IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 13-17
www.iosrjournals.org

Distributed Mobile Cloud Computing With Module for Secure Big Data

M.Sripriya M.Sc.,
Mphil Full Time Scholar Vivekanandha College For Women,
Tiruchengode Prakashpriya14084@gmail.com
S.Jayabharathi Msc., MCA., M.Phil., Assistant Professor, Vivekanandha College For Women,
Tiruchengode Jayabharathi8383@gmail.com

***Abstract**: mobilecloud computing applications. To ensure a correctness of users' data in the mobile cloud, our study an effective and secure distributed model including a Self-Proxy Server (SPS) with self-created algorithm. The model resolves a communication Mobile cloud computing provides a novel ecommerce mode for organizations without any upfront investment. Since cloud computing uses distributed resources in open environment, it is important to provide secure keys to share the data for developing bottleneck due to re-encryption of a shared data in the cloud whenever users are revoked. It offers to reduce security risks and protect their resources because a distributed SPS dynamically interacts with Key Manager (KM) when the mobile users take on cloud services. This paper describe a survey of comprehensive mobile cloud design which provides an effective and secure mobile cloud computing services on mobile devices.*

***Keywords:** Mobile Cloud Database, SPS, Key Management,, Multi key Distribution, Self Proxy Server*

I. Introduction

Managing and providing computational resources to client applications is one of the main challenges for the high performance computing community framework. To monitoring resources existing solutions rely on a job abstraction for resource control, where users submit their applications as batch jobs to a resource management system responsible for job scheduling and resource allocation. This usage model has served the necessities of a large number of users and the execution of numerous scientific application. However, this usage model requires the user to know very well the environment on which the application will perform. In addition, users can sometimes require administrative privileges over the resources to customize the execution environment job model. The manage and increasing availability of virtual machine technologies has enabled another form of resource control based on the abstraction of containers. A virtual machine can be leased and used as a container for deploying applications. Under this scenario, users lease a number of virtual machines with the operating system of their choice; these virtual machines are further customized to provide the software stack required to execute user applications. This form of resource control has allowed leasing abstractions that enable a number of usage models, including that of batch job scheduling. Investigate whether an infrastructure base operating its local cluster can benefit from using Cloud providers to improve the performance of its users' requests. Evaluate scheduling strategies suitable for a distributed cloud that is managed by proposed technology to improve its SQL operation with adaptive encryption data values. These strategies aim to utilize remote resources from the Cloud to augment the capacity of the SQL operation. However, as the use of Cloud resources incurs a cost, the problem is to the price at which this performance improvement is achieved. The focus of paper is exploring the trade between performance improvement and cost using decryption and encryption key. As an application, they suggested private data banks: a user can store its data on an untrusted server in encrypted form, yet still allow the server to process, and respond to, the user‘s data query (with responses more concise than the unimportant solution: the server just sends all of the encrypted data back to the user to process). Since then, cryptographers have accumulated a list of ―killer applications for fully homomorphism encryption. However, prior to this proposal, we did not have a viable construction.

This approach is rather original because relate work is evaluate the process and connection of porting logical applications to a distributed cloud platform, Besides the focus on a different context (logical versus database applications), the proposed model can be applied to any distributed cloud database service provider, and it takes into account that over a medium-term period the database workload and the distributed cloud prices may vary.

II. Litrature Survey

Mohamed al Morsy et al [1] describe a cloud computing is a new computational paradigm that offers an innovative business model for organizations to adopt IT without upfront investment. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption This paper [1] introduces a detailed analysis of the cloud security problem. To investigate the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders' perspective, and the cloud service delivery models perspective. Based on this analysis they derive a detailed specification of the cloud security problem and key features that should be covered by any proposed security solution.Cloud computing provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely used definition of the cloud computing model is introduced by NIST as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.An adaptive model-based approach is tackling the cloud security management problem. Models will help in the problem abstraction and the capturing of security requirements of different stakeholders at different levels of details. Adaptive-ness will help in delivering an integrated, dynamic and enforceable cloud security model. The feedback loop will measure the security status to help improving the current cloud security model and keeping cloud consumers aware with their assets' security status (applying the trust but verify concept).JJon Brodkin [2] describe a Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand (Leighton, 2009). According to Gartner, while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial (Gartner Hype-Cycle, 2012 As per the definition provided by the National Institute for Standards and Technology (NIST) "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 or service provider interaction". It represents a paradigm shift in information technology many of us are likely to see in our lifetime.Public cloud: Public clouds are provided by a designated service provider and may offer either a single tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off premises). All customers share he same infrastructure pool with limited configuration, security protections, and availability variances. One of the advantages of a public cloud is that they may be larger than an enterprisePrivate cloud: Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds:(i) on-premise private clouds and (ii) externally hosted private clouds. The on-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources.This is best suited for applications which require complete control and configurability of the infrastructure and security.

As the name implies, the externally hosted private clouds are hosted externally with a cloud provider in which the provider. Hybrid cloud: Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. With a hybrid cloud, service providers can utilize third party cloud providers in a full or partial manner, thereby increasing the flexibility of computing. The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload. Corporate partnerships and offshore outsourcing involve similar trust and regulatory issues. Similarly, open source software enables IT department to quickly build and deploy applications, but at the cost of control and governance. Similarly, virtual machine attacks and web service vulnerabilities existed long before cloud computing became fashionable. Indeed, this very overlap is reason for optimism; many of these cloud computing roadblocks have long been studied and the foundations for solutions exis Ramgovind.S et al [3] describe a Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure.

However the opportunity cost of the successful implementation of Cloud computing is to effectively manage the security in the cloud applications. Security consciousness and concerns arise as soon as one begins to run applications

III. Methodology

Like existing system, proposed system also manages the data using both cloud server side and client side. In addition, user group is maintained so that a single key is distributed to multiple users in the same group to reduce the key preparation overhead for each user. This makes less computation overhead in both client and server side. Also, based on the security level, different data is encrypted with different encryption mechanism and allowed to secure the data in inexpensive manner.

1. Multi-user key distribution scheme is proposed to provide data to the same group of users.
2. Encryption cost and thereby data transmission cost is less.
3. Different kind of encryption is maintained for various data saved in the cloud nodes based on the security level requirement.

An individual or an organization may not require purchasing the needed storage devices. Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware / software failures. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. Preserving authorized restrictions on information access and disclosure. The main there at accomplished when storing the data with the cloud. To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store the file to the cloud. If a third person downloads the file, he/she may view the record if he/she had the key which is used to decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. To overcome the problem there are lot of techniques introduced to make secure transaction and secure storage. Anonymous authentication is the process of validating the user without the details or attributes of the user. So the cloud server doesn't know the details or identity of the user, which provides privacy to the users to hide their details from other users of that cloud. Sp that proposes a secure cloud storage using decentralized access control with anonymous authentication. The files are associated with file access policies, that used to access the files placed on the cloud. Uploading and downloading of a file to a cloud with standard Encryption / Decryption is more secure. Revocation is the important scheme that should remove the files of

A. Service Layers of Cloud Computing

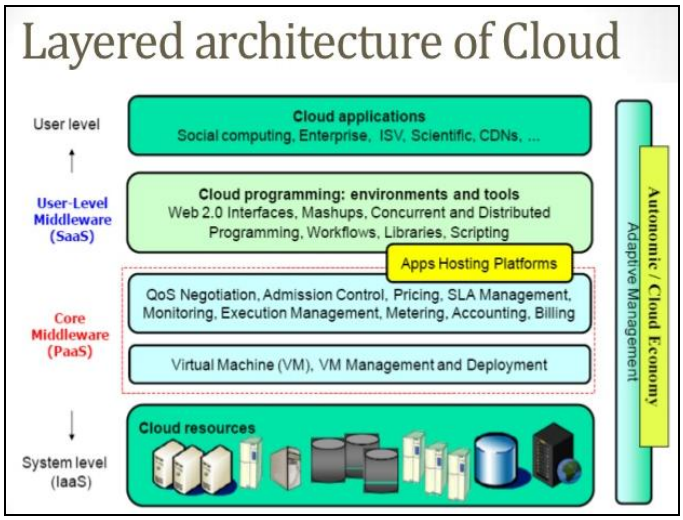
Cloud computing can be viewed as a collection of services, which can be represented as a layered cloud computing architecture. The cloud computing layered architecture has Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Monitoring as a Service (MaaS).

SaaS (Software as a Service): It is a model of software deployment whereby the provider licenses an application to the customers for use as a service on demand. The capability provided to the end users 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. The end users does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities with the possible exception of limited user specific application configuration settings.

PaaS (Platform as a Service): It is the delivery of computing platform and solution stack as a service. The capability provided to the end users is to deploy onto the cloud infrastructure user created or acquired applications created using programming languages and tools supported by the provider. The end user does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage. 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 (non-cloud computing) delivery of application platforms and databases.

IaaS (Infrastructure as a Service): It is the delivery of computer infrastructure (typically a platform virtualization environment) as a service. The capability provided to the end users is to provision processing, storage, networks, and other fundamental computing resources where the end user is able to deploy and run arbitrary software, which can include operating systems and applications. The user does not manage or control the underlying cloud infrastructure but it has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

MaaS (Monitoring as a Service): It is the outsourced provisioning of security, primarily on business platforms that leverages the internet to conduct business. MaaS has become increasingly popular over the last decade. Its popularity has grown even more because of the advent of cloud computing. Security monitoring involves protecting an enterprise or government client from cyber threats. A security team plays a crucial role in securing and maintaining the confidentiality, integrity, and availability of IT assets.The tools being offered by MaaS providers may vary in some ways, but there are very basic monitoring schemes that have become ad hoc standards simply because of their benefits. State monitoring is one of them, and has become the most widely used feature. It is the overall monitoring of a component in relation to a set metric or standard. In state monitoring, a certain aspect of a component is constantly evaluated, and results are usually displayed in real time or periodically updated as a report. For example, the overall timeout requests measured in a period of time might be evaluated to see if this deviates from what's considered an acceptable value.



B Secure Mobile Cloud Computing With Self-Proxy Server (SPS)

A cloud is basically a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. However, there are still a number of challenges because they are preventing the mobile users to take on cloud services. A model for key distribution based on data re encryption is applied to a cloud computing system to address the demands of a mobile device environment, including limitations on mobile data usage, storage capacity, processing power, and battery etc. When an encrypted data is stored and decryption key is allocated to user, they can access data from cloud.While a user is revoked and he has decryption key he can access data still, thus to overcome from this problem here is a need of immediate re encryption of data by data owner. When re-encryption is done the newly generated, decryption keys are distributed to authorized users. This resolution will lead to performance bottleneck, particularly when there are many user revocations. A solution is to apply a distributed self proxy re encryption technique, so this scheme proposes Self Proxy Server (SPS). It coordinates and chooses keys by Key Manager (KM) whenever group membership changes. The distributed SPS provides not only encryption and decryption keys but also immediate re encryption keys for shared data. After communicating with KM, it automatically receives necessary keys from KM by self created algorithm. A distributed SPS scheme is one solution where multiple proxy are automatically deployed in several clouds. Mobile Cloud Provider (MCP) has significant resources and expertise in building and managing distributed cloud storage servers and computational services to data, owns and operates live cloud computing systems. Data Owner (DO) has data to be stored in the cloud and rely on the cloud for data computation, consists of both individual consumers and organizations.

IV. Conclusion

In this experimental study, the existing system is describing the problem of secure verification for storage in cloud. In this paper, proposed FA which carries out a legible file-sharing scheme between an owner who stores the data in one cloud party and applications which are registered within another cloud party. The security analysis shows that our Fuzzy Authorized scheme provides a thorough security of outsourced data, including confidentiality, integrity and secure access control. Fuzzy Authorized approach reduces the storage consumption compared to other similar possible authorization schemes. It also asserts that our scheme could efficiently achieve distance tolerance and realize fuzzy authorization in practice research study. This work

mainly addresses the reading authorization issue on cloud storage. And it results to enable the TPA to perform audits for multiple users simultaneously and efficiently. The following enhancements are should be in future.

Acknowledgment

My heartfelt gratitude goes to my beloved guide Mrs.S.Jayabharathi Assistant Professor, Department of Computer Science, Vivekanandha College for Women, Tiruchengode, India for dedication and patience in assigning me her valuable advice and efforts during the course of my studies.

References

[1]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, ―Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,Future Generation Comput. Syst., vol. 25, no. 6, pp. 599–616, 2009.

[2]. T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. Sebastopol, CA, USA: O'ReillyMedia, Inc., 2009.

[3]. H.-L. Truong and S. Dustdar, ―Composable cost estimation and monitoring for computational applications in cloud computing environments, Procedia Comput. Sci., vol. 1, no. 1, pp. 2175–2184, 2010.

[4]. E. Deelman, G. Singh, M. Livny, B. Berriman, and J. Good, ―The cost of doing science on the cloud: The montage example, in Proc. ACM/IEEE Conf. Supercomputing, 2008, pp. 1–12.

[5]. H. Hacig€ um€ u¸ s, B. Iyer, and S. Mehrotra, ―Providing database as a service,‖ in Proc. 18th IEEE Int. Conf. Data Eng.,Feb.2002, pp. 29–38.

[6]. G.Wang, Q. Liu, and J. Wu, ―Hierarchical attribute-based encryption for fine-grained access control in cloud storage services, in Proc. 17th ACMConf. Comput. Commun. Security, 2010, pp. 735–737.

[7]. Google. (2014, Mar.). Google Cloud Platform Storage with server side encryption [Online]. blogspot.it /2013/08 /google-cloud-storage-now-provides.html.

[8]. A. N.Khana, M. L.M. Kiaha, S.U. Khanb and S. A. Madanic, "Towards Secure Mobile Cloud Computing: A Survey", Future Generation Computer Systems, vol.29, Issues 5, July 2013.

[9]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, Above the clouds: a Berkeley view of cloud computing, Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb. 2009.

[10]. R. Ranjan, A. Harwood, R. Buyya, Grid federation: an economy based distributed resource management system for large-scale resource coupling, Technical Report GRIDS-TR-2004-10, Grid Computing and Distributed Systems Laboratory, University of Melbourne, Australia, 2004.