Cloud Computing Data Security: A Review

Poonam M. Umbarkar[1], N. R. Borkar[2]

M.E. Department of Computer Science & Engineering, KGIET, Amravati, India [1]

Professor, Department of Computer Science& Engineering, KGIET, Amravati, India [2]

Abstract: Cloud computing has great potential of providing robust computational power to the society at reduced cost. With the advent of the World Wide Web and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. This data would be more useful to cooperating organizations if they were able to share their data. Two major obstacles to this process of data sharing are providing a common storage space and secure access to the shared data. All types of users who require the secure transmission or storage of data in any kind of media or network. We are in great need of encrypting the data. A method to build a trusted computing environment for Cloud Computing system by providing Secure cross platform in to Cloud Computing system. In this method some important security services including authentication, encryption and decryption are provided in Cloud Computing system. In this paper, we propose Data Storage Security by using Trusted Platform Module to achieve storage correctness incorporating Cloud's dynamic nature while maintaining low computation and communication cost and ensures the security of static data.

Keywords*: Cloud computing, Encryption/decryption service,*

*****

I. INTRODUCTION

In recent years, cloud computing fig 1 has become a hot topic in the global technology industry. The initiatives include Google's research project for building an infrastructure to support research needs of top-tier American universities. Weiss noted that cloud computing services include several existing computing technologies, such as service-oriented utility computing, grid computing with large amount of computing resources, and that using data centres for data storage services[1].

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centres into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centres[2]

Prior to the development of the concept of cloud computing Fig 1 critical industrial data was stored internally on storage media, protected by security measures including firewalls to prevent external access to the data and including organizational regulations to prohibit unauthorized internal access. In the cloud computing environment, storage service providers must have in place data security practices to ensure that their clients' data is safe from unauthorized access and disclosure. More importantly, the regulations and measures for preventing privileged users such as system administrators from unauthorized access must be rigorously established and implemented.[1]

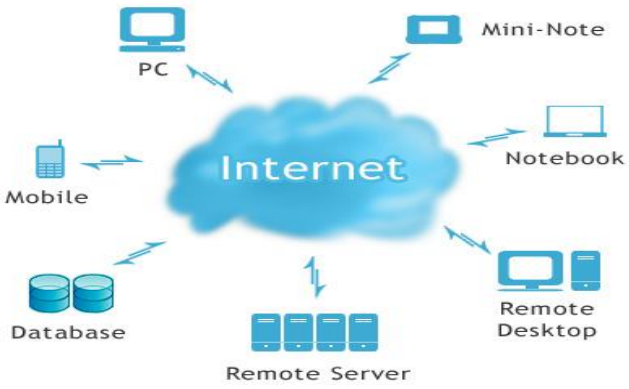

Fig.1 Cloud computing

A Simple approach for system to protect user data is that data of user is encrypted before it stored. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the user's perspective, this could put his stored data at risk of unauthorized disclosure.[1]

II. CLOUD COMPUTING

The term cloud has been used historically as a metaphor for the Internet. This usage was originally derived from its common

depiction in network diagrams as an outline of a cloud, used to represent the transport of data across carrier backbones (which owned the cloud) to an endpoint location on the other side of the cloud. This concept dates back as early as 1961,when Professor John McCarthy suggested that computer time-sharing technology might lead to a future where computing power and even specific applications might be sold through a utility-type business model. This idea became very popular in the late 1960s, but by the mid-1970s the idea faded away when it became clear that the IT-related technologies of the day were unable to sustain such a futuristic computing model. However, since the turn of the millennium, the concept has been revitalized. It was during this time of revitalization that the term cloud computing began to emerge in technology circles.[8]

III. LAYERS OF CLOUDS

A. Infrastructure-as-a-Service(IaaS)—the Infrastructure services layer:

In the case of IaaS, servers, network devices, and storage disks are made available to organizations as services on a need-to basis. Virtualization (a software technology that uses a physical resource such as a server and divides it up into virtual resources called Virtual Machines—VMs), allows IaaS providers to offer almost unlimited instances of servers to clients, while making cost-effective use of the hosting hardware. Companies can use IaaS to build new versions of applications or environments without having to invest in physical IT assets. Increasingly, organizations are using IaaS to host their websites, monitor their traffic and keep them running 24x7, without hogging up internal IT resources. IaaS is particularly beneficial for micro-, small and medium-sized businesses that can access server and storage systems, which they would otherwise have to purchase. Microsoft has been offering IaaS services, either through its own infrastructure or that of its partners.[9]

B. Platform-as-a-Service (PaaS)—the Platform layer:

This layer provides a platform for creating applications. PaaS solutions are essentially development platforms for which the development tool itself is hosted in the Cloud and accessed through a browser. With PaaS, developers can build Web applications without installing any tools on their computers and then deploy those applications without any specialized systems administration skills. Today, PaaS is being delivered like a utility say, water or electricity over the Internet, with ISVs and corporate IT departments, paying according to usage. Owing to PaaS, there has been a jump in the number of people who can develop, maintain and deploy web-based applications without requiring specialized expertise. An example of PaaS is Microsoft's Azure, which the company is providing as a cutting-edge cloud-based platform on which applications can be built.[9]

Fig. 3 Layers of clouds

C. Software-as-a-Service (SaaS)—the Application layer:

This layer includes applications that run off the Cloud and are available to Web users or enterprises on a pay-as-you-go, anytime-anywhere basis. Microsoft's Online Services are an example of SaaS for the enterprise. The Cloud, apart from its different layers, is also visible through three variants. There are the public Clouds for instance, a deployment option for enterprises where the infrastructure services are provided by a hosting partner. It is this third party vendor that hosts and manages these offerings. The other version is the private Cloud, where it is deployed within the enterprise and managed and maintained by the organization itself. A private cloud is a collection of virtualized infrastructure fabrics that are coupled with automated management. It is deeply integrated with the application platform and identity, protection and access technologies to create an internal service-oriented environment for enterprises. Although the private cloud does not offer the Capex to Opex advantage, with the hypervisor capability becoming integral to the operating system (e.g. Hyper-v within Windows Server 2008 R2), it is becoming increasingly affordable for enterprises. A more recent, architecturally new concept in Cloud computing is the hybrid Cloud, which is a blend of the public and private Cloud. The hybrid Cloud, created by the enterprise, can leverage the benefits provided by both public and private Clouds. However, issues related to the sharing of responsibilities between the enterprise and the third party vendor and governing such a Cloud, make it a slightly complex deployment option.[9]

IV. DEPLOYMENT MODES IN CLOUD

There are four types of cloud available in cloud computing i.e. private cloud, public cloud, hybrid cloud and community cloud.

A) Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units).[10] 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.[6]

B) Public cloud: The cloud infrastructure is provisioned for open use by the general public.[10] It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider [6].

C) Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations) [6]. 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.

D) Hybrid cloud: Hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that will be unique entities, but bound together by standardized technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [6],[10].

V. OVERVIEW OF CLOUD COMPUTING

Cloud computing as a delivery model for IT services is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST specify five characteristics of cloud computing that describe and differentiate Cloud services from conventional computing approaches:

- **Self Service**

Firstly On-demand self-service involves customers using a web site or similar control panel interface to provision computing resources such as additional computers, network bandwidth or user email accounts, without requiring human interaction between customers and the vendor.

- **Network Access**

Secondly broad network access enables customers to access computing resources over networks such as the Internet from a broad range of computing devices such as laptops and smart phones.

- **Resource Pooling**

Thirdly Resource pooling involves vendors using shared computing resources to provide cloud services to multiple customers. Virtualization and multitenancy mechanisms are typically used to both segregate and protect each customer and their data from other customers, and to make it appear to customers that they are the only user of a shared computer or software application.

- **Rapid elasticity**

Rapid elasticity enables the fast and automatic increase and decrease to the amount of available computer processing, storage and network bandwidth as required by customer demand.

- **Pay-per-use**

Lastly Pay-per-use measured service involves customers only paying for the computing resources that they actually use, and being able to monitor their usage. This is analogous to household use of utilities such as electricity.[12]

VI. INCREASING THE CLOUD SECURITY

Public and private cloud services, also known as multi-tenant infrastructure, are used increasingly in the enterprise and by government agencies. With their popularity come security issues that are now high priority. A number of TCG technologies and standards, including the Trusted Platform Module (TPM), network security, and self-encrypting drives can be used to provide security for systems, networks, and data. TCG also is addressing how to interface various technical standards to create an end-to-end enterprise solution that is tailored to meet mission and business needs and comply with security policies within public and private cloud networks. TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments [13].

VII. CONCLUSION

Hence this paper gives overall clue of all existing techniques for cloud data security and methods proposed for ensuring data authentication using TPA. , Cloud computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing hardware. we have create new technique which use TPA store encrypted data to cloud, which is hidden from other users. The data will be safe in the public cloud also. In TPM access to keys, data or systems is often protected and requires authentication by presenting a password.

ACKNOWLEDGMENT

I express my sincere gratitude to Prof. V. P. Nikam, Head Department of CSE, for his valuable guidance and advice. Also I would like to thanks to my guide Prof. N. R. Borkar and the faculty members for their continuous support and encouragement.

REFERENCES

[1] Jing-Jang Hwang, Hung-Kai Chuang,Yi-Chang Hsu, Chien-Hsing Wu, ”A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service,” Proceedings of the 2011 International Conference on Information Science and Application, April 2011.

[2] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou,” Ensuring Data Storage Security in Cloud Computing”

[3] Avi Kak Lecture 8: AES: The Advanced Encryption Standard Lecture Notes on “Computer and Network Security”

[4] Dieter Gollmann (2006). Computer Security Second Edition West Sussex, England: John Wiley &Sons,Ltd.

[5] Williamson, August 10, 1976. Diffie, W.; Hellman, M. (1976). "New directions in cryptography"(http://www-ee.stanford.edu/%7Ehellman/publications/24.pdf). IEEE Transactions on Information Theory 22 (6):644–654. doi:10.1109/TIT.1976.1055638 (http://dx.doi.org/10.1109%2FTIT.1976.1055638).

[6] Bhavna Makhija, Vinit Kumar Gupta, Indrajit Rajput, ”Enhanced Data Security in Cloud Computing with Third Party Auditor” proceeding of the , February 2013 International Journal of Advanced Research in Computer Science and Software Engineering.

[7] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, KuiRen, Member, IEEE, Wenjing Lou, Senior Member, IEEE, and Jin Li”Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”

[8] John W. Rittinghouse, James F. Ransome© 2010 by Taylor and Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business”Cloud Computing Implementation, Management, and Security”

[9] http://www.microsoft.com/india/msindia/perspective/interfaces_cloud_three_layers.aspx

[10] Cong Wang, Qian Wang, KuiRen, and WenjingLou,‖Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing‖ in IEEE INFOCOM 2010, San Diego, CA, March 2010.

[11] Ashish Bhagat, Ravi Kant Sahu “Using Third Party Auditor for Cloud Data Security: A Review” International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2011

[12] Hojabr, "Ensuring data storage security in cloud computing with effect of kerberos," International Journal of Engineering Research & Technology (IJERT),ISSN-2278-0181, Vol. 1.

[13] Qian Wang and Cong Wang and KuiRen, Wenjing Lou, Jin Li “Enabling Public Auditability And Data Dynamics For Storage Security in Cloud Computing” in IEEE transactions on parallel and distributed systems,vol. 22.