

# Privacy Preserving Searchable Encrypted Public Auditing for Secure Cloud Storage

<sup>1</sup>A.Gokilavani, <sup>2</sup>V.Gokulprasath, <sup>3</sup>K.Kishore Kumar, <sup>4</sup>S.Sivaprakash, <sup>5</sup>G.Thangavel

<sup>1</sup>Assistant Professor, Department of Computer Science Engineering, Jai Shriram Engineering College, Tirupur,  
Tamil Nadu, India

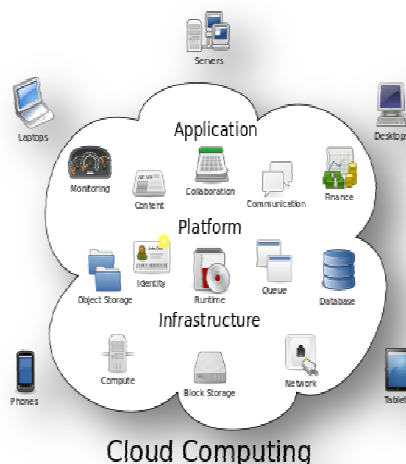
<sup>2,3,4,5</sup>UG Scholar, Department of Computer Science and Engineering, Jai Shriram Engineering College, Tirupur,  
Tamil Nadu, India

**ABSTRACT:** Cloud storage services have become commercially popular due to their overwhelming advantages. To provide ubiquitous always-on access, a cloud service provider (CSP) maintains multiple replicas for each piece of data on geographically distributed servers. A key problem of using the replication technique in clouds is that it is very expensive to achieve strong consistency on a worldwide scale. In this paper, we propose a privacy-preserving public auditing system for data storage security in cloud computing. which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task. In cloud computing and cloud garage environment, The audit logs support a seek at the encrypted audit .

**KEYWORDS:** C#, .Net , SQL , Visual studio 4.0

## I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers



**Fig 1:** Structure of Cloud Computing



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 7, Issue 3, March 2019

## II. CHARACTERISTICS AND SERVICES MODELS

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below

### FILE UPLOAD

The client made request to the key manager for the public key, which will be generated according to the policy associated with the file.

### FILE DOWNLOAD

The client can download the file after completion of the authentication process. As the public key maintained by the key manager, the client request the key manager for public key.

### FILE ACCESS CONTROL

Ability to limit and control the access to host systems and applications via communication links.

To achieve, access must be identified or authenticated. After achieved the authentication process the users must associate with correct policies with the files.

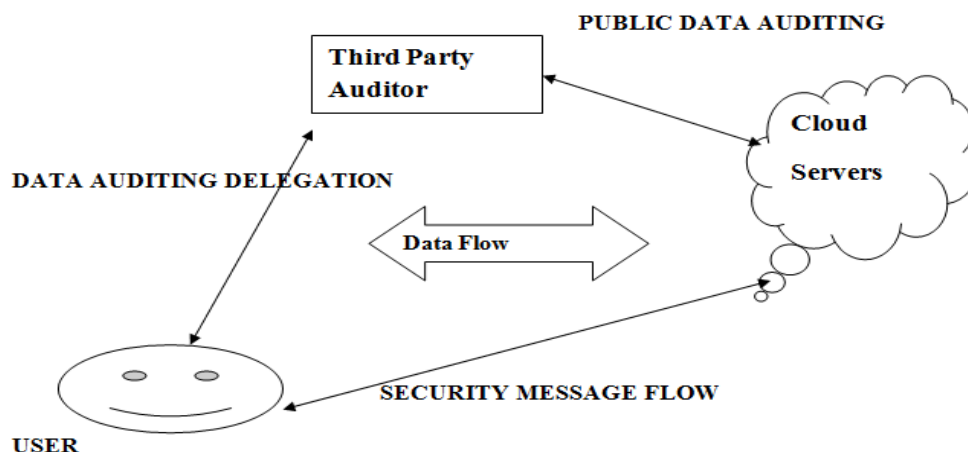
### INTEGRITY CHECKING

The user can restricted to read or write option means the file can be uploaded by admin gives permission to registered users. The write permission is accessed by user only can extra modification is possible. The admin can activate the users.

### USER REVOCATION MODULE

User can access the data is on particular time. So then user needs to get the keys again. Userrevocation is one of the biggest security threats in data sharing in groups. During userrevocation shared data block signed by revokeduser needs to download and re-sign by existing user. This task is very inefficacious due to the large size of shared data blocks on cloud.

### SYSTEM ARCHITECTURE





# International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 7, Issue 3, March 2019

## III. BENEFITS OF CLOUD COMPUTING

Achieve economies of scale – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets. Reduce spending on technology infrastructure. Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand. Globalize your workforce on the cheap. People worldwide can access the cloud, provided they have an Internet connection. Streamline processes. Get more work done in less time with less people. Reduce capital costs. There's no need to spend big money on hardware, software or licensing fees. Improve accessibility. You have access anytime, anywhere, making your life so much easier! Monitor projects more effectively. Stay within budget and ahead of completion cycle times. Less personnel training is needed. It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues. Minimize licensing new software. Stretch and grow without the need to buy expensive software licenses or programs. Improve flexibility. You can change direction without serious "people" or "financial" issues at stake.

### ADVANTAGES

- a. Price: Pay for only the resources used.
- b. Security: Cloud instances are isolated in the network from other instances for improved security.
- c. Performance: Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
- d. Scalability: Auto-deploy cloud instances when needed.
- e. Uptime: Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
- f. Control: Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
- g. Traffic: Deals with spike in traffic with quick deployment of additional instances to handle the load.

## IV. EXISTING SYSTEM

By using the cloud storage services, the customers can access data stored in a cloud anytime and anywhere using any device, without caring about a large amount of capital investment when deploying the underlying hardware infrastructures.

The cloud service provider (CSP) stores data replicas on multiple geographically distributed servers.

Where a user can read stale data for a period of time. The domain name system (DNS) is one of the most popular applications that implement eventual consistency. Updates to a name will not be visible immediately, but all clients are ensured to see them eventually.

### DISADVANTAGES OF EXISTING SYSTEM

The replication technique in clouds is that it is very expensive to achieve strong consistency. Hard to verify replica in the data cloud is the latest one or not

## V. PROPOSED SYSTEM

We presented a consistency as a service (CaaS) model and a two-level auditing structure to help users verify whether the cloud service provider (CSP) is providing the promised consistency, and to quantify the severity of the violations, if any. With the CaaS model, the users can assess the quality of cloud services and choose a right CSP among various candidates, e.g., the least expensive one that still provides adequate consistency for the users applications.



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 7, Issue 3, March 2019

## ADVANTAGES OF PROPOSED SYSTEM

Do not requires a global clock among all users for total ordering of operations.

The users can assess the quality of cloud services.

Among various candidates, e.g, the least expensive one that still provides adequate consistency for the users' applications

### Databases

A database in Microsoft SQL Server consists of a collection of tables that contain data, and other objects, such as views, indexes, stored procedures, and triggers, defined to support activities performed with the data. The data stored in a database is usually related to a particular subject or process, such as inventory information for a manufacturing warehouse.

## VI. ABOUT .NET

### Overview of the .NET Framework

The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet/Intranet. The .NET Framework is designed to fulfil the following objectives:

- To provide a consistent object-oriented programming environment whether object code is stored and executed locally, executed locally but Internet-distributed, or executed remotely.
- To provide a code-execution environment that minimizes software deployment and versioning conflicts.
- To provide a code-execution environment that guarantees safe execution of code, including code created by an unknown or semi-trusted third party.
- To provide a code-execution environment that eliminates the performance problems of scripted or interpreted environments.
- To make the developer experience consistent across widely varying types of applications, such as Windows-based applications and Web-based applications.
- To build all communication on industry standards to ensure that code based on the .NET Framework can integrate with any other code.
- .NET Support removing application.

The .NET Framework has two main components:

- The common language runtime.
- .NET Framework class library.

## VII. INTRODUCTION TO ASP.NET SERVER CONTROLS

In addition to (or instead of) using `<% %>` code blocks to program dynamic content, ASP.NET page developers can use ASP.NET server controls to program Web pages. Server controls are declared within an .aspx file using custom tags or intrinsic HTML tags that contain a `runat="server"` attributes value. Intrinsic HTML tags are handled by one of the controls in the `System.Web.UI.HtmlControls` namespace. Any tag that doesn't explicitly map to one of the controls is assigned the type of `System.Web.UI.HtmlControls.HtmlGenericControl`.

Server controls automatically maintain any client-entered values between round trips to the server. This control state is not stored on the server (it is instead stored within an `<input type="hidden">` form field that is round-tripped between requests). Note also that no client-side script is required.

In addition to supporting standard HTML input controls, ASP.NET enables developers to utilize richer custom controls on their pages. For example, the following sample demonstrates how the `<asp:adrotator>` control can be used to dynamically display rotating ads on a page.

ASP.NET Web Forms provide an easy and powerful way to build dynamic Web UI.

ASP.NET Web Forms pages can target any browser client (there are no script library or cookie requirements).

ASP.NET Web Forms pages provide syntax compatibility with existing ASP pages.



# International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 7, Issue 3, March 2019

ASP.NET server controls provide an easy way to encapsulate common functionality.  
ASP.NET ships with 45 built-in server controls. Developers can also use controls built by third parties.  
ASP.NET server controls can automatically project both uplevel and downlevel HTML.  
ASP.NET templates provide an easy way to customize the look and feel of list server controls.  
ASP.NET validation controls provide an easy way to do declarative client or server data validation.

## VIII. CONCLUSION

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user

## REFERENCES

- [1]S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.
- [2] C Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.
- [3] Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010.
- [4]S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.
- [5] Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.
- [6]Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ. craig, 2009.
- [7]J. Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271-2282, 2013.
- [8]Y. Zhu, H. Hu, G. Ahn, D. Huang, and S. Wang, "Towards Temporal Access Control in Cloud Computing," Proc. the 31st IEEE International Conference on Computer Communications (INFOCOM 2012), pp. 2576-2580, 2012
- [9]Z. Wan, J. Liu, and R. Deng, "HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754, 2012