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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

SEPDP: Secure Effective Provable Data Possession

K.Balachander[1], G.Mohanaprasad[2], Sk.Gouhar Ahamed[3], T.kishore[4], M.Santhosh Kumar[5]

Assistant Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India[1]

U.G Students, Department of CSE, Velammal Institute of Technology, Chennai, TamilNadu, India[2,3,4,5]

ABSTRACT : Distributed computing is dependable and strong framework to store their information and clients can get to the information from cloud servers. This diminishes capacity and keeps cost of the information owner. In the meantime, the information owner loses the physical control and ownership of information which brings out numerous security dangers. Along these lines, reviewing administration to check information trustworthiness in the cloud is fundamental. This issue has turned into a test as the ownership of information should be confirmed while keeping up the protection. To address these issues this work proposes a safe and productive protection safeguarding provable information ownership (SEPDP). Further, we stretch out SEPDP to help numerous owners in getting correct information.

KEYWORDS - ***PDP****(Provable Data Possession),* ***DU****(Data User),* ***TPA****(Third Party Authority)*

I. INTRODUCTION

Cloud computing and storage provides users with capabilities to store and process their data in third-party data centers.Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, public, hybrid,and community).Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.
When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance report, insider attacks are the sixth biggest threat in cloud computing.Therefore, cloud service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

The deterministic guarantee based schemes verify each block of data and therefore require a significant amount of storage and computation. Alternative kind of schemes called provable data possession (PDP) include use probabilistic checking method, in which a few blocks are randomly selected to detect manipulation. PDP is introduced in that uses random sampling of a few blocks for integrity verification designed two different integrity verification mechanisms. . Moreover, as signatures of the data blocks contain index number of the corresponding blocks, if one block is updated (inserted/modified/deleted), the corresponding verification meta-data (signature) of all other blocks need to be updated.

II. LITERATURE SURVEY

R.F. El-Gazza: On-demand self-service, where the consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider; 2.Broad network access, where the capabilities are available over the network and accessed through

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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations); 3.Resource pooling, where the provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Hansen's : Customers are only allowed to get access to data concerning themselves. Hence, they are not able to analyze complete protocols of administrative operations in the system since this could include other client's information. EU Directive 95/46/EC states that a provider is only allowed to process a client's data after he has been given instructions for this operation. As Cloud servers usually store data of different clients it is difficult for the provider to comply with the needs of a single customer without contradicting the requirements of another client [21]. Hypothetically, the provider is obligated to obtain permission every time he is about to process customer's data, which obviously leads to difficulties in practice considering information overflow

III. PROPOSED SYSTEM

Remote data integrity checking protocols can be broadly categorized into two kinds. The deterministic guarantee based schemes verify each block of data and therefore require a significant amount of storage and computation. One uses pseudo-random function (PRF) which fails to provide public verifiability, while the other one uses. Both the schemes support blocklessverification but fail to provide privacy of the DO's data. Blockless verification requires linear combination of sampled blocks which gives a clue to TPA to extract the data. As a result, TPA can simultaneously perform multiple auditing requests from different DUs. But, all these schemes fail to support data dynamics. This scheme fails to support batch auditing property extended their previous technique to support data dynamics proposed an efficient and secure dynamic auditing protocol that achieves all essential features of public auditing. Also it consumes lesser computation and communication cost.

IV. SYSTEM MODEL

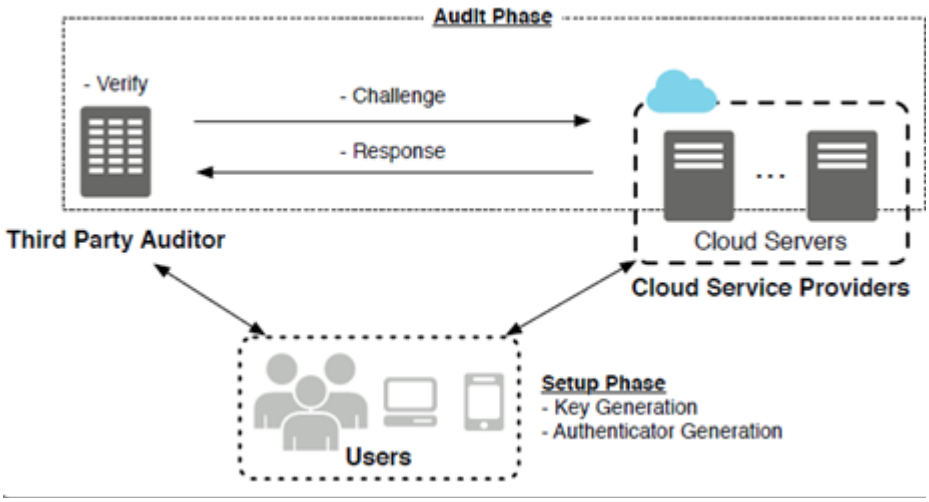


Fig 1.1 System model PDP -based remote data auditing

Service Request to TPA:

User will send request to Third Party Authenticator(TPA) for registration.

TPA Policy Creation:

TPA provides the rules and regulations to be followed by Creator, Reader and Writer.

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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

User File Upload or file creator:

File creator after getting proper authentication uploads his files in the cloud.

KDC Key generation

Key Distribution Centers which are decentralized generate different keys to different types of user after getting tokens from users.

Key revocation

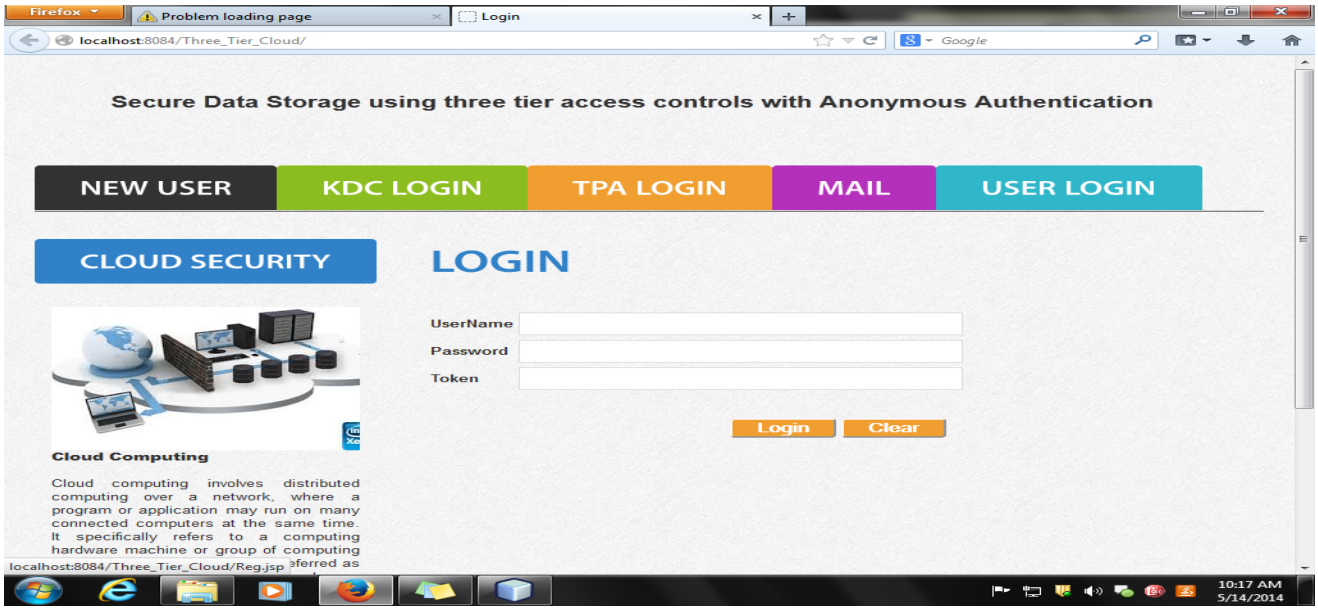
Whenever there is misbehavior detected upon a user his key is revoked and user can neither use or re-enter the cloud environment.

Cloud Admin:

Cloud admin has the list of key distribution centers and TPA. Admin sets the norms to be followed by TPA and KDC. It monitors the key generation policies and informs ubnormal behaviors.

V.RESULT

Fig 2.1 Home Page



This is the user login page where the exisiting user can login with their username and password with token that is generated to them. If the username and password doesn't match the user will not be authorized

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

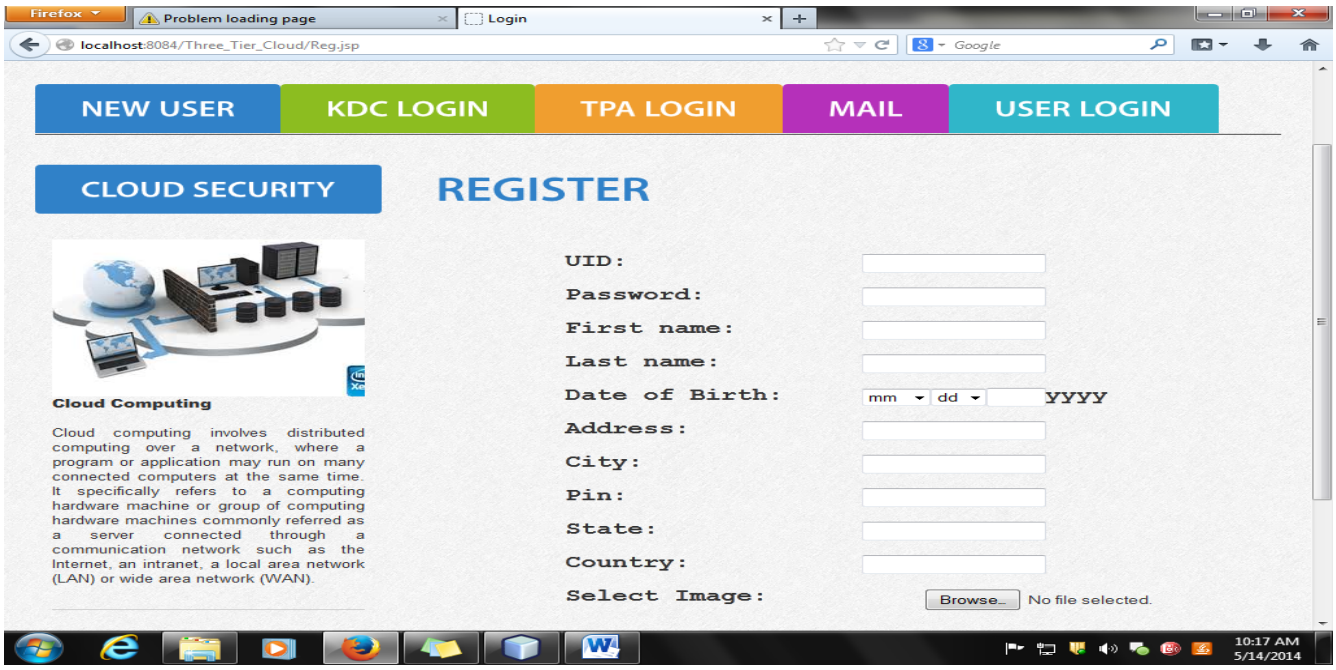
International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

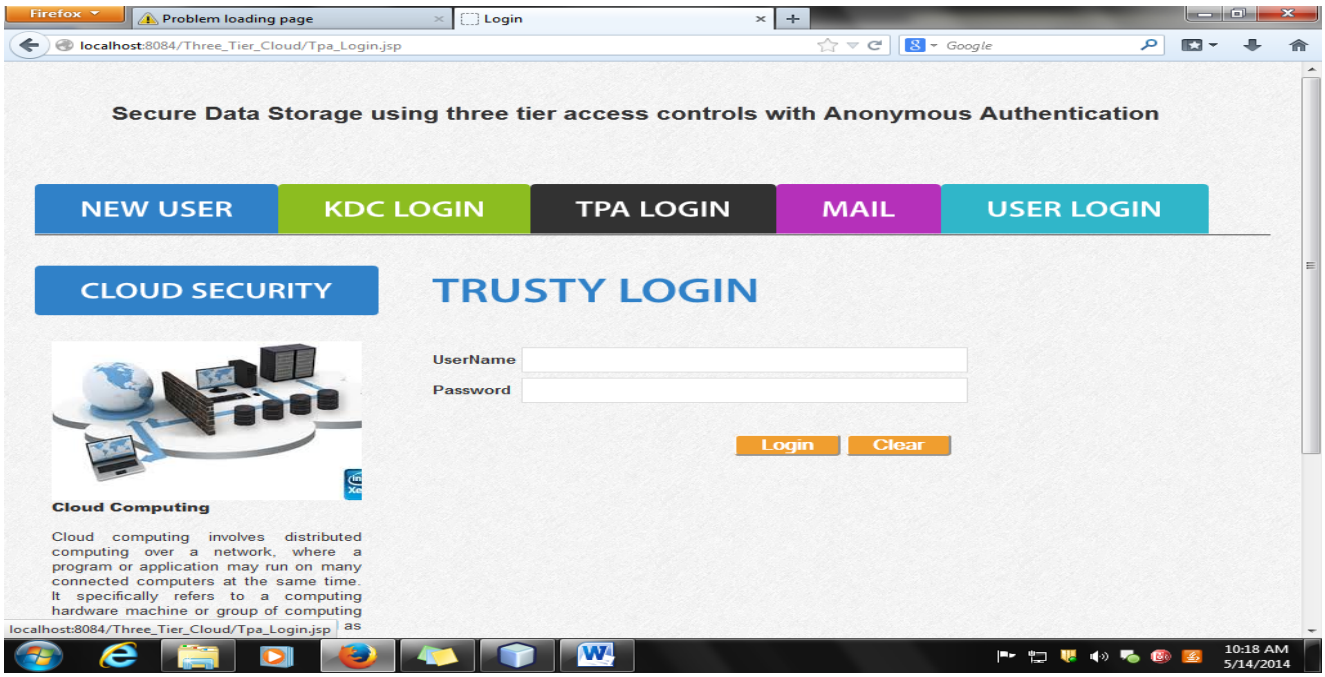
Vol. 7, Issue 2, February 2019

Fig 2.2 Send registration request to Cloud Trusty



In this data owner and data user made a request for registering an account in cloud environment by entering details.

Fig 2.3Third Party Login



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

International Journal of Innovative Research in Computer and Communication Engineering

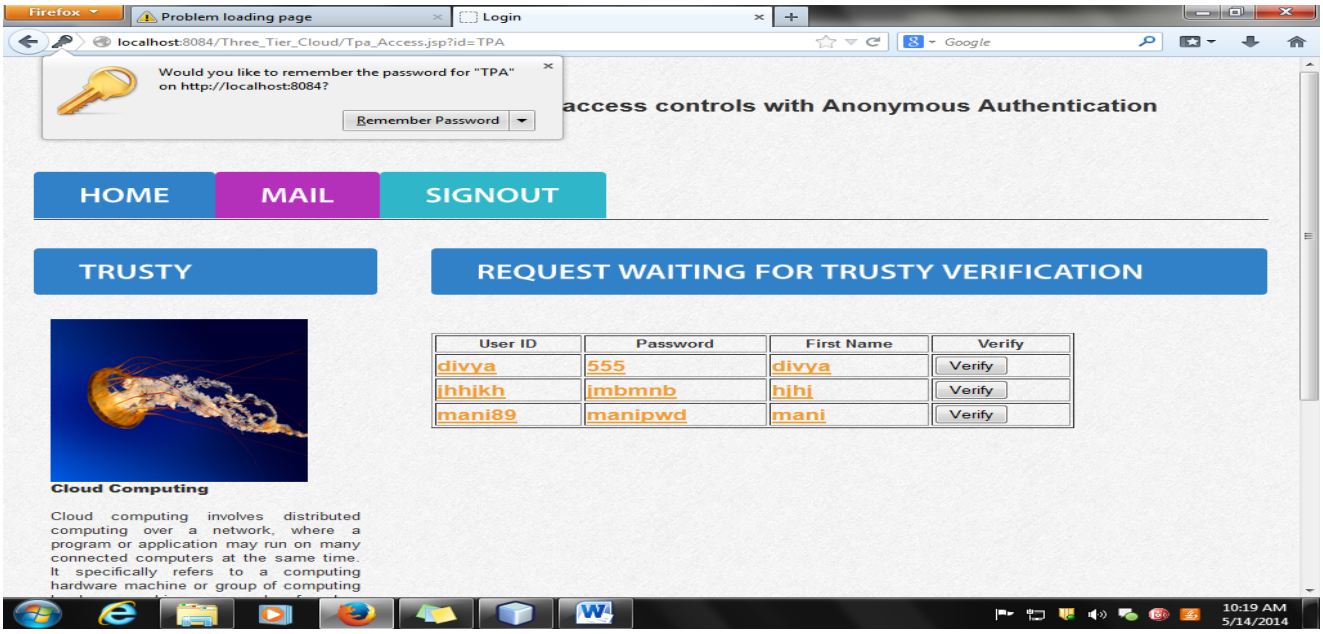
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

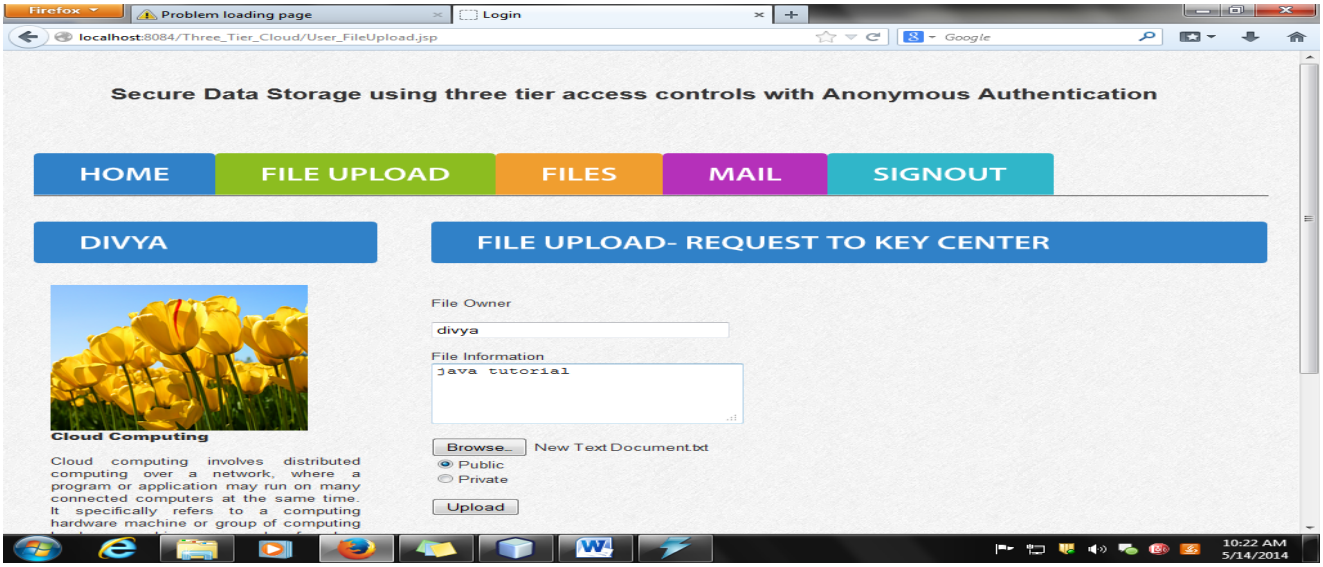
In this Third Party member will login and used to verify whether the data given by owner and the user.

Fig 2.4 Waiting for verification



In this once the data has been submitted by the user it will be under verification . If the user is authorized one he will be permitted to access the environment otherwise access will be denied.

Fig 2.5 File upload Request



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

International Journal of Innovative Research in Computer and Communication Engineering

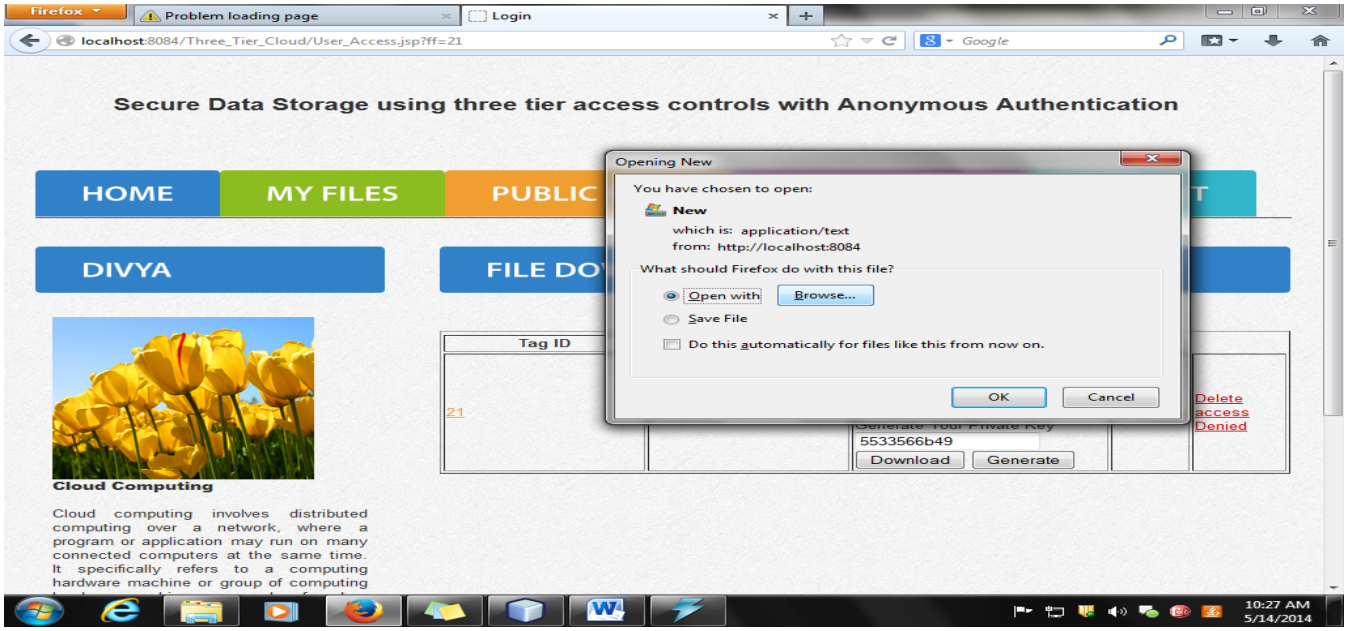
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

In this user will sent a request to the key center for uploading a file to cloud. And also specify in which format like if user select it as public it will available to all otherwise private is meant for restriction only within the user.

Fig 2.6 File download with slave key



In this files are downloaded with slave key. Slave key is meant for activators/Transponder Readers they are associated with.

VI. CONCLUSION

We extend our previous work with added features which enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. In this version we also address user revocation. We use attribute based signature scheme to achieve authenticity and privacy. our scheme is resistant to replay attacks, in which a user can replace fresh data with stale data from a previous write, even if it no longer has valid claim policy. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud.

VII.ACKNOWLEDGEMENT

We are grateful to the almighty for the successful completion of this paper. Special appreciation goes to Assisstantprofessor K.Balachander of Velammal Institute of Technology and everyone who provided their contribution and assistance throughout the project.

REFERENCES

[1] G. Ateniece, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In Proc. of the 14th ACM Conference on Computer and Communications Security (CCS'07), Alexandria, Virginia, USA, pages 598–609. ACM, October 2007.
[2] G. Ateniece, L. V. M. R.D. Pietro, and G. Tsudik.Scalable and efficient provable data possession. In Proc. of the 4th International Conference on Security and privacy in communication networks (SecureComm'08), Istanbul, Turkey, pages 1–10, 2008.

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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

[3] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In Proc. of the 22nd International Conference on Theory and Applications of CryptographicTechniques (Eurocrypt'03), Warsaw, Poland, LNCS, volume 2656, pages 416–432. Springer-Verlag, May2003.
[4] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. Journal of Cryptology,17(4):297–319, September 2004.
[5] C. Chen, Y. Lin, Y. Lin, and H. Sun. RCDA: Recoverable concealed data aggregation for data integrityin wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 23(4):727–734, April2012.
[6] W. Du, M. Murugesan, and J. Jia. Uncheatable grid computing. In Proc. of the 24th International Conference on Distributed Computing Systems, pages 4–11. IEEE, 2004.
[7] C. Erway, A. Kupclu, C. Papamanthou, and R. Tamassia.Dynamic provable data possession. In Proc. of the 16th ACM Conference on Computer and Communications Security (CCS'09), Chicago, Illinois, USA, pages 213–222. ACM, 2009.
[8] E. Esiner, A. Kachkeev, and O. Ozkasap.FlexList: Optimized skip list for secure cloud storage. Technical report, Ko University, 2013.
[9] G. R. Goodson, J. J. Wylie, G. R. Ganger, and M. K. Reiter.Efficient Byzantine-tolerant erasure-codedstorage. In Proc. of 2004 International Conference on Dependable Systems and Networks, pages 135–144. IEEE, June-July 2004.
[10] Q. Huang, G. Yang, D. Wong, and W. Susilo. Efficient strong designated verifier signature schemes without random oracle or with non-delegatability. International Journal of Information Security, 10(6):373–385,November 2011.
[11] H. Kai, H. Chuanhe, W. Jinhai, Z. Hao, C. Xi, L. Yilong, Z. Lianzhen, and W. Bin. An efficient publicbatch auditing protocol for data security in multi-cloud storage. In Proc. of the 2013 8th ChinaGrid AnnualConference (ChinaGrid'13), Changchun, China, pages 51–56. IEEE, August 2013.
[12] V. Kher and Y. Kim. Securing distributed storage: Challenges, techniques, and systems. In Proc. of the 2005 ACM Workshop on Storage Security and Survivability (StorageSS'05), Fairfax, Virginia, USA, pages 9–25. ACM, 2005.
[13] J. Ni, Y. Yu, Y. Mu, and Q. Xia. On the security of an efficient dynamic auditing protocol in cloud storage. IEEE Transactions on Parallel and Distributed Systems, (1):1, PrePrints, doi:10.1109/TPDS.2013.199.
[14] H. Shacham and B. Waters.Compact proofs of retrievability. In Proc. of the 14th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT' 08), Melbourne, Australia, LNCS, volume 5350, pages 90–107. Springer-Verlag, 2008.
[15] C. Wang, S. S.-M. Chow, Q. Wang, K. Ren, and W. Lou.Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers, 62(2):362–375, February 2013.
[16] C. Wang, Q. Wang, K. Ren, and L. Lou. Privacy-preserving public auditing for data storage security in cloud computing. In Proc. of The 29th IEEE Conference on Computer Communications (INFOCOM'10),San Diego, California, USA, pages 525–533. IEEE, March 2010.
[17] H. Wang and Y. Zhang.On the knowledge soundness of a cooperative provable data possession scheme in multicloud storage. IEEE Transactions on Parallel and Distributed Systems, 25(1):264–267, January 2014.
[18] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou. Enabling public verifiability and data dynamics for storage security in cloud computing. In Proc. of the 14th European Conference on Research in Computer Security(ESORICS'09), Saint-Malo, France, LNCS, volume 5789, pages 355–370. Springer-Verlag, 2009.
[19] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 22(5):847–859, May2011.
[20] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos. Security and privacy for storage and computation in cloud computing. Information Sciences, 258:371–386, 2014.
[21] C. Xu, X. He, and D. Abraha-Weldemariam. Cryptoanalysis of wang's auditing protocol for data storage security in cloud computing. In Proc. of the 3rd International Conference on Information Computing and Applications (ICICA'12), Part II, Chengde, China, CCIS, volume 308, pages 422–428. Springer-Verlag,September 2012.
[22] K. Yang and X. Jia. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 24(9):1717–1726, September 2013.
[23] J. Zhang and J. Mao. A novel ID-based designated verifier signature sheme. Information Sciences,178(3):766–773, February 2008.
[24] Y. Zhu, G., H. Hu, S. S. Yau, H. G. An, and C. Hu. Dynamic audit services for outsourced storages in clouds. IEEE Transactions on Services Computing, 6(2):227–238, 2013.
[25] Y. Zhu, H. Hu, G.-J.Ahn, and M. Yu. Cooperative provable data possession for integrity verification in multicloud storage. IEEE Transactions on Parallel and Distributed Systems, 23(12):2231–2244, December2012.