iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** X **Month of publication:** October 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure and Authorized De-duplication Model in Hybrid Cloud Implementation by Using Multi-Layered Cryptosystem

Kattemane Vannuru Swamy[1], Ramesh Kante[2,] Chandra Shekhar Ambarapu[3]
[1]*M. Tech Student,* [2]*Associate Professor & HOD,* [3]*Assistant Professor*
[1,2,3] *Department of CSE, Gates Institute of Technology, Gooty, 515401*

Abstract: ***Information de-duplication is a standout amongst imperative information layering systems for eliminating copy duplicates for repeat decimal data, and need been generally utilized within cloud capacity to decrease the measure of storage room also save transfer speed. To secure the privacy about slight information same time supporting de-duplication, the focused encryption method need been recommended should run the information preceding outsourcing. Should preferred ensure information security, this paper makes those initial effort with formally deliver the issue from declare authorized information de-duplication. Unique in relation to customary de-duplication systems, those differential rights for clients would further recognized to copy consider Furthermore those information itself. We also available a few new de-duplication constructions supporting sanctioned copy consider in a mixture cloud structural engineering. Security analysis exhibits that our plan may be secure as far as those definitions specified in the suggested security model. Concerning illustration a verification about concept, we actualize all the model about our suggested sanctioned copy check plan What's more direct tested examinations utilizing our model. We show that our suggested commissioned copy check plan gaining minor operating cost dissimilarity with ordinary operations.***
Keywords: De-duplication, authorized duplicate check, confidentiality, hybrid cloud

I. INTRODUCTION

Cloud registering gives actually vast. “Virtualized” assets on clients as benefits over the entire Internet, same time hide phase What's more usage. delicate elements. Today’s cloud administration suppliers offer both exceedingly. available store data also massively parallel registering assets. Toward moderately low is cost. Concerning illustration cloud registering gets to be. Prevalent, an expanding measure about information is, no doubt put away in. The cloud and imparted by clients with specified privileges,. Which define those entry greater part, however overlook the put away information. One incredulous. Test about cloud capacity benefits may be the management of the. Ever-increasing volume for ambiguity. With make information overlook economy versatile done cloud computing,. De-duplication [17] need been An well-known procedure. Furthermore need pulled in an ever increasing amount consideration as of late. Information. De-duplication may be An particular information layering method. For eliminating copy duplicates of revise decimal information on stored. Those technologies may be used to move forward store usage. What's more additionally make connected should system information transfers on. reduce the number from declare bytes that must make sent. As opposed to keeping various information duplicates with the same content,. De-duplication distribute with excess information eventually perusing keeping special case physical duplicate allowing other excess information should also that duplicate values. De-duplication can occur during whichever the record. Level or those square levels. For file-level de-duplication, it. distribute with copy duplicates of the same record. De-duplication could additionally occur at the square level, which dispenses with. Copy squares for information that happen for non-identical. Files produce those same focused key What's more in future those same cipher copy. Will forestall unapproved access, An secure verification from claiming proprietorship (POW) protocol [11] will be also required on furnish those verification that the client In fact claims the same document when An copy is found. After the proof, ensuing clients with the same record will be Gave An pointer from the server without expecting on transfer those same document. An client cam wood download the encrypted document for those pointer from the server, which can just make decrypted by those corresponding information managers with their major keys. Thus, focalized encryption permits the cloud should perform de-duplication on the cipher texts and the evidence about rights keeps those unapproved client will entry those document. However, past de-duplication frameworks can't help differential commission copy check, which will be significant secure along Numerous provisions. Over such an commissioned de-duplication system, every client is issued An set from claiming privileges Throughout framework introduction

(in area 3, we involved those meaning of a benefit with examples). Each record uploaded of the cloud will be additionally limited by a set of privileges will define which sort of clients is permitted to perform the copy evaluate What's more right those files. Preceding submitting as much copy consider appeal for an file, those client necessities will take this record and as much identity or privileges as inputs. The client has the capacity will find an duplicate to this document whether What's more just if there is a duplicate for this document furthermore an matched benefit saved in cloud. To overcome, a large number distinctive privileges will be doled out on employees. So as will spare expense and effectively management, those information will be moved of the capacity server supplier (S-CSP) in the government funded cloud with specified privileges and the de-duplication procedure will be connected to store special case duplicate of the same document. Due to security consideration, a few files will be encrypted and permitted the copy considered by representatives with specified privileges on understand the get control. Universal de-duplication frameworks In light of convergent encryption, In spite of giving work to secrecy will a few extent, don't help the copy check with differential privileges. Previously, different words, no differential privileges bring been recognized in the de-duplication In light of focalized encryption strategy. It appears should make repudiated whether we need to figure it out both de-duplication and differential authorization copy check toward the same the long run.

A. *Contribution*

In this paper, pointing during effectively realize those issue of de-duplication with differential privileges to cloud computing, we think about an mixture cloud structural engineering comprising of a open cloud What's more An private cloud. dissimilar to existing information de-duplication systems, those private cloud may be included as a proxy on permit information owner/users with safely perform copy weigh for differential privileges. Such a structural engineering is useful and need pulled in a significant part consideration from analysts. Those information holders main outsource their information capacity toward utilizing general population cloud same time those information operation is figured out how in private cloud. Furthermore, we improve our framework done security. Specifically, we available an propelled plan should help stronger security eventually Tom's perusing encrypting the record for differential benefit keys. In this way, those clients without relating privileges can't perform the copy weigh. Finally, we execute a model of the suggested sanctioned copy check also behavior tested experiments with assess those overhead of the model.

B. *Preliminaries*

In this paper, survey a few secure primitives utilized within our secure de-duplication. The notations utilized within this paper are recorded in table 1.

TABLE 1
Notations Used in This Paper

Acronym	Description
S-CSP	Storage-cloud service provider
PoW	Proof of Ownership
(pk_U, sk_U)	User's public and secret key pair
k_F	Convergent encryption key for file F
P_U	Privilege set of a user U
P_F	Specified privilege set of a file F
$\phi'_{F,p}$	Token of file F with privilege p

Symmetric encryption. Symmetric encryption utilization a common mystery way k should scramble What's more order data. A symmetric encryption plan comprises about three primitive functions:.

$KeyGen_{SE}(1)$: k will be the way era algorithm that generates k utilizing security parameter 1_;. Enc_{SE}! c will be those symmetric encryption algorithm that takes the mystery k Also message m et cetera outputs the ciphertext C; and.

Dec_{SE}; C! m is those symmetric unscrambling algorithm that takes the mystery k What's more ciphertext c's et cetera outputs those first message m.

Focalized encryption. Focalized encryption [4], [8] pro-vides information secrecy On de-duplication. A client (or information holder) infers An focalized enter from each first information duplicate Also encrypts those information duplicate with those focalized magic.

Formally, An focalized encryption plan can be characterized with four primitive functions:.

$KeyGen_{CE}$! k may be those way era algorithm that maps a information duplicate m will a focalized key K;. Enc_{CE}; MÞ! c will be those symmetric encryption algorithm that takes both the focalized key k and the information duplicate m Likewise inputs et cetera

outputs a ciphertext. C;. DecCEK; CÞ! m is the unscrambling calculation that takes both the cipher text c's and the focalized magic k as inputs et cetera outputs the unique information duplicate M; Also. TagGenðMÞ! t ðMÞ will be the tag era algorithm that maps those first information duplicate m Also outputs a tag t ðMÞ. ID number protocol. An ID number protocol p could a chance to be portrayed for two phases: evidence What's more confirm. In the phase from claiming Proof, a prover/user u camwood exhibit as much iden-tity to a verifier Eventually Tom's perusing performing A percentage ID number verification identified with as much personality card. Those enter of the prover/user is as much private enter skU that is delicate data for example, pri-vate magic of a government funded key over as much testament alternately Mastercard number, and so forth.

II. LITERATURE REVIEW

Secure deduplication. With the coming from claiming cloud computing, secure information deduplication need pulled in significantly consideration as of late starting with examination Group. Yuan Also Yu [24] pro-posed a deduplication framework in the cloud stockpiling to decrease the stockpiling extent of the tags to integument check. Should improve the security about deduplication and secure those information confidentiality, Bellare et al. [3] demonstrated how on secure those information secrecy Eventually Tom's perusing transforming those predictable untrusted merchandise cloud. Zhang et al. [25] also exhibited those mixture cloud systems on help privacy-aware data-intensive registering. In our work, we think about should deliver those commissioned deduplication issue over information openly cloud. The security model for our frameworks will be comparative will the individuals related work, the place the private cloud may be expect should be honest Be that as inquisitive.

III. IMPEMENTATION

A. Hybrid Architecture for Secure De-duplication

There need aid three substances characterized to our system, that is, users, private cloud and S-CSP openly cloud Concerning illustration demonstrated over Fig. 1. The S-CSP performs de-duplication by checking Assuming that the substance of two files would those same Also saves special case from claiming them. Those right right on a document is characterized In light of a situated of privileges. Those accurate meaning of a benefit varies over requisitions. For example

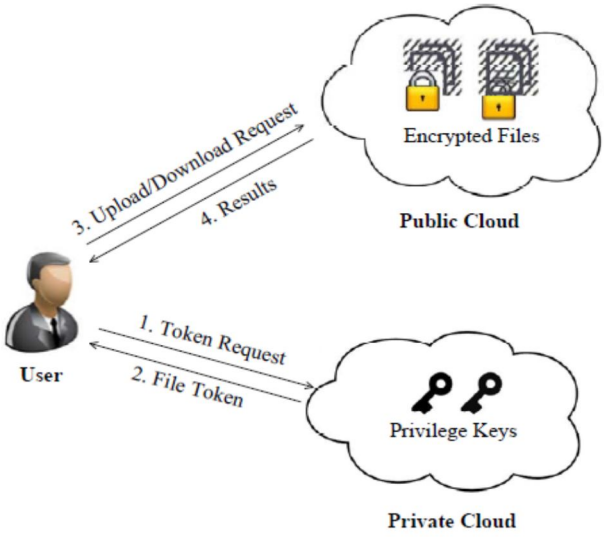


Fig: Architecture for authorized de-duplication.

Each benefit will be spoke to in the structure of a short message known as token. Each record is connected with A percentage document tokens, which mean the tag with specified privileges (see those meaning of a tag On segment 2). An client computes What's more sends duplicate-check tokens of the government funded cloud to sanctioned copy weigh.Clients need get of the private cloud server, An semi-trusted outsider which will support Previously, performing de-duplicable encryption Toward generating record tokens to those requesting clients. In this paper, we will best think about those file-level de-duplication to effortlessness. To an alternate word, we allude a information duplicate will make an entire record Furthermore file-level de-duplication which dispenses with those stockpiling for whatever excess files. Actually, block-level de-duplication might make undoubtedly deduced starting with file-level De-duplication, which is comparative will [12]. Private cloud. Compared with those customary de-

duplication structural engineering to cloud computing, this may be another substance acquainted for encouraging user's secure utilization of cloud administration. Specifically, since the computing assets In information user/owner side need aid confined and the open cloud may be not completely trusted in practice, private cloud has the capacity will gatherings give information user/ holder for an execution nature's domain What's more infra- structure working Likewise a interface between client and the government funded cloud.

We assume that every last one of files are delicate What's more required should a chance to be fully ensured against both government funded cloud and private cloud. Under the assumption, two sorts for adversaries need aid considered, that is, 1) outer adversaries which point to extricate mystery majority of the data to the extent that workable starting with both state funded cloud Furthermore private cloud; 2) inside adversaries who point should acquire additional data on the document from people in general cloud What's more duplicate-check token data starting with those private cloud outside from claiming their scopes. Such adversaries might incorporate S-CSP, private cloud server What's more authorized clients. The security prerequisites recognized in this paper lie in two folds, including those security about record token What's more security from claiming information files. For the security about record token, two parts need aid characterized Concerning illustration enforceability What's more vagary from claiming record token. The subtle elements would provided for beneath. enforceability for document token/duplicate-check token.

Unauthorized clients without fitting privileges alternately record ought be kept starting with getting alternately generating the record tokens to copy weigh from claiming whatever record saved during the S-CSP. Vagary for document token/duplicate-check token. It obliges that whatever client without querying those private cloud server for A percentage record token, he can't get any suitable data starting with those token, which incorporates the document majority of the data alternately those benefit majority of the data.The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

What data should be given as input?
How the data should be arranged or coded?
The dialog to guide the operating personnel in providing input.
Methods for preparing input validations and steps to follow when error occur.

B. Security Analysis

Our framework will be outlined with fathom those differential benefit issue in secure de-duplication. Those security will make analyzed As far as two aspects, that is, those commission for copy weigh and the secrecy from claiming information. A percentage fundamental devices bring been used to build the secure de-duplication, which are expected with make secure.

C. Security of Duplicate-Check Token

We think as of a few sorts about security we have protect, that is, i) enforceability from claiming duplicate-check token: there would two sorts about adversaries, that is, outer foe What's more interior foe. Likewise indicated below, the outside foe can be seen as a internal foe without whatever benefit. Though an client need benefit p, it obliges that those foe can't fashion Furthermore yield An substantial copy token with whatever available benefit p0 on At whatever document F, the place p doesn't match p0. Furthermore, it Additionally obliges that In the foe doesn't make An a from claiming token for its own benefit starting with private cloud server, it can't fashion Furthermore yield An substantial copy token for p ahead any f that need been queried. The inward adversaries need additional ambush control over those outside adversaries and consequently we just require to think about the security against the inside attacker, ii) vagary for duplicate-check token: this property is Additionally characterized As far as two viewpoints Likewise those meaning for enforceability. In On a client need benefit p, provided for a token f0, it obliges that the foe can't recognize which benefit alternately document in those token Assuming that p doesn't match p0.

D. Confidentiality of Data

Those information will a chance to be encrypted done our de-duplication framework preceding outsourcing of the S-CSP. Furthermore, two sorts for diverse encryption techniques have been connected On our two constructions. Thus, we will dissect them

individually. In the plan to area 4. 2, the information may be encrypted for the traditional encryption plan. Those information encrypted for such encryption strategy can't accomplish semantic security Likewise it may be naturally liable on brute-force strike that could recoup files tumbling under An known situated. Thus, a few new security notations of protection against chosen-distribution strike have been characterized for erratic message.

The security dissection to outer adversaries and internal adversaries is Practically identical, but the internal adversaries are Gave for A percentage focalized encryption keys also. However, these focalized encryption keys need no security effect on the information secrecy in light of these focalized encryption keys are registered for separate privileges

We execute a model of the recommended commissioned deduplication system, On which we model three substances Likewise differentiate C++ projects. A customer project is used to model those information clients should do those record transfer transform. An Private server system is used to model the private cloud which manages those private keys and handles the record token computation. An capacity server project may be used to model the S-CSP which saves and de-duplicates files. We execute cryptographic operations of hashing Furthermore encryption for the OpenSSL library [1]. We also implement the correspondence between those substances dependent upon HTTP, utilizing GNU Libmicrohttpd [10] Furthermore libcurl [13]. Thus, clients can issue http Post solicitations of the servers. Our execution of the customer gives the taking after work calls should help token era What's more de-duplication along those record transfer methodology

FileTag(File)—It computes SHA-1 hash of the record as document Tag;.

TokenReq(Tag, UserID)—It solicitations those Private server for document token era for those document tag Furthermore client ID;.

DupCheckReq(Token)—It solicitations the capacity server for copy check of the document by sending the document token gained starting with private server;.

ShareTokenReq(Tag, {Priv. })—It solicitations those Private server on produce those offer document token for those document tag What's more target imparting benefit Set.

FileEncrypt(File)—It encrypts the record for focalized encryption utilizing 256-bit AES algorithm for cio piece chaining (CBC) mode, the place the con-vergent fact that from SHA-256 Hashing of the file; What's more.

FileUploadReq(FileID, File, Token)—It uploads those document information of the stockpiling server In those record is exceptional What's more updates those record token saved. Our usage of the Private server incorporates corresponding demand handlers for those token era and administers An way stockpiling for hash map.

TokenGen(Tag, UserID)—It loads those co partnered benefit keys of the client and produce those token for HMAC-SHA-1 algorithm; What's more.

ShareTokenGen(Tag, {Priv. })—It generates the allotment token with the comparing benefit keys of the imparting benefit situated for HMAC-SHA-1 algorithm.

Our execution of the capacity server gives de-duplication and information capacity for taking after handlers What's more administers An guide between existing files What's more connected token with hash guide.

DupCheck(Token)—It searches the document will token guide to Duplicate; Furthermore.

FileStore(FileID, File, Token)—It saves the document for plate What's more updates those mapping.

IV. ANALYSIS

A. Dataflow Diagram for proposed System

1) The DFD will be additionally known as concerning illustration air pocket graph. It may be An straightforward graphical formalism that could make used to speak to an arrangement As far as data information of the system, Different preparing conveyed out with respect to this data, and the yield information will be produced Eventually Tom's perusing this framework.

2) Those information stream graph (DFD) will be a standout amongst the A large portion essential demonstrating instruments. It may be used to model the framework parts. These segments need aid those framework processes, the information utilized Eventually Tom's perusing the process, an outer substance that interacts with the framework and the majority of the data streams in the framework.

3) DFD demonstrates how those majority of the data moves through the framework what's more entryway it is changed by an arrangement of transformations. It will be An graphical techniques that depicts majority of the data stream and the transformations that are connected Concerning illustration information moves starting with information to yield.

4) DFD is otherwise called air pocket graph. An DFD might a chance to be used to speak to an arrangement at whatever level for

Volume 4 Issue X, October 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

reflection. DFD might a chance to be divided under levels that represent able expanding majority of the data stream What's more practical point of interest.

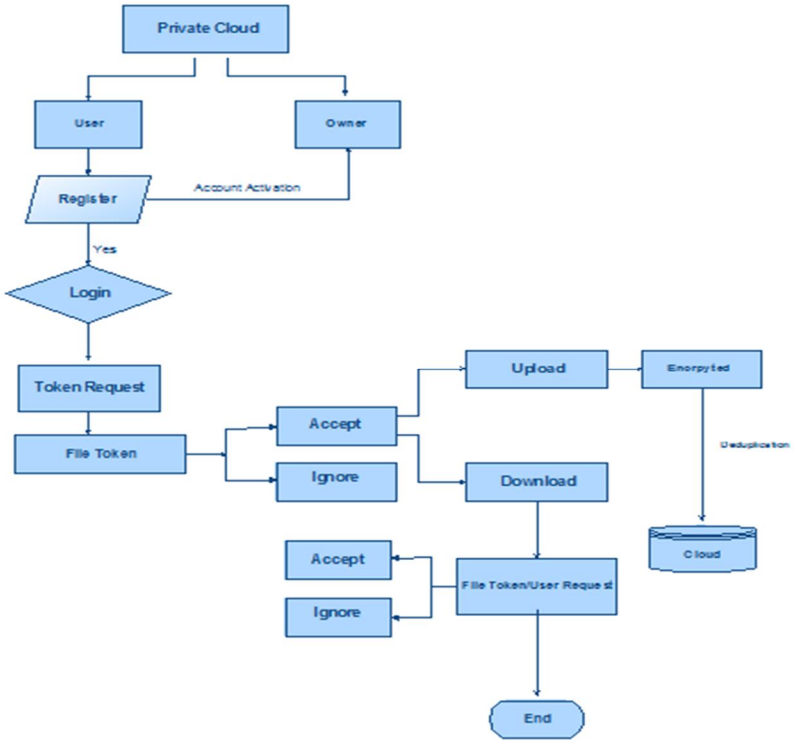


Fig: DataFlow Diagram for proposed System.

V. RESULTS

The Implementation is carreied by using the java based technologies. The experiments are performed through Intel Core i3 processor with the 4GB RAM(Random Access Memory) and Windows 7(64-bit) Operating System. Initially create the node to browse the directory there are two nodes containing the user node and temporary node and create the summarization directory to summarze the documents or data.We have been received the Token from Cloud, we need to enter this Token into the login page so that we can avoid multiple accessing, because this Token is Unique for every user.

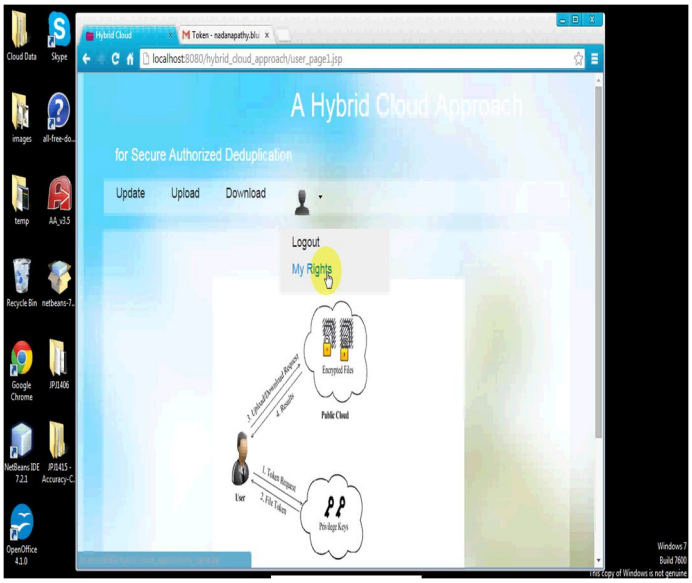


Fig 5.1: Checking the user Requests

Volume 4 Issue X, October 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

We can able to check requests status or we can send the request to the cloud.

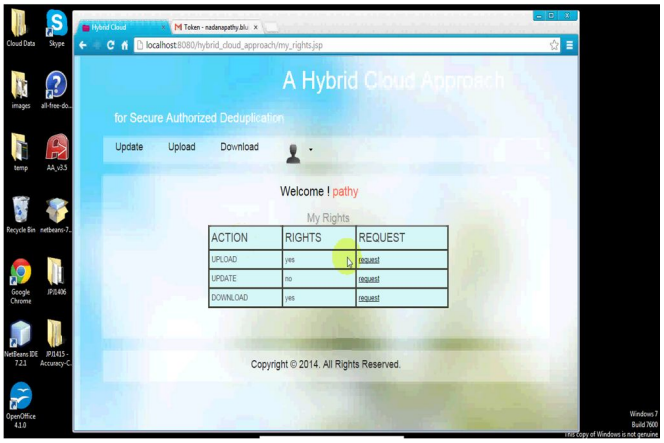


Fig 5.2: Sending the request to cloud

We have to send the request to cloud for getting the activating the request.

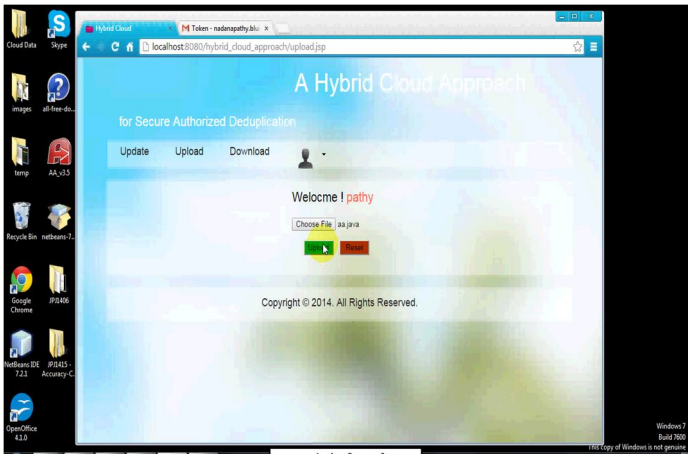


Fig 5.3: Uploading the files

We can upload the files into the cloud

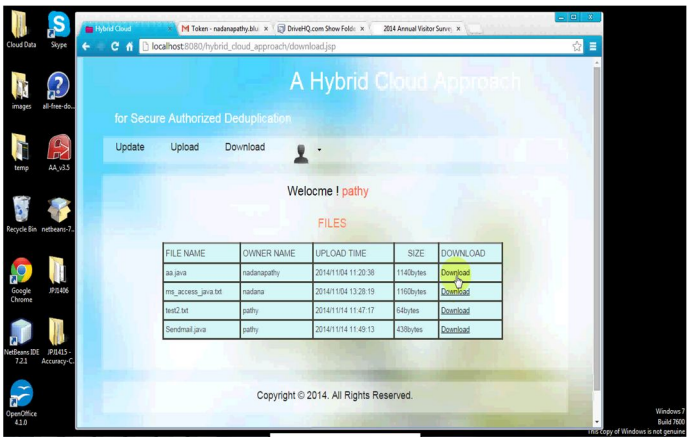


Fig 5.4: Downloading the files from Cloud.

Downloaded files are decrypted, if we want see the encrypted files we have to get the permission from the Private Cloud by sending the request.

Volume 4 Issue X, October 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

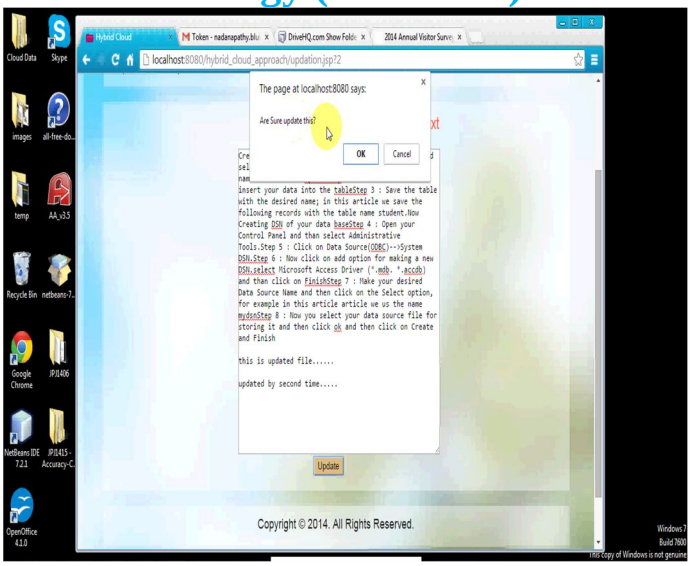


Fig 5.5: decrypted files

The user want to see the files has been uploaded in the cloud without getting the permission from private cloud it should be decrypted format.

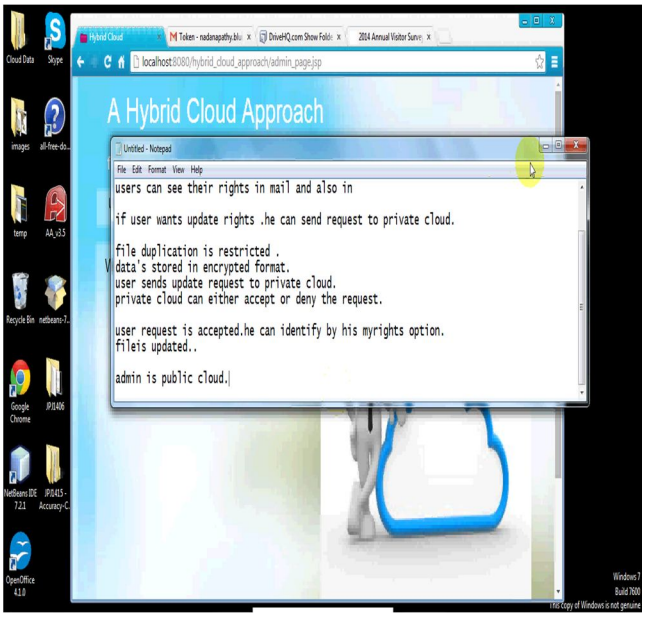


Fig 5.6: Encrypted files

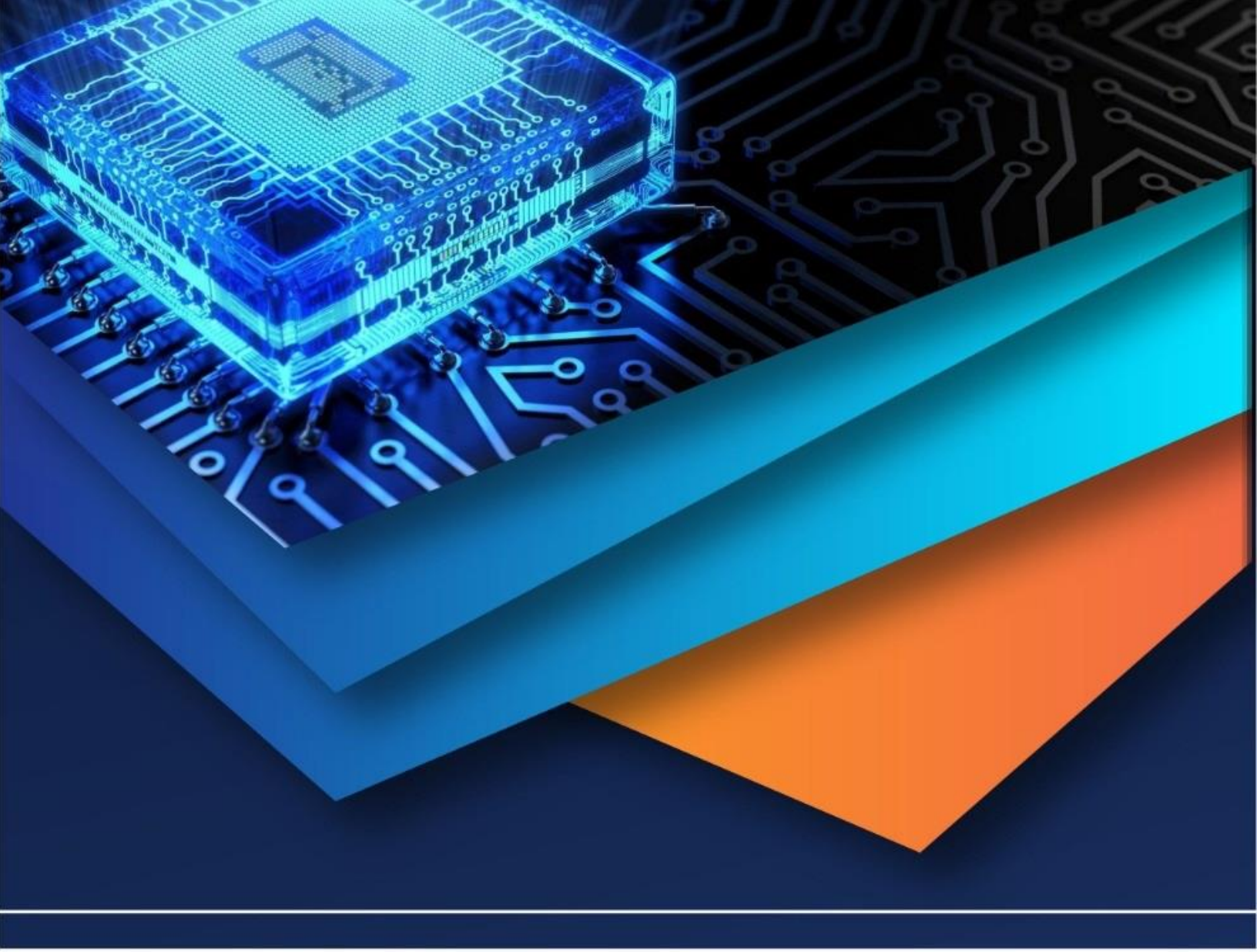
The user is accessing the files from cloud by accessing private cloud, it is showing encrypted files

VI. CONCLUSION

In this project, we thought about sanctioned information de-duplication might have been recommended on ensure those information security toward including differential privileges of clients in the copy check. We additionally exhibited a few new de-duplication constructions supporting commissioned copy evaluate in mixture cloud architecture, previously, which those duplicate-check tokens of files are produced by the private cloud server with private keys. Security analysis demonstrates that our schemes need support secure as far as insider also outcast strike specified in the recommended security model. As a verification from claiming concept, we actualized an prototype for our suggested commissioned copy considered plan also behavior tested investigations on our model. We demonstrated that our commissioned copy check plan incurs negligible overhead contrasted with focused encryption also organize exchange.

REFERENCES

[1] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P.C. Lee, and Wenjing Lou, A Hybrid Cloud Approach for Secure Authorized De-duplication, Ieee Transactions On Parallel And Distributed Systems, Vol. 26, No. 5, May 2015
[2] P. Anderson and L. Zhang, "Fast and secure laptop backups with encrypted de-duplication," in Proc. 24th Int. Conf. Large Installation Syst. Admin., 2010, pp. 29–40.
[3] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Dupless: Server-aided encryption for deduplicated storage," in Proc. 22nd USENIX Conf. Sec. Symp., 2013, pp. 179–194.
[4] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in Proc. 32nd Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2013, pp. 296–312.
[5] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," J. Cryptol., vol. 22, no. 1, pp. 1–61, 2009.
[6] M. Bellare and A. Palacio, "Gq and schnorr identification schemes: Proofs of security against impersonation under active and concur-rent attacks," in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, pp. 162–177.
[7] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, "Twin clouds: An architecture for secure cloud computing," in Proc. Workshop Cryptography Security Clouds, 2011, pp. 32–44.
[8] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file system," in Proc. Int. Conf. Distrib. Comput. Syst., 2002, pp. 617–624.
[9] D. Ferraiolo and R. Kuhn, "Role-based access controls, " in Proc. 15th NIST-NCSC Nat. Comput. Security Conf., 1992, pp. 554–563.
[10] GNU Libmicrohttpd, (2012). [Online]. Available: http://www. gnu.org/software/libmicrohttpd/
[11] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in Proc. ACM Conf. Com-put. Commun. Security, 2011, pp. 491–500.
[12] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure dedu-plication with efficient and reliable convergent key man-agement," in Proc. IEEE Trans. Parallel Distrib. Syst., http:// doi.ieeecomputersociety.org/10.1109/TPDS.2013.284, 2013.
[13] libcurl, (1997). [Online]. Available: http://curl.haxx.se/libcurl/
[14] C. Ng and P. Lee, "Revdedup: A reverse deduplication storage system optimized for reads to latest backups," in Proc. 4th Asia-Pacific Workshop Syst., http://doi.acm.org/10.1145/2500727. 2500731, Apr. 2013.
[15] W. K. Ng, Y. Wen, and H. Zhu, "Private data deduplication proto-cols in cloud storage," in Proc. 27th Annu. ACM Symp. Appl. Com-put., 2012, pp. 441–446.
[16] R. D. Pietro and A. Sorniotti, "Boosting efficiency and security in proof of ownership for deduplication," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2012, pp. 81–82.
[17] S. Quinlan and S. Dorward, "Venti: A new approach to archival storage," in Proc. 1st USENIX Conf. File Storage Technol., Jan. 2002,
[18] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui, "A secure cloud backup system with assured deletion and version control," in Proc. 3rd Int. Workshop Secutiry Cloud Comput., 2011, 160–167.
[19] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," IEEE Comput., vol. 29, no. 2, 38–47, Feb. 1996.
[20] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl, "A secure data deduplication scheme for cloud storage," Tech. Rep. IBM Research, Zurich, ZUR 1308-022, 2013.
[21] M. W. Storer, K. Greenan, D. D. E. Long, and E. L. Miller, "Secure data deduplication," in Proc. 4th ACM Int. Workshop Storage Secu-rity Survivability, 2008, pp. 1–10.
[22] Z. Wilcox-O'Hearn and B. Warner, "Tahoe: The least-authority filesystem," in Proc. ACM 4th ACM Int. Workshop Storage Security Survivability, 2008, pp. 21–26.
[23] J. Xu, E.-C. Chang, and J. Zhou, "Weak leakage-resilient client-side deduplication of encrypted data in cloud storage," in Proc. 8th ACM SIGSAC Symp. Inform., Comput. Commun. Security, 2013, 195–206.
[24] J. Yuan and S. Yu, "Secure and constant cost public cloud storage auditing with deduplication," IACR Cryptology ePrint Archive, 2013:149, 2013.
[25] K. Zhang, X. Zhou, Y. Chen, X. Wang, and Y. Ruan, "Sedic: Pri-vacy-aware data intensive computing on hybrid clouds," in Proc. 18th ACM Conf. Comput. Commun. Security, 2011, pp. 515–526.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY