ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Secured Authentication for De-Duplication by Using Hybrid Cloud Approach

Anucia Devi D.S.[1], Anuradha C.[2], K.G.S. Venkatesan[3]

Department of C.S.E., Bharath University, Chennai, India [1]

Associate Professor, Dept. of C.S.E., Bharath University, Chennai, India [2]

Associate Professor, Dept. of C.S.E., Bharath University, Chennai, India [3]

ABSTRACT: Data de-duplication is one in every of vital information compression techniques for eliminating duplicate copies of continuance information and has been wide employed in cloud storage to scale back the quantity of space for storing and save information measure to guard the confidentiality of sensitive information whereas supporting de-duplication, the confluent cryptography technique has been planned to encipher the info before outsourcing to higher shield information security, this paper makes the primary plan to formally address the matter of approved information de-duplication. Completely different from ancient de-duplication systems, the differential privileges of users are more thought of in duplicate check besides the info itself. We conjointly gift many new de-duplication constructions supporting approved duplicate sign in a hybrid cloud design. Security analysis demonstrates that our theme is secure in terms of the definitions per the planned security model. As an indication of construct, we tend to implement a model of our planned approved duplicate check theme and conduct test bed experiments victimization our model. We tend to show that our planned approved duplicate check theme incurs nominal over head compared to traditional operations.

KEYWORDS: De-duplication authorized duplicate check, confidentiality, hybrid cloud, storage.

I. INTRODUCTION

Cloud computing provides ostensibly unlimited "virtualized" resources to users as services across the full Internet, whereas concealing platform and implementation details. Today's cloud service suppliers provide each extremely available storage and massively parallel computing resources at comparatively low prices. As cloud computing becomes prevailing, Associate in Nursing increasing quantity of information is being stored within the cloud and shared by users with mere privileges, that outline the access rights of the keep data. One crucial challenge of cloud storage services is the management of the ever-increasing volume of information .To make knowledge management ascendable in cloud computing, de-duplication [1] has been a well known technique and has attracted additional and additional attention recently. Data de-duplication could be a specialized knowledge compression technique for eliminating duplicate copies of continuation data in storage. The technique is employed to enhance storage utilization and may even be applied to network knowledge transfers to scale back the quantity of bytes that has got to be sent. Rather than keeping multiple knowledge copies with the same content, de-duplication eliminates redundant knowledge by keeping only 1 physical copy and referring different redundant knowledge thereto copy. De-duplication will occur at either the file level or the block level. De-duplication also can occur at the block level that eliminates duplicate blocks of information that occur in non-identical files [3].

II. RELATED WORK

We proposed pcad scheme, pcad is able to securely "de-duplicate" and the authentication tags by aggregating the tags of the same file from different owner .Its make the storage over head independent to the number of owners of the file. Its cost on cloud users is also constant because most computational tasks can be securely offloaded to the cloud server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

[paper2] We are providing secure outsourced storage that both supports de-duplication and resists brute-force attacks. It provides strong security against external attacks which compromise a communication channels and the security of dup-less gracefully degrades in the face of comprised systems.

We provide the potential to significantly decrease backup times and storage requirements. It has presented a prototype backup program which achieves an optimal degree of sharing at the same time as maintaining confidentiality. it have described a implementation using a local server . we provides either security proofs or attacks for a large number of identity-based identification and signature schemes defined either explicitly or implicitly in existing literature. we provide weaker security and better storage and band-width for popular data, so that data de-duplication can be applied for the popular data. A remove the assumption of a trusted indexing service and explore different means of securing the indexes of unpopular less. We are the fade an overlay cloud storage system with access control and assured deletion. Cryptographic operations for policy-based file assured deletion

We are customers to process a large amount of data at a low cost. a hybrid computing paradigm needs to be supported by a new privacy aware computation framework. it protection cannot be expected from traditional secure outsourcing techniques, which often cannot handle the large amount of data such computation involves. It has several design goals: high storage efficiency, low memory usage, high backup performance, and high restore performance for latest backups. They are core design component of revdedup is reverse de-duplication, which removes duplicates of old backups and mitigates fragmentation of latest backups. We are write to once model and the ability to coalesce duplicate copiesof a block makes venti a useful building block for a number of interesting storage applications. it is useful building block for a number of interesting storage applications. It is used to counter attacks on file de-duplication systems where the attacker obtains a “short summary” of the file and uses it to fool the server into thinking that the attacker owns the entire file.

III. EXISTING SYSTEM

Existing information de-duplication systems, the non-public cloud is occupied as a unique to permit information owner/users to firmly perform duplicate ask differential privileges. In design is sensible and has concerned a lot of interest from researchers. The information homeowners solely source their data storage by utilizing public cloud whereas the info operation is managed in camera cloud [6]

IV. PROPOSED SYSTEM

In victimization advanced de-duplication system supporting approved duplicate check. during this new de-duplication system, a hybrid cloud design is introduced to unravel the matter .The non-public keys for privileges won't be issued to users directly, which is able to be unbroken and managed by the non-public cloud server in its place .In this method, the users cannot share these non-public keys of privileges during this papered construction, which suggests that it will forestall the privilege key sharing among users within the higher than easy construction. to induce a file token, the user has to send an invitation to the non-public cloud server [5].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

V. ARCHITECTURE DIAGRAM

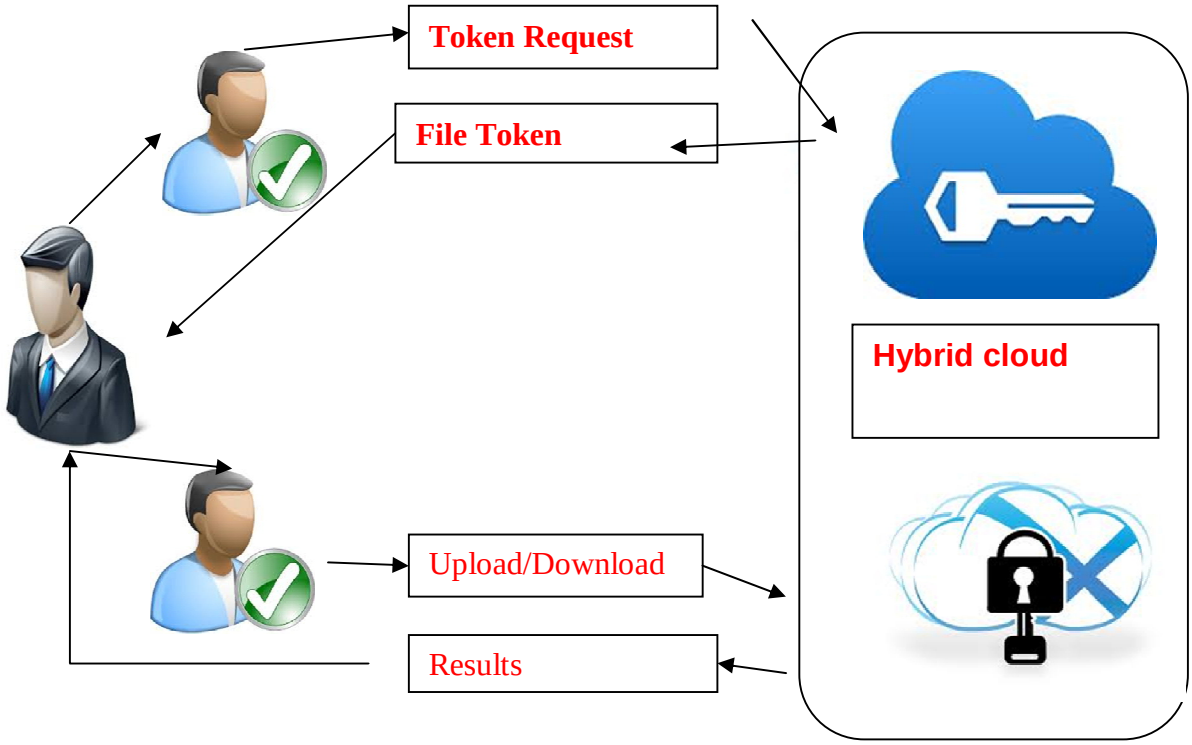

Fig 1 : Architecture diagram for Hybrid cloud for uploading and downloading the results.

VI. MODULE DESCRIPTION

A. AUTHORIZATION CONTROL CREATION AND KEY GENERATION :

Authorized user is ready to use her individual personal keys to come up with question sure as shooting file and also the privileges she closely held with the assistance of personal cloud, whereas the general public cloud performs duplicate check directly and tells the user if there's any duplicate. Unauthorized users while not acceptable privileges or file ought to be prevented from obtaining or generating the file tokens for duplicate check of any file hold on at the S-CSP. In system, the S-CSP is honest however curious and can honestly perform the duplicate check upon receiving the duplicate request from users. The duplicate check token of users ought to be issued from the personal cloud server in our theme [10].

B. OWNER UPLOADING AND BUILT HYBRID CLOUD :

In this new de-duplication system, a hybrid cloud design is introduced to unravel the matter. T he personal keys for privileges won't be issued to users directly, which is able to be unbroken and managed by the personal cloud server instead. during this approach, the users cannot share these personal keys of privileges during this papered construction, which suggests that it will stop the privilege key sharing among users within the on top of easy construction to urge a file token, the user has to send letter of invitation to the personal cloud server.. To perform the duplicate check for a few file, the user has to get the file token from the personal cloud server. The personal cloud server will check the user's identity before supply the corresponding file token to the user. The licensed duplicate check

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

for this file will be performed by the user with the general public cloud before uploading this file. Supported the results of duplicate check, the user either uploads this file or runs prisoner of war [11].

C. DETECT DEDUPLICATION :

Convergent encoding provides information confidentiality in de-duplication. A user derives a merging key from every original information copy and encrypts the info copy with the merging key. Additionally, the user additionally derives a tag for the info copy, such the tag are going to be accustomed sight duplicates. Here, we have a tendency to assume that the tag correctness property holds, i.e., if 2 information copies ar an equivalent, then their tags ar an equivalent. To sight duplicates, the user initial sends the tag to the server facet to see if the identical copy has been already keep. Note that each the merging key and therefore the tag ar severally derived and therefore the tag cannot be accustomed deduce the merging key and compromise information confidentiality. each the encrypted information copy and its corresponding tag are going to be keep on the server facet [12].

D. KEY EXCHANGING :

The non-public keys for the privileges square measure managed by the non-public cloud, the file token requests from the users. The interface offered by the non-public cloud permits user to submit files and queries to be firmly hold on and computed severally. The non-public cloud server also will check the user's identity before supplying the corresponding file token to the user. The licensed duplicate check for this file is performed by the user with the general public cloud before uploading this file [20].

E. VERIFICATION AND FILE RETRIEVING :

A symmetrical key x for every user are going to be choose and set of keys are going to be sent to the personal cloud. Associate degree identification protocol equals to proof and verify is additionally outlined, wherever Proof and Verify are the proof and verification algorithmic program severally. Assume that user U has the privilege set PU. It conjointly initializes a prisoner of war protocol prisoner of war for the file possession proof [19]. It initial sends missive of invitation and also the file name to the S-CSP Upon receiving the request and file name, the S-CSP can check whether or not the user is eligible to transfer file. If failed, the S-CSP sends back associate degree abort signal to the user to point the transfer failure. Otherwise, the S-CSP returns the corresponding cipher text CF. Upon receiving the encrypted knowledge from the S-CSP, the user uses the key kF hold on domestically to recover the initial file [15].

VII. ALGORITHM

A. SYMMETRIC ENCRYPTION :

It uses a common secret key κ to encrypt and decrypt information. A symmetric encryption scheme consists of three primitive functions:

KeyGenSE $(1\lambda) \rightarrow \kappa$ is the key generation algorithm that generates κ using security parameter 1λ.

EncSE $(\kappa, M) \rightarrow C$ is the symmetric encryption algorithm that takes the secret κ and message M and then outputs the ciphertext C.

DecSE $(\kappa, C) \rightarrow M$ is the symmetric decryption algorithm that takes the secret κ and cipher text C and then outputs the original message M.

B. CONVERGENT ENCRYPTION :

It provides knowledge confidentiality in de-duplication. A user derives a confluent key from every original knowledge copy and encrypts the information copy with the confluent key. Additionally, the user conjointly derives a tag for the information copy, such the tag are going to be accustomed find duplicates. Here, we tend to assume that the tag correctness property holds, i.e., if two knowledge copies area unit a similar, then their tags area unit a similar [21]. To find duplicates, the user 1st sends the tag to the server facet to envision if the identical copy has been already kept. Note

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

that each the confluent key and also the tag area unit severally derived, and also the tag can't be accustomed deduce the confluent key and compromise knowledge confidentiality. Each the encrypted knowledge copy and its corresponding tag are going to be keeping on the server facet.Formally, a convergent encryption scheme can be defined with four primitive functions:

KeyGenCE $(M) \rightarrow K$ is the key generation algorithm that maps a data copy M to a convergent key K. EncCE $(K, M) \rightarrow C$ is the symmetric encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs a cipher text C.

DecCE $(K, C) \rightarrow M$ is the decryption algorithm that takes both the cipher text C.

The convergent key K as inputs and then outputs the original data copy M.

TagGen $(M) \rightarrow T(M)$ is the tag generation algorithm that maps the original data copy M and outputs a tag $T(M)$.

VIII. EXPERIMENTAL SETUP AND RESULT

A Hard drive of twenty G and a RAM memory of 256 MB (min) square measure used for the implementation. Java JDK 1.7 is employed because the front-end java and five.0 is employed because the back-end with MySQL [22]

A. *SCREENSHOTS*

The following screenshots show the sample output for De-duplication multiple files and gives an idea on splitting of the hybrid cloud.

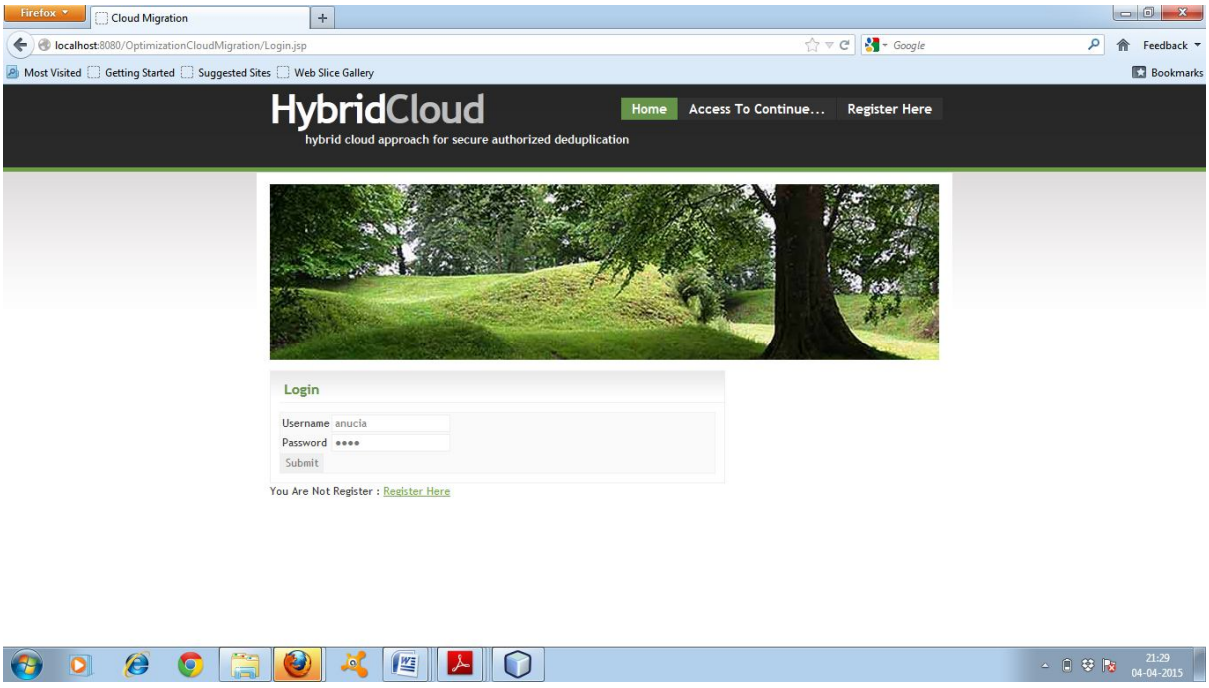

Fig No.1 Login on user name

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

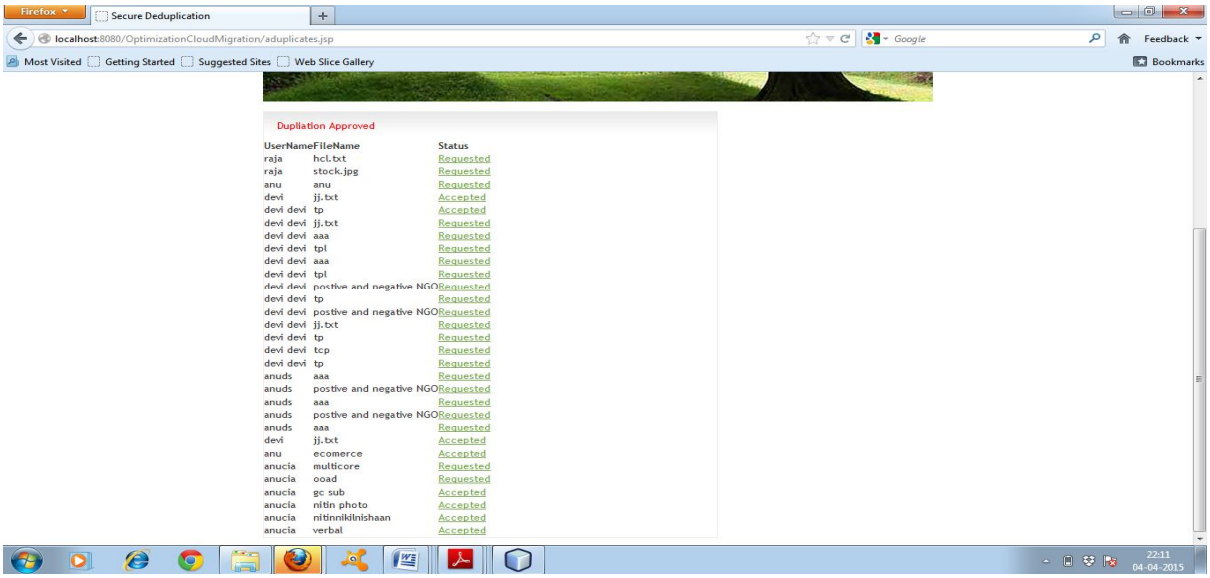

Fig No .2 Duplicated approved

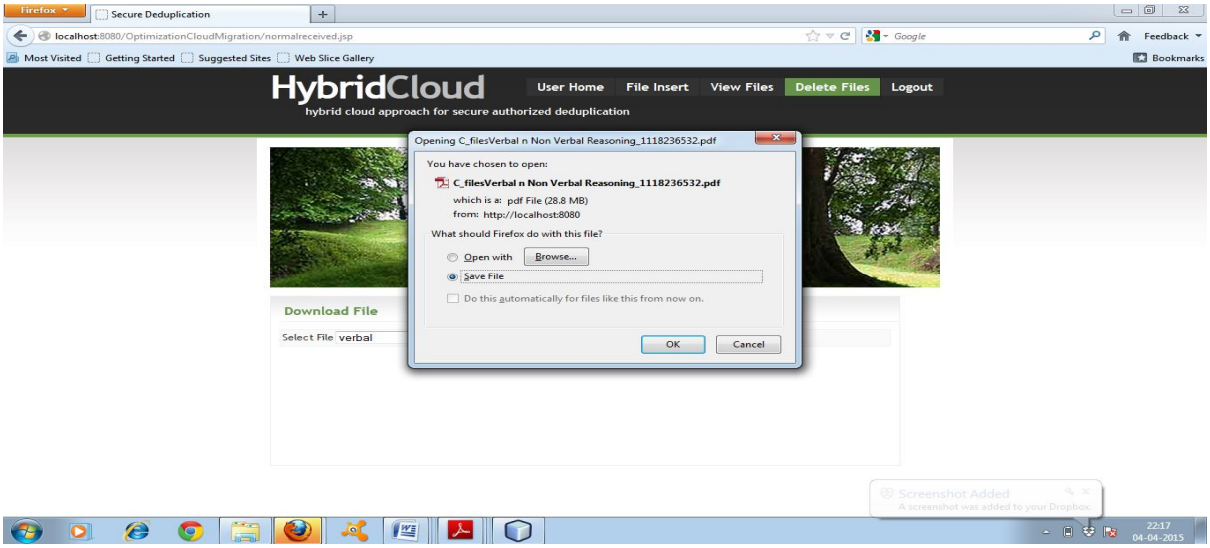

Fig No .3 Open file and download

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

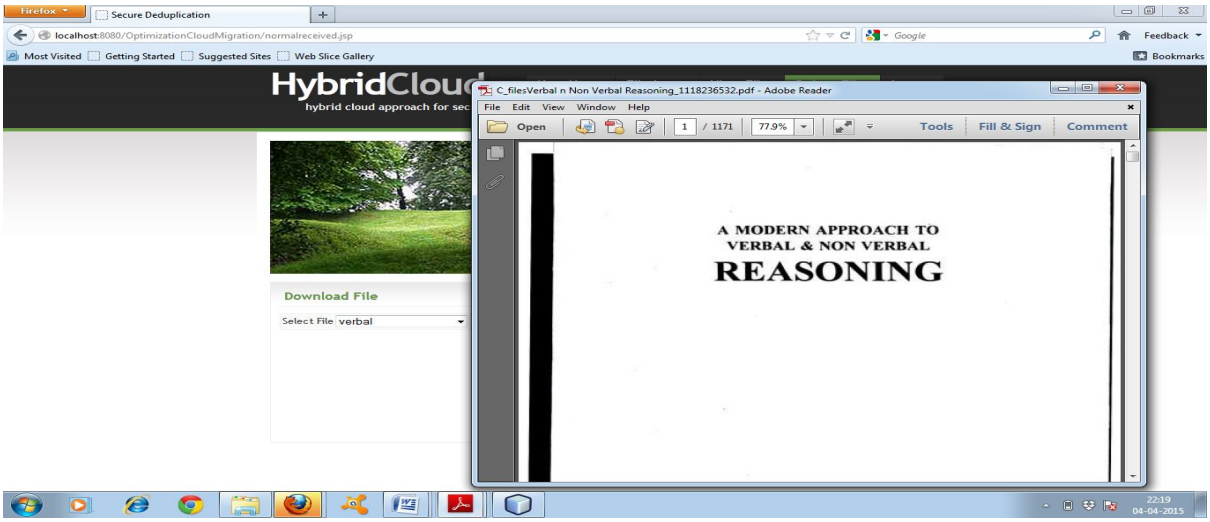

Fig No.4 Output result

B. Comparison with Existing System

Existing information de-duplication systems, the personal cloud is occupied as a distinct to permit information users to firmly perform duplicate see differential privileges. In design is sensible and has concerned abundant interest from researchers.The information homeowners solely source their data storage by utilizing public cloud whereas the information operation is managed privately cloud. [22].

XI. CONCLUSION

In this paper, the notion of authorized data de-duplication was proposed to protect the data security by including differential privileges of users in the duplicate check. We a proof of concept, we implemented a prototype of our proposed authorized duplicate check scheme and conduct test bed experiments on our prototype.

XII. ACKNOWLEDGMENT

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, HOD of Computer Science & Engineering, Dr. K.P. Kaliyamurthie, Bharath University, Chennai for their motivation and constant encouragement. The author would like to specially thank **Dr. A. Kumaravel**, **Dean , School of Computing**, for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science &Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

1. P. Anderson and L. Zhang. Fast and secure laptop backups with encrypted de-duplication. In Proc. of USENIX LISA, 2010.
2. M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Server- aided encryption for deduplicated storage. In USENIX Security Symposium, 2013.
3. M. Bellare, S. Keelveedhi, and T. Ristenpart. Message-locked encryption and secure deduplication. In EUROCRYPT, pages 296- 312, 2013.
4. M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. J. Cryptology, 22(1):1-61, 2009.
5. M. Bellare and A. Palacio. Gq and schnorr identification schemes: Proofs of security against impersonation under active and concur- rent attacks. In CRYPTO, pages 162-177, 2002.
6. S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloud computing. In Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

7. K.G.S. Venkatesan. Dr. V. Khanna, Dr. A. Chandrasekar, "Autonomous System(AS) for mesh network by using packet transmission & failure detection", Inter. Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 12, PP. 7289 – 7296, December -2014.
8. K.G.S. Venkatesan and M. Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 778 – 785, 2013.
9. Teerawat Issariyakul • Ekram Hoss, "Introduction to Network Simulator NS2".
10. S. Sathish Raja and K.G.S. Venkatesan, "Email spam zombies scrutinizer in email sending network Infrastructures", International journal of Scientific & Engineering Research, Vol. 4, Issue 4, PP. 366 – 373, April 2013.
11. G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE J. Sel. Areas Communication., Vol. 18, No. 3, PP. 535–547, Mar. 2000.
12. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
13. P. Indira Priya, K.G.S.Venkatesan, "Finding the K-Edge connectivity in MANET using DLTRT, International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5898 – 5904, 2014.
14. K.G.S. Venkatesan and M. Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, PP. 75 – 80, April 2013.
15. Ms. J.Praveena, K.G.S. Venkatesan, "Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.
16. K.G.S. Venkatesan. Dr. V. Khanna, "Inclusion of flow management for Automatic & dynamic route discovery system by ARS", International Journal of Advanced Research in computer science & software Engg., Vol.2, Issue 12, PP. 1 – 9, December – 2012.
17. Needhu. C, K.G.S. Venkatesan, "A System for Retrieving Information directly from online social network user Link ", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6023 – 6028, 2014.
18. K.G.S. Venkatesan, R. Resmi, R. Remya, "Anonymizimg Geographic routing for preserving location privacy using unlinkability and unobservability", International Journal of Advanced Research in computer science & software Engg., Vol. 4, Issue 3, PP. 523 – 528, March – 2014.
19. 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 ICDCS, pages 617-624, 2002
20. A. Ferraiolo and R. Kuhn. Role-based access controls. In 15th NIST-NCSC National Computer Security Conf., 1992.
21. 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.
22. J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.