**StatusBased Data source with complete Review in cloud storage**

**Abstract**

The goal of Cloud review is to provide cloud service providers with a way to make their performance and security data readily available for potential customers. The specification provides a standard way to present and share detailed, automated statistics about performance and security.Cloud storage system provides facilitative file storage and sharing services for distributed clients. To address the status, controllable outsourcing and origin auditing concerns on outsourced files. First, our IBDO scheme allows a user to authorize dedicated proxies to upload data to the cloud storage server on her behalf, e.g., a company may authorize some employees to upload files to the company’s cloud account in a controlled way. The proxies are identified and authorized with their recognizable identities, which eliminates complicated certificate management in usual secure distributed computing systems. Second, our IBDO scheme facilitates comprehensive auditing, i.e., our scheme not only permits regular integrity auditing as in existing schemes for securing outsourced data, but also allows to audit the information on data origin, type and consistence of outsourced files. Security analysis and experimental evaluation indicate that our IBDO scheme provides strong security with desirable efficiency.

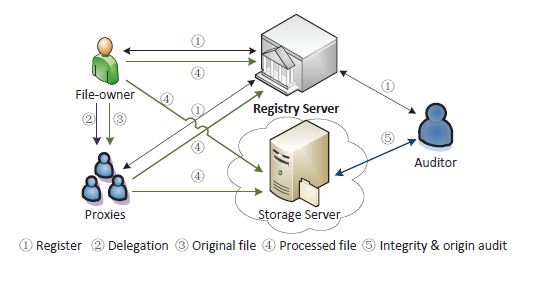
**Existing System**

We observe two serious issues not well instructed in existing applications. First, most organizations lack a measured way of delegablesubcontracting. One can note that several cloud packing systems (e.g., Amazon, Dropbox, Google Cloud storage) allow the interpretationholder to create signed URLs consuming which somewhat other selectedarticle can upload,andadjust content on behalf of the worker. But, in this state, the delegator cannot confirmwhether or not the authorized one has uploaded the file as detailed or prove whether or not the uploaded file has been reservedwhole. Hence, the delegator has to entirely trust the delegates and the cloud server. In fact, the file-owner can not only need to approve some others to producerecords and upload to a cloud, but also need to verifiably assurance that the uploaded documents have been kept unaffected. For example, in Electronic Health Systems (EHS), wheninspection a doctor, the persistent needs to delegate her specialist to create electronic health records (EHRs) and stock them at a isolated EHRs center preserved by a CSP . In extra typical set-up of cloud-aided workplaceclaims, a group of plots in unlike places may justify a job in collaboration. The group front-runner can make a cloud padding account and approve the followers with secret licenses. The performance of the collectionaffiliates and the cloud server must be provable. Second, presentPoS-like systems, counting PDP and Proofs of Retrievability (PoR) , do not care data log related inspecting in the procedure of data possession proof. The energies are serious in speakingrows in practice. For example, when the persevering and doctor in EHS get complex medical clashes, it would be helpful if some detaileddata such as outsourcer, type and producingtime of the outsourced EHRs are auditable. However, there occur no PoS-like schemes that can agreeauthentication of these significantevidence in a multi-user location.

**Proposed System**

Argument and answering to the clients’ recording, and also allows the recorded clients to store the public limitations of subcontracted files. The cloud loading server provides storage services to the recorded clients for storing outsourced files. In real-world claims, an organization buys storage services from some CSP, and the IT department of the organization can play the role of a registry server. In this way, the registered clients (employees) can take plus of the loading services.The file-owner and her approved proxies can subcontract files to the cloud server. Specifically, on behalf of the owner, the approveddelegation processes the file, sends the managed results to the loading server, and uploads the agreeing public restrictions of the file to the archive server. Neither the file-owner nor the substitution is required to store the unique file or the managed file nearby. The duty of the inspector is to check the integrity of outsourced files and their origin likeoverall log data by networking with the cloud storage server without regaining the complete file.In proposed system, involve of file-owners, substitutions, auditors, archive server, and loading server. Generally, the file-owners, substitutions and auditors are cloud clients.

**Architecture diagram**



**System Requirements**

# H/W System Configuration:-

# Processor - Pentium –III

Speed - 1.1 Ghz

RAM - 256 MB(min)

Hard Disk - 20 GB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

# S/W System Configuration

* Operating System : Windows95/98/2000/XP
* Application Server : Tomcat5.0/6.X/8.X
* Front End : HTML, Java, Jsp, Javascript
* Server side Script : Java Server Pages.
* Database Connectivity : Mysql.

**Algorithm implementation**

**Diffie–Hellman**

Diffie–Hellman key exchange (D–H) [[nb 1]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-1) is a specific method of securely exchanging [cryptographic keys](https://en.wikipedia.org/wiki/Key_(cryptography)) over a public channel and was one of the first [public-key protocols](https://en.wikipedia.org/wiki/Public-key_cryptography) as originally conceptualized by [Ralph Merkle](https://en.wikipedia.org/wiki/Ralph_Merkle) and named after [Whitfield Diffie](https://en.wikipedia.org/wiki/Whitfield_Diffie) and [Martin Hellman](https://en.wikipedia.org/wiki/Martin_Hellman).[[1]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-Merkle_1978-2)[[2]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-Diffie_1976-3) D–H is one of the earliest practical examples of public [key exchange](https://en.wikipedia.org/wiki/Key_exchange) implemented within the field of [cryptography](https://en.wikipedia.org/wiki/Cryptography).

Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted [courier](https://en.wikipedia.org/wiki/Courier). The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a [shared secret](https://en.wikipedia.org/wiki/Shared_secret) key over an [insecure](https://en.wikipedia.org/wiki/Data_security) [channel](https://en.wikipedia.org/wiki/Channel_(communications)). This key can then be used to encrypt subsequent communications using a [symmetric key](https://en.wikipedia.org/wiki/Symmetric_key) [cipher](https://en.wikipedia.org/wiki/Cipher).

Diffie–Hellman is used to secure a variety of [Internet](https://en.wikipedia.org/wiki/Internet) services. However, research published in October 2015 suggests that the parameters in use for many D–H Internet applications at that time are not strong enough to prevent compromise by very well-funded attackers, such as the security services of large governments.[[3]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-imperfectfs-4)

The scheme was first published by Whitfield Diffie and Martin Hellman in 1976,[[2]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-Diffie_1976-3) but in 1997 it was revealed that [James H. Ellis](https://en.wikipedia.org/wiki/James_H._Ellis),[[4]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-5) [Clifford Cocks](https://en.wikipedia.org/wiki/Clifford_Cocks) and [Malcolm J. Williamson](https://en.wikipedia.org/wiki/Malcolm_J._Williamson) of [GCHQ](https://en.wikipedia.org/wiki/Government_Communications_Headquarters), the British signals intelligence agency, had previously shown how public-key cryptography could be achieved.[[5]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-6)

Although Diffie–Hellman key agreement itself is a non-authenticated [key-agreement protocol](https://en.wikipedia.org/wiki/Key-agreement_protocol), it provides the basis for a variety of authenticated protocols, and is used to provide [forward secrecy](https://en.wikipedia.org/wiki/Forward_secrecy) in [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)'s [ephemeral](https://en.wikipedia.org/wiki/Ephemeral_key) modes (referred to as EDH or DHE depending on the cipher suite).

The method was followed shortly afterwards by [RSA](https://en.wikipedia.org/wiki/RSA_(algorithm)), an implementation of [public-key cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography) using asymmetric algorithms.

**K Means algorithm**

k-means clustering is a method of [vector quantization](https://en.wikipedia.org/wiki/Vector_quantization), originally from [signal processing](https://en.wikipedia.org/wiki/Signal_processing), that is popular for [cluster analysis](https://en.wikipedia.org/wiki/Cluster_analysis) in [data mining](https://en.wikipedia.org/wiki/Data_mining). k-means clustering aims to [partition](https://en.wikipedia.org/wiki/Partition_of_a_set) n observations into k clusters in which each observation belongs to the [cluster](https://en.wikipedia.org/wiki/Cluster_(statistics)) with the nearest [mean](https://en.wikipedia.org/wiki/Mean), serving as a [prototype](https://en.wikipedia.org/wiki/Prototype) of the cluster. This results in a partitioning of the data space into [Voronoi cells](https://en.wikipedia.org/wiki/Voronoi_cell).

The problem is computationally difficult ([NP-hard](https://en.wikipedia.org/wiki/NP-hard)); however, there are efficient [heuristic algorithms](https://en.wikipedia.org/wiki/Heuristic_algorithm) that are commonly employed and converge quickly to a [local optimum](https://en.wikipedia.org/wiki/Local_optimum). These are usually similar to the [expectation-maximization algorithm](https://en.wikipedia.org/wiki/Expectation-maximization_algorithm) for [mixtures](https://en.wikipedia.org/wiki/Mixture_model) of[Gaussian distributions](https://en.wikipedia.org/wiki/Gaussian_distribution) via an iterative refinement approach employed by both algorithms. Additionally, they both use cluster centers to model the data; however, k-means clustering tends to find clusters of comparable spatial extent, while the expectation-maximization mechanism allows clusters to have different shapes.

The algorithm has a loose relationship to the [k-nearest neighbor classifier](https://en.wikipedia.org/wiki/K-nearest_neighbor), a popular [machine learning](https://en.wikipedia.org/wiki/Machine_learning) technique for classification that is often confused with k-means because of the k in the name. One can apply the 1-nearest neighbor classifier on the cluster centers obtained by k-means to classify new data into the existing clusters. This is known as [nearest centroid classifier](https://en.wikipedia.org/wiki/Nearest_centroid_classifier) or Rocchio algorithm.

**Conclusion**

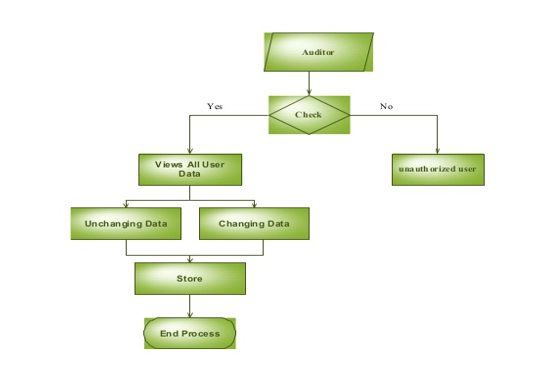
In this paper, we investigated proofs of storage in cloud in a multi-user setting. We introduced the notion of identitybased data outsourcing and proposed a secure IBDO scheme. It allows the file-owner to delegate her outsourcing capability to proxies. Only the authorized proxy can process and outsource the file on behalf of the file-owner. Both the file origin and file integrity can be verified by a public auditor. The identity-based feature and the comprehensive auditing feature make our scheme advantageous over existing PDP/PoR schemes. Security analyses and experimental results show that the proposed scheme is secure and has comparable performance as the SW scheme.

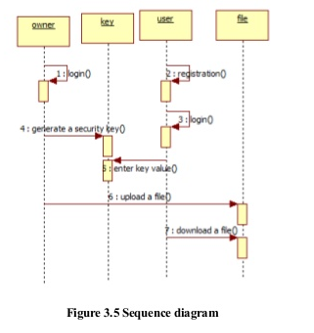
**Future Enhancement**

We presented the first efficient Identity-Based Encryption scheme that is secure in the full model without random oracles. We proved our the security of our scheme by reducing it to the decisional Bilinear Diffie-Hellman problem. Additionally, we showed how our Identity-Based encryption scheme can be converted to an efficient signature scheme that depends only upon the computational Diffie-Hellman assumption in the standard model. This work motivates two interesting open problems. The first is to find an efficient IdentityBased Encryption system (without random oracles) that has short public parameters. The second, is to find an IBE system with a tight reduction in security. Such a solution would also likely permit an efficient reduction for an analogous HIBE scheme.

ADMIN 
Yes No 
Check 
unauthorized user 
End Process 
Auditing Details 
View User View Data 
Registration Derails 
View De...

Check 
unauthorized user 
Yes No 
Upload Data 
View Data 
End Process 
USER 
Changed Data With Un Changed Data 
Alert Mess...





**Literature Survey:**

Average business organization are realizing that simply exchange to the cloud can get access to excellent business claims and increase up their infrastructure assets in a very low-cost, Internet on an as-needed basis [1].

This new and exciting paradigm has generated significant interest in the marketplace and the academic world [2], resulting in a number of notable commercial and individual cloud computing services, e.g., form Amazon, Google, Microsoft, Yahoo, and Sales force [3]. Also, top database vendors, like Oracle, are adding cloud support to their databases.

The providers are enjoying the superficial opportunity in marketplace but they should ensure that they possess the right security features. The cloud provide facilities like fast development, lower cost on pay-for-use, quick provisioning, quick flexibility, everywhere network contact, hypervisor defense against network vulnerability, economicalfailure recovery and data storage solution, on-request security checks, synchronized detection of system altering and rapid re-construction of services. The cloud provides this compensation, until some of the risks are better understood.

The basic concept of the cloud , based on the services they offer, from application service provisioning, grid and service computing, to Software as a Service [1, 4, 5]. Despite of the specific architecture, the dominant concept of this computing model is that customers’ data, which can be of individuals, organizations or enterprises, is processed remotely in unknown machines about which the user not aware. The ease and efficiency of this approach, however, comes with privacy and security risks [3, 6, 7]. Confidentiality of data is the main hurdle in implementation of cloud services.

**REFERENCES**

[1]. Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, “Achieving efficient cloud search services: multi keyword ranked search over encrypted cloud data supporting parallel computing,” IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.

[2]. Y. Ren, J. Shen, J. Wang, J. Han, S. Lee, “Mutual verifiable provable data auditing in public cloud storage,” Journal of Internet Technology, vol. 16, no. 2, pp. 317-323, 2015.

[3]. C. Wang, Q. Wang, K. Ren, W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing”, INFOCOM 2010, pp. 1-9, 2010.

[4]. H. Guo, Z. Zhang, J. Zhang, “Proxy re-encryption with unforgeable reencryptionKeys”, Cryptology and Network Security, LNCS 8813, pp. 20-33, 2014.

[5]. G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, “Scalable and efficient provable data possession”, SecureComm 2008, 2008.

[6]. Lynn B., “On the implementation of pairing-based cryptosystems”, Ph.D. dissertation, http://crypto.stanford.edu/pbc/thesis.pdf, Stanford University,2008.

[7]. Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, “Enabling public auditability and data dynamics for storage security in cloud “.

# Spiral Methodology

The Spiral Lifecycle Model is a sophisticated lifecycle model that focuses on early identification and reduction of project risks. A spiral project starts on a small scale, explores risks, makes a plan to handle the risks, and then decides whether to take the next step of the project - to do the next iteration of the spiral. It derives its rapiddevelopment benefit not from an increase in project speed, but from continuously reducing the projects risk level - which has an effect on the time required to deliver it. Success at using the Spiral Lifecycle Model depends on conscientious, attentive, and knowledgeable management.It can be used on most kinds of projects, and its risk-reduction focus is always beneficial.

The spiral methodology extends the waterfall model by introducing prototyping. It is generally chosen over the waterfall approach for large, expensive, and complicated projects.

At a high-level, the steps in the spiral model are as follows:

1. The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.

2. A preliminary design is created for the new system.

3. A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.

4. A second prototype is evolved using four steps:

* Evaluate the first prototype and identify its strengths, weaknesses, and risks.
* Define the requirements of the second prototype.
* Plan and design the second prototype.
* Construct and test the second prototype.

5. At the project sponsor's option, the entire project can be aborted if the risk is deemed too great. Risk factors might involve development cost overruns, operating-cost miscalculation, or any other factor that could result in a less-than-satisfactory final product.

6. The existing prototype is evaluated in the same manner as was the previous prototype, and, if necessary, another prototype is developed from it according to the fourfold procedure outlined above.

7. The preceding steps are iterated until the customer is satisfied that the refined prototype represents the final product desired.

8. The final system is constructed, based on the refined prototype.

9. The final system is thoroughly evaluated and tested. Routine maintenance is carried out on a continuing basis to prevent large-scale failures and to minimize downtime.