DATA STORAGE, SECURITY AND TECHNIQUES IN CLOUD COMPUTING

[1]Sai Shobha R [2]Dinesh Arpitha R
[1,2]Lecturer,
[1,2]Department of Computer Science & Engineering,
Loyola Degree and PG College, Secunderabad, TS, India

ABSTRACT

Cloud computing is the computing technology which provides resources like software, hardware, services over the internet. Cloud computing provides computation, software, data access, and storage services that do not require end- user knowledge of the physical location and configuration of the system that delivers the services. Cloud computing enables the user and organizations to store their data remotely and enjoy good quality applications on the demand without having any burden associated with local hardware resources and software managements but it possesses a new security risk towards correctness of data stored at cloud. The data storage in the cloud has been a promising issue in these days. This is due to the fact that the users are storing their valuable data and information in the cloud. The users should trust the cloud service providers to provide security for their data. Cloud storage services avoid the cost storage services avoids the cost expensive on software, personnel maintains and provides better performance less storage cost and scalability, cloud services through internet which increase their exposure to storage security vulnerabilities however security is one of the major drawbacks that preventing large organizations to enter into cloud computing environment. This work surveyed on several storage techniques and this advantage and its drawbacks.

Keywords: Cloud computing, Data Storage, Data Security, Storage Techniques.

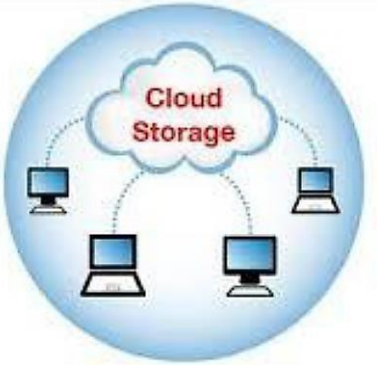
I. INTRODUCTION

Cloud computing is the next gen technology in the Internet's technology that provides the user everything in terms of services like computing power to computing infrastructure, applications, business processes as per the need of user over the internet. Cloud computing is an environment for providing information resources that are delivered as services to the end users over the internet. On demand cloud is a cloud file with defined essential characteristics such as on-demand self-services, Broad network access, resource pooling, rapid elasticity, measured services. The reason for people are moving towards cloud computing is that it allows the user to access data and resources from any geographical location and at any time. It has numerous advantages as reduced infrastructure costs, scalability, no maintenance and need to pay only for what user access.

One major use of cloud storage is long-term archival, which represents a workload that is written once and Arely read. While the stored data is rarely read, it remains necessary to ensure its integrity of its disaster recovery or compliance with legal requirements. Deployment models of cloud computing includes public cloud, private cloud, hybrid cloud and community cloud. Though there are many advantages of cloud computing, security concern has become the biggest obstacle in the adoption of cloud as data is completely under the control of cloud service provider (CSP), which leads to lack of control.

II. DATA STORAGE

Cloud storage is a model of data storage in which 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, and yet the physical environment protected and executing. People and organizations buy or lease storage space from the providers to store data of user, organization, or application.



Cloud storage services may be accessed through a co- located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

It 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. Cloud storage services can be utilized from an off-premises service (Amazon S3) or deployed on-premises.

Data storage in cloud is characterized by:

Is made up of many distributed resources, but still acts as one often referred to as federated storage clouds

Is highly fault tolerant through redundancy and distribution of data

Is highly durable through the creation of versioned copies

Is typically eventually consistent with regard to data replicas

Some of the advantages of storing data in cloud are:

Companies need only pay for the storage they actually use, typically an average consumption during a month. This does not mean that cloud storage is less expensive, only that it incurs operating expenses rather than capital expenses.

Businesses using cloud storage can cut their energy consumption by up to 70% making them a more green business. At the vendor level they deal with higher levels of energy thereby equipping to cut down the cost.

Storage availability and data protection is intrinsic to object storage architecture, so depending on the application, the additional technology, and effort and cost to add availability and protection can be eliminated.

Storage maintenance tasks like purchasing additional storage capacity are offloaded to the responsibility of a service provider.

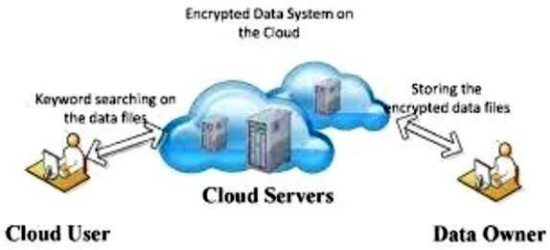
Cloud storage provides users with immediate access to a broad array of resources and applications hosted in the infrastructure of another organization through a web service interface.

Cloud storage can be used for copying virtual machine images from the cloud to on-premises locations or to import a virtual machine image from an on-premises location to the cloud image library. In addition, cloud storage can be used to move virtual machine images between user accounts or between data centers.

Cloud storage can be used as natural disaster proof backup, as normally there are 2 or 3 different backup servers

III. DATA SECURITY

Cloud computing security or in simple terms, cloud security is an evolving sub-domain of computer security, network security and more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.



Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. Organizations use the Cloud in a variety of different service models (SaaS, PaaS and IaaS) and deployment models (Private, Public, Hybrid, and Community). However security concern has become the biggest issues to adaption as cloud becomes all information and data are completely under the control of cloud service provider.

The major security aspect is **Confidentiality, Integrity, Authentication, Authorization, Non-repudiation and Availability** which are further explained below:

Confidentiality: Confidentiality specifies that only the sender and the intended-recipient should be able to access the intended information. It gets compromised if an unauthorized person is to access a message. Data encryption is one of the most popular options of security before pushing the data into cloud.

Integrity: It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. When the content of a message is changed before it reaches the intended recipient, the integrity of the message is lost. Hashing techniques, digital signatures and message authentication codes are used to preserve data integrity. Integrity problems are in big scale due to the multi-tenancy characteristic of cloud.

Authentication: Authentication is the mechanism by which the systems may securely identify their users. It determines the level of access to system resources attributed to a particular authenticated user.

Authorization: Authorization is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud computing.

Non-repudiation: Non-repudiation is an extension to the identification and authentication service. It does not allow the sender of a message to refute the claim of not sending the message. It is used to ensure that the messages sent are properly received and acknowledgements are sent back to the sender. In other words, establishing a two way communication between a sender and a receiver.

Availability: The principle of availability states that resources should be available to third-parties at all times. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's also important to keep system upgrades updated.

IV. STORAGE TECHNIQUES

This section details various existing techniques which are prevalent. Cloud storage is regarded as a system of disseminated data centers that generally utilizes virtualization technology and supplies interfaces for data storage:

Implicit Storage Security to Data in Online: In this scheme data is partitioned in such way that each unit is implicitly secure and does not to be encrypted. These units are stored on different servers on the network which are known only to the user. Several variations of this scheme are described, which include the implicit storage of encryption keys rather than the data and where a subset of the partition may be brought together to recreate the data.

Identify Based Authentication: In Cloud Computing, resources and services are distributed across numerous consumers. So there is a chance of various security risks. Thus authentication of users as well as services is an important requirement for cloud security and trust. SSL Authentication Protocol (SAP) once applied in cloud computing will become so complicated, that users will undergo heavily loaded point both in computation and communication. When comparing performance, authentication protocol based on identity is very weightless and more efficient and also weightless protocol for client side.

Public Auditing with Complete Data Dynamic Support: Verification of data integrity at unreliable servers is the major concern in cloud storage. Public auditing system that supports an external auditor to audit user's outsourced data in the cloud without learning knowledge on data content. Public auditing system with protocol that supports complete dynamic data operations to be presented.

Efficient Third Party Auditing (TPA): Cloud consumers save data in cloud server so that security as well as data storage correctness is primary concern. The data owners having huge amount of outsourced data and the take of auditing the data correctness in a cloud environment can be difficult and expensive for data owners. To support third party auditing where user safely delegate in integrity checking tasks to third party auditors(TPA)this scheme can almost guarantee the simultaneous localization of data error(i.e. the identification of misbehaving servers)

Way of Dynamically Store Data in Cloud: Data storage is cloud may not be completely trustable because the clients did not have local copy of data stored in cloud. To address these issues proposed a new protocol system using the data reading protocol algorithm to check the data integrity services providers help the clients to check the data security by the proposed effective automatic data reading algorithm. To recover data in future, also presented a multi-server data comparison algorithm with overall data calculation in each update before outsourcing it to server's remote access point.

Effective and Secure Storage Protocol: A secure and efficient storage protocol is proposed that guarantees the data storage confidentiality and integrity. Cloud Server challenges a random set of blocks that generates probabilistic proof of integrity. Challenge-Response protocol is credential so that it will not exposes the contents of data to outsiders. Data dynamic operations are also used to keep the same security assurance and also provide relief to users from the difficulty of data leakage and corruptions problems.

Storage Security of Data: The data is secured in server based on user's choice of security method so that data is given high secure priority resources are being shared across server trouble to data security in cloud.

The proposed effective and flexible distribution scheme two-way handshakes based on token management by utilizing the homomorphic token with distributed verification of erasure coded data, our scheme achieves the integration of storage correctness insurance and data error location (i.e) the identification of misbehaving server.

Secure and Dependable Storage Services: Storage service of permits consumers to the data in cloud as well as allowed to utilize the available well qualified application with no worry data storage maintenance. Although cloud providers benefits, such a service gives up the self-control of user's data that introduced fresh volubility hazards to cloud data correctness. The proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed coded-data. The proposed design further support secure and efficient dynamic operation on outsource data including block modification, deletion and append.

Optimal Cloud Storage Systems: Cloud data storage which requires no effort is acquiring more popularity for individual, enterprise and institutions data backup and synchronization. A taxonomic approach to attain storage service optimality with resource provider, consumer's lifecycle is presented. Cloud data storage which requires no effort is acquiring more popularity for individual, enterprise and institutions data backup and synchronization. The proposed system describes, at a high level, a possible architecture for a cryptographic storage service. At this core, the architecture consists of three components, a data processor (DP) that processes data before it is sent to the cloud a data verifier (DV) that checks whether the data in the cloud has been tampers with, and a token generator (TG) that generator token which enables the cloud storage providers to retrieve segments of consumer data.

Process of access and Store Small Files with Storage: To support internet services extensively, Hadoop distributed file system (HDFS) is acquired. Several reasons are examined for small file trouble of native Hadoop distributed file system: Burden on NameNode of Hadoop distributed file system is enforced by large amount of small files, for data placement correlations are not considered, prefetching mechanism is not also presented. In order to overcome these small size problems, proposed an approach that improves the small files efficiency on Hadoop distributed file system.

File Storage Security Maintenance: To assure the security of stored data in cloud, two ways are used namely master server and a set of slave server. Master server is responsible to process the client's request and at slave server chunking operation in order to provide data backup for file recovery in future. Clients file is stored in the form of tokens on main server and files were chunked on slave server for file recovery.

CONCLUSION

Cloud computing is a new computational paradigm that offers an innovative business model for organization to adopt. Cloud computing moves the application software and database to the large data centre where the data management and service may not be worthy. The security is an important aspect of quality of service. Cloud storage is much more beneficial and advantageous than the earlier traditional storage systems especially in terms of scalability, cost reduction, portability and functionality requirements. This paper gives an idea about the data storage techniques and in future only focus on data storage along with compression in cloud computing that promises the security to data in cloud.

VI. REFERENCES

Judith Hurwitz, Robin Bloor, Marcia Kaufman, and Fern Halper," what is Cloud Computing For Dummies", "http://www.dummies.com/how- to/content/what-is-cloud-computing.html", last modified 2013.

Jason, "Defining Cloud Deployment Models":" http://bizcloudnetwork.com/defining-cloud- deployment-models", Last modified on AUGUST 4, 2010.

Margaret Rouse, "Cloud Application Performance Management: Doing The Job Right", last modified December 2010.

Anju Bala, Inderveer Chana, "Fault Tolerance- Challenges, Techniques and Implementation in Cloud Computing", in the year of January 2012.

Tadapaneni, N. R. (2018). Cloud Computing: Opportunities And Challenges. International Journal of Technical Research and Applications.

Rakhi Bhardwaj, Vikas Maral, "Dynamic Data Storage Auditing Services in Cloud Computing", in the year of April 2013.

Yogita Gunjal, Prof. J.Rethna Virjil Jeny, "Data Security and Integrity of Cloud Storage in Cloud Computing", in the year of April 2013.

Wang C , Wang Q et al . (2012),Towards secure And dependable Storage Services in Cloud Computing , IEEE Transactions on Services Computing ,vol5(2),220-232.

Tadapaneni, N. R. (2017). Different Types of Cloud Service Models. Available at SSRN 3614630.

] Dong B , Zheng Q et al.(2012). An optimized Approach for storing and Accessing small files on cloud storage,Journal of Network and Computer Applications ,35(6),1847-1862

] Deahmukh P M,Gughane A S et al.(2012).Maintaining Files Storage Security in Cloud Computing International Journal of Emerging Technology and Advance Engineering ,vol2(10),2250-2459.

] Tang Y,Lee P P C et al(2010).FADE: A Secure overlay Cloud Storage System with File assured Deletion ,6th International ICST Conference, Secure Comm.

] Wang W,Li Z et al(2009).Secure and efficient Access to outsource Data, CCSW '09 Proceedings of the 2009 ACM workshop on Cloud Computing Security,55-66.

] Tadapaneni, N. R. (2016). Overview and Opportunities of Edge Computing. Social Science Research Network.

] Ensuring Data Storage Security in Cloud Computing. IOSR Journal of engineering – vol 2 (12) - (2012) 225.

] Spillner J, Muller J et al (2012).Creating Optimal Cloud Storage System,future Generation Computer Systems ,vol29(4),1062-1072

] Liu, Allan and Yu, Ting, Overview of Cloud Storage And Architecture (2018). International Journal of Scientific & Technology Research

] R. Yogamangalam and V.S. Shankar Sriram, "A Review on Security Issues in Cloud Computing", in the year of 2013.

] Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387, 103-115.