RESEARCH ARTICLE OPEN ACCESS

Publicly Verifiable Shared Dynamic Electronic Health Record Databases with Functional Commitment Supporting Privacy Preserving Integrity Auditing

Mr D Purushothaman MCA., M.E., [1], R.Hemasundar [2]

[1] Asst. Professor, Department of Computer Applications
[2] Student, Department of Computer Applications
[1], [2] Chadalawada Ramanamma Engineering College (Autonomous)

ABSTRACT

As information technology creates, distributed storage has been broadly acknowledged for keeping volumes of information. Far off information inspecting plan empowers cloud client to affirm the honesty of her reevaluated document by means of the evaluating against distributed storage, without downloading the record from cloud. Taking into account the critical computational expense brought about by the inspecting cycle, rethought reviewing model is proposed to cause client to reevaluate the substantial evaluating undertaking to third party auditor (TPA). Albeit the first rethought reviewing plan can secure against the pernicious TPA, this plan empowers TPA to have perused admittance directly over client's reevaluated information, which is a likely danger for client information protection. In this paper, we present the thought of User Focus for rethought inspecting, which underscores that allows client to overwhelm her own information. In view of User Focus, our proposed plot not exclusively can keep client's information from spilling to TPA without relying upon information encryption yet in addition can keep away from the utilization of extra free irregular source that is hard to meet by and by. We likewise depict how to make our plan support dynamic updates. As indicated by the security examination and trial assessments, our proposed plot is provably secure and fundamentally effective.

Keywords: - Information technology creates, distributed storage has been broadly acknowledged for keeping volumes of information.

I. INTRODUCTION

Lately, distributed computing has set off significant technology changes in the field of information industry, advancing the quick improvement of IoT (Internet of things) and large information that have acquired such a lot of consideration in our every day social and monetary exercises [1]. As one of the fundamental administrations of distributed computing, distributed storage offers numerous alluring benefits, including the area free assets, omnipresent organization access, and on-request extra room [2], persuading an ever increasing number of undertakings and people to re-appropriate their own information to cloud. Profiting with the huge information that is assembled into the cloud, a wide range of information driven strategies, for example, information mining [3, 4] and information signal preparing [5, 6], can be sent upon the distributed storage climate to assume their compelling parts for making more information abundance.

Regardless of that reality that numerous potential additions can be accomplished dependent on the distributed storage, there additionally exists new dangers according to the cloud client's perspective. After client transfers every last bit of her own information to cloud, quite possibly the most major problems for client is the way to confirm the uprightness of re-appropriated information put away at distant cloud side. Note that client loses the actual belonging over her information with regards to information rethinking, so it is obviously not doable to straightforwardly apply conventional nearby information confirmation methods that expect admittance to the whole information, since both client and cloud workers can't bear the cost of the weighty correspondence cost of as often as possible moving all the reevaluated information across an organization to play out the information respectability check. For this situation, an assortment of distant information examining plans [7–23] are planned, which can uphold the intermittent honesty confirmations upon rethought information and at the same time try not to move every one of these information for the base correspondence overhead. Also, as a significant component to additionally lessen the weight on the client, public reviewing is

first proposed by Ateniese et al. [7] and has been embraced broadly by the resulting further developed plans [13–22], which empowers a third party auditor (TPA) to review cloud workers in the interest of client for guaranteeing the rethought information respectability. Regardless, satisfaction won't come so without any problem. At the point when TPA is presented, the accompanying security hazard emerges. Malignant TPA. TPA is considered as a trusted (or semitrusted, i.e., legitimate yet inquisitive) element who can't abuse the evaluating conventions in existing public inspecting plans [13–22]. In any case, really TPA may be untrusted [23]. Clearly, if the flippant TPA is sluggish and sits idle, there is no distinction between entrusting a pernicious TPA and projecting endlessly all earlier open evaluating plans for client. To secure against the above malevolent TPA, Armknecht et al. [23] first introduced the reevaluated inspecting plan Fortress to accomplish this objective. In the mean time, Fortress can shield the legit TPA from a malignant client, which is likewise a potential security issue that has not been considered in existing public evaluating models. Be that as it may, during the information preprocessing step, Fortress empowers TPA to have perused admittance directly over the entire client's re-appropriated information in cloud, which is a critical constraint for useful applications. From one viewpoint, since Fortress uncovered all re-appropriated information to TPA, in Fortress the lone way for information security assurance against inquisitive TPA is to encode client's records prior to reevaluating. By the by, as displayed in [13, 14], in spite of the fact that information encryption alone is a way to deal with assuage the protection worry in distributed storage, encryption itself is frequently insufficient to keep client's information from spilling to TPA during the inspecting interaction. Then again, in the period of huge information, client's reevaluated information is one sort of center business resources of CSP [15], which implies the abundance and the future for CSP. Hence, CSP is self centered and has no motivators to uncover client's re-appropriated information to TPA regardless. In addition, client is likewise regularly hesitant to open her information to a third party [24]. For this situation, for the different online distributed storage applications (e.g., online recordings) where client can't encode her information before rethinking and just retreats to CSP to ensure against re-appropriated information spillage, it is obviously that the immediate augmentation of Fortress upon these online applications is illogical, since the plan of uncovering re-appropriated information to TPA is unavoidable in Fortress. Along these lines, it is vital for a re-appropriated examining plan to incorporate the security protecting instrument that is free of information encryption to shield against inquisitive TPA. Besides, Fortress contends that the difficulties for examining can't rely upon any of the elaborate three substances since they may be noxious. So Fortress requires the guide of extra autonomous irregular source to create the safe difficulties for securing against any noxious element. Notwithstanding, as displayed in [25], under the climate of distributed storage, the prerequisite of extra autonomous workers is as of now a solid presumption that is hard to meet in business settings, and subsequently the comparable supposition of requiring extra free arbitrary source in Fortress is a similar circumstance. To resolve the above issues, in this paper, we present for rethought evaluating model a novel thought User Focus, which stresses reestablishing client's information self-rule lost in distributed storage setting. As displayed in Sections 2.2 and 2.3, User Focus intends to allow client to control all difficulties all through the cycle of rethought inspecting, staying away from the restriction of presenting the extra bitcoin pseudo-irregular hotspot for creating difficulties as in existing Fortress conspire. Moreover, the client's self-governance empowered by User Focus is additionally reflected in that the information just should be preprocessed by client herself, staying away from the troublesome circumstance in Fortress that TPA should bring all client's information from cloud for introduction. With presenting User Focus, we propose an effective and secure rethought examining plan, which not exclusively can shield against any pernicious element yet in addition can shield client's re-appropriated information from inquisitive TPA without relying upon information encryption. When all is said in done, the commitments of this paper can be summed up as follows. By engaging client to assume the main part, we propose a proper User Focus rethought evaluating model alongside the security definitions, which don't rely upon any extra

pseudo-arbitrary source. Our model broadens the model of Fortress and considers the issue of safeguarding client's information protection while presenting TPA, which isn't shrouded in Fortress. In light of our proposed model, we plan a substantial User Focus re-appropriated inspecting plan, the security of which is broke down. Albeit the idea of User Focus engages client to create the difficulties, it doesn't imply that a noxious client can do anything she desires to do, since our plan can likewise safeguard against the vindictive client. Moreover, under the climate of rethought examining, our plan can empower client to predefine enough difficulties for trying not to keep client online constantly and furthermore support the unique information refreshes by depending on the MHT confirmed information structure. Our plan applies the RSA public key cryptography as opposed to the symmetric cryptography technology as used in Fortress and accordingly empowers TPA to finish his preliminary work for reviewing without expecting admittance to client's rethought information at cloud side, which tackles the huge presentation issue looked by Fortress. We assess the run season of our plan through substantial execution when contrasted with Fortress. The assessment results show that our answer is promising as indicated by the further developed presentation.

Problem Statement

In this segment, we present the thought of User Focus, which ought to be a significant necessity for user in the setting of storage re-appropriating. Then, at that point we propose a formal User Focus outsourced auditing model and the comparing security definitions.

Outsourced Auditing for Cloud Storage

Different far off information auditing plans [7–23] give a cloud user the capacity of affirming that her outsourced information is flawless at the cloud, with the benefit that it is no compelling reason to get the information from cloud. The private auditing plans [8, 12] just incorporate two substances: a user and CSP, where user needs to review CSP consistently without anyone else to learn that CSP holds the put away information constantly. Considering user's restricted assets and the costly calculation cost caused by the incessant reviews, the public auditing plans are proposed [13–22], which acquaint a confided in TPA with perform the above auditing task. By utilizing TPA, user is lightened from the auditing trouble. Nonetheless, believed TPA is only an optimal speculation in genuine world.

In view of the earlier auditing arrangements, the first outsourced auditing plan [23] is proposed to safeguard against the malignant TPA. Contrasted and the public auditing model, despite the fact that there are likewise three elements remembered for outsourced auditing setting, the significant distinction is that anybody of the three elements may be untrustworthy, as depicted as follows:

(i) User may be an exploitative substance, who transfers her information to the cloud workers. User needs to distantly refresh outsourced information as essential. And user may malignantly deny the way that the auditing work performed by TPA against CSP is right for guaranteeing pay from TPA.

(ii) CSP may be an unscrupulous substance, who is the proprietor of cloud workers (so CSP and the cloud workers are not recognized in our paper), holding a lot of assets to store and keep up with outsourced information. CSP may attempt to undermine reviewer when information misfortune or information defilement happens in cloud.

(iii) TPA may be a deceptive substance, who has capacities and ability, for the benefit of user, to routinely review CSP for affirming the flawlessness of user's information in cloud. Yet, TPA may be sluggish and neglect to perform the auditing task needed by user. Moreover, TPA may be interested and attempt to derive user's outsourced information during performing his auditing task against CSP.

User Focus

"Client Focus" is a promoting term that implies remembering client and bringing client the great experience of administrations. Plainly, "The client is a God" isn't just reality in business, yet in addition a comparable circumstance in our cloud storage climate, where the user is the designated client of

CSP and a wide range of auditing arrangements. User experience is a deciding component connoting if an auditing plan is acknowledged by and by. In the event that user experience of a plan is poor, regardless of whatever refined innovation is embraced, it is outlandish for this plan to get a viable application broadly.

Notwithstanding different auditing plans that are proposed to cover numerous basic issues, however user experience is disregarded. From one perspective, whichever of the private auditing plans depends on the plan that the auditing convention should be much of the time executed by user, bringing about the nonnegligible calculation overhead at user side. Clearly, this is a horrendous encounter for user who simply holds restricted assets, for example, cell phone. Then again, inside open auditing plans, the presumption of a "believed" TPA is likewise an awful encounter for user, since it is unfeasible for each common user to track down a hopeful "trusted" TPA.

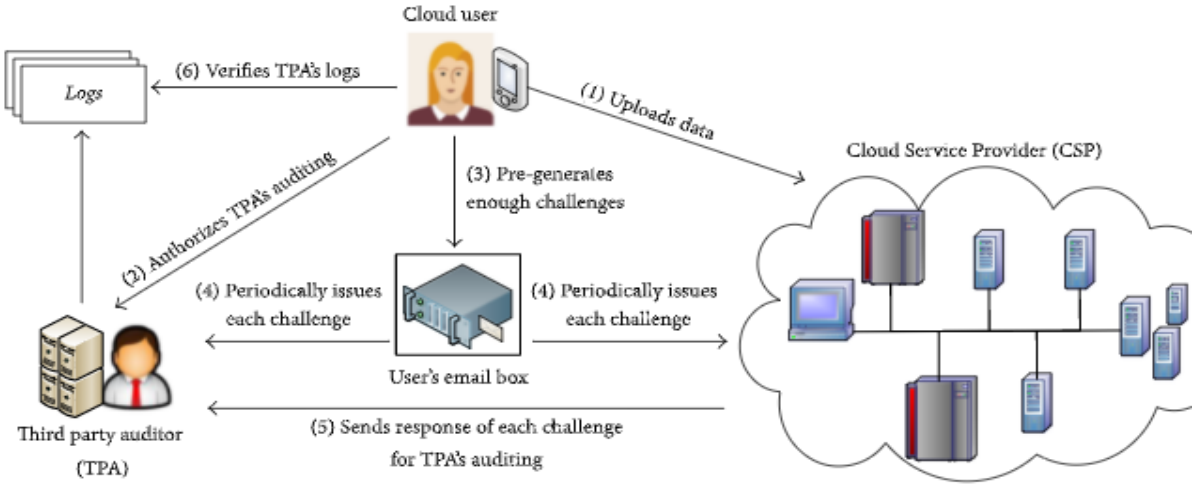
Note that the motivation behind distant information auditing is to give user a system for affirming the security of her outsourced information. Here, user is viewed as the demander. Therefore, user should be put at the middle when planning the auditing plan, and her experience ought not be disregarded. For this explanation, we present the idea of User Focus, which is characterized as follows:

User is the initiator of the auditing protocols and controls every one of the difficulties, who can opportune get the special case message of her outsourced information without regularly working, since both CSP and TPA need to oftentimes give all evidences around user's requirements.

In reality, the fundamental idea of cloud administrations is the incorporated administration of user's information in cloud, which projects a mental shadow on user. To save the storage space or accessibly access information without limitation of time and area, user is needed to re-appropriate her information to cloud, which implies that user is not, at this point ready to truly have all her information. As such, information rethinking causes user to lose the actual possession and self-governance of her information, which is one of the primary deterrents for the application and advancement of cloud storage.

While re-appropriating information to cloud is unavoidable, the thought of User Focus can make user get out of the mental shadow brought by cloud storage, empowering user to appreciate cloud benefits all the more unhesitatingly. User Focus communicates the possibility that let user rule her own information, which is acknowledged in our model by the manner that "the increase counterbalances the misfortune." By enabling user to acquire the control right of difficulties, user gets back the self-sufficiency that is lost after information rethinking and can proactively check the flawlessness of the particular information just by changing difficulties, which can bring user the inclination that there is actually no distinction for soundness affirmation between her information put away in nearby circles and outsourced in cloud, since everything is leveled out according to the user's point of view. Obviously, User Focus will be an alluring property for user. Particularly when our proposed conspire is executed as a cloud administration and CSP trusts that this help can be comprehensively acknowledged by expected clients, User Focus will be an entrancing component to convince each client to attempt this cloud administration.

User Focus Outsourced Auditing Model



Presently, we start with the portrayal of User Focus outsourced auditing model, as displayed in Figure 1. To keep away from the impressive user online direct communications during the successive TPA's auditing against CSP, user will pregenerate enough difficulties which can uphold running the auditing convention for a very long time. Since the size of a test can be little (e.g., just 88 bytes for a test as displayed in Section 5), every one of these pregenerated difficulties can be put away in user's email box (e.g., just 8.5 MB email box memory is needed for putting away 100,000 pregenerated challenges). For this situation, after user transfers her information to cloud and delegates the auditing work to TPA, in view of the underlying clock of email box, each challenge will be occasionally given from user's email box to consequently trigger TPA's auditing against CSP without including user herself. Besides, TPA should deliver the comparing log when he completes each auditing against CSP. In light of the agreement set up by three substances, TPA needs to quickly inform user (e.g., gives user a call) when any remarkable circumstance about user's outsourced information is identified. In the event that TPA is lethargic and consequently doesn't discover the information debasement chancing upon the tested information blocks, when user dispatches her auditing to TPA by checking TPA's logs, the languid TPA will be related to deterministic proof. At long last, when all the pregenerated challenges are depleted, user will add the new difficulties to her email box. Nonetheless, note that such activity for adding difficulties and the auditing against TPA's logs are just once in a while executed by user, so user can go disconnected more often than not all through our model.

Rather than existing outsourced auditing model of [23], one significant distinction in our model is that the thought of User Focus is presented, empowering user to assume the main part on her outsourced information with negligible effort. So user is the one in particular who can have the extra mystery key, other than a marking key pair, to preprocess the information. In view of the advanced lawful society with the soul of agreement, our model can accomplish that no legit element will be violated and that any pernicious substance can be caught. All the more explicitly, User Focus outsourced auditing model comprises of five protocols Setup, Preproccess, AuditCSP, AuditTPA, and IdentifyMalice

II. RELATED WORK

With the advocacy of capacity rethinking, the issue of far off information honesty evaluating has drawn in expanding considerations. A wide range of provable information ownership (PDP) and confirmation of retrievability (POR) plans [7–23] are proposed to safeguard against the untrusted far off worker.

Ateniese et al. given a progression of PDP plans for the capacity security of rethought information. In [7], they initially depicted the formalized meaning of PDP and proposed the first PDP plots by using the homomorphic unquestionable labels that are built dependent on the public key cryptological strategy. All the while, to permit anybody, not simply the information proprietor, to review the untrusted worker for information ownership, the idea of public examining is first presented in [7]. Whereafter, as far as the symmetric key cryptological procedure, Ateniese et al. [10] proposed another provably secure PDP plot for considering the issues of versatility and information elements that are not canvassed in the first PDP technique. Moreover, in [11], they additionally introduced two more effective PDP plans that go above and beyond than the first plans of [7]. To help the completely unique tasks with regards to far off reviewing, Erway et al. [12] broadened the PDP model of [7] and introduced the main powerful PDP plot by utilizing the position based confirmed skip list. Also, Wang et al. [16] and Zhu et al. [19] likewise proposed other productive powerful plans for public examining, which depend on the information designs of Merkle Hash Tree (MHT) and Index-Hash Table (IHT), separately.

Juels and Kaliski Jr. [8] first proposed a formal POR model alongside the relating security definitions. As indicated by the model of [8], Shacham and Waters [9] developed two POR plans upon the static information stockpiling yet supporting the limitless number of difficulties. The primary plan is worked from the pseudorandom capacities to empower private inspecting, and the second plan with public evaluating is worked from the BLS signature [33]. Given that TPA may be interested during the cycle of public reviewing, Wang et al. [13] coordinated the irregular cover procedure with the BLS-based public reviewing plan to keep client's reevaluated information from spilling to TPA, and the plan of [13] has been additionally improved to help information elements in [15]. Additionally, under the climate of public reviewing, numerous different plans are likewise intended to fulfill the needs of various situations, for example, quick information mistake confinement [17], the examining against shared information [18], cluster evaluating for various mists [20], fine-grained information refreshes [21], and the lightweight calculations for low execution end gadgets [22].

As of late an assortment of distributed storage application plans have been proposed, for example, watchword based information recovery and picture duplicate identification at cloud side. Xia et al. [34] developed a unique tree-based record structure and proposed a protected multikeyword positioned search conspire empowering dynamic updates upon reevaluated encoded information. Fu et al. [35] planned the equal pursuit calculation and proposed another adaptable accessible encryption conspire supporting both multikeyword positioned search and equal hunt. In the setting of multikeyword fluffy hunt, to take care of the faulty issues during the positioning cycle, Fu et al. [16] additionally fostered another catchphrase change technique and introduced the relating productive inquiry plot. Taking into account that conventional catchphrase based hunt conspires that can't totally coordinate with clients' inquiry aim, the imaginative semantic pursuit plot dependent on the idea pecking order is proposed in [27], making the customized search more viable and setting mindful. Also, the substance based inquiry plan of [18] has additionally tackled the issues of semantic hunt by using the applied charts and the productive proportion of "sentence scoring." On the other hand, to secure the pictures put away in cloud, Xia et al. [29] proposed a security protecting and duplicate discouragement CBIR conspire utilizing encryption and watermarking methods, which can keep the picture client from unlawfully appropriating the recovered pictures. Li et al. [4] introduced an answer for identify the duplicate move fraud in a picture, by first portioning the designated picture into semantically autonomous patches preceding keypoint extraction and examination. For identifying the picture duplicates of a given unique picture produced by subjective turn, Zhou et al. [15] proposed a novel duplicate identification strategy dependent on two worldwide highlights removed from revolution invariant allotments. Also, Zhou et al. [12] planned a worldwide setting check plan to channel bogus counterparts for duplicate discovery, which further resolves the issues of restricted discriminability and quantization blunders that exist clinched of-visual-

words (BOW) model received by past identification techniques. In any case, since all application plans referenced above are planned upon the reevaluated information of distributed storage, so we must initially zero in on the most proficient method to review and affirm the uprightness of far off rethought information. Be that as it may, the current public examining plans can't secure against the malignant TPA. As displayed in [23], pernicious TPA is a potential security hazard for re-appropriated information honesty and hence ought not be disregarded, which is the inspiration of this paper.

III. IMPLEMENTATION

- Thirdparty Auditor

  In this module, the wearable device Collect Patient data and Upload to Cloud like pid,pname,paddress,pcno,pemail,ppulse,pecg,pSymptoms,brwose and attach about symptoms with Digital sign,addpimage(Encrypt all parametes except pname) and View all patient collecte data in enc format with digital sign.

- Cloud Server
  The Cloud server manages which is to provide data storage service for the wearable devices and also View all patients and authorize and View all doctors and authorize ,Vliew all patient Cloud data with enc format ,View Patient data access request and authorize ,View all Cloud Intruders details and View patient details recovered details ,View No.Of same symptoms in Chart(Symptom name vs No. Of Patients),ViewNo.Of Patients refered same doctor in Chart(Doctor name vsNo.Of Patients).
- Patient
  In this module, the patient Register and Login, View profile ,Request Data Access permission from cloud and view Response, Access Your data and select doctor from combo box and send to corresponding doctor and View doctor response with Medical prescription, Verify your data and recover and View and delete your details.
- Doctor
  The doctor is the one who will perform the following operations such as Register and Login,View Profile, View patient details and give solution like Medicine details,Medical prescription details View all patient Medical prescription Details.

IV. EXPERIMENTAL EVALUATION

In this segment, we reproduce the calculations of our proposed User Focus conspire and the Fortress plan of [23] on the Inspur NF5270M4 workers with Intel Xeon CPU E5-2620 at 2.10 GHz, 16 GB RAM, and 7200 RPM 1 TB Serial ATA drive with a 32 MB support. Our trials are carried out by utilizing python language, and every one of the cryptographic capacities are gotten from the python cryptography tool compartment [30]. We utilize SHA1 to deliver the 160 piece hash esteem, and the size of RSA module is 1024 bit for security. Concerning the Fortress conspire, we likewise use the apparatuses of bitcoin block voyager [31] to get to bitcoin asset for getting the arbitrary difficulties, and we commonly set the area size to be 1 KB (e.g., each 64 KB document block comprises of 64 areas in Fortress).

Note that the regular square size for distributed storage is 64 KB–256 KB, as displayed in [32]. Since re-appropriated inspecting plan runs over the distributed storage, the sensible lower cutoff of square size ought to be no under 64 KB. In our evaluation, client's re-appropriated record is picked to 1 GB. We don't gauge the hour of transferring the re-appropriated document from client to CSP, since this overhead is normal to the two explored plans. Our measurable outcomes are a normal of 20 rounds.

First and foremost, client's record should be preprocessed prior to re-appropriating. Figure 3 shows the necessary all out an ideal opportunity for the comparing preprocessing periods of the two plans. Besides, we likewise assess the registering time devoured by client for our plan and Fortress, individually. It worked out that for the two plans the

computational overhead caused at client side records for the majority of thetotal time while preprocessing the reevaluated information, and the preprocessing execution of our plan is significant degrees quicker than of Fortress. As displayed in [23], TPA needs to download the entire client's record from cloud and persuade the client that he accurately preprocessed . For this situation Fortress expects client to complete a tedious zero-information confirmation (ZKP) with TPA, bringing about the weighty computational overhead for client. Contrasted with Fortress, our User Focus plan can successfully stay away from such ZKP activity since TPA isn't engaged with preprocessing and consequently acquire the presentation improvement.

CONCLUSION

Any open examining/confirmation plan can be changed into a private plan, just by causing client to play out the reviewing work that ought to be appointed to TPA. Obviously, public evaluating plans may be all the more effectively enormous scope received by cloud clients by and by, since client's significant weight caused by as often as possible reviewing can be moved to TPA. By and by, how to shield client from a vindictive TPA is a key issue that is never considered by different existing public reviewing plans. The originally rethought inspecting plan Fortress is proposed to safeguard against the pernicious TPA, yet Fortress empowers TPA to download all reevaluated information and along these lines just depends on information encryption to secure client's information protection. A protected rethought evaluating plan against malignant TPA ought to be intended to deny TPA of the entrance rights over client's reevaluated information in cloud, which is accomplished in this paper. Despite the fact that our proposed conspire is planned without depending on extra autonomous irregular source, it likewise accomplishes the security of ensuring against any malevolent element. Likewise, in view of the MHT information structure, we stretch out the reevaluated reviewing plan to help dynamic updates. With the investigation and evaluations, our plan is provably secure and essentially productive.

REFERENCES

1. J. Xiao, X. Li, S. Chen, X. Zhao, and M. Xu, “An inside look into the complexity of box-office revenue prediction in China,” *International Journal of Distributed Sensor Networks*, vol. 13, no. 1, 2017.View at: Publisher Site | Google Scholar

2. M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, “A review on remote data auditing in single cloud server: taxonomy and open issues,” *Journal of Network and Computer Applications*, vol. 43, pp. 121–141, 2014.View at: Publisher Site | Google Scholar

3. S. Fong, R. Wong, and A. Vasilakos, “Accelerated pso swarm search feature selection for data stream mining big data,” *IEEE Transactions on Services Computing*, 2015.View at: Publisher Site | Google Scholar

4. F. Tian, T. Lan, K.-M. Chao et al., “Mining suspicious tax evasion groups in big data,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 10, pp. 2651–2664, 2016.View at: Publisher Site | Google Scholar

5. X. Hu, S. Peng, and W.-L. Hwang, “EMD revisited: a new understanding of the envelope and resolving the mode-mixing problem in AM-FM signals,” *IEEE Transactions on Signal Processing*, vol. 60, no. 3, pp. 1075–1086, 2012.View at: Publisher Site | Google Scholar | MathSciNet

6. X. Hu, S. Peng, and W.-L. Hwang, “Adaptive integral operators for signal separation,” *IEEE Signal Processing Letters*, vol. 22, no. 9, pp. 1383–1387, 2015.View at: Publisher Site | Google Scholar

7. G. Ateniese, R. Burns, R. Curtmola et al., “Provable data possession at untrusted stores,” in *Proceedings of the 14th ACM Conference on Computer and*

Communications Security (CCS '07), pp. 598–609, Virginia, Va, USA, November 2007.View at: Publisher Site | Google Scholar

8. A. Juels and B. S. Kaliski Jr., "Pors: proofs of retrievability for large files," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 584–597, ACM, Alexandria, VA, USA, November 2007.View at: Publisher Site | Google Scholar

9. H. Shacham and B. Waters, "Compact proofs of retrievability," in *Advances in Cryptology—ASIACRYPT 2008: Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 2008*, vol. 5350 of *Lecture Notes in Computer Science*, pp. 90–107, Springer, Berlin, Germany, 2008.View at: Publisher Site | Google Scholar | MathSciNet

10. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (SecureComm'08)*, pp. 1–10, ACM, Istanbul, Turkey, September 2008.View at: Publisher Site | Google Scholar

11. G. Ateniese, R. Burns, R. Curtmola et al., "Remote data checking using provable data possession," *ACM Transactions on Information and System Security*, vol. 14, no. 1, article 12, 2011.View at: Publisher Site | Google Scholar

12. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proceedings of the Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, pp. 213–222, ACM, Chicago, Ill, USA, November 2009.View at: Publisher Site | Google Scholar

13. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proceedings of the IEEE INFOCOM 2010*, usa, March 2010.View at: Publisher Site | Google Scholar

14. H. Tian, Y. Chen, C.-C. Chang et al., "Dynamic-hash-table based public auditing for secure cloud storage," *IEEE Transactions on Services Computing*, vol. PP, no. 99, 2015.View at: Publisher Site | Google Scholar

15. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.View at: Publisher Site | Google Scholar | MathSciNet

16. 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*, vol. 22, no. 5, pp. 847–859, 2011.View at: Publisher Site | Google Scholar

17. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.View at: Publisher Site | Google Scholar

18. 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.View at: Publisher Site | Google Scholar

19. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," *IEEE Transactions on Services Computing*, vol. 6, no. 2, pp. 227–238, 2013.View at: Publisher Site | Google Scholar

20. 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*, vol. 24, no. 9, pp. 1717–1726, 2012.View at: Publisher Site | Google Scholar

21. C. Liu, J. Chen, L. T. 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*, vol. 25, no. 9, pp. 2234–2244, 2014.View at: Publisher Site | Google Scholar

22. J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong, "Privacy-Preserving Public Auditing Protocol for Low-Performance End Devices in Cloud," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2572–2583, 2016.View at: Publisher Site | Google Scholar

23. F. Armknecht, J.-M. Bohli, G. O. Karame, Z. Liu, and C. A. Reuter, "Outsourced proofs of retrievability," in *Proceedings of the 21st ACM Conference on Computer and Communications Security, CCS 2014*, pp. 831–843, usa, November 2014.View at: Publisher Site | Google Scholar

24. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in *Proceedings of the 11th USENIX workshop on Hot topics in operating systems*, vol. 7, 2007.View at: Google Scholar

25. J. Liu, N. Asokan, and B. Pinkas, "Secure deduplication of encrypted data without additional independent servers," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS 2015*, pp. 874–885, usa, October 2015.View at: Publisher Site | Google Scholar

26. R. C. Merkle, "A Certified Digital Signature," in *Proceedings of the Theory and Application of Cryptology, Lecture Notes in Computer Science*, vol. 435, pp. 218–238, 1989.View at: Google Scholar

27. I. Damgård, "Towards practical public key systems secure against chosen ciphertext attacks," in *Proceedings of the Annual International Cryptology Conference*, pp. 445–456, 1992.View at: Google Scholar

28. M. Bellare and A. Palacio, "The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols," in *Advances in Cryptology*, vol. 3152 of *Lecture Notes in Comput. Sci.*, pp. 273–289, Springer, Berlin, 2004.View at: Publisher Site | Google Scholar | MathSciNet

29. M. Abe and S. Fehr, "Perfect NIZK with adaptive soundness," in *Theory of cryptography*, pp. 118–136, 2007.View at: Google Scholar | MathSciNet

30. D. C. Litzenberger, "Python Cryptography Toolkit," https://pypi.python.org/pypi/pycrypto, 2017.

31. Bitcoin real-time status and tools, https://block-explorer.com/api-ref, 2017.

32. E. Stefanov, M. V. Dijk, E. Shi et al., "Path ORAM: an extremely simple oblivious RAM protocol," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 299–310, 2013.View at: Google Scholar

33. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *International Conference on the Theory and Application of Cryptology and Information Security, Advances Cryptology*, vol. 2248, pp. 514–532, 2001.View at: Google Scholar

34. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp.

340–352, 2016.View at: Publisher Site | Google Scholar

35. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, vol. E98B, no. 1, pp. 190–200, 2015.View at: Publisher Site | Google Scholar

36. Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2706–2716, 2016.View at: Publisher Site | Google Scholar