Computer and Information Science; Vol. 11, No. 1; 2018
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Enhancing Big Data Auditing

Sara Alomari[1], Mona Alghamdi[1] & Fahd S. Alotaibi[1]

[1] Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Correspondence: Fahd S. Alotaibi, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. E-mail: S.aloamrii93@gmail.com, Monagh5454@gmail.com, fsalotaibi@kau.edu.sa

Received: October 27, 2017 Accepted: November 4, 2017 Online Published: January 27, 2018

doi:10.5539/cis.v11n1p90 URL: http://dx.doi.org/10.5539/cis.v11n1p90

Abstract

The auditing services of the outsourced data, especially big data, have been an active research area recently. Many schemes of remotely data auditing (RDA) have been proposed. Both categories of RDA, which are Provable Data Possession (PDP) and Proof of Retrievability (PoR), mostly represent the core schemes for most researchers to derive new schemes that support additional capabilities such as batch and dynamic auditing. In this paper, we choose the most popular PDP schemes to be investigated due to the existence of many PDP techniques which are further improved to achieve efficient integrity verification. We firstly review the work of literature to form the required knowledge about the auditing services and related schemes. Secondly, we specify a methodology to be adhered to attain the research goals. Then, we define each selected PDP scheme and the auditing properties to be used to compare between the chosen schemes. Therefore, we decide, if possible, which scheme is optimal in handling big data auditing.

Keywords: big data, data auditing, provable data possession, pdp schemes

1. Introduction

Big data "is a set of techniques and technologies that require new forms of integration to uncover large hidden values from large datasets that are diverse, complex, and of a massive scale" [Hashem et al.,2015]. It represents a gold mine for businesses with the patterns and trends hidden in it [Hashem et al., 2015]. It also gives a better insight on how to increase the productivity, helps to predict the future and make better decisions. Such a critical role of big data necessitates keeping it correct, consistent and integrated. Considering the cost of storing big data for businesses, they tend to migrate such data to the cloud environment which relieves the cost by providing on demand resources. Despite the significant benefits provided by the using of the cloud, the security and privacy-preserving are still very challenging issues. The idea of outsourcing data and no longer locally managing them makes the protection of data a tough task. Some cloud service providers could act unfaithfully to maintain a reputation. They can hide the data loss incidents or delete rarely accessed data for monetary reasons without user's permission. These security issues can threaten users and companies, cost them money and make the auditing services demanding enough [Liu et al., 2013]. To ensure the security of the outsourced data, many auditing schemes have been proposed in previous studies. RDA-based schemes are considered the most popular and used schemes. Particularly for PDP schemes, they have been extensively enhanced to produce many other versions with different capabilities. The proliferation of PDP schemes makes it worthy to have a paper that includes a structured comparison clarifies the significant differences among these schemes. Such a contribution will assist to have a complete view of the chosen PDP schemes related to specific auditing features. In this paper, we will investigate the differences and similarities and conclude the optimal scheme among them, if possible. Firstly, we review the literature work related to data auditing services and schemes. Then, we define the research methodology and explain the concept and system model of PDP. Afterwards, we give a brief description of the selected PDP schemes and the auditing properties. Therefore, we conduct a comparison between PDP schemes in terms of the auditing properties in order to come up with an optimal scheme that can handle big data auditing efficiently. At last, we introduce the work to be achieved in future to enhance the proposed comparison.

2. Method

To specify the criteria of PDP schemes comparison, we will go through a broad investigation of pre-conducted studies and surveys of PDP schemes. This method helps to collect further than enough data to conduct the intended comparison and the required analysis to spot the prominent advantages and disadvantages and to come up with the optimal scheme, if possible. According to what we have read in multiple research papers, we prefer to choose five schemes that have variations in features which are PDP, Public PDP, SPDP, CPDP, and DPDP. Some selected schemes support batch auditing, and others do not and the same goes for dynamics auditing and public auditing features. The goal of picking variant -featured schemes is to provide people of interest with a comprehensive and mostly completed comparison based on the most significant properties of data auditing process. To achieve this research, we need to thoroughly understand the definition of each selected scheme besides the auditing properties that will be used as criteria to conduct the comparison. We are going to construct tables that illustrate these criteria against every PDP scheme. For every scheme, we will mention the auditing algorithm used and find out whether this scheme supports particular auditing features or does not.

3. Related Work

Rasheed [2014] has defined the current cloud service providers' capabilities for meeting auditing requirements. He has ended up with that cloud services market is fully committed to customer demands and the auditing features must be demanded by a significant number of customers to be fulfilled by cloud service providers. Therefore, big data and cloud computing are receiving more and more researchers' attention and many contributions. The researchers try to introduce solutions and schemes to verify the data stored in the cloud environment and ensure its correctness [Assunção et al., 2015]. Access control mechanisms have been proposed by Thangavel et al. [2016] to control who can access which part of data They have used the concepts of user roles, policy-based, attribute based, group based, course grained and fine grained to preserve the privacy of outsourced data from accessing data illegally and promote more security.

Almost, all the schemes suggested by the researchers are based on public auditability. The user of cloud can resort to a third-party auditor (TPA) to check and remotely audit his data. The TPA must be able to audit the outsourced data with no need to demand a copy, and the auditing process should be done efficiently, so it brings no new vulnerabilities [Wang et al., 2010b]. Wang et al. [2010a] have suggested a set of properties for public auditing services to make the management of data fully trustworthy and the auditing process more practical. It includes minimize auditing overhead, protect data privacy, support data dynamics and batch auditing. These properties besides collaborative auditing have been seen as challenges of data storage auditing by Yang and Jia [2012]. They have deeply surveyed the existing storage auditing methods such as MAC-based and RSA based homomorphic methods, and analyzed them in term of security, storage overhead, communication cost and computation complexity. Wang et al. [2010b] have proposed TPA-based scheme that was implemented by the use of a public key based homomorphic authentication along with random masking to achieve privacy-preserving cloud data auditing system. Also, batch auditing was considered to make the scheme more efficient using the technique of bilinear aggregate signature. A similar scheme has been proposed by Wang et al. [2011] with significant improvements. Both schemes perform public batch auditing using bilinear aggregate signature. The major improvement has been made in this scheme is data dynamics verification capability accomplished by the utilization of Merkle Hash Tree. An authorized TPA-based scheme has been proposed by Suresh et al. [2014]. It is supposed to encrypt the data before uploading to cloud server and decrypt it when retrieving for seeking more security. It also eases the performing of block level operation and promotes lower overhead for big data applications because of the verification of fine grained data updates using Ranked Merkle Hash Tree (RMHT).

Liu et al. [2014] have enhanced the existing research work which can support fixed-size data blocks data dynamics and made it possible to support fine-grained data updates. They have proposed a modification with the purpose of reducing communication overheads for auditing small updates. Yang and Jia [2013] have introduced an auditing framework and protocol with the aim of assuring data owner that data is correctly stored in the cloud. It is supposed to support dynamic operations. The protocol has also combined the cryptography methods with bilinearity of bilinear pairing to protect the privacy of data against the auditor. Therefore, batch auditing is done with no need for any additional organizer.

The researchers of [Sookhak et al., 2015b] have explained the concept of Remotely Data Auditing (RDA) used to protect outsourced data in distributed servers. RDA is intended to analyze a data sample according to its integrity and correctness to ensure the reliability of cloud service providers. They classified RDA into three categories whic are replication-based RDA, erasure-coding-based RDA, and network-coding-based RDA. They have presented a taxonomy helps in classifying different RDA methods and highlighting the similarities and differences. RDA technique is mostly not applicable for data dynamics and causes high computational costs. Therefore, it has been enhanced by Sookhak et al. [2015a] to overcome these major drawbacks. They have introduced a design of a new data structure which is divide and conquer Table (DCT). DCT is constructed based on algebraic signature which is useful for verifying the correctness of outsourced data. The proposed solution can be implemented for large-scale data storage, reduce the processing time of dynamic data update operations and afford the minimum computational cost.

The authors of [Liu et al., 2013] assert that although the cloud computing has outstanding advantages, data security is still a critical issue in the cloud. In other words, user's data outsourced to the cloud on server-side but the service provider is totally untrusted, for this reason, the verification mechanisms should be done on the client side without having to retrieve data which makes it very challenging to do so. The researchers have proposed multiple of schemes to ensure integrity verification, which they are provable data possession (PDP), proofs of retrievability (POR), Compact POR, DPDP (Dynamic PDP), Public Auditing of Dynamic Data, Authorized Auditing with Finegrained Data Updates, each of them has a different achievement. Liu [2014] has delivered new schemes for the verification of outsourced data which are FU-DPA and MuR-DPA. He has conducted a comparison between the proposed schemes and the existing schemes regarding some properties in public auditing. The comparison has contributed in highlighting the improvements that have been done in the proposed schemes.

A lot of PDP-based schemes were presented by different researchers such as DPDP, SPDP and CPDPD, each of which shows kind of enhancements compared to the previous one. The emergence of many PDP auditing schemes motivated other researchers to conduct a comparative study of these variations to bring out the fundamental differences and conclude the advantages and disadvantages. Such as the paper introduced by Natu and Pachouly [2014]. They investigated the PDP schemes considering the functionality used, pros and cons. As a result, they proposed an enhanced scheme which initiates the verification of data on behalf of the client and frees the client from intactness checking. The proposed scheme also involves a log to facilitate performing administrative tasks. Another paper was written by Shin and Kwon [2015] presented a survey study of PDP schemes which have a batch auditing capability. Shin and Kwon [2015] illustrated the features and performance of each scheme of batch auditing and come up with a challenging issue which is the urgent need to have a corrupt data identification protocol. Such a protocol will assist to avoid the effect of corruption on the communication and computation costs.

4. Various PDP Schemes

Provable Data Possession (PDP)

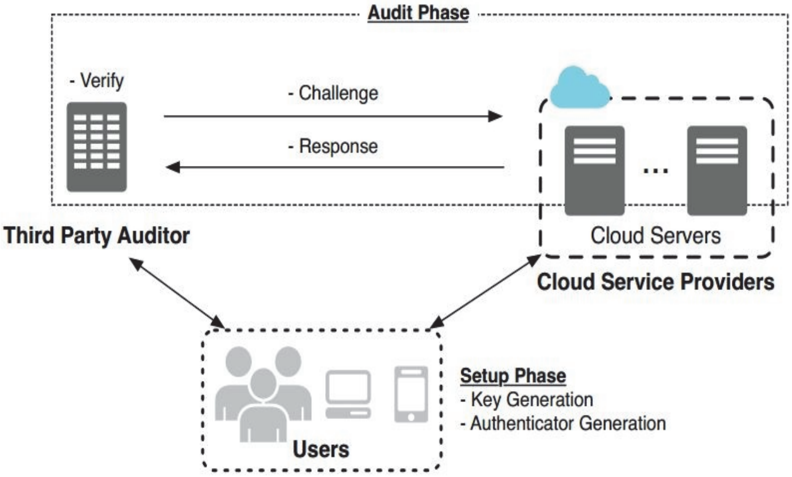

Figure 1. PDP-based remote data auditing system model (Shin and Kwon, 2015)

A remote data auditing technique proposed by Ateniese et al. [2007] to validating data integrity over remote servers. The system model of PDP illustrated in Figure 1. The users or data owners store their data in the remote cloud servers (CSP) and delegate them the maintenance of their data. The auditing process can be done by a third party (TPA) on behalf of the user upon request. PDP technique involves two phases which are setup and audit. The setup phase includes a key generation in which users can negotiate the keys with CSP and TPA and an authentication generation where users can compute authenticators as data tags of their data. However, the audit phase is usually done via a challenge-response procedure which follows challenge, response and verify steps. In the challenge step, a challenge message which includes indexes of randomly selected data blocks will be sent by the TPA to a CSP or multiple CSPs. Then, in response step, CSP receives the message and accordingly sends a response message includes both a data proof and the authenticator proof to the TPA. At last, the TPA, in turn, verifies the correctness of the proof to complete the verify step [Shin and Kwon, 2015].

- **Public PDP**

A scheme that is proposed by Wang et al. [2011] which performs the auditing process as in basic PDP scheme with two additional features. Using Merkle Hash Tree (MHT) to authenticate block tags enables Public PDPD scheme to support both public auditability and dynamic updates. It also supports batch auditing for multiple users in a single cloud [Shin and Kwon, 2015].

- **Scalable PDP (SPDP)**

A highly secure and efficient PDP scheme which is a symmetric-key cryptography based that extends the basic PDP to partially support dynamic data operations [Ateniese et al., 2008].

- **Cooperative PDP (CPDP)**

A scheme that is used to ensure the integrity of the outsourced data by utilizing the existence of multiple clouds to perform the auditing cooperatively. It supports the verification of data dynamics for distributed cloud and ensuring the integrity of stored data [Kolte et al., 2013].

- **Dynamic PDP (DPDP)**

It is deemed to be the first scheme that guarantees the integrity verification to support full data dynamics [Liu et al., 2013]. It works as PDP scheme along with additional steps to achieve data dynamics auditing service.

5. Comparison Criteria

- **Auditing technique**

It identifies the methods that a scheme uses to perform the auditing of the outsourced data and to ensure its correctness and integrity.

- **Privacy-preserving**

A protocol that is used to ensure that no private information shared will be leaked in the case of the verification is done by a third party [Natu and Pachouly, 2014]. The protocol must guarantee that the TPA will not reveal the outsourced data during the time of auditing.

- **Dynamic auditing**

It enables the client to perform dynamic operations on the data such as insert, delete, and update while assuring the correctness and consistent integration of data files stored in the cloud.

- **Batch auditing**

The ability of the TPA-based auditing scheme to do multiple auditing tasks simultaneously for multiple users which enhances the scheme performance. It is important to maintain the privacy among users and TPA whenever this feature is being enabled [Natu and Pachouly, 2014].

- **Blockless verification**

For efficiency and security purposes, the blockless verification is used to guarantee that the challenge file blocks will be retrieved by the verifier whether it was a TPA or the data owner himself [Natu and Pachouly, 2014]. The verification of a data file is done by verifying only a part of it.

- **Stateless verification**

The availability of this feature enables the auditor to dispense the frequent maintenance of information state at the auditor side during the auditing process [Shinde and Sulochana, 2015].

- **Identification of corruption**

The ability of the auditing scheme method to detect the corruption of data whenever the verification fails [Shin and Kwon, 2015].

- **Computation cost**

The auditing schemes should achieve lowered computation complexity to enable the user to perform data verification contentiously with less computational requirements [Natu and Pachouly, 2014].

- **Communication cost**

Sending and receiving data in verification and auditing services occur very frequently which increase the network traffic on the server. Therefore, the auditing and verification schemes must try to reduce the network traffic as much as possible by reducing network communication [Natu and Pachouly, 2014].

6. Comparative Analysis of PDP Auditing Schemes

In this section, we compare the PDP auditing schemes regarding features and performance. Table I illustrates a comparison of PDP schemes based on multiple features. Auditing technique feature represents the cryptographic algorithms utilized in the auditing process. For PDP, Public PDP and CPDP, they employ homomorphic encryption mechanisms to perform auditing and verification of data integrity. However, homomorphic linear authentication (HLA) which used in Public PDP introduces less computation cost than homomorphic erification token (HVT) that employed in PDP because of the utilization of BLS signature mechanism. On the other hand, CPDP has used homomorphic verification response (HVR) which performs the verification of data by aggregating multiple responses from distributed clouds into a single value [Sookhak et al., 2015b]. In SPDP, Merkle Hash Tree (MHT) has been used to audit outsourced data and ensure its correctness securely. Moving to DPDP, the rank-based authenticated skip list is used to efficiently authenticate dynamic operations on outsourced data, such as authenticated insert and delete [Shin and Kwon, 2015].

The privacy-preserving feature is considered as an objective that must be achieved by any auditing scheme to ensure that no private information shared with TPA is leaked. Unlike PDP and public PDP, other schemes preserve the privacy of data. In particular, SPDP and DPDP ensure the privacy of outsourced data by taking the advantage of MHT and rank-based authenticated skip list techniques, respectively. While CPDP empowers HVR technique with random masking to make the scheme able to achieve privacy of data [Shin and Kwon, 2015].

Public PDP, SPDP, and DPDP promote dynamic operations such as insert, delete, and update operations while verifying the correctness and integrity of data stored in the cloud [Zhang and Blanton, 2013]. To accomplish more efficient data dynamics, MHT is integrated to Public PDP and SPDP schemes. Whereas authenticated skip list has been incorporated to DPDP to support full dynamics operations [Elamathi and Selvanayagi, 2014].

For the purpose of enhancing the performance, Public PDP attains batch auditing for multiple users in a single cloud server by manipulating the bilinear aggregate signature scheme. But regarding CPDP scheme, the batch auditing is achieved for multi-clouds with the help of an additional organizer which submits a final proof of response to the TPA for verification. In contrast of Public PDP, CPDP does not satisfy batch auditing for multi-users because of the differences between the authenticators generated for each user which makes it impractical to aggregate them into a single proof for multiple users'data auditing [Shin and Kwon, 2015].

Except for CPDP, all the other schemes realize blockless verification feature to verify data integrity with no need to have all data file blocks. In detail, the verifier only verifies a part of the file by aggregating of precomputed HVTs or HLAs tags of the outsourced file [Barsoum and Hasan, 2010]. In either case, the TPA ought to download the whole data file to perform the verification. As a result, the time to accomplish the verification will increase in addition to the consumed bandwidth [CHITRA et al., 2015].
The stateless verification is supported by all schemes presented in Table 1. It omits the necessity of state information maintenance at the verifier side between audits throughout the long term of data storage[Wang et al.,2011].

As a final property, identification of corruption is a feature of PDP and DPDP schemes which detects corrupt data blocks in case of the verification failure. Homomorphic verification token (HVT) is used by PDP to verify the correctness of data along with data error localization which locates the misbehaving server(s) where DPDP scheme has employed RSA trees to do so. Table 2 presents the performance comparison of PDP auditing schemes concerning computation complexity and communication complexity. The computation complexity is preferred to be reduced to constant to enable the users to perform data verification from time to time with less computational requirements [Natu and Pachouly, 2014]. On the other hand, the communication complexity is better to be reduced by reducing the network communications since the verification process includes many sending and receiving of data across the network

Table 1． Comparison of PDP auditing schemes on the basis of features

Scheme\ Criteria	PDP	Public PDP	SPDP	CPDP	DPDP
Auditing technique	HVT	HLA	MHT	HVR with random masking	Rank-based Authenticated Skip List
Privacy-preserving	✗	✗	✓	✓	✓
Dynamic auditing	✗	MHT	MHT	✗	Rank-based

					Authenticated Skip List
Batch Auditing **Multi-users or Multi-clouds**	✗	✓	✗	✓	✗
Blockless verification	✓	✓	✓	✗	✓
Stateless verification	✓	✓	✓	✓	✓
Identification of corruption	✓	✗	✓	✗	✓

Table 2. Comparison of PDP auditing schemes on the basis of performance

Schemes	**Computation**		**Communication**		
	CSP	**TPA**	**Individual auditing**	**Batch Auditing** **Challenges**	**Response**
PDP	O(t)	O(t)	O(1)	Does not support	Batch Auditing
Public PDP	O(t log n)	O(t log n)	O(t log n)	O(KCst)	O(KCst log n)
SPDP	O(t)	O(t)	O(t)	Does not support	Batch Auditing
CPDP	O(ts)	O(t+s)	O(t+s)	O(KCt)	O(KCs)
DPDP	O(t log n)	O(t log n)	O(t log n)	Does not support	Batch Auditing

n = total number of data blocks of a file

s = the number of sectors in each data block

t = the number of challenged data blocks in the auditing phase.

K = users

C =clouds.

7. Research Results

From the previous analysis, it has been noticed that the only schemes which promote batch auditing are Public PDP and CPDP. They correspondingly do not identify the corrupt data which almost indicates a performance that is lower than the expected. Therefore, we can recover this drawback by incorporating recursive binary search technique to enable the detection of which data blocks or authenticators are corrupted. This feature is critical especially for batch auditing schemes since all proofs are aggregated into a single proof for auditing. Subsequently, without the ability to detect the corrupt data, even if a single proof was invalid this would necessitate repeating the whole auditing process again. However, the inclusion of this feature introduces some communication overhead and affects the performance of the scheme.

Moreover, CPDP scheme needs to be enhanced to perform a blockless auditing which will significantly lower the communication cost and improve the scheme performance. Besides, the support of dynamics ought to be activated to increase the reliability and to ensure the integrity of the updated data. On the other hand, Public PDP does not preserve the privacy of data while performing the auditing which is deemed to be a reasonable cause to not to use the scheme for auditing, principally, the sensitive data. Therefore, such an impediment should be overcome by the utilization of random masking, or any more appropriate technique helps in achieving the privacy. Basically, there is no scheme supports all the features. However, SPDP and DPDP are most likely to be ideal schemes for auditing. They possess all the essential features that are taken into account in designing any auditing scheme except for the batch auditing which heavily affects the performance when handling big data. At last, the priorities determined by the service providers play a critical role in selecting the appropriate auditing scheme. The service providers will decide the priorities based on users' needs.

8. Conclusion and Future Work

In this research, after the review of literature, we specified the research problem which is conducting a comparative study between some PDP techniques to conclude the optimal one. The study aims to provide people of interest with the best perception of the chosen PDP techniques. Then, we defined the method that is used to achieve the research goals. Besides, we selected some PDP techniques and justified our choice. Moreover, we explained each criterion of the comparison and made two tables that summarize the differences as well as the similarities of the selected sample. The significant addition of this paper is to facilitate the search for auditing techniques by grouping such major schemes and highlighting their similarities and differences. Such a kind of research usually requires a complete dedication to reading and looking up for all schemes since the auditing of outsourced data is a hot topic that catches many researchers' attention.

As stated previously, there are many auditing schemes have been introduced in literature. Most of them are enhanced to produce new versions with more capabilities. The differences of the schemes and their versions cannot be recognized easily without a deep investigation and analysis of each of them. The difficulty of finding out the variations between schemes comes from the struggling to find the required knowledge aggregated at one source. Consequently, we are going to enhance our paper by scaling up the auditing schemes and classifying them into categories based on specific auditing features. Subsequently, the resulted comparison gains more value and provides the people of interest with more structured knowledge.

Acknowledgement

We would like to show our gratitude to our instructor, Dr. Fahad Alotaibi, for sharing his pearls of wisdom with us during the course and guiding us through this research. We are immensely grateful to his so-called insights and comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of this esteemed person.

References

Ayad, F. B., & Anwar, M. H. (2010). Provable possession and replication of data over cloud servers. *Centre For Applied Cryptographic Research (CACR), University of Waterloo, Report, 32*.

CHITRA, N., SANTHOSHKUMAR, S. P., BABY, V. V., & ANURADHA, V. (2015). Privacy-preserving public auditing for shared data in the cloud.

Chris, C. E., Alptekin, K., Charalampos, P., & Roberto, T. (2015). Dynamic provable data possession. *ACM Transactions on Information and System Security (TISSEC), 17*(4), 15.

Elamathi, N., & Selvanayagi, B. (2014). Secured data storage for rdpc protocol with enhanced tpa auditing scheme using mht in cloud computing. *JIREEICE, 2*(11), 2173–2178.

Giuseppe, A., Randal, B., Reza, C., Joseph, H., Lea, K., Zachary, P., & Dawn, S. (2007). Provable data possession at untrusted stores. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 598-609. Acm.

Giuseppe, A., Randal, B., Reza, C., Joseph, H., Osama, K., Lea, K., Zachary, P., & Dawn, S. (2011). Remote data checking using provable data possession. *ACM Transactions on Information and System Security (TISSEC), 14*(1), 12.

Giuseppe, A., Roberto, D. P., Luigi, V. M., & Gene, T. (2008). Scalable and efficient provable data possession. In *Proceedings of the 4th international conference on Security and privacy in communication netowrks*, p. 9. ACM.

Hassan, R. (2014). Data and infrastructure security auditing in cloud computing environments. *International Journal of Information Management, 34*(3), 364-368.

Ibrahim, A. T. H., Ibrar, Y., Nor, B. A., Salimah, M., Abdullah, G., & Samee, U. K. (2015). The rise of big data on cloud computing: Review and open research issues. *Information Systems*, *47*, 98-115.

Liu, C. (2014). Toward efficient and secure public auditing for dynamic big data storage on cloud. PhD thesis.

Liu, C., Chen, J. J., Yang, L. T., Zhang, X. Y., Yang, C., Ranjan, R., & Ramamohanarao, K. (2014). Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates. *IEEE Transactions on Parallel and Distributed Systems, 25*(9), 2234-2244.

Liu, C., Rajiv, R., Zhang, X. Y., Yang, C., Dimitrios, G., & Chen, J. J. (2013). Public auditing for big data storage in cloud computing–a survey. In *Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference on*, pages 1128-1135. IEEE.

Madhumati, S., & Sonkamble, S. (2015). Secure public auditing for cloud data storage. *International Journal of Science and Research (IJSR), 4*.

Marcos, D. A., Rodrigo, N. C., Silvia, B., Marco, A. S. N., & Rajkumar, B. (2015). Big data computing and clouds: Trends and future directions. *Journal of Parallel and Distributed Computing*, *79*, 3-15.

Mehdi, S., Abdullah, G., Hamid, T., Adnan, A., Samee, U. K., Rajkumar, B., & Albert, Y. Z. (2015b). Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues. *ACM Computing Surveys (CSUR), 47*(4), 65.

Mehdi, S., Abdullah, G., Muhammad, K. K., & Rajkumar, B. (2015a). Dynamic remote data auditing for securing big data storage in cloud computing. *Information Sciences*.

Mohammad, E., & Alptekin, K. (2015). A generic dynamic provable data possession framework.

Pooja, N., & Shikha, P. (2014). A comparative analysis of provable data possession schemes in cloud *International Journal of Computer Science and Information Technologies, 5*(6), 7927-7931.

Roshan, R. K., Rahul, D., & Niraj, V. T. (2013). Cpdp scheme to provide data integrity in multicloud. *International Journal of Computer Applications, 83*(10).

Sooyeon, S., & Taekyoung, K. (2015). A survey of public provable data possession schemes with batch verification in cloud storage. *Journal of Internet Services and Information Security (JISIS), 5*(3), 37-47.

Sun, X., Chen, L., Xia, Z., & Zhu, Y. (2014). Cooperative provable data possession with stateless verification in multicloud storage. *J. Comput. Inf. Syst, 10*(8), 3403-3411.

Suresh, A., Pachaiappan, S., & Pasupathi, P. (2014). Authorized third party auditing and integrity verification in cloud computing. *International Journal of Research in Science and Technology*, 95.

Thangavel, M., Varalakshmi, P., & Sridhar, S. (2016). An analysis of privacy preservation schemes in cloud computing. In *Engineering and Technology (ICETECH), 2016 IEEE International Conference on*, 146-151. IEEE.

Wang, C., Ren, K., Lou, W. J., & Li, J. (2010a). Toward publicly auditable secure cloud data storage services. *IEEE network, 24*(4), 19-24.

Wang, C., Wang, Q., Ren, K., & Lou, W. J. (2010b). Privacypreserving public auditing for data storage security in cloud computing. In *INFOCOM, 2010 Proceedings IEEE*, p. 1-9. Ieee.

Wang, J. X. (2011). A rank-based skip lists in dynamic provable data possession. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li. Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE Transactions on Parallel and Distributed Systems, 22*(5), 847-859.

Yang, K., & Jia, X. H. (2012). Data storage auditing service in cloud 14 computing: challenges, methods and opportunities. *World Wide Web, 15*(4), 409-428.

Yang, K., & Jia, X. H. (2013). An efficient and secure dynamic auditing protocol for data storage in cloud computing. *IEEE Transactions on Parallel and Distributed Systems, 24*(9), 1717-1726.

Zhang, Y. H., & Blanton, M. (2013). Efficient dynamic provable possession of remote data via balanced update trees. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, 183-194. ACM.

Copyrights