Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Nontoxic Storage of Self-Motivated Audit Services in Cloud

J. P. Satheesh*
Computer Science & Engineering,
PG Student, Bharath University,
Chennai, India

R. Karthikeyan
Computer Science & Engineering,
Assistant Professor, Bharath University,
Chennai, India

Abstract*— Cloud computing provides a ascendable setting for growing amounts of information and processes that employment on numerous applications and services by suggests that of on-demand self-services. The cloud storage service relieves the burden for storage management and maintenance. Audit service is built supported the techniques, fragment structure, sampling, and index-hash table, supporting demonstrable updates to outsourced knowledge and timely anomaly detection. rather than native knowledge storage and maintenance, the user is assisted with the cloud storage so the user will remotely store their knowledge and revel in the on-demand top quality application from a shared pool of resources. during this project, we have a tendency to propose a technique that hash message authentication code to enhance the performance of audit services. to boost the correctness of information, auditing method is completed that is disbursed by Third Party Auditor. The TPA should be economical to audit while not tightened the native copy of information. within the cloud storage, user place their knowledge within the cloud and not posses the info domestically. one amongst the key issue is to notice the modification and corruption throughout the auditing method by TPA. The third party auditing enable to avoid wasting time and computation resources with reduced on-line burden of the user.

Keywords*— Cloud Storage Service, Third Party Auditor, HMAC, Scalable, Authentication

I. INTRODUCTION

Cloud computing has been pictured because the next-generation info technology (IT) design for enterprises, because of its long list of unexampled blessings within the IT history: on-demand self-service, present network access, location freelance resource pooling, fast resource snap, usage-based evaluation and transference of risk. As a troubled technology with profound implications, Cloud Computing is reworking the terribly nature of however businesses use info technology. One elementary side of this paradigm shifting is that knowledge is being centralized or outsourced to the Cloud. From users' perspective, as well as each people and IT enterprises, storing knowledge remotely to the cloud in a very versatile on-demand manner brings appealing benefits: relief of the burden for storage management, universal knowledge access with freelance geographical locations, and turning away of cost on hardware, software, and personnel maintenances, etc. whereas Cloud Computing makes these blessings additional appealing than ever, it additionally brings new and difficult security threats towards users' outsourced knowledge. Since cloud service suppliers (CSP) area unit separate body entities, knowledge outsourcing is truly relinquishing user's final management over the fate of their knowledge. As a result, the correctness of the info within the cloud is being place in danger because of the subsequent reasons. 1st of all, though the infrastructures below the cloud area unit far more powerful and reliable than personal computing devices, they're still facing the broad vary of each internal and external threats for knowledge integrity. To firmly introduce a good third party auditor (TPA), the subsequent 2 elementary necessities ought to be met: TPA ought to be ready to expeditiously audit the cloud knowledge storage while not hard the native copy of knowledge, and introduce no further on-line burden to the cloud user. Specifically, our contribution during this work will be summarized because the following 3 aspects:

Motivate the general public auditing system of knowledge storage security in Cloud Computing and supply a privacy-preserving auditing protocol, i.e., our theme supports associate degree external auditor to audit user's outsourced knowledge within the cloud while not learning data on the info content.

Our theme is that the 1st to support scalable and economical public auditing within the Cloud Computing. specifically,our theme achieves batch auditing wherever multiple delegated auditing tasks from totally different users will be performed at the same time by the TPA.

Prove the protection and justify the performance of our planned schemes through concrete experiments and comparisons with the progressive.

The traditional science technologies for knowledge integrity and availableness, supported Hash functions and signature schemes cannot work on the outsourced knowledge. it's not a sensible resolution for knowledge validation by downloading them because of the valuable communications, particularly for giant size files. Moreover, the flexibility to audit the correctness of the info in a very cloud surroundings will be formidable and valuable for the cloud users. Therefore, it's crucial to understand public audit ability for CSS, in order that knowledge house owners might resort to a 3rd party auditor, World Health Organization has experience and capabilities that a standard user doesn't have, for

sporadically auditing the outsourced knowledge. This audit service is considerably necessary for digital forensics and believability in clouds. To implement public audit ability, the notions of proof of retrievability and demonstrable knowledge possession are planned by some researchers. Their approach was supported a probabilistic proof technique for a storage supplier to prove that clients' knowledge stay intact.

Dynamic audit service for confirmative the integrity of associate degree untrusted and outsourced storage. audit service is made supported the techniques, fragment structure, sampling, and index-hash table, supporting demonstrable updates to outsourced knowledge and timely anomaly detection. additionally, they planned a way supported probabilistic question and periodic verification for rising the performance of audit services. Our experimental results not solely validate the effectiveness of our approaches, however additionally show our audit system verifies the integrity with lower computation overhead and requiring less further storage for audit data. The consumer (DO) uses a secret key to pre-process a file, that consists of a group of n blocks, generates a group of public verification parameters (PVPs) and IHT that area unit keep in TPA, transmits the file and a few verification tags to CSP, and will delete its native copy By mistreatment associate degree interactive proof protocol of retrievability, TPA (or different applications) problems a "random sampling" challenge to audit the integrity and availableness of the outsourced knowledge in terms of verification info (involving PVP and IHT) keep in TPA.An AA, World Health Organization holds a DO's secret key sk, will manipulate the outsourced knowledge and update the associated IHT keep in TPA. The privacy of sk and also the checking algorithmic rule make sure that the storage server cannot cheat the AAs and forge the valid audit records .Since the appropriate operations need that the AAs should gift authentication info for TPA, any unauthorized modifications for knowledge are detected in audit processes or verification processes. supported this type of robust authorization-verification mechanism, we tend to assume neither CSP is sure to ensure the protection of keep knowledge, nor a DO has the aptitude to gather the proof of CSP's faults once errors are found.

II. RELATED WORK

M. Xie, H. Wang, J. Yin, and X. Meng.. In C. Koch, J. Gehrke, M. N.Garofalakis, D. Srivastava, K. Aberer, A. Deshpande,D. Florescu, C. Y. Chan, V. Ganti, C.-C. Kanne, W. Klas, and E. J. Neuhold, editors, VLDB, pages 782–793. ACM,2007.An increasing variety of enterprises source their IT services to 3rd parties United Nations agency offers these services for a far lower price because of economy of scale. Quality of service could be a major concern in outsourcing. above all, question integrity, which implies that question results came by the service supplier area unit each correct and complete, should be assured. Previous work needs shoppers to manage knowledge regionally to audit the results sent back by the server, or information engine to be changed for generating documented results.

A.Yavuz and P. Ning. Baf:. In ACSAC, pages 219–228, 2009.

Audit logs, providing info regarding the present and past states of systems, area unit one amongst the foremost vital elements of recent laptop systems. Providing security for audit logs on AN untrusted machine during a massive distributed system could be a difficult task, particularly within the presence of active adversaries. In such a system, it's essential to possess forward security such once AN someone compromises a machine, she cannot modify or forge the log entries accumulated before the compromise. sadly, existing secure audit work schemes have important limitations that build them impractical for real-life applications: Existing Public Key Cryptography (PKC) based mostly schemes area unit computationally expensive for work in task intensive or resource-constrained systems, whereas existing regular schemes don't seem to be in public verifiable and incur important storage and communication overheads. a completely unique forward secure and combination work theme known as Blind- Aggregate-Forward (BAF) work theme, that is appropriate for giant distributed systems. BAF will turn out in public verifiable forward secure and combination signatures with near-zero process, storage, and communication prices for the loggers, while not requiring any on-line sure Third Party (TTP) support. we tend to prove that BAF is secure underneath acceptable process assumptions, and demonstrate that BAF is considerably additional economical and ascendable than the previous schemes. Therefore, BAF is a perfect resolution for secure work in each task intensive and resource-constrained systems.

C. Wang, Q. Wang, K. Ren, and W. Lou.. In INFOCOM, 2010 Proceedings IEEE, pages 1 –9, 14-19 2010 mistreatment Cloud Storage, users will tenuously store their knowledge and luxuriate in the on-demand top quality applications and services from a shared pool of configurable computing resources, while not the burden of native knowledge storage and maintenance. However, the actual element that users not have physical possession of the outsourced knowledge makes the info integrity protection in Cloud Computing a formidable task, particularly for users with strained computing resources. Moreover, users ought to be ready to simply use the cloud storage as if it's native, without fear regarding the necessity to verify its integrity. Thus, sanctioning public auditability for cloud storage is of essential importance in order that users will resort to a 3rd party auditor (TPA) to visualize the integrity of outsourced knowledge and be worry-free. To firmly introduce an efficient TPA, the auditing method ought to usher in no new vulnerabilities towards user knowledge privacy, and introduce no further on-line burden to user. during this project, a secure cloud storage system supporting privacy-preserving public auditing. we tend to any extend our result to modify the TPA to perform audits for multiple users at the same time and expeditiously. intensive security and performance analysis show the planned schemes area unit demonstrably secure and extremely economical.

S.Ezhil Arasu, B.Gowri, S.Ananthi "In International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013 Cloud computing is that the arising technology to reduce the user burden within the updation of information in business mistreatment net. rather than native knowledge storage and maintenance, the user is assisted with the cloud storage in order that the user will remotely store their knowledge and luxuriate in the on-demand top quality application from a shared pool of resources. the info hold on should be protected within the cloud

storage. to reinforce the correctness of information, auditing method is finished that is disbursed by TPA(Third Party Auditor). The TPA should be economical to audit while not strict the native copy of information. during this paper we've planned a technique that uses the keyed Hash Message Authentication Code (HMAC) with the Homomorphic tokens to reinforce the safety of TPA .In the cloud storage, user place their knowledge within the cloud and not posses the info regionally. one amongst the key issue is to find the modification and corruption throughout the auditing method by TPA. The third party auditing enable to avoid wasting time and computation resources with reduced on-line burden of the user. Security for {the knowledge |the info |the information} hold on in cloud throughout the auditing method will be provided by HMAC along side the homomorphic tokens with erasure coded data.

III. PROPOSED WORK

Design Engineering deals with the varied UML [Unified Modeling language] diagrams for the implementation of project. style may be a important engineering illustration of a factor that's to be engineered. software package style may be a method through that the wants ar translated into illustration of the software package. style is that the place wherever quality is rendered in software package engineering. style is that the suggests that to accurately translate client necessities into finished product.This design explains the project work flow with the most functions of the construct. we have a tendency to introduce associate audit system design for outsourced knowledge in clouds as shown in Fig 1.

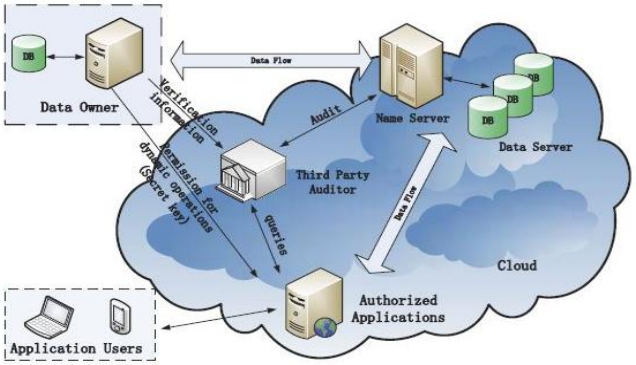
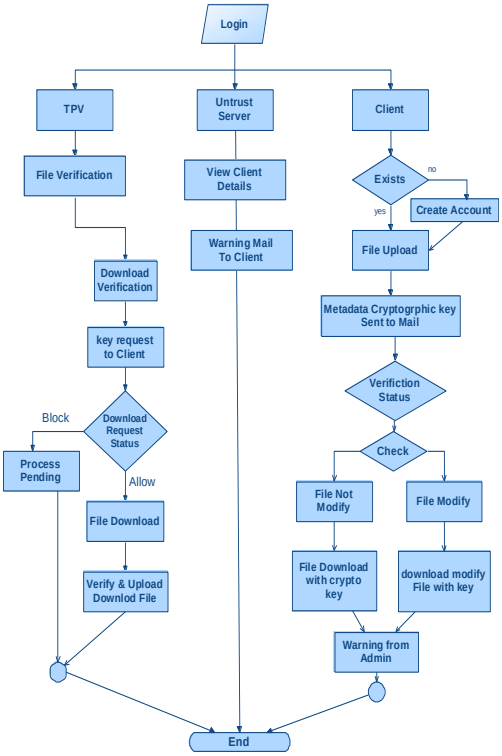


Fig.1 System architecture of the proposed system

In this design, we have a tendency to contemplate information |a knowledge |an information} storage service involving four entities: data owner (DO), World Health Organization includes a great deal of information to be keep within the cloud; clou service supplier (CSP), World Health Organization provides knowledge storage service and has enough storage spce and computation resources; third party auditor (TPA), World Health Organization has capabilities to manage or monitor the outsourced knowledge below the delegation of information owner; and licensed applications (AA), World Health Organization have the proper to access and manipulate keep knowledge. Finally, application users will get pleasure from varied cloud application services via these licensed applications.

A. Data Flow Diagram



B. Modules

1) Key Generation:

The owner generates a public/secret key combine (pk, sk) by himself or the system manager, then sends his public key pk to TPA. Note that TPA cannot acquire the client's secret key sk; second, the owner chooses the random secret.

2) Tag Generation:

The consumer (data owner) uses the key key sk to pre-process a file, that consists of a group of n blocks, generates a collection of public verification parameters and index-hash table that are keep in TPA, and transmits the file and a few verification tags to CSP.

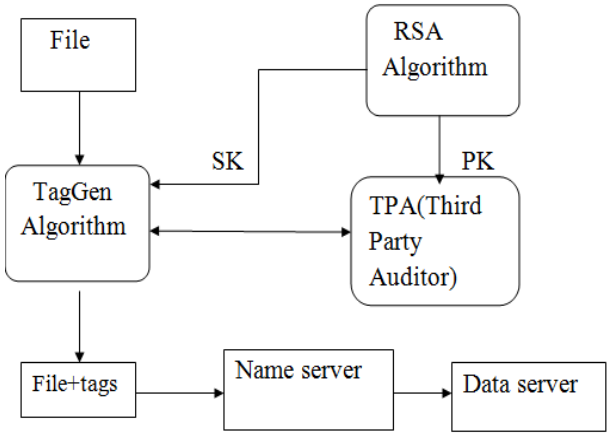


Fig.2 Tag Generation

3) Periodic Sampling Audit:

TPA problems a "Random Sampling" challenges to audit the integrity and convenience of outsourced information in terms of the verification info keep in TPA

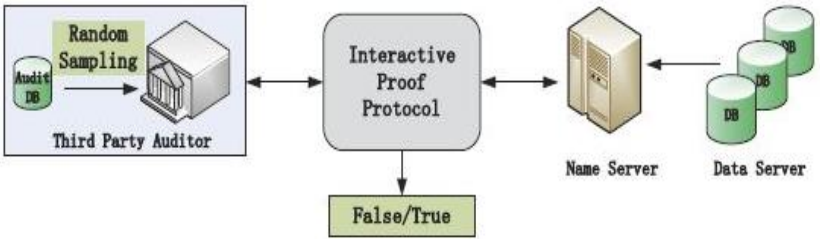


Fig.3 Periodic Sampling Audit Flow

4) Audit for Dynamic Operations:

An authorized application, that holds knowledge owner's secret key sk, will manipulate the outsourced knowledge and update the associated index hash table hold on in TPA. The privacy of sk and therefore the checking rule make sure that the storage server cannot cheat the licensed applications and forge the valid audit records.

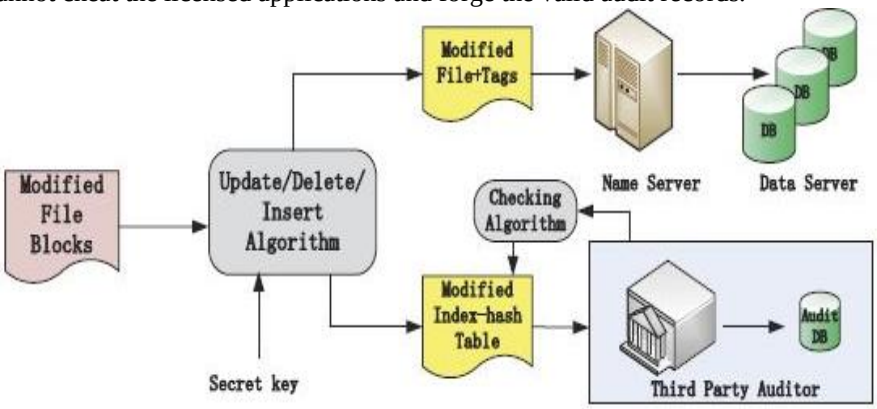


Fig.4 Flow of dynamic data operations

C. HMAC

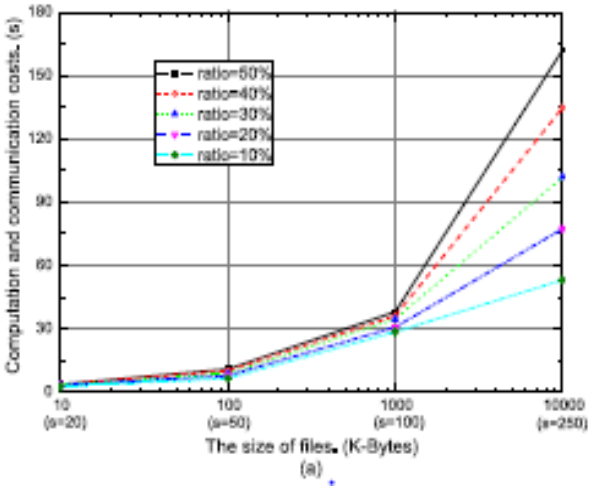
Hash primarily based message authentication code is science hash perform that is all concerning the concatenation of message and therefore the key and hash them along. it's the strategy of shrewd message authentication code with science hash perform by victimization secret science key. The hash formula wont to generate the authentication code is SHA.

1) Formation of HMAC Which implement the function:

HMACk = Hash [(K+ XOR opad)] | | Hash [(K+ XOR ipad) | | M)]

K+ is K cushioned with zeros on the left so the result's b bits long ipad could be a pad price of thirty six hex perennial to fill block opad could be a pad price of 5C hex perennial to fill block M is that the message given as input to HMAC[10]. The output of the HMAC is that the binary authentication code that equals within the length to it of the hash operate digest. the safety of the HMAC is directly proportional to the underlying hash operate. hence security of HMAC is claimed to be weaker if the underlying hash operate is MD5 and stronger if the underlying hash operate is SHA – 512. The threats of the HMAC ar aforementioned to be forgery and therefore the key recovery attacks, however these threats want sizable amount of message pairs for the analysis.

IV. EXPERIMENTAL RESULTS



V. PERFORMANCE RATIO

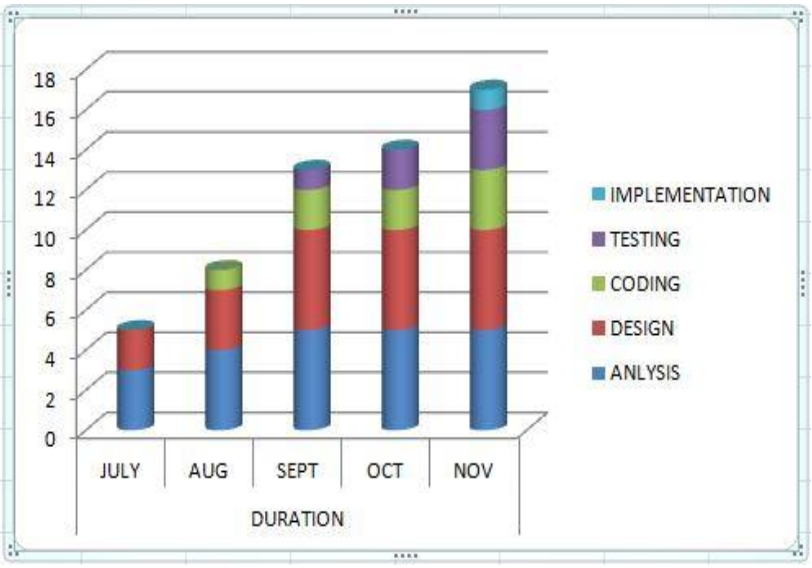


Fig. Feasibility Report

VI. CONCLUSION

In this work, we have a tendency to planned a construction of dynamic audit services for untrusted and outsourced storage. we have a tendency to conjointly planned associate degree economical methodology for Hash Message Authentication Code (HMAC) to reduce the computation prices of third party auditors and storage service suppliers. RSA formula accustomed encipher and rewrite the cloud knowledge .Our experiments showed that our answer features a little, constant quantity of overhead, that minimizes computation and communication prices. HMAC is employed as a result of it ensures the usage of hash functions with none modifications and these hash functions may be utilized in any code that's wide on the market. The HMAC provides the advantage of protective the initial performance of the hash operate while not subjecting it to any degradation. Cloud service suppliers to supply associate degree economical audit service to see the integrity and availableness of the keep knowledge. Future Work, so as to attain constant quantity of overhead, that minimizes computation and communication value, we have a tendency to extend the audit service potency by HMAC formula in dynamic audit services for outsourced storages in cloud. . Cloud service suppliers to supply associate degree economical audit service to see the integrity and availableness of the keep knowledge. The planned theme inherits the property of demonstrable knowledge possession (PDP). the final word goal of this audit infrastructure is to reinforce the believability of CSSs, however to not increase DO's burden. we have a tendency to analyze the planned theme, user access the cloud knowledge is versatile and licensed .

REFERENCES

[1] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song. Provable data possession at untrusted stores. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, pages 598–609, 2007.

[2] [6] Lu, Huang, Ting-tin Hu, and Hai-shan Chen. "Research on Hadoop Cloud Computing Model and its Applications.". Hangzhou, China: 2012, pp. 59 – 63, 21-24 Oct. 2012.

[3] Boneh and M. Franklin. Identity-based encryption from the weil pairing. In Advances in Cryptology (CRYPTO'01), volume 2139 of LNCS, pages 213–229, 2001.

[4] Y, Amanatullah, Ipung H.P., Juliandri A, and Lim C. "Toward cloud computing reference architecture: Cloud service management perspective.". Jakarta: 2013, pp. 1-4, 13-14 Jun. 2013.

[5] H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H. Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang. A study of user-friendly hash comparison schemes. In ACSAC, pages 105–114, 2009.

[6] Juels and B. S. K. Jr. Pors: proofs of retrievability for large files. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, pages 584–597, 2007.

[7] C.-P. Schnorr. Efficient signature generation by smart cards. J. Cryptology, 4(3):161–174, 1991.

[8] H. Shacham and B. Waters. Compact proofs of retrievability. In Advances in Cryptology – ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, pages 90–107, 2008.

[9] Wang, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for data storage security in cloud computing. In INFOCOM, 2010 Proceedings IEEE, pages 1 –9, 14-19 2010.

[10] M. Xie, H. Wang, J. Yin, and X. Meng. Integrity auditing of outsourced data. In C. Koch, J. Gehrke, M. N. Garofalakis, D. Srivastava, K. Aberer, A. Deshpande, D. Florescu, C. Y. Chan, V. Ganti, C.-C. Kanne, W. Klas, and E. J. Neuhold, editors, VLDB, pages 782–793. ACM, 2007.

[11] Boneh, X. Boyen, and H. Shacham. Short group signatures. In proceedings of CRYPTO'04, volume 3152 of LNCS, pages 41–55. Springer-Verlag, 2004.

[12] Yang, K., Jia, X.: Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web 15(4), 409–428 (2012)

