

# Data Storage in Cloud Using HMAC-SHA-1 & Proof of Ownership Protocol

Sainadh Bommidi<sup>1</sup> & L V Ramesh<sup>2</sup>

<sup>1</sup>M-Tech Dept of ANDHRA LAYOLA INSTITUTE OF ENGG AND TECHNOLOGY

Vijayawada, AP Mail id: - [sainadhbommidi@gmail.com](mailto:sainadhbommidi@gmail.com)

<sup>2</sup>M-Tech Dept of ANDHRA LAYOLA INSTITUTE OF ENGG AND TECHNOLOGY

Vijayawada, AP Mail id: - [lvarunramesh@gmail.com](mailto:lvarunramesh@gmail.com)

## Abstract

A Hybrid cloud is a coalescence of public and private clouds bound together by either standardized or proprietary technology that alters information plus application immovability. Proposed system aiming to expeditiously resolving quandary from deduplication on derivative favors in remote location computing. A hybrid remote location structure lying of a populace remote location plus a individual remote location plus ye information owners simply source their information storage by utilizing public cloud while the information operation is managed in private cloud. To build information management scalability in cloud computing, deduplication has been a very well-kenned technique recently is use. Deduplication reduces your bandwidth requisites, expedites the data transfers, and it keeps your cloud storage needs to a minimum. Proposed system demonstrates respective incipient deduplication expressions fortifying sanctioned duplicate assure inside hybrid remote location structure. To hold the secrecy of in formationye convergent encoding proficiency holds made up used to encrypt ye information afore source. Sanctioned deduplication system support differential sanction duplicate check. As a proof of concept, a prototype is implemented in sanctioned duplicate check scheme and conduct test bed experiments utilizing prototype, sanctioned duplicate check scheme incurs minimal overhead compared to mundane operations.

**Keywords:** Deduplication, Proof of Ownership, Convergent Encryption, Key Management.

## 1. INTRODUCTION

To make information management scalable in cloud computing, deduplication has been a well-kenned technique plus has magnetized more plus more care recently. Information deduplication is a specialized information compression method for repudiating duplicate

replicas of reiterating information in recollection. The method is utilized to ameliorate recollection utilization plus can withal be acclimated to network information transfers to reduce ye number of bytes that must be sent. In lieu of keeping numerous information copies with yesimilar content,

deduplication excretes superfluous information by holding only solitary physical copy plus referring further redundant information to redundant imitate. Deduplication can carry lay at yedata records level or yechunk level. For data records level deduplication, infotech rejects reiterate facsimiles from yelike data records. Deduplication can adscitiously choose home astatine yechunk level, which excretes double chunks from information that occur in non-identical data records. Albeit information deduplication brings an plethora of profits, aegis plus secrecy pertains stand up while utilizer's sensitive information are sensitive to some insider plus foreigner approaches. Traditional encoding, while supplying information confidentiality, is uncongenial with information deduplication. Concretely, natural encoding desires different utilizer's to encipher their information with their possess keys. Thus, very information replicas of different utilizers will lead to different ciphertexts, building deduplication infeasible. Convergent encryption has been suggested to enforce information confidentiality while building deduplication feasible. Infotech cipher text/mundane text a information copy with a confluent key, which is incurred through calculating the cryptanalytic hash measure from yemessage from yeinformation imitate. Afterward key propagation plus information encoding,

utilizer's hold yekey values plus send out ye ciphertext to yeremote location. Afterwards ye encryption procedure is deterministic plus is derived from the information content, identical 1 information copies will engender the same convergent key plus hence the same ciphertext. To avert wildcat access, a insure proof of ownership protocol is withal needed to supply the proof that the utilizer indeed owns yeLapp data file whenever a double is detected. Afterward ye proof read, subsequent utilizer's on yeLapp data file volition be supplied anarrow of yewaiter less wanting to transfer yelike data file. A utilizer can download yecipher text records with yearrow of yehost, which can alone be decoded by yerepresenting information owners with their focused keys. Hence, convergent encryption sanctions yeremote location to perform deduplication on yeciphertexts plus ye proof of ownership obviates ye unauthorized utilizer to get at yedata files.

## 2. RELATED WORK

Hybrid cloud can be built utilizing any technology it changes granting to unlike vendors. Key constituents In many of the situations, implementation of the hybrid cloud has a comptroller that will hold track of all placements of private and public clouds, IP address, servers and other resources that can run systems efficiently.

### 2.1 Existing System:

Data deduplication be solitary of consequential information compression techniques for rejecting duplicate replicas of reiterating information, and has been widely used in cloud memory to reduce the sum of memory space plus preserve bandwidth. To forfendye confidentiality of sensitive information while fortifying deduplication, Cloud computing provide ostensibly illimitable “virtualized” resources to users as accommodations across the whole Internet, while obnubilating platform and implementation details. Today’s cloud accommodation providers offer both highly useable storage plus massively parallel calculating resources at relatively low costs. As remote location computing turns prevailing, a incrementing number from information makes up restored in yeremote location and shared by utilizer’s with designated favors, which determine the approach corrects of yememoryinformation.

#### Disadvantages of Existing System:

- One critical challenge of cloud memory accommodations is the management of ye ever-incrementing volume of information.

#### 2.2 Proposed System:

Hybrid Cloud can be built utilizing any technology it changes granting to unlike vendors. Key components In many of the situations, implementation of the hybrid cloud has a comptroller that will hold track of all

positions of private and public clouds, IP address, servers plusearlyresources that can run systems efficiently.

Some of the key components include

- Orchestration manager plus cloud purveying for storage, populace cloud resources which includes virtual machines and networks, the private and public clouds, which are not compulsorily compatible or identical.
- Synchronization element and Data transfer expeditiously replace information among private plus public clouds.
- Changing configurations of storage, network and some early resources are constituting crossed by configuration monitor.[1]

In the Fig 1, the simplest view of hybrid cloud is allowed for, a single off-premises public cloud plus on-premises private cloud is within the Enterprise Datacenter is shown plus public cloud demonstrates the safe association to store information on to the cloud is denoted by the arrow:

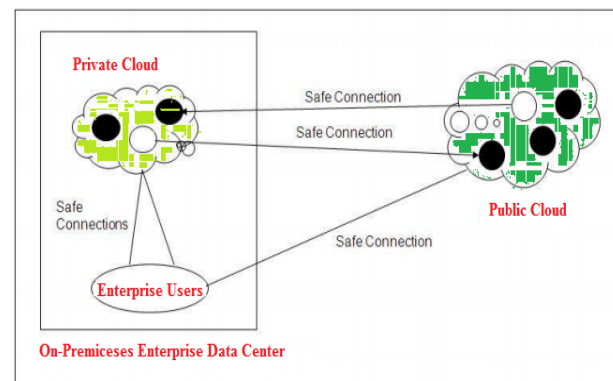


Fig 1: Hybrid Cloud Environment.

The ebony circles shows active virtual server images and white circles shows virtual server images which have been migrated by utilizing safe connections. The arrows designate that the direction of migration. Utilizing safe connections initiative utilizers are linked to ye clouds, which can be secure HTTP browsers or virtual private networks (VPNs) .A hybrid cloud could additionally can consist of multiple public or/and private clouds. [3]

Data de-duplication has many patterns. Generally, there is no one best way to enforce information de-duplication across an entire an organization. Instead, to maximize the gains, systems may spread more than one de-duplication strategy. It is very essential to understand the backup and backup challenges, when culling de-duplication as a solution.

We have introduced a hybrid cloud architecture in our aimed deduplicationscheme. The private keys for exclusive right will not be supplied to utilizer's directly, which will be held plus plus led by ye private cloud server rather. In this manner, the utilizer's cannot contribution these private keys of favors in this suggested structure, which betokens that it can avoid ye privilege key distributingamongst utilizers in the over straight structure. To get a data filekeys, ye utilizer inevitably to ship a call for to yeindividual remote locationwaiter. Ye suspicion fromsuch building can be reported

as follows. To perform the duplicate check for some data file, the utilizer wants to get yedata file keysonyeindividualremote locationwaiter. The Individualremote locationwaiter will additionally assure yeutilizer'sindividuality afore publishing ye representing data file keys to ye utilizer. The sanctioned double assure as such information data file bum be did throughye utilizer on yepopulateremote location afore transferring this data records. Predicated on yeanswers of double assure, ye utilizer either uploads this data file or runs PoW.

### 3. IMPLEMENTATION

Afore affording our construction of yededuplicationscheme, we determine an binary cognation  $R = f((p, p')g$  because comes. Given 2 privileges  $p$  plus  $p'$ , we verbally show that  $p$  corresponds  $p'$  if plus only if  $R(p, p') = 1$ .

#### 3.1 System Setup:

An identification protocol  $\_ = (\text{Proof}, \text{Verify})$  is additionally determined, where Proof plus swear constitute ye proof plus check algorithm severally. Moreover, for apiece one utilizer  $U$  exists surmised to have a mystery key  $sk_U$  to execute ye identification with waiters. Postulate that utilizer  $U$  features yefavor adjust  $PU$ . It additionally formats a PoWset of rules POW for yedata records ownership proof. The private cloud server will control a table which shops each utilizer's public

information plus its representing privilege set PU.

### 3.2 File Uploading:

Suppose that information proprietor requires to transfer plus apportion an data records F on user's whose privilege belongs to ye set PF = fpjg. The information owner demands act with yeseecret remote location afore doing duplicate assure with ye S-CSP. Information owner does anrecognition to try out infoteches individuality on secret tokenskU. If it is communicated, yesecreteremote locationwaitertestamentget yerepresenting favors PU of ye utilizer of its memory table list. The utilizer calculates plus sends ye information data records tag  $\phi F = \text{TagGen}(F)$  to yesecreteremote locationwaiter, who will return  $\phi' F; p_ = \text{TagGen}(\phi F, kp_ )g$  back to the utilizer for total  $p_ \text{ gratifying } R(p, p_ ) = 1$  plus  $p_ 2$  PU. Then, the utilizer will actplus ship ye file token  $\phi' F; p_ g$  to ye S-CSP.

- If andouble data is detected by ye S-CSP, ye utilizer continues proof of ownership of this data file with ye S-CSP. If the cogent evidence is passed, the utilizer will be assigned a pointer, which approves him to access ye file.
- Otherwise, if no duplicate is found, the utilizer computes the encrypted file  $CF = \text{EncCE}(kF, F)$  with ye convergent key  $kF = \text{KeyGenCE}(F)$  plus uploads  $(CF, \phi' F; p_ g)$  to ye cloud server. The

convergent key kF is stored by the utilizer locally.

### 3.3 File Retrieving:

Guess a utilizer requires to getting a data records F. It beginning sends out ancalle for plusyedata records name to the S-CSP. Upon getting the request plus data file designation, the S-CSP will assure whether ye utilizer is worthy to download F. If failed, the S-CSP sends back anterminate signal to the utilizer to denote yedata getting from networkloser. Differently, ye S-CSP affords the representing ciphertextCF .on experiencing yeciphered information from ye S-CSP, the utilizer utilizes ye key kFmemorytopically to recuperate ye pristine €file F.

## 4. EXPERIMENTAL WORK

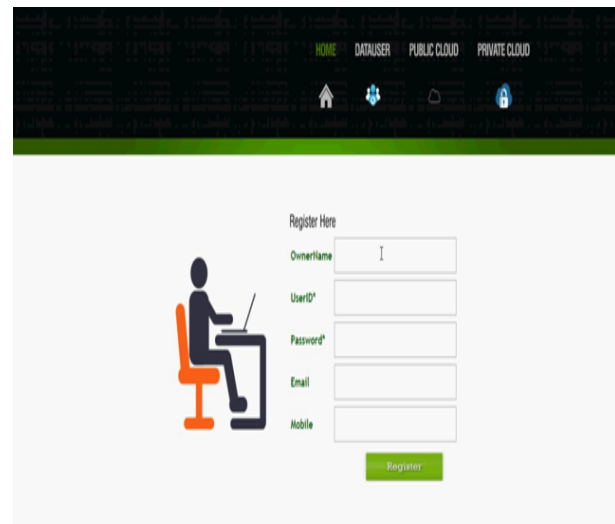
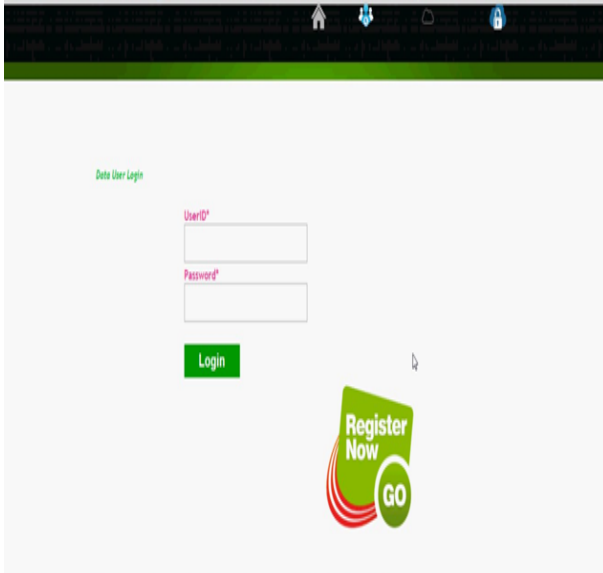


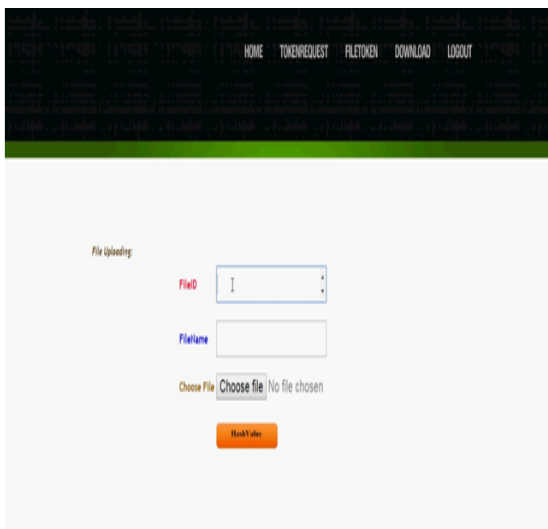
Fig:-2 New Account Opening



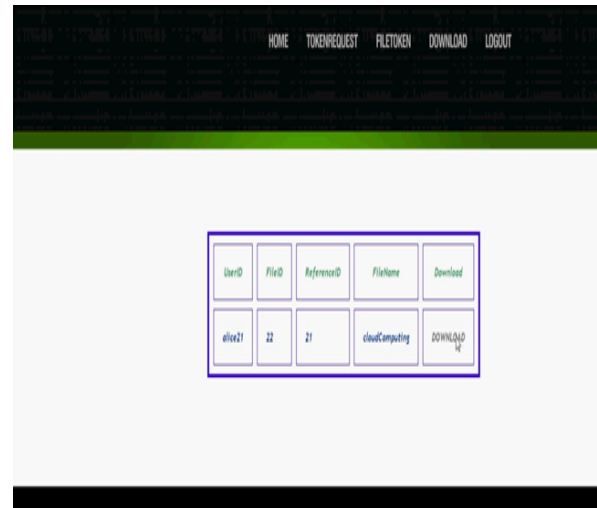
**Fig:-3 Authentication & Authorization**



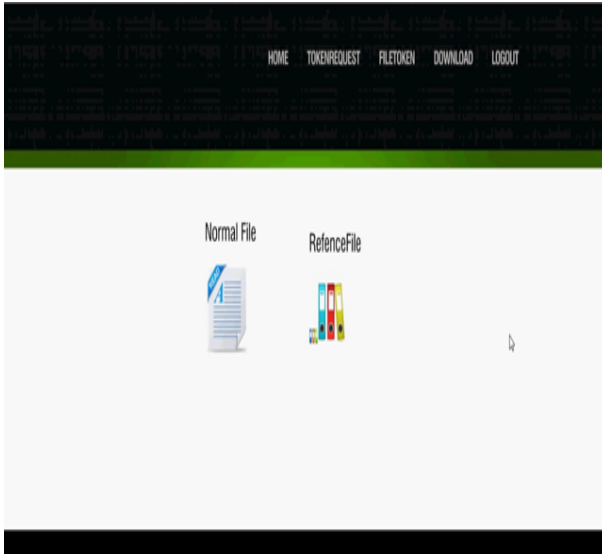
**Fig:-5 SHA-Data**



**Fig:-4 Data upload**



**Fig:-5 Data Access**



**Fig:-5 File**

## 5. CONCLUSION

The celebration of sanctioned information deduplicationbesuggested to ascertain the information security through counting disparity gains of clients in yeduplicate replica check. The presentation of aelite incipient deduplicationgrowths fortifying sanctioned duplicate re-create in hybrid cloud architecture, in that ye duplicate assure tokens of documents are caused via ye private remote locationwaiterholding secrete keys. Security check presents that ye methods are assure regarding insider plus outsider assaults detailed in the suggested security model. As an issue verification of conception, the developed model of the proposed sanctioned duplicate copy check method and tested the model. That showed the sanctioned duplicate copy check method experience minimum overhead comparing convergent encryption and data transfer.

## 6. REFERENCES

- [1] Bugiel, Sven, et al. "Twin clouds: Secure cloud computing with low latency." Communications and Multimedia Security.Springer Berlin Heidelberg, 2011.
- [2] Anderson, Paul, and Le Zhang. "Fast and Secure Laptop Backups with Encrypted Deduplication." LISA. 2010.
- [3] Bellare, Mihir, SriramKeelveedhi, and Thomas Ristenpart. "DupLESS: server-aided encryption for deduplicated storage." Proceedings of the 22nd USENIX conference on Security.USENIX Association, 2013.
- [4] Bellare, Mihir, SriramKeelveedhi, and Thomas Ristenpart. "Message-locked encryption and secure deduplication."Advances in Cryptology–EUROCRYPT 2013.Springer Berlin Heidelberg, 2013.296-312.
- [5] Bellare, Mihir, ChanathipNamprempre, and Gregory Neven. "Security proofs for identity-based identification and signature schemes." Journal of Cryptology 22.1 (2009): 1-61.
- [6] M. Bellare, S. Keelveedhi, and T. Ristenpart.Dupless: Serveraided encryption for deduplicated storage. In *USENIX Security Symposium*, 2013.
- [7] K. Zhang, X. Zhou, Y. Chen, X.Wang, and Y. Ruan.Sedic: privacyaware data intensive computing on hybrid clouds. In *Proceedings of the 18th ACM conference on Computer and*



*communications security*, CCS'11, pages 515–526, New York, NY, USA, 2011. ACM.

[8] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote

storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, *ACM Conference on Computer and Communications Security*, pages 491–500. ACM, 2011.