Scientific Journal of Impact Factor (SJIF): 4.72
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

Survey On Proficient Data Integrity For Cloud Storage System

Attar Swaleha Bashir[1], Sherkhane Ankita Deepak[2], Sonawane Shradha Ramesh[3],
Pangudwale Dipika Raju[4], Prof. Bhagayshree Bhoyar[5]

[1]*BE Student, Department of Computer Engineering,*
Dr.D.Y.Patil Institute Of Technology,Pimpri,Pune. Maharashtra, India,

[2]*BE Student, Department of Computer Engineering,*
Dr.D.Y.Patil Institute Of Technology,Pimpri,Pune. Maharashtra, India,

[3]*BE Student, Department of Computer Engineering,*
Dr.D.Y.Patil Institute Of Technology,Pimpri,Pune. Maharashtra, India,

[4]*BE Student, Department of Computer Engineering,*
Dr.D.Y.Patil Institute Of Technology,Pimpri,Pune. Maharashtra, India,

[5]*Assistant Professor ,Department of Computer Engineering,*
Dr.D.Y.Patil Institute Of Technology,Pimpri,Pune. Maharashtra, India

Abstract — *Cloud storage service permit users to source their information to cloud servers to avoid wasting local information storage value. Victimization native storage devices users don't physically manage the data hold on cloud servers. The info integrity of the outsourced data has become a problem. Several public verification themes are planned to alter the third party auditor to verify the info integrity for users. there's have to be compelled to focus on work to generalize resolution that may be applied to unravel the higher than downside taking into thought following issue performance, memory, user- friendliness, verification, information integrity, validation of information, authentication of information. Need to work on developing a system which will at the bound options to the present system and by victimization the AES (advanced cryptography data), SHA-1 not for security but making certain that the has not modified thanks to accidental corruption and malicious activity and therefore the access policy on the user facet.*

INTRODUCTION

Cloud storage services modify users to source their information to cloud servers and access the outsourced information remotely from a spread of places and devices (e.g. Drop box, One Drive, and Google Drive). Such services give users with economical and versatile thanks to manage their information while not deploying and maintaining the native device and repair. While individuals get pleasure from the fascinating advantages from the cloud storage service, essential security issues in information outsourcing are raised seriously. One in every of the foremost vital security issues is information integrity. Since users don't physically own their information once outsourcing the information to cloud servers, they're continually troubled concerning the information integrity, i.e. whether or not their information remains intact on the cloud servers. The integrity check on users' information may be performed by a cloud server, but the cloud server might continually generate a decent integrity report permanently name although some information square measure broken or missing AN economical and secure verification methodology is commonly needed by the users to confirm the integrity of their information. Some information verification schemes think about users themselves to execute the verification.

We propose a unique public verification theme, during which the general public auditor will verify the integrity of cloud hold on information in AN economical method. Our projected theme may support batch verification, wherever the verification overhead on the auditor facet is freelance of the amount of users. Furthermore, by exploitation the Markel hash tree technique, our theme will support information dynamics. we tend to envision that the auditor will perform the auditing operations employing a low-power device with restricted computation capability. This might be economic and favorable in observe wherever the necessity on auditor's device is considerably reduced and therefore the information integrity verifications square measure performed of times. To attain this goal, our plan is to delegate the significant computation operations (originally performed by the auditor) to the cloud server. Specifically, the auditor initial specifies a set of information within the cloud server, and therefore the cloud server checks the integrity of the information set. as long as the checking succeeds, the cloud server generates a commitment on the information set, and sends the commitment to the auditor. The auditor solely has to verify the validity of the commitment to ascertain the information integrity. We tend to significantly adopt a highly-efficient commitment theme supported the message authentication code (MAC) technique, as a result of its existential enforceability and light-weight verification.

II. LITERATURE SURVEY

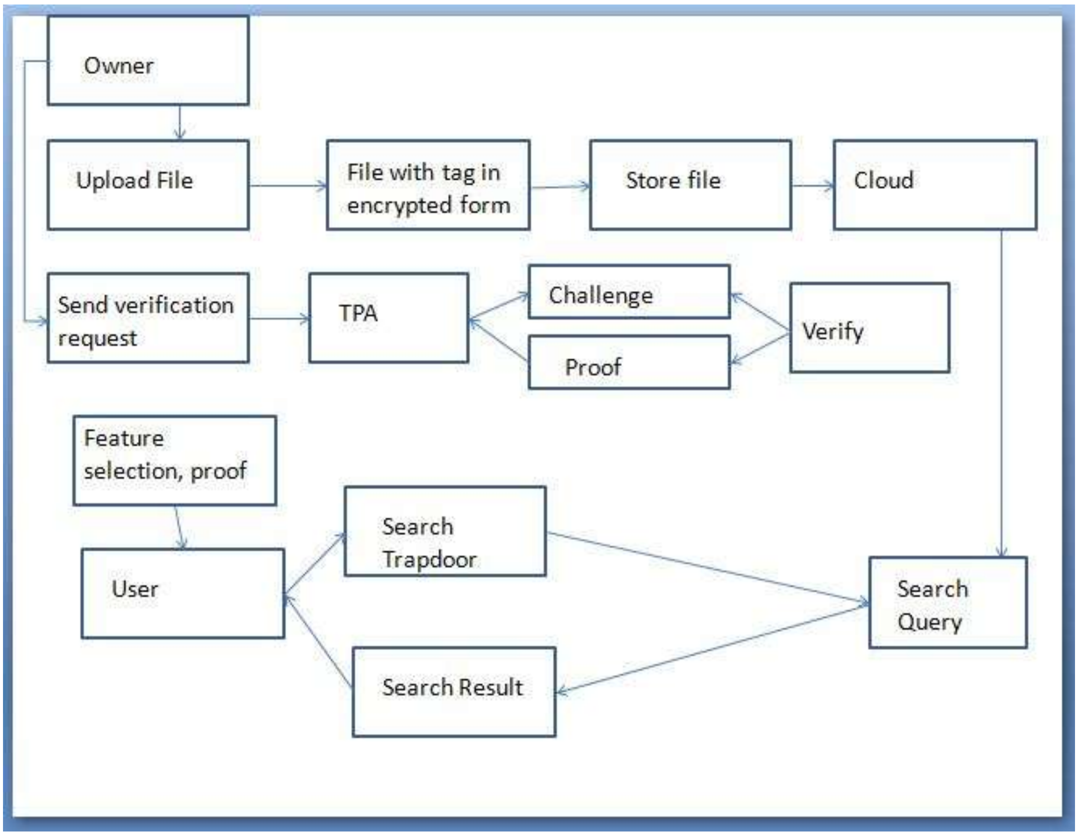
According to literature survey after studying various IEEE paper, collected some related papers and documents some of the point describe here:

Sr.No.	Paper name	Paper Description	Algorithms	Limitations
1	Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing	To achieve economical information dynamics, we have a tendency to improve the present proof of storage models by manipulating the classic Markel Hash Tree construction for block tag authentication. To support economical handling of multiple auditing tasks, we have a tendency to additional explore the technique of linear combination signature to increase our main result into a multiuser profile based, Any TPA will perform multiple auditing tasks at the same time. In depth security and performance analysis show that the planned schemes area unit extremely economical and demonstrably secure.	Merkle Hash Tree	Identify the difficulties and potential security problems of
2	Engineering searchable encryption of mobile cloud networks: when Qoe meets Qop	A fine-grained information search theme and discuss its implementation on encrypted mobile cloud information, which is an efficient balance between QoE and QoP in mobile cloud information outsourcing.	Privacy-preserving fine-grained search	Security and privacy issues related to outsourced data becoming a rising concern
3	Provable Data Possession at Untrusted Stores	Experiments exploitation our implementation verify the utility of PDP and reveal that the performance of PDP is delimited by disk I/O and not by cryptological computation.	Provable data possession, KeyGen, GenProof,	The overhead at the server is low (or even constant), as opposed to linear in the size of the data.
4	On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage	We show that the mortal is ready to randomly modify the cloud information while not being detected by the auditor within the auditing method.	Key gen, Tag gen	trigger many security concerns
5	Cryptanalysis of an integrity checking scheme for cloud data sharing	In this very first the mortal will modify the shared information and tamper with the interaction messages between the cloud server and therefore the TPA, therefore disconfirming shared information integrity checking. Any secondly, AN mortal, United Nations agency records a fraction of the cloud-stored	cryptanalysis	fooling the third-party auditor (TPA) into trusting that the data is well maintained by the cloud server

		information, will write the overwhelming majority of the shared information by exploitation the recorded information and spending shared information integrity verification.		
6	Dynamic Proofs of Retrievability Via Oblivious RAM	In this technique initial level answer providing proofs of retrievability for dynamic storage, wherever the shopper will perform discretional reads/writes on any location among her information by running an economical protocol with the server.	polylogarithmic	do not allow it to be efficiently updated, they all store a redundant encoding of the data on the server
7	Remote Data Auditing in Cloud Computing Environments: A Survey, Taxonomy, and Open Issues	To investigate similarities and variations of such a framework on the idea of the thematic taxonomy to diagnose important and explore major outstanding problems.	RDA	outsourced data is not always trustworthy due to the loss of physical control and possession over the data.
8	SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors	Providing stronger security guarantees of SCLPV in terms of remedying the safety vulnerability of the CLPV and resistance against malicious auditors. The communication value between the auditor and therefore the cloud server of the SCLPV is freelance of the dimensions of the processed information, meanwhile, the auditor within the SCLPV doesn't have to be compelled to manage certificates.	Bilinear	very expensive for users to store large data sets
9	Dynamic remote data auditing for securing big data storage in cloud computing	Presenting the look of a brand new information structure-Divide and Conquer Table (DCT)—that will expeditiously support dynamic information operations like append, insert, modify, and delete. Our planned arrangement are often applied for large-scale information storage and can incur minimum process value.	DCT	lack of control and physical possession over the data. not applicable to big data storage because of the high computational overhead on the auditor
10	Scalable and Efficient Provable Data Possession	Constructing a extremely economical and demonstrably secure PDP technique based mostly entirely on rhombohedral key cryptography, whereas not requiring any bulk secret writing. Also, in distinction	Setup	main issue is how to frequently, efficiently and securely verify that a storage server is faithfully storing its client's (potentially very

		with its predecessors, our PDP technique permits outsourcing of dynamic information, i.e, it expeditiously supports operations, like block modification, deletion and append.		large) outsourced data.

VI.SYSTEM DESIGN



VII.ADVANTAGES

High level Verification.
Good Performance analysis.
High Security.

IV.DISADVANTAGE

Do not physically manage information
Outsourced information become a problem
Enough computation value

VIII.CONCLUSION

We propose AN economical public verification theme for cloud storage mistreatment identicalness obfuscation. The auditor within the planned theme solely has to reckon a message authentication code tag for verification. We tend to additional extend our theme to support batch verification, wherever multiple verification tasks is performed by the auditor at the same time. The auditor's overhead in our batch verification theme is freelance of the quantity of verification tasks. Moreover, the planned theme conjointly achieves information dynamic operations, that embrace insertion, deletion and change.

IX.REFERENCES

[1] "Dropbox," https://www.dropbox.com.

[2] "Onedrive," https://onedrive.live.com.

[3] "Googledrive," http://www.google.com/drive/index.html.

[4] Y. Cui, Z. Lai, X. Wang, N. Dai, and C. Miao, "Quicksync: Improving synchronization efficiency for mobile cloud storage services," in Proceedings of MobiCom. ACM, 2015, pp. 592–603.

[5] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, 2016.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage securityin cloud computing," in Proceedings of ESORICS. Springer, 2009, pp. 355–370.

[7] R. C. Merkle, "Protocols for public key cryptosystems," in Proceedings of S & P. IEEE, 1980, pp. 122–134.

[8] J. Katz and Y. Lindell, Introduction to Modern Cryptography. CRC Press, 2014.

[9] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, "Candidate indistinguishability obfuscation and functional encryption for all circuits," in Proceedings of FOCS. IEEE, 2013, pp. 40–49.

[10] S. Garg, E. Miles, P. Mukherjee, A. Sahai, A. Srinivasan, and M. Zhandry, "Secure obfuscation in a weak multilinear map model," in Proceedings of TCC 2016—B. Springer, 2016.

[11] E. Miles, A. Sahai, and M. Zhandry, "Secure obfuscation in a weak multilinear map model: A simple construction secure against all known attacks," Cryptology ePrint Archive, report 2016/588, 2016.

[12] A. Sahai and B. Waters, "How to use indistinguishability obfuscation: Deniable encryption, and more," in Proceedings of STOC. ACM, 2014, pp. 475–484.

[13] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, "Hiding secrets in software: A cryptographic approach to program obfuscation," Communications of The ACM, vol. 59, no. 5, pp. 113– 120, 2016.

[14] S. Hohenberger, V. Koppula, and B. Waters, "Universal signature aggregators," in Proceedings of EUROCRYPT. Springer, 2015, pp. 3–34.

[15] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetrickey based proofs of retrievability supporting public verification," in Proceedings of ESORICS. Springer, 2015, pp. 203–223.

[16] 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, vol. 8, no. 1, pp. 92–106, 2015.

[17] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in Proceedings of ASIACRYPT. Springer, 2001, pp. 514–532.

[18] Y. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang, "Sclpv: Secure certificateless public verification for cloud-based cyber-physical-social systems against malicious auditors," IEEE Transactions on Computational Social Systems, vol. 2, no. 4, pp. 159–170, 2015.