IPHV8I2008X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

A DISTRIBUTED STORAGE SYSTEM FOR STRUCTURED CLOUD DATABASE

[#1]V.MANASA, M.Tech Student,
[#2]P.BALAKISHAN, Associate Professor,
Department of CSE
JYOTHISHMATHI INSTITUTE OF TECHNOLOGICAL SCIENCES,KARIMNAGAR,T.S,INDIA.

ABSTRACT: Today, users effectively lose control of their data in the cloud, if either the cloud infrastructure or cloud applications are compromised, users' privacy will be at risk. The ubiquitous concern over cloud environment data privacy demands a paradigm shift, such that users can continue to have control of their data in the cloud environment, and verify that the cloud providers have correctly enforced their privacy policies .We offering strong data security to cloud users while enabling valuable applications is a challenging task. We explore a new cloud environment architecture called Data Security as a Service (DSaaS) and, which dramatically reduces the per-application development effort required to offer data security, while still allowing rapid improvement and maintenance.

Keywords: *Cloud computing, Data security as a Service, availability, privacy, Integrity, Confidentiality, perspecsys.*

I.INTRODUCTION

Cloud computing is an evolving term that describes the development of many existing technologies and approaches to computing into something different. The NIST defined cloud computing as "Cloud computing is 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 of service provider interaction"[1]. In the traditional desktop computing, we run copies of software programs in our system. The documents that we created are stored in the same system. i.e. PC centric. With cloud computing, the software programs are not run from our computer rather stored on servers and accessed via the Internet. i.e., service centric. Theadvantage is that if our system crashes, the software is still available. The same thing will happen in the case of the data that stored in the cloud. Anyone with permission can access and modify the cloud data. "Cloud" consists of huge number of computers and servers, linked and accessible via internet [2].Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing environment allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud computing technology allows for much more efficient computing by centralizing data storage, processing and bandwidth

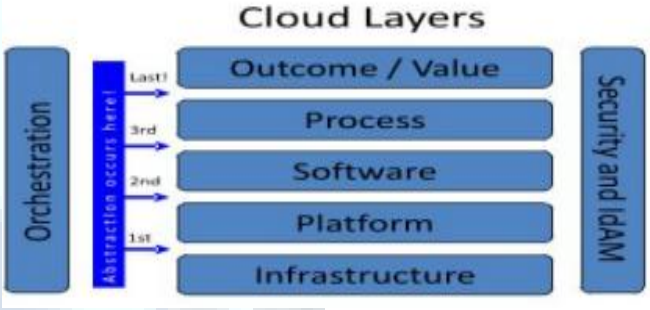

Fig 1: cloud layers

Cloud computing is mainly classified into 3 segments: application, storage, and connectivity. Each segment serves a different purpose and offers different products for businesses and individuals around the world. Cloud computing environment promises lower costs, easier maintenance, rapid scaling, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. A recent Microsoft survey found that "58% of the public and 86% of business leaders are excited about the possibilities of cloud computing. But more than 90% of them are worried about security, availability, and privacy of their data as it rests in the cloud." [1] PerspecSys Inc. is a cloud security company that provides cloud data protection software. PerspecSys specializes in cloud data privacy, data residency/sovereignty, and data security software that helps organizations comply with industry regulations and directives, and security requirements when adopting cloud. Banking and financial services, healthcare, retail, and government organizations must adhere to strict guidelines when handling sensitive personal data in cloud applications. These organizations must comply with regulations that include: PCI DSS, ITAR, FERPA, HIPAA, and HITECH. Cloud computing architecture refers to the components and subcomponents required for cloud computing environment. These components typically consist of a front end platform

(fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network. Combined, these components make up cloud computing architecture.

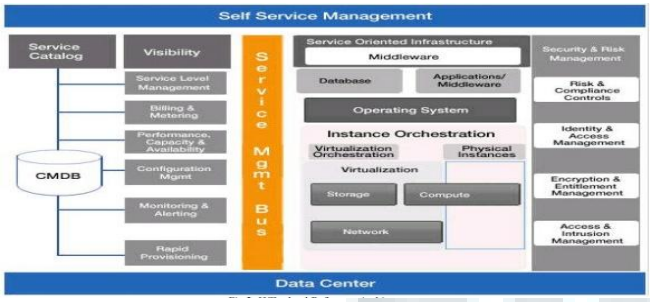

Fig 2: HCL cloud Reference Architecture

I. Cloud Storage

Online network storage where data is stored and accessible to multiple clients in cloud computing environment. Cloud storage is generally deployed into three configurations: public, private, community, or some combination of the three is also known as hybrid cloud. The cloud storage needs to be agile, flexible, consistent, scalable, multi-tenancy, and secure.

II. Cloud Based Delivery

Software as a service (SaaS) service-model involves the cloud provider installing and maintaining software in the cloud and users running the software from their cloud clients over the Internet. The users' client machines require no installation of any application-specific software - cloud applications run on the server. Software as a service is scalable, and system administration may load the applications on several servers. In the past, each customer would purchase and load their own copy of the application to each of their own servers, but with the Software as a service the customer can access the application without installing the software locally. Software as a service typically involves a monthly or annual fee. Software as a service provides the equivalent of installed applications in the traditional (noncloud computing) delivery of applications. SaaS has four common approaches: single instance, multi instance, multi tenant, flex tenancy. Development as a service (DaaS) is web based and community shared development tools. This is the equivalent to locally installed development tools in the traditional (non-cloud computing) delivery of development tools. Platform as a service is cloud computing service which provides the users with application platforms and databases as a service. This is equivalent to middleware in the traditional delivery of application platforms and databases. Infrastructure as a service (IaaS) is taking the physical hardware and going completely virtual system (e.g. all servers, networks, storage, and system management all existing in the cloud). This is the equivalent to infrastructure and hardware in the traditional method running in the cloud. In other words, businesses pay a fee to run proxy servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level.

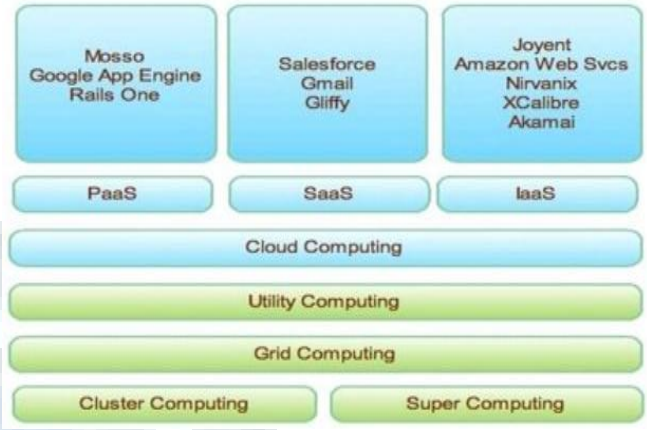

Fig 3: cloud computing service layers

Cloud computing security is an evolving sub-domain of computer security, network security, and information security. Cloud computing security refers to a broad set of policies, technologies, and controls deployed to secure data, applications, and the associated infrastructure of cloud computing. Cloud computing security is not to be confused with security software offerings that are cloud-based such as security as a service.

III. Security Issues Associated With The Cloud

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). There are number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and related hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

IV. Cloud Security Controls

Cloud computing security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that

will arise with security management. The security management addresses these issues with security controls. Security controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack.

Deterrent controls: Deterrent controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, deterrent controls do not reduce the actual vulnerability of a system.

Preventative controls: Preventative controls upgrade the strength of the system by managing the vulnerabilities. This control will safeguard vulnerabilities of the system. If an attack were to occur, these controls are in place to cover the attack and reduce the damage and violation to the system's security.

Corrective controls: These controls are used to reduce the effect of an attack. Unlike the preventative controls, these controls take action as an attack is occurring.

Detective controls: These controls are used to detect any attacks that may be occurring to the system. In the event of an attack, this control will signal the preventative or corrective controls to address the issue.

V. Security and Privacy

Identity management: Every enterprise will have its own identity management system to control access to information and computing resources. Cloud computing providers either integrate the customer's identity management system into their own infrastructure, using federation or Single Sign-On technology, or provide an identity management solution of their own.

Physical and personnel security: cloud computing Providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented.

Availability: Cloud computing providers assure customers that they will have regular and predictable access to their data and applications.

Application security: Cloud computing providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. Application security requires application security measures be in place in the production environment.

Privacy: Finally, cloud computing providers ensure that all critical data are masked or encrypted and that only authorized users have access to data in its entirety. Digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud. Legal issues: cloud computing providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.

II. RELATED WORK

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in [5]. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more, if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. Depending on the political context this trust may touch legal obligations. For instance, Italian legislation requires that government data of Italian citizens, if collected by official agencies, have to remain within Italy. Thus, using a cloud provider from outside of Italy for realizing an e-government service provided to Italian citizens would immediately violate this obligation. Hence, the cloud users must trust the cloud provider hosting their data within the borders of the country and never copying them to an off-country location nor providing access to the data to entities from abroad. An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. This might be done once, multiple times, or continuously. An attacker that also has access to the processing logic of the cloud can also modify the functions and their input and output data. Even though in the majority of cases it may be legitimate to assume a cloud provider to be honest and handling the customers' affairs in a respectful and responsible manner, there still remains a risk of malicious employees of the cloud provider, successful attacks and compromisation by third parties, or of actions ordered by a subpoena. In [6], an overview of security flaws and attacks on cloud infrastructures is given. Some examples and more recent advances are briefly discussed in the following. Ristenpart et al. [7], [8] presented some attack techniques for the virtualization of the Amazon EC2 IaaS service. In their approach, the attacker allocates new virtual machines until one runs on the same physical machine as the victim's machine. Then, the attacker can perform cross-VM side channel attacks to learn or modify the victim's data. The authors present strategies to reach the desired victim machine with a high probability, and show how to exploit this position for extracting confidential data, e.g., a cryptographic key, from the victim's VM. Finally, they propose the usage of blinding techniques to fend cross-VM side-channel attacks. In [9], a flaw in the management

interface of Amazon's EC2 was found. The SOAP-based interface uses XML Signature as defined in WS-Security for integrity protection and authenticity verification. Gruschka and Iacono [9] discovered that the EC2 implementation for signature verification is vulnerable to the Signature Wrapping Attack.

In this attack, the attacker—who eavesdropped a legitimate request message—can add a second arbitrary operation to the message while keeping the original signature. Due to the flaw in the EC2 framework, the modification of the message is not detected and the injected operation is executed on behalf of the legitimate user and billed to the victim's account. A major incident in a SaaS cloud happened in 2009 with Google Docs. Google Docs allows users to edit documents online and share these documents with other users. However, this system had the following flaw: Once a document was shared with anyone, it was accessible for everyone the document owner has ever shared documents with before. For this technical glitch, not even any criminal intent was required to get unauthorized access to confidential data. Recent attacks have demonstrated that cloud systems of major cloud providers may contain severe security flaws in different types of clouds (see [12], [10]). As can be seen from this review of the related work on cloud system attacks, the cloud computing paradigm contains an implicit threat of working in a compromised cloud system. If an attacker is able to infiltrate the cloud system itself, all data and all processes of all users operating on that cloud system may become subject to malicious actions in an avalanche manner. Hence, the cloud computing paradigm requires an in-depth reconsideration on what security requirements might be affected by such an exploitation incident. For the common case of a single cloud provider hosting and processing all of its user's data, an intrusion would immediately affect all security requirements: Accessibility, integrity, and confidentiality of data and processes may become violated, and further malicious actions may be performed on behalf of the cloud user's identity.

II. LITERATURE SURVEY

Dr Elaine Shi [4] described several enabling technologies towards this vision. Specifically, she told about 1) how to safeguard users' data against potentially compromised applications; 2) how to safeguard users' data against a potentially compromised computation provider; and 3) how to safeguard users' data against a potentially compromised storage provider. She told about our ongoing effort at integrating these technologies to provide a cloud infrastructure which offers data security at the platform level. In this way, users can benefit from the rich cloud applications without worrying about the privacy of their data; and application developers can focus on developing functionality while offloading the burden of providing security and privacy to the cloud platform. Performance According to a recent survey, 49% of users abandon a site or switch to a competitor after experiencing performance issues.[5] And the need for speed is only increasing: in 2000, a typical user was willing to wait 8 sec for a webpage to load before navigating away; by 2009, that number dropped to 3 sec. Platform verifiability: The DSaaS approach provides logging and auditing at the platform level, sharing the benefits with all cloud computing applications running on top. Offline, the cloud auditor can verify that the platform implements each data protection feature as promised. At runtime, the cloud platform provider can use trusted computing (TC) technologies to attest to the particular software that's running. TC uses the tamper proof TPM as well as the virtualization and isolation features of modern processors, such as Intel VT-x or AMD-V. TC also allows for a dynamic root of trust—while the system runs, the Central Processing Unit can enter a clean state, and the Trusted Platform Module (TPM) can verify, load, and execute a trusted computing base (TCB), TCB is responsible for security-critical functionalities such as access control, isolation enforcement, key management, and logging. Moreover, a third-party cloud auditor can verify the code of the trusted computing base that has been loaded on to the cloud computing platform. In this way, users and developers can gain confidence that the applications are indeed running on the correct trusted computing base and consequently trust the security guarantees and the audit logs the trusted computing base provides. One challenge in code attestation is how to establish a set of acceptable binaries in the presence of rapid software updates such as bug fixes and latest features. One potential way is to log the history of software updates and perform verification a posteriori. For the application itself, getting from verifiable to verified isn't easy; in a system with a lot of cloud users, doing all cloud pairs verification is prohibitively expensive. This is where cloud auditors come in. Certifications such as Statement on ASN70 (Auditing Standards Number 70) and others serve the important function of reducing the verification burden on both clients and service providers compared to pair wise examinations. Since applications have the data-security piece in common from the platforms, the application verifications in turn can be simpler than they otherwise would have been.

III.CLOUD STORAGE

Cloud storage [13] is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible.

People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources.

Figure 4: Cloud Storage

Cloud storage is made up of many distributed resources, but acts as one – often referred to as federated storage clouds. It is highly fault tolerant through redundancy and distribution of data. It is efficient and cost effective. i.e., through cloud storage, companies need only pay for the storage and service they actually use. Cloud storage provides users with immediate access to a broad range of resources and applications hosted in the infrastructure of another organization via a web service interface. The service provider handles the storage capacity so the user need not worry about the capacity and capability of storage. It also provides mechanism for creating, accessing and updating the outsourced data. The examples of cloud storage are Amazon S3, Microsoft Azure, etc. In cloud environment, the sensitive data of data owners are stored in the cloud storage and can be accessed from anywhere, everywhere and at any time. To protect data privacy, some cryptographic techniques like encryption can be introduced [14]. Thus the sensitive data is encrypted before uploading to the cloud storage. Mass storage and low expense provided by the cloud storage invites more and more enterprises and organizations to store their private data in cloud with effective security. A virtual private storage service is designed by taking the advantages of both public and private clouds. A public cloud provides scalable and dynamic storage and provides availability and reliability of data where as private clouds provide security and privacy for the data. Thus the virtual private storage service based on cryptographic techniques achieves both the security of a private cloud and functionality and cost savings of a public cloud. Other advantages of cryptographic cloud storage are the control of data is in the hands of customer and security properties are taken from cryptography.

IV CONCLUSION

In this paper we solve many problems that come in our cloud system like confidentiality and Integrity. By using this service we can make our cloud highly secure and efficient. Those users who have less resources and limited computing capability, they can use this service and it is most efficient service for them. Our service is also secured at the time of Dynamic Data operation like insertion deletion and updating. Secure Multiparty Computation (SMC) and Secret Sharing (SS) algorithm are used to improve the cloud security. Intrusion detection scheme is integrated with the multi-cloud environment for malicious attack handling. The system supports data and application model. Integrated security solution schemes are used to protect data and services. Attack resistant resource sharing system controls the service based attacks. Risk free resource management mechanism assures service availability in all situations.

REFERENCES

[1] C. Dwork, "The Differential Privacy Frontier Extended Abstract," Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, pp. 496-502, 2009.

[2] Mell, P. and Grance, T. (September 2011). "The NIST Definition of Cloud Computing. NIST Special Publication 800-145 (September 2011). National Institute of Standards and Technology, U.S. Department of Commerce" Retrieved 2012-05-20.

[3] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 179-80. Print., 2010.

[4] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control" PARC Fujitsu Laboratories of America.

[5] E. Naone, "The Slow-Motion Internet," Technology Rev., www.technologyreview.com/files/54902/ GoogleSpeed_charts.pdf. Mar./Apr. 2011;

[6] Kartik Sharma, Renuka Sharma, Gitesh Dalal International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 2348 ISSN 2229-5518 IJSER © http://www.ijser.org "A Secure Protocol for Data storage Security in cloud computing, 2013

[7] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory Computing (STOC 09), ACM, pp. 169-178. 2009.

[8] "Security Policy and Key Management: Centrally Manage Encryption Key". Slideshare.net. 2012-08-13. Retrieved 2013-08-06.

[9] E. Bertino, F. Paci, and R. Ferrini, "Privacy-Preserving Digital Identity Management for Cloud Computing," IEEE Computer Society Data Engineering Bulletin, Mar. 2009, pp. 1–4.

[10] M. Ko, G.-J. Ahn, and M. Shehab "Privacy-Enhanced User-Centric Identity Management," Proc. IEEE Int'l Conf. Communications, IEEE Press, 2009, pp. 998–1002.