Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

A SURVEY ON SECURE MULTI-OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD (MONA)

V Gokula Krishnan[1], J Gowtham Kumar[2], I Kalyyanasundar[3], R Sanjay[4]

Associate Professor[1], UG Scholars[2,3,4]
Department of Computer Science and Engineering
Panimalar Institute of Technology, Chennai, Tamil Nadu, India

gokul_kris143@yahoo.com[1], gowthamk50@gmail.com[2], kalyyan31011997@gmail.com[3], sanjay.ravishankar@yahoo.com[4]

ABSTRACT - *The genuine function of this strategy is a secure multi-proprietor data sharing arrangement. It derives that any user at intervals the social affair can firmly offer data to others by the untrusted cloud. This arrangement can support dynamic social occasions. Profitably, especially, new permissible customers can clearly unscramble data archives modified before their backing whereas not coming to with data proprietors. User revocations are typically successfully sensible through a novel foreswearing list whereas not modification the puzzle Keys of notwithstanding remains of the purchasers. The dimensions and count overhead of secret writing are steady and freelance with the amount of revoked user. We gift a secure and security guaranteeing access management to customers, which guarantee any half in a very event to anonymously utilize the cloud resource. The veritable identities of information proprietors will be disclosed by the get-together government once open deliberation happen. We have a tendency to offer careful security examination, and perform expansive generations to point out the adequacy of our arrangement to the extent limit and estimation overhead. Disseminated calculation provides a traditionalist and paying response for sharing event resource among cloud customers. Sharing knowledge an exceedingly multi-proprietor means shielding knowledge and identity security from an untrusted cloud continues to be a testing issue.*

KEYWORDS - *Encryption, Cloud Computing, Dynamic Broadcast, Servers, Data Sharing, Privacy Preserving, Access Control, Multi Owner, User Revocation*

I. INTRODUCTION

Cloud computing, with the characteristics of intrinsic information sharing and low maintenance, provides a stronger utilization of resources. In cloud computing, cloud service suppliers provide an abstraction of infinite space for storing for clients to host information. It will facilitate clients scale back their money overhead of information managements by migrating the native managements system into cloud servers. However, security considerations become the most constraint as we have a tendency to currently source the storage of information, which is probably sensitive, to cloud providers. To preserve information privacy, a standard approach is to encode information files before the clients transfer the encrypted

information into the cloud. Unfortunately, it's tough to style a secure and more efficient information sharing scheme, particularly for dynamic clusters within the cloud.

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). As an abstraction for the difficult infrastructure it contains in system diagrams, the name comes from the common use of a cloud-shaped symbol Cloud computing entrusts remote services with a user's information, computer code and computation. Cloud computing is recognized as an alternate to ancient info technology because of its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service suppliers (CSPs), like Amazon, are ready to deliver numerous services to cloud users with the assistance of powerful datacentres. By migrating, the native information management systems into cloud servers, users will get pleasure from high-quality services and save important investments on their native infrastructures.

II. LITERATURE SURVEY

Title	Authors	Journal	Techniques Used	Advantage	Disadvantage
NPP: A New Privacy - Aware Public Auditing Scheme For Cloud Data Sharing With Group Users.	sAnmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang	IEEE Transactions on Big Data, Volume: PP, Issue: 99, pp.1-10, 05 May 2017.	Data Integrity. Homomorphic Verifiable. Non Frame ability. Provable Security	Group users will trace information changes through designated binary tree. Group users will recover the most recent correct information block once the present information block is damage.	It doesn't offer security for sharing the information among the teams. It doesn't offer privacy protective access management to the users.
Privacy-Preserving Public Auditing For Secure Cloud Storage.	Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou	IEEE Transactions on Computers, Volume: 62, Issue: 2, pp.362-375, February 2013.	Data Storage. Privacy Preserving. Public Auditability. Cloud Computing. Delegation. Group Verification.	The user's worry of their outsourced information leak. Considering TPA could concurrently handle multiple audit sessions from totally different users for his or her outsourced information files. The TPA will perform multiple auditing tasks in an exceedingly batch manner for higher potency. It is demonstrably secure and extremely economical.	It is typically short to observe the information corruption only accessing the information, because it doesn't provide users correctness assurance for those accessed information and may be too late to recover the information loss or harm. There is no successful deployment of cloud design some address drawback.
Storing Shared Data on the Cloud Via Security-Mediator.	Boyang Wang, Sherman S.M. Chow, Ming Li, and Hui Li	Distributed Computing Systems (ICDCS), 2013 IEEE International Conference on Collaboration and Internet Computing, pp.124-133, 12 December 2013.	Cloud Computing. Shared Data. Security-Mediator. Data Integrity. Anonymity.	The right approach to attain anonymity is to store information to the cloud with publicly-verifiable data-integrity. Decouple the anonymous protection mechanism from the provable information possession mechanism via the utilization of security intermediates. They minimize the computation and bandwidth demand, however additionally minimize the trust placed on that in terms of information privacy and identity privacy.	To preserve identity privacy from the TPA, as a result of the identities of signers on shared information might indicate that a specific user within the cluster or a special block in shared information may be a more valuable target than others. The information is confidential to the cluster and will not be unconcealed to any third party.
Enabling Cloud Storage Auditing With	Jia Yu, Kui Ren, Cong Wang,	IEEE Transactions on	Data storage. Cloud storage. Auditing.	Auditing protocols will take into account their important issue of the way to cope with the client's	To reduce the harm of the customer's key disclosure in distributed storage

Key -Exposure Resistance.	and Vijay Varadharajan	Information Forensics and Security, Volume: 10, Issue: 6, pp. 1167-1179, 05 February 2015.	Cloud computation. Key Exposure Resistance.	secret key exposure for cloud storage auditing. This protocol overcomes drawback on any exposure of the client's secret auditing key would build most of the present auditing protocols unable to figure properly.	evaluating, and supply the essential convenient illustration for this new drawback setting. The integrity of the information once stored in cloud will still be substantiated although the client's current secret key for cloud storage auditing is vacant in these types of protocols.
Enabling Public Auditability And Data Dynamics for Storage Security in Cloud Computing.	Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li	IEEE Transactions on Parallel and Distributed Systems, Volume: 22, Issue: 5, pp. 847-859, May 2011.	Data storage. Public Auditability. Data dynamics. Cloud Computing.	While not retrieving a replica of the entire information or introducing additional on line burden to the cloud users, Public auditability is to permit TPA for verifying the correctness of the cloud information on demand. Batch Auditing is to change TPA with secure and economical auditing capability to cope up with multiple auditing delegations from probably sizable amount of various users at the same time.	To ensure cloud information storage security, it's vital to enable a third party auditor (TPA) to judge the service qualities from an objective and independent perspective.
Oruta: Privacy-Preserving Public Auditing For Shared Data In The Cloud.	Boyang Wang, Baochun Li and Hui Li	IEEE Transactions on Cloud Computing, Volume: 2, Issue: 1, pp.43-56, 13 January 2014.	Public Auditing. Privacy-preserving. Shared data. Cloud Computing.	Proposed secured system and information owner will decide whether or not the user will access the system or not. A public verifier is ready to properly verify shared information integrity. The ring signatures produced for not exclusively prepared to safeguard identity however furthermore prepared to help block less verifiability.	Cloud Storage system provides the user for safe and consistent place to save lots of valuable information and documents. The third party auditing process ought to bring in no new vulnerabilities towards user information privacy.
Panda: Public Auditing For Shared Data With Efficient User Revocation In The Cloud.	Boyang Wang, Baochun Li, and Hui Li	IEEE Transactions on Services Computing, Volume: 8, Issue: 1, pp. 92-106, January 2015.	Public auditing. Shared data. User revocation. Cloud Computing.	Easily revocable of Signatures for existing users. The Public verifier will audit the integrity of shared information while not retrieving the complete information from the cloud.	Especially once the quantity of re-signed blocks is quite giant. Existing users might access their information sharing services provided by the cloud with resource restricted devices, like mobile phones.
Authorized Public Auditing Of Dynamic Big Data Storage On Cloud With Efficient Verifiable Fine - Grained Updates	Chang Liu, Jinjun Chen, Laurence T. Yang, Xuyun Zhang, Chi Yang, Rajiv Ranjan, and Ramamohana rao Kotagiri	IEEE Transactions on Parallel and Distributed Systems, Volume: 25, Issue: 9, pp.2234-2244, September 2014.	Cloud Computing. Big Data. Data Security. Provable data Possession. Authorized Auditing. Fine-Grained. Dynamic Data Update.	Our theme supports updates with size that's not restricted by the scale of the file blocks, thereby offers further flexibility and measurability com-pared to existing schemes. For higher security, our plan in organization a further authorization method with aim of eliminating threats of unapproved audit challenge from malicious or pretended TPA.	Efficiency in process tiny updates is usually essential in huge information applications. Coarse-grained updates will pro-vide an integrity verification scheme with basic scalability, information updating operations in observe will always be more difficult.
Public Integrity Auditing For Shared Dynamic Cloud Data With Group User	Tao Jiang, Xiaofeng bird genus, and Jianfeng Ma	IEEE Transactions on Computers, Volume: 65, Issue: 8,	Public Integrity Auditing. Dynamic Data. Vector Commitment. Group	System to research on the secure and efficient shared information integrates auditing for multi user operation for cipher text information. Propose an efficient information auditing scheme	Unexpected privilege increase can expose with shared information. User revocation drawback isn't considered and also the auditing cost is linear to the

Revocation.		pp.2363-2373, 01 August 2016.	Signature. Cloud Computing.	whereas at a similar time providing some new options like traceability and count ability. Provide the safety and efficiency analysis of our scheme and therefore the analysis results show that our scheme is secure and economical.	cluster size and information size. Auditing cost of the scheme is linear to the cluster size.
Identity - Based Distributed Provable Data Possession In Multi -Cloud Storage.	H. Wang	IEEE Transactions on Services Computing, Volume: 8, Issue: 2, pp.328-340, March 2015.	ID – DPDP. Cloud Storage. Data Possession.	The distributed cloud storage is indispensable. Efficient and Flexible. Elimination of the certificate management.	CDH problem is hard. This implies that the tip device is also mobile and restricted in computation and storage. A public verifier doesn't check the information in multi cloud.
Achieving Secure, Scalable, And Fine-Grained Data Access Control In Cloud Computing.	Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou	Proceedings of IEEE INFOCOM, pp.1-9, 06 May 2010.	Cloud Computing. Data Security. Attribute Based Encryption (ABE).	Lower maintenance and operation costs. Higher utilization through virtualization. Easier disaster recovery.	Software update may modify security settings, assignment privileges too low. Control of your information or system by third party.

III. CONCLUSION

Cloud computing is extremely engaging surroundings for business world in term of providing needed services in an exceedingly very price effective approach. However, reassuring and enhancing security and privacy practices can attract a lot of enterprises to world of cloud computing. Therefore to realize the reliability and scalability in Mona, during this paper we tend to are measure the new framework for Mona. For dynamic teams in a not trustable cloud, In Mona, a user is ready to share knowledge with others within the cluster while not revealing identity privacy to the cloud. To boot, Mona supports economical user revocation and new user change of integrity. a lot of specially, economical user revocation is achieved through a public revocation list while not change the personal keys of the remaining users, and new users will directly decode files keep within the cloud before their participation. Moreover, the storage overhead and also the coding computation price are constant and length of the signature and also the period of the signing algorithmic rule are freelance of the quantity of cluster members. Intensive analyses show that our planned theme satisfies the required security needs and guarantees potency furthermore.

REFERENCES

[1] Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users" IEEE Transactions on Big Data, Volume: PP, Issue: 99, pp.1-10, 05 May 2017.

[2] C. Wang, Q. Wang, K. Ren, et al, "Privacy Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers, Volume: 62, Issue: 2, pp.362-375, February 2013.

[3] Boyang Wang, Sherman S.M. Chow, Ming Li, and Hui Li, "Storing Shared Data on the Cloud via Security-Mediator" Distributed Computing Systems (ICDCS), 2013 IEEE International Conference on Collaboration and Internet Computing, pp.124-133, 12 December 2013.

[4] Jia Yu, Kui Ren, Cong Wang, and Vijay Varadharajan, "Enabling Cloud Storage Auditing with Key-Exposure Resistance" IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 6, pp. 1167-1179, 05 February 2015.

[5] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE Transactions on Parallel and Distributed Systems, Volume: 22, Issue: 5, pp. 847-859, May 2011.

[6] B. Wang, B. Li, and H. Li, "Oruta: Privacy Preserving Public Auditing for Shared Data in the Cloud," IEEE Transactions on Cloud Computing, Volume: 2, Issue: 1, pp.43-56, 13 January 2014.

[7] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud" IEEE Transactions on Services Computing, Volume: 8, Issue: 1, pp. 92-106, January 2015.

[8] C. Liu, J. Chen, L. Yang, et al, "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine Grained Updates" IEEE Transactions on Parallel and Distributed Systems, Volume: 25, Issue: 9, pp.2234-2244, September 2014.

[9] T. Jiang, X. Chen, and J. Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation" IEEE Transactions on Computers, Volume: 65, Issue: 8, pp.2363-2373, 01 August 2016.

[10] H. Wang, "Identity Based Distributed Provable Data Possession in Multi Cloud Storage" IEEE Transactions on Services Computing, Volume: 8, Issue: 2, pp.328-340, March 2015.

[11] S. Yu, C. Wang, K. Ren, et al, "Achieving Secure, Scalable and Fine Grained Data Access control in cloud computing," Proceedings of IEEE INFOCOM, pp.1-9, 06 May 2010.