# A Security Framework in Cloud Computing Infrastructure

G. Radha Devi
Research Scholar, Department of CSE
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal, MP (India)

## ABSTRACT

In a typical cloud computing diverse facilitating components like hardware, software, firmware, networking, and services integrate to offer different computational facilities, while Internet or a private network (or VPN) provides the required backbone to deliver the services. The security risks to the cloud system delimit the benefits of cloud computing like “on-demand, customized resource availability and performance management”. It is understood that current IT and enterprise security solutions are not adequate to address the cloud security issues. This paper explores the challenges and issues of security concerns of cloud computing through different standard and novel solutions. We propose analysis and architecture for incorporating different security schemes, techniques and protocols for cloud computing, particularly in Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) systems. The proposed architecture is generic in nature, not dependent on the type of cloud deployment, application agnostic and is not coupled with the underlying backbone. This would facilitate to manage the cloud system more effectively and provide the administrator to include the specific solution to counter the threat. We have also shown using experimental data how a cloud service provider can estimate the charging based on the security service it provides and security-related cost-benefit analysis can be estimated

## I. Introduction

Cloud computing advanced procedure power and improved storage capabilities. Cloud computing permits the sharing of services over the web, which may be seen as a long unreal vision of computing utility. The framework tend to store data and run application at the Cloud, consists of an oversized group of interconnected computers. Value savings is the main advantage over the cloud on the opposite hand its security is leading disadvantage. Several computer code industries use cloud like Amazon, Google, e-Bay and Facebook etc. Many institutions adopt their own structure for the data security. Security is not guaranteed over the cloud since the information placed at cloud is accessed by anybody.

**Types of cloud computing:**

**Public Cloud:** Referred to as Shared Cloud as resources and services area unit shared among large no of users. Example of combination of SaaS and Public Cloud is Google Docs where each user can manufacture their document and share among completely different users. Throughout this Google Docs is code on Public cloud that is freely on the market to all or any users. Example of combination of PaaS and Public Cloud is Windows Azure. Example of combination of IaaS and Public cloud is Amazon EC2 Cloud.

**Private Cloud:** It is kind of cloud that is developed for single organization. In this kind of cloud, services are managed by third party or by organization by themselves. Maintenance, security are managed by organization solely. Individuals working in organization can use the services and resource of cloud while others are restricted to use. Main advantage of private cloud over public cloud is that control over all services and resources in hands of organization, they'll customize services and resources according to their organization requirements.

**Community Cloud:** It is an extension to private cloud. Community cloud has similar options to private cloud in terms of services and resources however it's utilized by large number of user than private cloud users. Community cloud is combination of three or four personal cloud that has common options. Community clouds are ruled by a community or by third party and completely different organization users will use community cloud.

**Hybrid Cloud:** As the name suggests this sort of clouds are combinations of different quite cloud (public, private, community). Its combine the public and private cloud and community cloud's characteristics. Its advantage is that each type of user wherever insider or outsider of organization will access the cloud services and resources.

Cloud computing services

**SaaS (Software as Service):** In this Cloud Service provider develops or install code on cloud and accessible these code to users on rental basis. It’s the front layer in style of cloud computing that represents face application of cloud computing. Among each variety of services it is best service to use and users need to contemplate solely a number of things to use it. Most of the appliance of SaaS is directly accessible via internet browsers whereas some are developed for Desktop Application. SaaS is that the simplest services on cloud and want not any code to place in on your machines to use it. Cloud Service provider style these service with care that user can user them terribly simply.

**PaaS Platform as a Service:** If people expect regarding Service Model as layer design than users will say Platform as Service is layer once coding system as service layer. Platform as service means providing platform like net server, software. Really Platform provides atmosphere for the event of coding systemapplications on cloud.

The entire pc code services area unit developed on the premise of underline platform. Platform as a service is provided via virtual machines place in on cloud.

**IaaS Infrastructure as Service:** It is the bottom abstraction layer of service model. It’s also mentioned as Hardware as a Service. All the physical devices like server, network devices, storage disk comes below IaaS. During this CSP provides Infrastructure only and users need to set their own platforms like operating systems, data servers, net servers and need to develop their own code packages. All reasonably terms and condition to use this code is created by users only. Security, resource pooling like issues are handled by users only. Users have a tendency to the Cloud- Migration system that provides each configuration validation and installation automation which minimize the configuration errors and installation complexness.

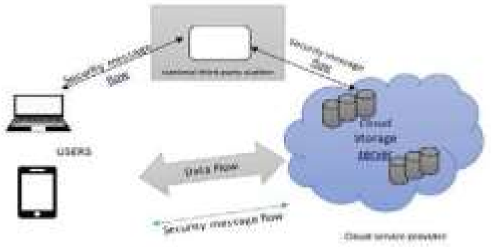

**Figure 1: Architecture of cloud data storage**

## 2. Related Work

Many researchers have conducted work related to the security and privacy problem in cloud computing.

We summarize this work here: In Popovic et al. presented some standards that can be used to address security issues in cloud computing such as: Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO 27001/27002) and Open Virtualization Format (OVF). In Ramgovind et al. presented guidelines for managing cloud security which include: cloud governance, cloud transparency and cloud computing security impacts.

In the authors proposed an Effective Privacy Protection Scheme (EPPS) to provide the appropriate privacy protection for cloud services. EPPS satisfies users' privacy requirements and maintains system performance simultaneously. First, they analyzed the privacy level users require and quantified the security degree and performance of encryption algorithms. Then, an appropriate security composition is derived by the results of analysis and quantified data. Their simulation results showed that the EPPS not only fulfils users' privacy requirements but also maintains the cloud system performance in different cloud environments. The execution results show that EPPS outperforms other security schemes by 35% to 50%.

In order to satisfy the assurances of cloud data integrity and availability and enforce the quality of cloud storage services for users, the authors proposed a highly efficient and flexible distributed storage verification scheme with two salient features. By utilizing a homomorphic token with distributed erasure coded data, their scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior work, the new scheme further supports secure and efficient dynamic operations on outsourced data, including: block modification, deletion and appending. Extensive security and performance analysis showed that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attacks, and even server collusion attacks.

The work studied the problem of ensuring the integrity of data storage in Cloud Computing. In particular, the authors considered the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminated the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for cloud computing. They stated that a significant step toward practicality is the support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, since services in cloud computing are not limited to archive or backup data only. While prior work on ensuring remote data integrity often lacks support for either public auditability or dynamic data operations, this work achieves both. The authors showed how to construct an elegant verification scheme for the seamless integration of these two salient features in their protocol design. In particular, to achieve efficient data dynamics, they improved the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, they explored the technique of bilinear aggregate signature to extend their main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis showed that the proposed schemes are highly efficient and provably secure.

## 3. Proposed work

This research proposes an efficient and versatile distributed theme with express dynamic data support to confirm the correctness of users' data in the cloud. This analysis considers erasure correcting code within the file distribution preparation to produce redundancies and guarantee the information reliability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our theme achieves the storage correctness insurance as well as knowledge error localization: whenever information corruption has been detected during the storage correctness verification, our theme can virtually guarantee the concurrent localization of knowledge errors, i.e., the identification of the misbehaving server(s).

1. In contrast to most prior works for making certain remote data integrity, the new theme supports secure and economical dynamic operations on knowledge blocks, including: update, delete and append.

2. Extensive security and performance analysis shows that the proposed theme is extremely economical, malicious knowledge modification attack, and even server colluding attacks. The foremost of the dominant databases like MySQL, MSSQL, etc. do not appear to be cross platform by itself. But the vendors provide versions for each platform. In databases like MySQL there is restriction inside the foremost vary of cursors that will be used. Therefore it cannot support style of applications as rear at constant time. Next disadvantage arises inside the case of knowledge format they use. Proprietary information storage formats cause issue in porting the information and feeding information to applications

## 4. Conclusion

The problem information security in cloud data storage that is actually a distributed storage system. To make sure the correctness of user's information in cloud information storage, the research define an efficient and versatile migration scheme with specific dynamic information support, as well as block update, delete, and append. And consider code within the preparation of file distribution to produce redundancy parity vectors and guarantee the information reliable. By utilizing with distributed verification of coded information, i.e., whenever information corruption has been detected throughout correctness of the storage verification across the distributed servers, user can nearly guarantee the concurrent identification of the misbehaving server(s).

## References

[1] GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," White Paper, GTSI Corporation, 2009.

[2] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review, Volume 39 Issue 1, pages 50-55, January 2009.

[3] M. Boroujerdi and S. Nazem, "Cloud Computing: Changing Cogitation about Computing," World Academy of Science, Engineering and Technology, 2009.

[4] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin,

I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.

[5] Kresimir Popvoic and Zeljko Hocenski, "Cloud Computing Security Issues and Challenges" MIPRO, Opatijia, Croatia, May 24-28, 2010.

[6] Radu Prodan and Simon Ostermann, "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers", 10th IEEE/ACM International Conference on Grid Computing, 2009

[7] http://en.wikipedia.org/wiki/Cloud_computing

[8] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing" Communication of the ACM, Vol. 53, No. 4, April 2010.

[9] K. Chard, S. Caton, O. Rana and K. Bubendorfer, "Social Cloud: Cloud Computing in Social Networks" 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.

[10] L. Tang, J. Dong, Y. Zhao and L. Zhang "Enterprise Cloud Service Architecture" 3rd IEEE International Conference on Cloud Computing,Miami, FL, USA, July 5-10,2010.

[11] W. Jansen and T.Grance "Guidelines on Security andPrivacy in Public Cloud Computing", NIST Draft SpecialPublication800-144, 2011.http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[12] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S.Creese and P. Hopkins, "The Cloud: Understanding theSecurity, Privacy and Trust Challenges",RANDCorporation, 2010.http://cordis.europa.eu/fp7/ict/security/docs/the-cloudunderstanding-security-privacy-trust-challenges- 2010_en.pdf

[13] NIST, http://www.nist.gov/itl/cloud/index.cfm

[14]CloudComputingvs.Virtualization http://www.learncomputer.com/cloud-computing-vsvirtualization/

## About Author

G.Radha Devi
Research Scholar
Department of CSE
Sri Satya Sai University of Technology and Medical Sciences Bhopal MP (India)