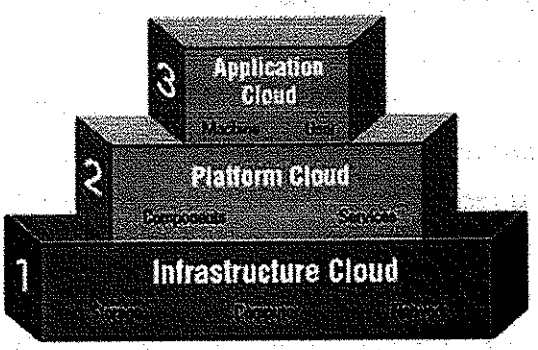


Figure1: Service model of cloud computing [14]

- **Infrastructure as a Service (IaaS):** This model offers the state agency the facility to utilize processing, storage, networks, and other computing resources where the consumer is able to install and run any software, which may include operating systems and applications. The state agency does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications.

DEPLOYMENT MODELS OF CLOUD COMPUTING

- **Private cloud:** [2]The cloud infrastructure is commissioned for exclusive use by a single organization/state agency comprising multiple consumers (e.g., different departments). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. It may also existin or outside the country.

- **Community cloud:** The cloud infrastructure is commissioned for exclusive use by a specific community/sector of consumers from organizations that have shared nature of work and obligations (e.g., same mission, ICT security requirements, legal, and sector specific compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. It may also existin or outside the country. (e.g., Qatari Government Network).

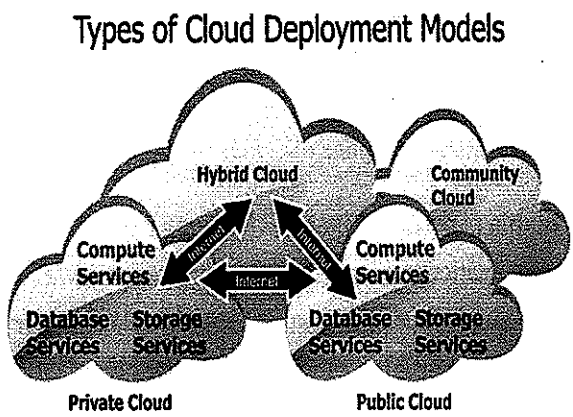


Figure 2 : Types of Cloud Deployment models [13]

- **Public cloud:** The cloud infrastructure is commissioned for open use by any organization. It may be owned, managed, and operated by a private or public organizations or a combination of them. It exists on the premises of the cloud service provider.

- **Hybrid cloud:** The cloud infrastructure is a composition of two or more different cloud infrastructures (private, community, or public) that remain separate entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., load balancing between clouds).

Literature review

Cloud computing comes with [4] numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success.The security challenges for [5] cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security.Cloud users' personal data security [3] is thus a crucial

concern in a cloud computing environment. In terms of customers' personal or business data security, the strategic policies of the cloud providers are of highest significance as the technical security solely is not adequate to address the problem. Trust is another problem which raises security concerns to use cloud service for the reason that it is directly related to the credibility and authenticity of the cloud service providers. Security and privacy both are concerns in cloud computing due to the nature of such computing approach. The approach by which cloud computing is done has made it prone to both information security and network security issues. Third party relationship might emerge as a risk for cloud environment along with other security threats inherent in infrastructural and virtual machine aspects. Factors like software bugs, social engineering, human errors make the security for cloud a dynamically challenging one. Intrusion detection is the most important role in seamless network monitoring to reduce security risks. If the contemporary IDSs (Intrusion detection Systems) are inefficient, the resultant consequence might be undetected security breach for cloud environment.

SECURITY CONCERNS IN CLOUD COMPUTING

1) **Loss of governance**: When the potential business activities moved from the customer premises to cloud environment then there is a lack of control over the resources deployed in the cloud. It comprises transferring data to the cloud, it refers to losing control over location, redundancy and file system [9]. Service-level agreement (SLA) may not have guaranteed on cloud provider zone [10].

2) **Loss of trust**: Cloud user may not aware the security policies implemented by the cloud providers and also what measures are taken by the provider in case of data loss or data stolen by the other cloud users.

3) **Vendor lock-in:** The lack freedom the cloud user faces at the time of dissatisfaction of services rendered by the cloud service provider.

4) **Data loss or Data Leakage**: It may be possible when the encrypted keys lost or theft by intruders. Vulnerable authentication code and access privileges are the major cause for data leakage or loss.

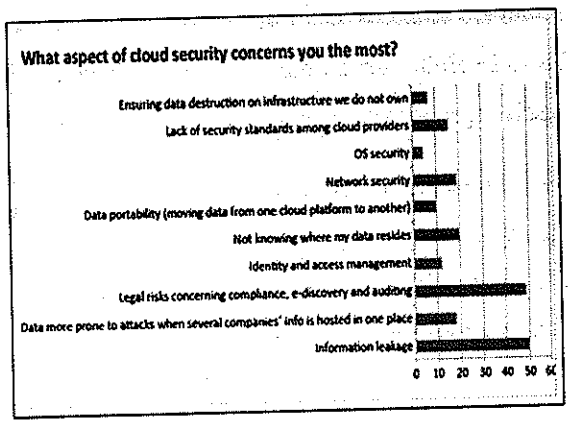


Figure 3 : Aspect of Security Concerns [12]

5) **OS and Network Security:** A cloud service provider must attempt to allow legitimate network traffic and drop malicious network traffic, just as any other Internet-connected organization does. However, unlike many other organizations, a cloud service provider will not

necessarily know what network traffic its consumers plan to send and receive. Nevertheless, consumers should expect a certain amount of external network perimeter and internal network separation measures from their cloud service providers.The operating system implements the level of security and quality of service to ensure that applications are able to access the resources needed to deliver an acceptable level of performance.

6) **Identity and access management** : It is necessary to have suitable Identity & Access Management (IAM) in place to ensure that a person must identify and authenticate themselves when using the cloud service and that they are granted access rights which are appropriate to their role. The cloud service customer should demand fine grained access control and a separation of roles between cloud service users and cloud service administrators.

7) **Security Standards**: The exiting security standards common use around the world can be applied to the governance of cloud computing. Because there are no specific security standards available for cloud computing.

8) **Multi-tenancy**: Multi-tenancy means that the cloud infrastructure is shared andused by multiple users. As such, in a virtual environment, data belonging to differentusers may be placed on the same physical machine, based on a certain resourceallocation policy. Although multi-tenancy is an essential choice of cloud vendorsdue to its economic efficiency, it provides new vulnerabilities to the cloud platform. That is, malicious users may exploit this co-residence issue to perform flooding attacks [8].

Fundamentals on Cryptography

For many years, cryptography was the exclusive domain of military, diplomatic and governmental secret services, and has been used to mainly provide security properties, such as data confidentiality, data integrity and data origin authentication [ISO89]. Presentedas the art of coding information into secrets, cryptography enables the intended receivers to recover the original content of messages. During the second part of the twentieth century, the field of cryptography has expanded due to the proliferation of computers and networks and the appearance of new cryptographic systems.

Cloud Storage is an evolving paradigm, shifting the computing and storage capabilities to external service providers. Especially due to this loss of direct control onoutsourced data, users are reluctant for adopting cloud services. The data security andprivacy concerns are quite legitimate, given the latest mediated revelations.

Data security concerns

Securing the data in the cloud environment poses the challenges- data confidentiality and data integrity which influence on the security and performances of the cloud system. Security designers propose a high level security assurance, such as storing encrypted data in cloud servers to support data privacy and confidentiality, and to be resistant to unauthorized access to data during the sharing process.

The client data transit protection policy is to be ensured through encryption and network protection mechanisms. Current WAN technology has no means of protection of customer data that result in loss of confidentiality and data integrity.

Proper SLA must be written between the cloud service provider and cloud service consumer on physical location transparency where client data is stored. There may be multi-tenancy approach deployed by the CSP that gives threat to the business opponents.

Cloud provider may store the client data in multiple locations to avoid the any loss of data and provide potential data backup facilities. However, those data under the CSP hand to be protected by their own local unauthorized personals. In this scenario the service provider should implement the robust encryption algorithm to protect business transaction and also provide physical security controls such as validation procedures that facilitate a comprehension data protection system.

Cloud data storage services bring many challenging design issues, considerably due to the loss of physical control. These challenges have significant influence on the data security and performances of cloud systems. That is, cloud data are often subject to a large numberf attack vectors

This is largely due to the fact that users outsource theirdata on remote servers, which are controlled and managed by possible untrusted CloudService Providers (CSPs). It is commonly agreed that data encryption at the client side isa good alternative to mitigate such concerns of data confidentiality [7].

Data storage integrity is one of the challenging tasks in the cloud. Thus, in [11] author proposes a novel approach for overcome this data integrity issue by using remote data integrity checking protocol, which is based on RSA and HLA signature with the support of public verification.

Conclusion

This paper studied the security policies to be adhered by the organization to secure their data. Suggests stern legal agreements must be laid between the cloud service provider and cloud service consumer. It also identified the spectrum of security risks and provided the solutions to improper use of security policies. By applying secure coding and implementing data protection techniques the confidential data of the business activity can be protected from unauthorized usage. Cloud security concerns have emergedto be of an increasing interest and importance, in the applied cryptography and computerresearch community, while demanding adequate measures for cloud challenges. For thispurpose, we consider a storage scenario, where the client outsources data in remote servers.

References

[1] Scan Marston a, Zhi Li a, Subhajyoti Bandyopadhyay a, Juheng Zhang a, AnandGhalsasi, Cloud computing —The business perspective, 2011.

[2] CLOUD SECURITY POLICY for Government Agencies [2014].

[3] Joint, A., Baker, E. and Eccles, E. (2009). Hey, you, get off of that cloud? Computer Law & Security Review, 25, 270–274. doi:10.1016/j.clsr.2009.03.001.

[4] Khorshed, T.M., Ali, A.B.M.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 28, 833–851. doi:10.1016/j.future.2012.01.006.

[5] King, N.J. and Raja, V.T. (2012).Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, 308-319.

[6] Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16, 102-107. doi:10.1016/j.istr.2011.08.005

[7] S. Kamara and K. Lauter. Cryptographic cloud storage. In Proceedings ofthe 14th international conference on Financial cryptography and data security,FC'10, Berlin, Heidelberg, 2010. Springer-Verlag.

[8] K.Zunnurhain. Fapa: a model to prevent flooding attacks in clouds. InProceedings of the 50th Annual Southeast Regional Conference, ACM-SE '12,pages 395–396, New York, NY, USA, 2012. ACM.177

[9] VinayakShukla,ShobhitSrivastava, Nidheesh Sharma, *"Cloud Computing: Security Issues and Solutions"*, International Journal of Emerging Trends & Technology in Computer Science,Vol.3, Issue 5, 2014.

[10] Mitchell Cochran,Paul D. Witman, *"Governance And Service Level Agreement Issues In A Cloud Computing Environment"*, Journal of Information Technology Management, Vol. XXII, Number 2, 2011.

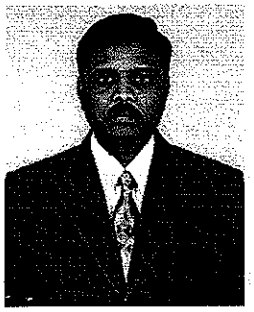
[11] B. R. Kandukuri, V. R. Paturi, A. Rakshit, *"Cloud Security Issues,"* IEEE International Conference on Services Computing, 21-25 pp. 517-520, 2009.

[12] http://www.computerweekly.com/news/2240036468/Cloud-computing-adoption-remains-tepid.

[13] http://www.techinmind.com/what-is-cloud-computing-what-are-its-advantages-and-disadvantages/

[14] http://www.tatvasoft.com/blog/cloud-computing-models/

Authors Biography :



M. Joseph Rajakumar He is currently working in HCL Technologies, Training and Staffing Services, as a Lead Trainer, Madurai. He was Associate Professor and Head, the Department of

Computer Science, St. Joseph's PG College, Hyderabad from June 2005 to Feb 2016. He has done his Post-Graduation in Master of Computer Application and Master of Philosophy in Network Security. His research interests are in the area of Cloud based technologies, Big Data Analytics & Network Security. He has participated a number of National and state level conferences. He has supervised about ten M.Phil Research scholars of various Universities to his credit. He is a member of Professional body - CSTA (Computer Science Teachers Association), USA, for the voice of K-12 computer science education and its educators.

She is **Dr. S. Manju Priya,** working as Associate Professor, Dept. of Computer Science, Karpagam University. She has completed her Ph.D in Karpagam University. She has published more than 15 papers in national and international journals. Her area of interest is sensor networks, cloud storage, communications.