Publicly Verifiable Vibrant Digital Medical Information Systems

Shaik Sumi Anju¹, Mrs. BSN Sravani², Srinivasa Rao Madala³

¹ M.Tech., Scholar, Department of Computer Science and Engineering.
² Asst. Professor, Department of Computer Science and Engineering.
³ Professor & HOD, Department of Computer Science and Engineering
PACE Institute of Technology and Sciences

Abstract- As data processing advances, decentralized media has been widely recognized for its ability to store large amounts of data. By comparing a revisited content to a dispersed repository, a cloud provider may verify the document's integrity without having to retrieve it. A reconsidered examining strategy is offered to lead the customer to reconsider the significant assessing task to third sector inspector, taking into consideration the important computing cost brought up by the checking process (TPA). TPA may be deterred by the primary revisited evaluating strategy, but the second plan gives the harmful organization the right of inspection over the readaddressed data of users, which poses a significant risk to patient privacy. Human Emphasis for reconsidered inspection is presented in this work, which emphasizes that the service user can be overwhelmed by her own data. Based on user-centered design, our suggested methodology not only prevents patient's data from leaking to TPA without depending on cryptographic algorithms, but can also avoid the use of additional free unpredictable supply that is impossible to fulfill on a daily basis. Also, we start to make our approach work with continuous changes. Our recommended scheme is both verifiably safe and essentially productive, as shown by the privacy analysis and test evaluations.

1. Introduction
The rapid development of IoT (Internet of things) and big data that have gained so much attention in our daily societal and financial activities has been accelerated by decentralized computation in recent years. Decentralized warehousing, as one of the basic comptroller of dispersed cryptography, offers innumerable enticing advantages, such as the location vector graphics, omnipotent organization availability, and on-request additional space [2], persuading an ever growing amount of commitments and individuals to re-probably their own data to fog. [3]. Many data methods, such as data extraction and signal processing [3, 4], may be applied to the cloud's dispersed data center to maximize data richness.

Despite the fact that data computing allows for a wide range of prospective enhancements, there are also new risks from the clouds customer's standpoint. Just after customer has transferred each and every piece of her own data to the internet, one of the biggest difficulties for the customer is how to verify the accuracy of the re-usually data stored on the cloud's other side. When it comes to data reconsidering,
the customer ends up losing ownership of her data. Therefore, it isn't suitable to implement standard nearby data verification programs that involve access to the entire data, since both the customer and fog employees can't afford to pay the high communications costs of as frequently as probable trying to move all of the stored data. As a result of this, a variety of remote data scrutinizing strategies [7–23] have been devised, which may maintain the periodic truthfulness affirmations on reconsidered data while at the similar moment attempting not to transfer all of these data for foundation communication cost. Ateniese et al. [7] initially offered open evaluating, which has been widely adopted by subsequent designs [13–22], which allows a foreign government inspector (TPA) to evaluate internet employees in the benefit of the customer for ensuring the reconsidered data legitimacy. Nevertheless, contentment will not arrive easily. When TPA is provided, the security danger that comes with it is revealed. TPA has aggressive characteristics. When it comes to open inspection schemes, TPA is regarded a trustworthy (or semi-trusted) component that can't misuse the evaluation norms [13–22]. In any event, it's possible that TPA isn't reliable [23]. A cavalier TPA is obviously inefficient if it sits about doing nothing. There is no difference among committing an unreliable TPA and extending indefinitely all previous public assessing intentions for customer. Armknecht et al. [23] originally developed the readdressed schedule stronghold to attain this aim in order to protect against the aforementioned malicious TPA. It is possible to protect a legitimate TPA from a malicious customer using Castle, whatever the case may be, throughout the data preparation phase. Using Castle, TPA may have per used access on any re-appropriated data in the internet, which is important for usable solutions. In light of the fact that Castle revealed all re-probably data to TPA, the only method to ensure data privacy toward an investigative TPA is to encrypt customer accounts ahead to re-concerned in Castle.

Even while data decryption simply is a means to cope with dispersed storage's security concerns [13, 14], cryptography is often inadequate to avoid customer's data from leaking to TPA throughout the inspection transaction, as demonstrated in [13, 14]. Then in the age of big data, readdressed customer data is some of CSP's most important commercial assets [15], implying that CSP has a bright potential. Because of this, CSP is personality and has no motivation to expose customer misappropriated data to TPA irrespective of whether it is true or not. The customer is apprehensive to divulge her personal data to an unauthorized entity [24]. There's no rational reason to add Castle to cloud processing implementations (e.g., digital tracks) in this scenario, because the customer can't encrypt her data prior to actually reconsidering and resorts to CSP to prevent re data leakage, so it's completely irrational to add Castle immediately to these web apps, because the strategy of discovering re-probably data leakage is completely irrational. The privacy preserving equipment must be devoid of data cryptography in order to guard against intrusive TPA.

Apart from that, Castle says the challenges for testing can't be based on any of the complicated four chemicals because they could be toxic. Therefore a guidance from an additional unpredictable resource is required in order to produce the secure challenges with guarding against any harmful component. To be sure, as shown in [25], in a world where there is dispersed storage, the requirement for more independent employees is already a valid presupposition that is difficult to satisfy in commercial environments. As a solution to the foregoing problems, we offer in this work a unique user-centric evaluation approach that provides the restoration of the customer's data self-rule destroyed in a data deduplication scenario. Clients will be able to manipulate all challenges throughout the reconsidered inspection cycle, as opposed to being restricted to the additional cryptocurrency completely non location for producing problems as in current Castle systems. Customer identity, enabled by Customer Awareness, also manifests in the fact that data just has to be planned carefully by the consumer, as opposed to Fortress's need that TPA provide all customers' data from the internet for presentation. We provide a revamped review strategy that can both protect against dangerous elements and safeguard customer data without having to depend on data protection. By getting clients to take charge, we're able to redefine the customer emphasis and rethink the models, which don't depend on any additional quasi intellectual sources. Our framework enlarges the Castle paradigm and addresses the issues of user online privacy and TPA display, which aren't found in Castle. After considering our recommendations, we intend to pursue a significant user-centered re-definitely inspection process that is explained in more detail.
The concept of Consumer Attention will also cause problems for the customer, but this does not mean that a malicious customer may do whatever she pleases, because our strategy can also defend from vengeful clients. Our strategy will also enable clients to anticipate potential issues by creating a personalized MHT architecture. This will also help clients get data updates more quickly, and it will be based on the MHT verified data framework. While Fortress's TPA could only continue the background research he started after gaining access to a client's internal data, our approach enables TPA to complete his background research without the need for customer reevaluated data at the cloud level, which would've helped Frontier. Compared to Castle, we measure the success of our strategy via significant action. Our response is apparently favorable, given that our exposition has been much improved.

2. Problem Statement
For the purpose of re-appropriation, repository users must concentrate on the needs of others. We next recommend the following for your consideration: an offsite Customer Experience assessment and an assessment comparison of safety standards.

2.1 Auditing for Cloud Storage through third-party services
The fog consumer has the ability to verify that her exported details are correct in the clouds and to realize that she does not need to get the data from the internet because it is already available. There are two products included in the secret inspection arrangement [8, 12]: the client and the CSP, where the user must scrutinize the CSP without anybody knowing that the CSP retains put away data all the time. Open accounting schemes, which enlist the trust of a TPA to do the tasks of the above accounting, are suggested due to the lack of available resources and the high cost of recalculation induced by the constant inspections. Consumer benefits from an inspection, because TPA reduces the amount of work required. However, TPA was just a realistic possibility in the real world. Given the former procedures for external monitoring, the initial delegated inspection [23] is recommended to prevent the spread of a harmful TPA. While open inspection systems do indeed have three components: external, external+ internal, and internal, the difference between them is that one or more of the components may be unreliable.

The primary issue is that the User is a material who may be predatory, allowing data to be sent to the internet employees. It is critical for the user to do an outsourcing document update over a remote network. Additionally, the client may maliciously discredit the method that TPA audits CSP to ensure proper payment to TPA. Second, since CSP is the owner of virtualized personnel (and as such, CSP and cloudy personnel are not treated in our article), it stores and maintains a lot of assets for data outsourcing. CSP may try to retaliate against a reviewer if a data disaster or data violation occurs in the web. Additionally, TPA may be a deceitful entity that has the capacity and competence to examine CSP for the patient's advantage to regularly verify the accuracy of customer computing assets. On the other hand, TPA may not execute the accounting job demanded by the client. Furthermore, TPA may try to utilise their audit results to learn what users have contracted to CSP.

2.2 Client Attention
"Customer Attention" is a promotional phrase meaning that we provide customers with a wonderful encounter by recognizing them and assisting them. There are two situations where this applies in the data retention space: the customer is both the subscriber of the cloud service provider and the subject of many monitoring procedures. The customer satisfaction is a vital factor that will influence whether or not an evaluation process is agreed upon. Even if the strategy employs sophisticated invention, it is illogical for it to get widespread adoption if the customer satisfaction is bad.

Despite various inspection proposals to address a variety of fundamental problems, customer satisfaction is neglected. When seen from one viewpoint, regardless of the confidential monitoring plan, the usage of the accounting standard by a user is standard and introduces additional user-side computational burden. It's obvious that this will be a very bad situation for someone who only possesses limited resources, like a mobile phone. Because a result, within public inspection designs, assuming a "certified" TPA is equally difficult for the consumer, as the average consumer would be unable to identify
a potentially "reputable" TPA. It's important to remember that the primary goal of doing a remote data assessment is to provide a user with a tool to ensure that her exported data is secure. The customer is considered the superior here. This means that in order to design the inspection properly, customers should be seen as the intermediate ground, and their previous learning should not be overlooked. To explain the concept of Customer Attention, we offer the following attributes:

The customer is the one who initiates the monitoring procedures and manages all the problems; therefore, the client has the ability to frequently get unique situation data about exported data, because both the CSP and TPA frequently have to provide all evidence related to the user's needs. The concept of internet management is to create a virtual counterpart of a person, thereby controlling all their data. For the sake of archival capacity or the ease of accessing data regardless of place or location, users need to repurpose their data to internet, which means that they are not yet ready to keep their data entirely under their control. That said, data virtualization is detrimental to user control of their data and therefore a major obstacle to the growth of cloud services. The need of re-appropriating content to the web is inescapable, but an emphasis on the customer may make online archiving seem less burdensome, allowing the user to enjoy the advantages of internet archiving all the more wholeheartedly. In our approach, we have considered the potential that users may take control of their own data, which is what Customer Attention talks about by noting that "the rise compensates the tragedy." Person's capacity to check the validity of the data is improved by allowing her to obtain the right to regulate the difficulty level of an item. This return of self-sufficiency from the cloud makes it possible for the subscriber to confidently verify for flaws without feeling that there is a significant difference between data held locally and that in the web, since the two are made equal by the subscribers perspective. Customer Attention is clearly an attractive feature for the user. By working with a public administering and CSPs that have full confidence in our proposal, Customer Attention will be a compelling piece to encourage every customer to participate in this public administering. At this time, we will begin with a description of the Customer Centric contracted monitoring architecture, which can be seen in Figure 1. To avoid the tempting internet personal contact that will take place as part of consecutive TPA audits against the CSP, the customer may create sufficient obstacles to last through the investigation. Because each of these futuristic dystopian problems only requires a little of the person's email program (such as just 8.5 Megabytes of emailing container capacity for storing 1 million futuristic dystopian tasks), they may be kept and used again and again.

![Fig. 1. Portrayal of Customer Attention](image)
Since the message container's time display shows the ongoing time of the exchange, TPA will receive each customer query, through the inbox, in turn provoking TPA's audited versus the CSP, without customer involvement. In addition, TPA must provide the comparison log after the inspection with CSP is completed. TPA is bound under the terms of the two elements' arrangement to notify the customer (for example, by calling the customer) when significant facts regarding the person's leased data are discovered. In the case that TPA is too sluggish to find the data devaluation when reviewing the evaluated systematic approach, the indolent TPA will be linked to undeniable evidence when the customer does TPA's inspection by looking at TPA's records. Finally, after all the simulation problems are over, the user adds additional problems to his email box. Nevertheless, customers are able to check this kind of work out just on occasion, thus it may happen that customers may be removed at any time throughout our system. In our approach, instead of the current external accounting paradigm (which is described in [23]), one major variation is that the concept of Customer Attention is included, allowing users to take on the primary role in their exported data with little effort. In example, the user may have a supplementary cypher secret, apart from a key pair, to process information in advance. Now that we have a country with a sense of unity, our system can succeed in not violating any of the legitimate things and stopping any dangerous elements. Customer Mainly focuses offshore monitoring paradigm, which is made up of five procedures: Configuration, Preprocess, Inspect CSP, Inspect TPA, and Detect risk, is all the more clearly defined.

3. Related Work

The problem of distant data integrity assessment has attracted a wider discussion with the backing of capability reassessment. A broad array of strategies for the proven possession of data (PDP) and verification of revocation (POR) [7–23] are recommended to protect from the remote operator that cannot be recognized. Ateniese et al. provided a series of PDP strategies for cybersecurity capability development. The technical definition of PDP was originally defined by [7] and the earliest PDP graphs were created using elliptic curve definite labeling based off of the cryptographic algorithms approach. The concept of open examination, in which everyone may see the contents of a job, originally appears in [7]. The subsequent PDP design, presented by Ateniese et al. [10], considered the problems of adaptability and data components not addressed in the original PDP method. And furthermore, in [11], they presented two new PDP designs that are more successful than the initial PDP designs of [7]. Erway et al. [12] extended the PDP paradigm of [7] to assist tackle complicated remote evaluating problems, using the leadership role skipping listing [7] to strengthen the PDP graphic. Wang et al. [16] and Zhu et al. [19] have suggested further strong examination systems that use Cryptographic Graph (MHT) and Indicator Tree (IHT) data layouts, respectively.

Juels and Kaliski Jr. [8] originally suggested a formalized POR framework, which incorporates the descriptions of related safety concepts. The concept of [8] shows that Shacham and Waters [9] created two POR strategies based on the dynamic data hoarding, allowing for several problems to be addressed. The two-step approach utilises permutation generators to enable personal inspection and uses the BLS official signing to conduct public evaluation [33]. Wang et al. [13] enhanced their strategy for data items in [15] by coordinating the BLS-based open evaluating strategy with the inconsistent coverage process. The strategy helps to prevent the spillage of customer data to TPA throughout the open evaluating process. Furthermore, in the environment of community critique, a wide range of strategies have correspondingly been proposed to satisfy the requirements of diverse scenarios, such as error correction in a hurry [17], evaluation of sharable data [18], pattern computation for various foggs [20], ultra-light recharges of details [21], and low-performance device estimations [22].

A variety of applications, including keyword-based data restoration and image duplication detection, have been suggested for the cloud recently. Xia et al. [34] presented a novel tree-based document architecture and a dynamic, two-keyword method to enable updated data after reevaluation of
ciphertext. Fu et al. [35] suggested an adjustable transportable cryptography arrange that incorporates multi-keyword looked for and identical investigation. In their multi-keyword fuzzy pursuit study, Fu et al. [16] explored another method for dealing with the errors that arise throughout the placement phase and presented a useful research question. To help resolve the conflicts that arise between customers' searching goals and traditional catch phrase-based seek colludes, a linguistic search scheme depending on the concept hierarchy was suggested in [27]. This makes the tailored searching more feasible and ensures conscious choices. [18] also employs the use of query expansion via applicable graphs and effective proportions of "word grading." But for safeguarding photos internet server, Xia et al. [29] has suggested a CBIR scheme that uses cryptography and copyrighting techniques to prevent customers from illegally copying the restored images. To fight duplicated movement deception, Li et al. [4] proposed the use of linguistically independent patchwork for gating factor collection and analysis prior to the allocation of a secret. Zhou et al. [15] developed a new duplication image detection method, which relies on two main features of revolutionary consistent sets that were deleted from global circles. They also devised a global environment assessment system to block artificial substitutions, which was suggested by Zhou et al. [12] as a way to handle the limited discriminability and quantitative errors that have so far plagued the BOW model's graphic (BOW) approach. Regardless, since all of the applications mentioned above rely on latest updates about offsite replication, we need to focus first on the most efficient way to examine and verify the accuracy of the readdressed data. While this may be true, the present planning for official examinations can't defend from the disease. In [23], it was shown that TPA, which is a potential security risk for data re, should not be ignored, which the motivation for this work is.

4. Implementation

The smart gadget they designed gather patients code and transfer to the internet, such entry Identity, entry Name, entry Address, entry Email, entry Pulse, entry ElectroCardioGram, entry Symptoms and entry Image (all except entry Name must be encrypted). Insert an unique identifier, see the results, and use Encode to save it all in a single file. Internet servers take care of all of that, which means they also offer big data for portable tech, as well as allow physicians and nurses to see all customers and then approve them, respectively. All medical registry information in encoded form may be seen review and approve health information ease privileges. The following is a list of Fog Invasion and Client Recovery information found: complaint title vs. No. of entry) to get a list of people who have the same complaints as you (Doctor name vs No.Of Patients). The client may get the permissions to see clouds and get reply and information. Pick the physician and their patients from a combination menu, then forward information to them See physician reaction using prescribed medication -> See physician reply with prescribed medication Check your data, get back lost or deleted information, and see or erase your personal details. In order to conduct the Signup and Authenticate, Browse Account, View client information, and provide answer, such as Pharmaceutical information, Healthcare medication info, the physician is someone who will access the participant's medical records. The Installation and Preparation the expense of performance time is given in figure 2.
Installation and Preparation the expense of performance time

4.1 Experimental Evaluation

[23]'s Fortress concept is implemented on the Inspur NF5270M4 workstation with Nvidia GeForce Processor E5-2620 at 1.7 Mhz, 16 Giga Bytes RAM, and a 7000 Revolutions per minute 1Tera Bytes SATA disc with 32Megabit capability. Each element of the encryption powers are gained from django encryption toolbox [30]. 100-block cipher text is delivered by SHA1, and the RSA component is 512 bits in length to ensure safety. With regards to the Castle conspiracy, we similarly employ the gadgets of block chain system traveler [31] in order to get to crypto currency property for solving the random problems, and we often select the region dimension to be 1 KB (e.g., every 512 Kb record blockage has 64 places in Castle).

According to [32], a 128 KB to 32 Mb square of data systems is the norm. It's important to note that because the reappropriated checking scheme runs across memory devices, the rectangle area should be limited to no less than 256 Bytes. Customer's misappropriated data is set to 1 GB in our assessment. We do not even keep track of how long it takes to move the misappropriated content from the server to CSP, because this cost is standard for both of the schemes we've considered. The average number of cycles required to measure our results is 20. Before reappropriating, the customer's data should be normalized. As you can see in Figure 3, there is a perfect opportunity to compare data pre-processing times for the different layouts. In addition, we evaluate the amount of time a customer spends enrolling for our program and Fortress, separately. When synthesizing readressed data, operational cost produced at the web based accounts for the remainder of the overall duration, and our policy's pretreatment implementation is significantly faster than Fortress. After downloading the complete customer's data from the internet, TPA must convince the customer that it was appropriately normalized, as shown in [23]. A laborious nil verification (ZKP) with TPA is expected from the customer in this case. Due to the fact that TPA is not involved in preparation, unlike Fortress, our Customer Concentration approach is able to avoid ZKP work and achieve the visual enhancement. The Batching Certification duration and inspection phase total cost is given in figure 3.
5. Conclusion

It is possible to convert any public analyzing strategy into a confidential strategy by having the user carry out the evaluating activity that should be assigned to TPA. Customers’ considerable burden generated by more often than feasible examining can be passed to TPA. As a result, open examining strategies may be even more successful in the long run. A significant question that is never addressed in any of the present formal reviewing schemes is how to protect the customer from a spiteful TPA in the future. Fortress, a reconsidered inspection plan, is offered as a defense against TPA. Since TPA can obtain all readdressed data, Fortress relies solely on data cryptography to safeguard patient’s data. TPA should be denied access to patient’s readdressed data in the cloud by a secure reevaluation procedure, which is what this article does. Aside from not relying on an additional abnormal resource, our suggested conspiracy achieves the safety of guarding against any hostile component. Similarly, in light of the MHT data framework, we extend the readdressed evaluating strategy in order to provide continuous updating. Our approach has been proven to be safe and effective based on the research and assessments.

References

[1] Madala, S. R., Rajavarman, V. N., & Vivek, T. V. S. (2018). Analysis of Different Pattern Evaluation Procedures for Big Data Visualization in Data Analysis. In Data Engineering and Intelligent Computing (pp. 453-461). Springer, Singapore.
[2] Madala, S. R., & Rajavarman, V. N. (2018). Efficient Outline Computation for Multi View Data Visualization on Big Data. International Journal of Pure and Applied Mathematics, 119(7), 745-755.
[3] Vivek, T. V. S., Rajavarman, V. N., & Madala, S. R. (2020). Advanced graphical-based security approach to handle hard AI problems based on visual security. International Journal of Intelligent Enterprise, 7(1-3), 250-266.
[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 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*, 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 *Advances in Cryptology*, Lecture Notes in Computer Science, vol. 843, usa, November 2014.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—CRYPTO 2008: Proceedings of the 28th Annual International Cryptology Conference*, pp. 445–456, 1992.View at: Google Scholar

[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/pycrypt, 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