International Journal of Computer Engineering and Technology (IJCET)
Volume 10, Issue 06, November-December 2019, pp. 10-21, Article ID: IJCET_10_06_002
Available online at http://iaeme.com/Home/issue/IJCET?Volume=10&Issue=6
Journal Impact Factor (2019): 10.5167 (Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

CHALLENGES AND ISSUES ON THE RECENT DATA INTEGRITY PRESERVING TECHNIQUES IN THE MULTIUSER CLOUD

K. Ambika
Department of CSE, BIT campus, Anna University, Tiruchirappalli, India

Dr. M. Balasingh Moses
Department of EEE, BIT Campus, Anna University, Tiruchirappalli, India

ABSTRACT

Over the decade, the usage of data had increased exponentially, which led to the demand for its effective storage and retrieval. The cloud environment has developed to handle that demand with its huge storage space and easy accessibility. However, the open nature of the cloud resulted in the data integrity issues and multiuser cloud enriched it. The other issues like group signature and user revocation took the central part to ensure integrity of data in the cloud. The present study summarizes various techniques that were developed in recent times to address the security issues on data integrity, user revocation, and group signature. To reflect on the novelty of each approach, along with its performance in providing integrity for the cloud data stands as the primary objective of the study. From the extensive study, it was found that the overhead on the computational and communication overhead increase proportionally with an increase in the number of the user during the group signature generation and recurrent user revocation. There was a need for an effective cryptic mechanism with effective cloud storage and recovery of data. Finally, it was suggested to develop a robust framework that can provide enhanced security with reduced overhead and ensure data integrity.

Key words: Data integrity, Group signature, Storage, Security, User revocation

Cite this Article: K. Ambika, Dr. M. Balasingh Moses, Challenges and Issues on the Recent Data Integrity Preserving Techniques in the Multiuser Cloud, *International Journal of Computer Engineering and Technology* 10(6), 2019, pp. 10-21.
http://iaeme.com/Home/issue/IJCET?Volume=10&Issue=6

1. INTRODUCTION

There are several view points in the age of cloud computing through which the data are remotely stored on mobiles, computer systems or other internet appliances for temporary backup. Cloud has many benefits such as resource pooling, data storage, multi-tenancy; however, cloud computing also subjected to has security flaws. It is necessary to assist the cloud storage so that the user may find that their data are safe and secure within the cloud

environment [1]. Many types of research have been performed to accomplish secure data in multiuser cloud environments, and so far, recommended numerous novel solutions for ensuring the data integrity, such as preserving -privacy techniques [2,3,4], dynamic data approach [5,6,7], and multi-replica methods [8,9]. Recently, data sharing has become more common with collaboration and teamwork in the cloud and turned as an interesting area in the cloud field in which securing the data integrityis the focal point of the work [10,11,12].

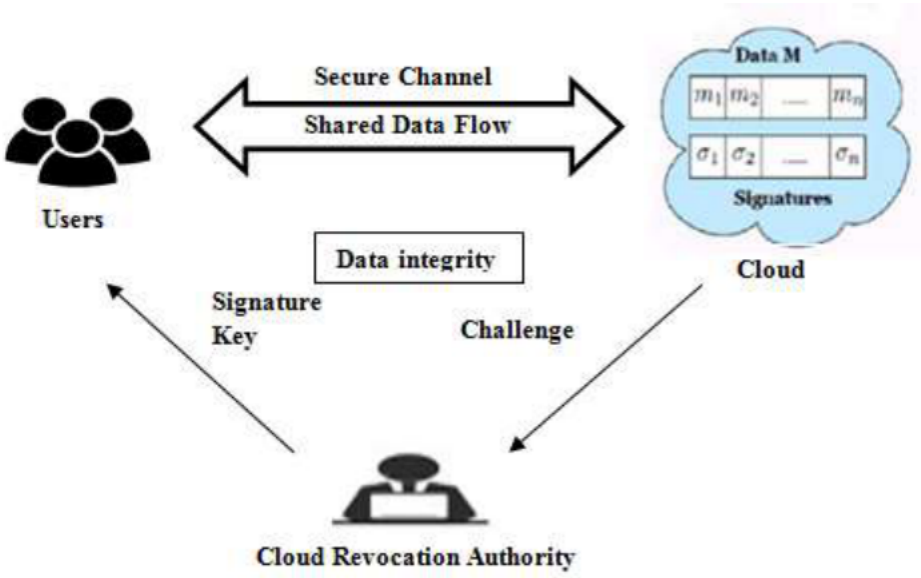

Figure 1: Architectural system of cloud

One of the stable, secure and robust approaches that provide group keys of either symmetric or asymmetric is the Group key agreement. Just like the case of symmetrical Group key agreement, all members of the group are given a session key after negotiation. By employing the session key, the group members can encrypt or decrypt information on group interaction, meaning that receivers and senders use the same group key [13].

Contradictory, when a user acquires the individual data, all authorized users access may be changed within group shared cloud data, e.g. organization staff and team collaborators. The cloud document's sharing and collaborative nature creates huge issues on several integrity audit schemes. In addition to data protection, data batching support and adaptive verification, the audit currently has several limitations such as traceability, increase in verification time and signature size proportionality with several group user, Data freshness and many more[14].

This survey paper outlines the key challenges of Cloud computing data reliability and then presents some working schematics and possible solutions related to achieve and enhance group signature/user revocation. The retrospect is structured into the following segments. Segment 1 represented in the form of introduction, Segment 2 gives a specific overview of digital group signature, and the subsequent section 3 addresses the study on user revocation. Segment 4 addresses the approaches in data integrity and the segment 5 deliberate overview on the third party auditing. Segment 6 presents a comparative study over the three major topics of the study, and the segment7 provide the identified research gaps. Finally, Segment 8 encapsulates the central findings of the retrospect for future research avenues.

2. GROUP DIGITAL SIGNATURE

By building homomorphic authenticable ring signatures [11] or computer common private group key tags, the authority is unable to know each block signed to a particular user in the group. [2]. All approaches apprehend about complete privacy, the user actual identity is not

possible to be traced. An advanced growth on the group signature scheme with homomorphic authentication [6] devised to protect integrity. In one way, each signer detail is anonymous; similarly, the group manager may detect the true signer identity after a chaos. In the meantime, the index hash table-based data structure[15, 2, 6,11] and Merkle Hash Tree (MHT) was used to assist data dynamics. [16,17,18,19].

A certificateless signature-based scheme using *identity-based cryptography* (IBC) was proposed [20] to avoid problems with the management of certificates and key escrow. Group user's private key contains two parts: a partial key and a hidden value. Every user chooses an anonymous value, and group owner generates a partial key for each user group. All the blocks of data are signed with a group user to get separate tags for authentication. Based on Computational Diffie Hellman algorithm (CDH) and Discrete Logarithm (DL) assumptions, they proved the protection for their program and suggested it has good efficiency. On realizing the significance of issues in the existing public integrity checking (PIC), a new identity-conserving public integrity control system with dynamic communities (IPIC-DG) for processing in the cloud. It was observed that the proposed scheme was capable of providing identity preserving, efficient user revocation, and verification on remote data integrity along with ensuring anonymity under attack. Moreover, it was deliberated that the scheme performed more efficiently than state-of-art. [21]

An improved secure KAC scheme with Chosen Ciphertext Attack (CCA) security was recommended for fine-grained encrypted data sharing. The two leak-proof auxiliary input schemes identified as auxiliary input chosen plain-text attack (AI-CPA) and AI-CCA was proposed and suggested that the scheme's decryption correctness proof is very identical to the basic KAC auxiliary input scheme proof [23]. Finally, it was validated that under the strong auxiliary input extractor, the basic and enhanced scheme secured the resilient schemes. With more time complexity, it was suggested to be suitable only for the IoT end-devising [22]. Another study described that the authentication of data owner could not be certified through the existing scheme. Thus, a new scheme in anonymizing and signing the access policy agreement was recommended, and it was secure against indistinguishable CCA. On evaluation, it was found that the proposed scheme performed similarly as the existing access control scheme based on attributes.[24]

Ciphertext-policy attribute-based encryption (CP-ABE) was exceptionally appropriate for transforming cloud computing it into a secure one. With this idea of Canetti–Halevi–Katz (CHK) method, the test on decryption was performed with a one-time signature. The recommended scheme was featured with constant ciphertext size and computation cost. Finally, it was recommended to create a scheme with CCA2-secure and CP-ABE, that can support AND_m^* policies efficiently [25].For addressing the issue of user anonymity, an efficient scheme for public auditing was proposed for preserving the identity of group members along with privacy and traceability. From the evaluation, it was evident that the proposed scheme performed effectively [26].

A novel homomorphic authenticator was designed with BLS signature for auditing the Regenerating-Code-Based Cloud Storage through the generation of two secret keys and publicly verifying them. After extensive analysis, the proposed signature scheme proved to be highly efficient, securable, and viable for Cloud storage system and reduce the owner burden [27].The notion of proxy re-signatures was utilized for protecting the cloud data legitimacy, that resign the existing user blocks during revocation of other users. The trial outcomes displayed that mechanism had significantly enhanced the efficiency of user revocation with lesser computation and communication overheads [11]. A program of a novel multi-replica public auditing (MuR-DPA) was proposed to address security and multi-replica Merkle hash tree (MR-MHT) based efficiency issues. Form the analysis; it was observed that the

developed scheme incurred less communication overhead and provided the security against corrupt service providers in clouds. It was found that the emphasis should be on dynamic data and streaming data with proof of integrity of a constant volume.[9].

3. USER REVOCATION

A common inclusion in the schemes is the User revocation, because users may be subject to changes in group membership for their unethical behavior or expiry of their term. The overhead after the revocation had turned as a heavy burden due to the accumulation of the data exchanged in the cloud. Hence, the concept for reducing the operating processing costs or the computational overhead was resulting from the primary research challenge of user revocations accomplishing the data auditing in the cloud [28]. Specifically, the BLS signature performs the shortest question and effective response among all the public verifiability proof-of-retrievability schemes. As a result of these properties, the BLS was widely engaged in building auditing schemes with effective user revocation [3, 11, 12, 19, 29].

Most of the existing schemes on ABE were subjected to drawbacks with high overheads on computation and fragile data security. For overcoming these drawbacks, an auxiliary function to define the ciphertexts was added considering the updation on the revocation events. The elaborative analysis showed that the recommended scheme was secure and effective with reduced overheads. The system did not apply direct attribute revocation in data sharing across a resource-limited cloud environment [30]. A proxy re-signature had been employed to consent the calculation of group's re-signatures in the cloud. To ensure the shared data integrity with effective collusion-resistant user revocation, a novel scheme was introduced based on public auditing. The analysis findings showed that the scheme proposed was safe and processing was more affordable for mobile devices [31].

A*Hierarchical Attribute-Set-based Access Control* (HASAC) program that supports hierarchical user grants files creation, revocation and file deletion. The implemented HASAC was tested on the basis of its efficiency and the experimental results showed that the HASAC performance was appropriate, even immune to fraud and collusion attacks [32].

For cloud data sharing and storage framework, an attribute-based access control scheme was introduced. The findings showed that the proposed scheme boosted the backward secrecy with an effective attributes revocation algorithm. However, improvement needed efficiency in decryption and encryption. With decryption outsourcing, a new multi-authority ciphertext-policy ABE (MA-CP-ABE) scheme was developed. The implemented outcomes showed that the scheme was efficient, scalable and securable. The scheme was supportable and adaptive for monotone linear secret sharing scheme access policy [34]. Since ID-based cryptosystem streamlines revocation and certificate management in conventional PKI, an active protocol for ID-based auditing was proposed for the integrity of cloud data in comparison with others[46].ID-based remote protocol testing possession of data was found to be more appropriate to the large-scale storage system in the cloud[35].

For addressing the security loophole, new method to management of fine-grained access control was proposed to secure sign-cryptic sharing (sign-then-encrypt) of data to accomplish the requirements of cloud computing. The outcome exhibited that the proposed approach was effective and corrected.[36]. A critical issue was how to assist in cloud computing with a secure data collaboration system that provides software updating and access. An experiment was performed to study the secure collaboration of data in the cloud that comprised of several encryption paradigms and fine-grained regulation of access along with the data writing operation. The outcome exhibited high efficiency with low computation, storage and communication overhead. [37].

4. DATA INTEGRITY

A serious concern was to define whether the Cloud service provider (CSP) fulfills the users ' legal expectations of data integrity [38, 39, 40], for which there are too many explanations. The first cause was the fear of loss of control over cloud data, so data controllers are no longer able to authenticate their data integrity by conventional methods that are popularly involved in local data processing. In addition, the storage infrastructure in cloud is exceptionally secure compared to individual computing apps; they are particularly susceptible to security threats both externally and internally due to the structure of cloud.

A group management system based on lazy-revocation was designed to produce effectual activities of group that had to endure attacks of collusion when increasing computational costs considerably. The outcome demonstrated the effective achievement towards secure auditing [41]. For important sensitive data, an efficient multi-copy scheme of Provable Data Possession (PDP) was recommended, and it supported the data integrity verification of file copies anywhere and anytime, without any information leakage. The scheme has proven successful against replacement attacks, forging attacks and replicating attacks [42].

Integrity check with Authentications is employed to identify the Users and Data Publishers to be verified for avoiding illegal impersonation and adjustment attack. For solving these issues *distributed authentication and authorization scheme* (DAAS) was proposed and exhibited lesser bandwidth cost [43]. For verifying the cloud data integrity, a Third-Party Medium (TPM) was developed to conduct time-consuming operations on behalf of the user. The scheme employed blind data with easy processes during the data audit phase and data uploading. From the performance and proof generation, the proposed scheme was found to be secure and efficient [44]. Generally, the data owned by various stakeholders was stored in various locations with different permissions. Upon evaluating the cross-party communication requirements to address the issues, a multi-server information sharing solution was introduced on a private cloud. Validation showed that the approach proposed is feasible for maintaining and avoiding possible issues on data copyrights and other legal issues [45].

A mid cloud computing's technical and economic advantages, many potential consumers of the cloud remained hesitant to accept cloud computing because of its security and privacy concerns. By taking these issues, a novel *triangular data privacy-preserving* (TDPP) model was supported public auditing ability to audit every major investors and results verified the effectiveness and efficiency after the completion of auditing [46]. A 'proxy re-encryption' scheme was proposed after studying the issue on the public key integrity which was employed during the re-encryption keys generation. The result exhibited that the system is practical for real-life usage. [47].

Based on the Dolev-Yao model, safety targets like resistance to anti-collusion, active attack, along with security revocation attributes cannot be certain for most schemes since the unnecessary target, such as listening, overhear, replay and subjective data synthesis to open channels of communication are possible. For overcoming this issue, scheme *Secure Data Sharing Scheme in Multi-Authority Cloud-storage-systems*(SDSS-MAC)was formulated to accomplish control with fine-grained access along with efficiency in decryption through verifiable and the cloud’s off-loaded transformation. The overall performance exhibited high efficiency on large storage, reduced overheads on communication and computation[48].

A security concept IND-CCA was described for systems of CP-ABPRE and recommended the first adaptive CCA-secure setup and proved the scheme as a standard model [49]. The model was enhanced to gain re-encryption efficiency phase and creation of the re-encryption key. After studying the four components of the security concern in the cloud environment, it was observed that data integrity checking is very significant. A prototype

scheme for accessing and sharing of the large scale medical data was implemented. Experimental outcomes exhibited are improved and made effective [50].

5. OVERVIEW OF THIRD -PARTY AUDITOR (TPA)

Several mechanisms based on different techniques have been proposed to ensure the data security of stored data in cloud servers. In general, a trusted cloud revocation authority to reduce the burden on users is appointed to carry out the verification for secure purposes [58]. Third-party auditor (TPA) can be a public auditor with the ability to authenticate the outsourced data for its integrity, dependency and independency on behalf of the owners of the data at regular times or on request. As in the current public cloud storage review schemes [3,4,6,7,10,11,12,15,44,51], we consider the TPA as an exciting prospect. The TPA can offer results that are credible and independent in auditing but potentially inquisitive on cloud data nature and generators of identity data. The CSP is widely reflected as a semi-trusted model that can offer on-demand and scalable services on data storage in normal circumstances. For hiding the information corruption reality, the CSP can facilitate TPA attacks like Forge attack Replacing attack, etc.

In general, two cloud data auditing models exist, one to be private auditing [52,53] and the other is public auditing[5,51]. In private auditing, the authentication has been performed between CSPs and users but during the public audit a certified third-party auditor (TPA) is presented to accomplish the authentication. An approach of multi-level authentication that is cloud-centric proposed as an approach for service that discusses and illustrates the efficacy of time and scalability constraints and shows its efficiency. The prime goal was to build a cloud-centered public safety network that is not based on resilience but reliability as well. Such a cyber-physical network was designed in order to allow seamless integration of physical and cyber elements (i.e. computing, sensing, networking and control) [54].

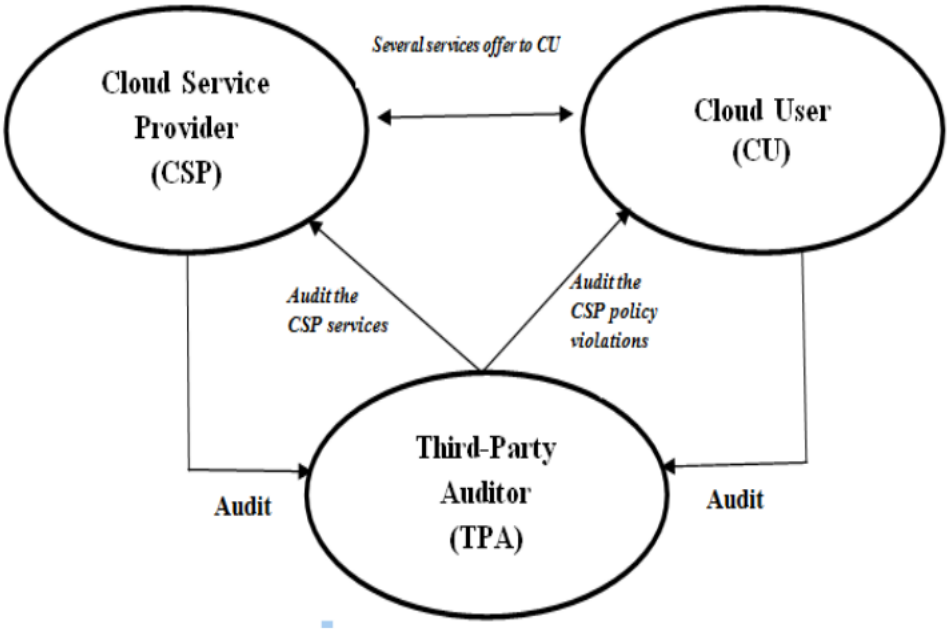

Figure 2: Privacy-Preserving Authentication system in Cloud Computing

To ensure a secure public safety network, privacy and security are required. Several systems have been allowed to ensure the shared data integrity for designing the public verifiers for efficiently auditing the integrity of data by collecting data from the cloud from all

individual clients. Unfortunately, the public audit for the credibility of the shared datamay expose the sensitive information of data owners to the TP auditor [55].

6. COMPARISON AND DISCUSSION ON THE RETROSPECT STUDIES

A comparative study was conducted on the basis of three factors namely Group signature, User revocation and Data Integrity. Comparisons from retrospect are provided for the cloud computing environment's problems and challenges from a period of 2015-2019. The insight processing outcomes form the composed reviewing articles which produced certain demonstration towards better efficiency solution. Thereafter, we compare the performance with fairly standard approaches that are the best suitable schemes for Cloud computational system performance in providing Group signature, User revocation and Data Integrity to its user's.

Table 1: Issues and limitations in a cloud computing environment based on Group signature, User revocation, and Data Integrity

Factors	Year	Issues sorted	Limitations	References
Group signature	2018	Each user can select a secret value privately	Public key infrastructure does not exist due to the usage of both partial and secret key	[20]
	2017	Improved secured scheme for the security issues	validation was proved to be suggestible for the IoT end-devising alone	[22,23,24]
	2016	Public audit systems for shared cloud data concealed group members' identities	computational burden reduction and lightweight authenticator generation had not been proved	[25][26]
	2015	Regenerating-coded data only provided private auditing	Constant proof of integrity remains an open issue	[9,11,27]
User revocation	2018	provided better security by the fully-secure scheme	processing was more affordable and efficient for mobile devices alone	[30, 31]
	2017	Resistant against cheating and collusion attacks	data sharing in the cloud, or secure communication was limited	[32]
	2016	Improved backward secrecy with efficiency attributes revocation	the model seems to be weak or lack of efficiency in user revocation	[33,34,35]
	2015	the experimental outcome showed low overhead on computation, communication, and storage	attribute/user revocation was not achieved effectively	[36,37]

Data Integrity	2019	comprehensive public auditing scheme proved better performance	have some problems for ensuring data integrity and usability	[41]
	2018	storage auditing scheme was provided	the scheme was not conducted real-time environment	[21]
	2017	Multi scheme stated that supports the integrity verification	The scheme was not proved to be efficient.	[42,43,44,45]
	2016	The validity of the public key used to create re-encryption keys	Schemes for incorporating additional features such as indexing, deduplication were not strongly applied.	[46,47,48]
	2015	Adaptive/secure scheme models developed	each task may require specific security services	[49, 50]

6.1. Discussion of Retrospect studies

The retrospect sought to review of above articles had their proposed scheme verifying protocols with 1) Group Signature Management 2) User revocationand3) integrity of data. From the findings of reviewed studies particularly from 2018-2015, it was evident that the performance was evaluated based upon Communication cost, Computation cost and effectiveness Group signature[9, 11, 20, 22-27]. Some studies reflected the initial cloud setup and private key generation were numerically analyzed based on three main phases 1) The phase of Authenticator Generation 2) The phase of Auditing and 3) The User Revocation [30-37].

Majority of 2015 studies reported that Cloud and their components environment had specific security services towards attribute/user revocation that was not achieved effectively. Conclusively, the constant-sized integrity proofs remain an open problem. From the 2016 literature studies established the theoretical review and empirical results suggesting that the recommended scheme was appropriate for sharing data in cloud under resource-restricted environment. Whereas in 2017 studies, the issues of data synchronization were prioritized and multi-level schemes were developed that supported the integrity verification for cloud data against cheating and collusion attacks. In certain 2018 studies, the security issues of user with storage auditing suggested a major requirement for better performance in group signature particularly concerned with user revocation, still, the schemes were not demonstrated in a

real-time environment. Based on the findings, a research agenda for cloud computing is drawn up to support study for the development of conceptual and heuristic techniques to provide enhanced user management and data security.

6.2. Research Gaps Reports

The research gaps identified on the group signature, data integrity and user revocations are as follows:

- Group signature: The group signature generation was the most important phase of the multiuser cloud. Over the years, various techniques were implemented to address the security issues on cloud accessibility. However, still there are issues of computational overhead which increase as the users increases. In general, there is a need for a complex signature that can resist any attacks.
- User revocation: The user revocation is the fundamental process that ensures the proper management of the cloud. Even though several revocation models were integrated into the security frameworks, the major issues evolved in the form of overheads due to recurrent change in the user end.
- Data integrity: The preservation of data integrity is an important aspect of the multiuser cloud environment. Many researches proposed several integrative techniques for verifying the integrity of the cloud data. However, there is some implementation problem that includes the overheads on key generation and computation along with communication overhead in maintaining the data integrity and its usability.

7. CONCLUSION

The significance of cloud computing was explored in this retrospect, yet there are several threats related with the process and procedure cloud computing. This paper also illustrated the group signature, data integrity and user revocation problem that were compared with the existing schemes in the cloud computing environment. Different data protection schemes/techniques and models have been defined that show their impact on cloud computing. The current Public Verifier will verify the integrity of the shared data and will not recover the complete data, but some of the shared data will be re-signed via the cloud itself. This system allows for batch auditing by synchronizing multiple tasks. In most of the schemes or framework, it was observed that the issues on computation and communication overhead persist along with its effectiveness. These overhead escalates with the growing number of users in groups. Henceforth, there is a need for the robust framework to address these issues effectively.

REFERENCES

[1] Khan, M. A. (2016). A survey of security issues for cloud computing. Journal of Network and Computer Applications, 71, 11–29.doi:10.1016/j.jnca.2016.05.010

[2] Hao, Z., Zhong, S., & Yu, N. (2011). A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability. IEEE transactions on Knowledge and Data Engineering, 23(9), 1432-1437.

[3] Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on computers, 62(2), 362-375.

[4] Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2017). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 12(4), 767-778.

[5] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling public auditability and data dynamics for storage security in cloud computing. IEEE transactions on parallel and distributed systems, 22(5), 847-859.

[6] Yang, K., &Jia, X. (2013). An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. IEEE Trans. Parallel Distrib. Syst., 24(9), 1717-1726.

[7] Zhu, Y., Ahn, G. J., Hu, H., Yau, S. S., An, H. G., & Hu, C. J. (2013). Dynamic audit services for outsourced storages in clouds. IEEE Transactions on Services Computing, 6(2), 227-238.

[8] Barsoum, A. F., &Hasan, M. A. (2015). Provable Multicopy Dynamic Data Possession in Cloud Computing Systems. IEEE Trans. Information Forensics and Security, 10(3), 485-497.

[9] Liu, C., Ranjan, R., Yang, C., Zhang, X., Wang, L., & Chen, J. (2015). MUR-DPA: top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud. IEEE Transactions on Computers, (9), 2609-2622.

[10] Jiang, T., Chen, X., & Ma, J. (2016). Public integrity auditing for shared dynamic cloud data with group user revocation. IEEE Transactions on Computers, 65(8), 2363-2373.

[11] Wang, B., Li, B., & Li, H. (2015). Panda: Public auditing for shared data with efficient user revocation in the cloud. IEEE Transactions on services computing, 8(1), 92-106.

[12] Yuan, J., & Yu, S. (2015). Public integrity auditing for dynamic data sharing with multiuser modification. IEEE Transactions on Information Forensics and Security, 10(8), 1717-1726.

[13] Tian, H., Nan, F., Chang, C. C., Huang, Y., Lu, J., & Du, Y. (2019). Privacy-preserving public auditing for secure data storage in fog-to-cloud computing. Journal of Network and Computer Applications, 127, 59-69.

[14] Zhang, Q., Wang, X., Yuan, J., Liu, L., Wang, R., Huang, H., & Li, Y. (2018). A hierarchical group key agreement protocol using orientable attributes for cloud computing. Information Sciences.

[15] Wang, B., Li, B., & Li, H. (2014). Oruta: Privacy-preserving public auditing for shared data in the cloud. IEEE transactions on cloud computing, 2(1), 43-56.

[16] Liu, C., Chen, J., Yang, L. T., Zhang, X., Yang, C., Ranjan, R., &Kotagiri, R. (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.

[17] Wang, H., & Zhang, Y. (2014). On the knowledge soundness of a cooperative provable data possession scheme in multicloud storage. IEEE Transactions on Parallel and Distributed Systems, 25(1), 264-267.

[18] Huang, L., Zhang, G., & Fu, A. (2016). Privacy-preserving public auditing for dynamic group based on hierarchical tree. Journal of Computer Research and Development, 53(10), 2334-2342.

[19] Yu, Y., Ni, J., Au, M. H., Mu, Y., Wang, B., & Li, H. (2015). Comments on a public auditing mechanism for shared cloud data service. IEEE Transactions on Services Computing, 8(6), 998-999.

[20] Li, J., Yan, H., & Zhang, Y. (2018). Certificateless public integrity checking of group shared data on cloud storage. IEEE Transactions on Services Computing.

[21] Hu, A., Jiang, R., &Bhargava, B. (2018). Identity-Preserving Public Integrity Checking with Dynamic Groups for Cloud Storage. IEEE Transactions on Services Computing.

[22] Wang, Z. (2017). Provably secure key-aggregate cryptosystems with auxiliary inputs for data sharing on the cloud. Future Generation Computer Systems.

[23] Patranabis, S., Shrivastava, Y., &Mukhopadhyay, D. (2017). Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud. IEEE Transactions on Computers, 66(5), 891-904.

[24] Sabitha, S., &Rajasree, M. S. (2017). Access control based privacy preserving secure data sharing with hidden access policies in cloud. Journal of Systems Architecture, 75, 50-58.

[25] Zhang, Y., Zheng, D., Chen, X., Li, J., & Li, H. (2016). Efficient attribute-based data sharing in mobile clouds. Pervasive and Mobile Computing, 28, 135-149.

[26] Yang, G., Yu, J., Shen, W., Su, Q., Fu, Z., &Hao, R. (2016). Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability. Journal of Systems and Software, 113, 130-139.

[27] Liu, J., Huang, K., Rong, H., Wang, H., & Xian, M. (2015). Privacy-preserving public auditing for regenerating-code-based cloud storage. IEEE transactions on information forensics and security, 10(7), 1513-1528.

[28] Zhang, Y., Yu, J., Hao, R., Wang, C., &Ren, K. (2018). Enabling efficient user revocation in identity-based cloud storage auditing for shared big data. IEEE Transactions on Dependable and Secure Computing.

[29] Yu, Y., Li, Y., Ni, J., Yang, G., Mu, Y., &Susilo, W. (2016). Comments on "public integrity auditing for dynamic data sharing with multiuser modification". IEEE Transactions on Information Forensics and Security, 11(3), 658-659.

[30] Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. Computers & Security, 72, 1-12.

[31] Luo, Y., Xu, M., Huang, K., Wang, D., & Fu, S. (2018). Efficient auditing for shared data in the cloud with secure user revocation and computations outsourcing. Computers & Security, 73, 492-506.

[32] Ahuja, R., Mohanty, S. K., & Sakurai, K. (2017). A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing. Computers & Electrical Engineering, 57, 241-256.

[33] Han, K., Li, Q., & Deng, Z. (2016). Security and efficiency data sharing scheme for cloud storage. Chaos, Solitons& Fractals, 86, 107-116.

[34] Li, Q., Ma, J., Li, R., Liu, X., Xiong, J., & Chen, D. (2016). Secure, efficient and revocable multi-authority access control system in cloud storage. Computers & Security, 59, 45-59.

[35] Zhang, J., & Dong, Q. (2016). Efficient ID-based public auditing for the outsourced data in cloud storage. Information Sciences, 343, 1-14.

[36] Liu, J., Huang, X., & Liu, J. K. (2015). Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption. Future Generation Computer Systems, 52, 67-76.

[37] Dong, X., Yu, J., Zhu, Y., Chen, Y., Luo, Y., & Li, M. (2015). SECO: Secure and scalable data collaboration services in cloud computing. computers& security, 50, 91-105.

[38] Kolhar, M., Abu-Alhaj, M. M., & El-atty, S. M. A. (2017). Cloud data auditing techniques with a focus on privacy and security. IEEE Security & Privacy, 15(1), 42-51.

[39] Li, J., Liu, Z., Chen, X., Xhafa, F., Tan, X., & Wong, D. S. (2015). L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing. Knowledge-Based Systems, 79, 18-26.

[40] Sookhak, M., Gani, A., Talebian, H., Akhunzada, A., Khan, S. U., Buyya, R., &Zomaya, A. Y. (2015). Remote data auditing incloud computing environments: a survey, taxonomy, and open issues. ACM Computing Surveys (CSUR), 47(4), 65.

[41] Tian, H., Nan, F., Jiang, H., Chang, C. C., Ning, J., & Huang, Y. (2019). Public auditing for shared cloud data with efficient and secure group management. Information Sciences, 472, 107-125.

[42] Yi, M., Wei, J., & Song, L. (2017). Efficient integrity verification of replicated data in cloud computing system. Computers & Security, 65, 202-212.

[43] Li, R., Asaeda, H., Li, J., & Fu, X. (2017). A distributed authentication and authorization scheme for in-network big data sharing. Digital Communications and Networks, 3(4), 226-235.

[44] Shen, W., Yu, J., Xia, H., Zhang, H., Lu, X., &Hao, R. (2017). Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium. Journal of Network and Computer Applications, 82, 56-64.

[45] Zhang, J., Liu, Q., Hu, Z., Lin, J., & Yu, F. (2017). A multi-server information-sharing environment for cross-party collaboration on a private cloud. Automation in Construction, 81, 180-195.

[46] Razaque, A., &Rizvi, S. S. (2016). Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment. Computers & Security, 62, 328-347.

[47] Canard, S., &Devigne, J. (2016). Highly privacy-protecting data sharing in a tree structure. Future Generation Computer Systems, 62, 119-127.

[48] Jiang, R., Wu, X., &Bhargava, B. (2016). SDSS-MAC: Secure data sharing scheme in multi-authority cloud storage systems. Computers & Security, 62, 193-212.

[49] Liang, K., Au, M. H., Liu, J. K., Susilo, W., Wong, D. S., Yang, G., ...& Yang, A. (2015). A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. Future Generation Computer Systems, 52, 95-108.

[50] Yang, J. J., Li, J. Q., &Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Generation Computer Systems, 43, 74-86.

[51] Tian, H., Chen, Z., Chang, C. C., Huang, Y., Wang, T., Huang, Z. A., .& Chen, Y. (2018). Public audit for operation behavior logs with error locating in cloud storage. Soft Computing, 1-14.

[52] Erway, C. C., Küpçü, A., Papamanthou, C., &Tamassia, R. (2015). Dynamic provable data possession. ACM Transactions on Information and System Security (TISSEC), 17(4), 15.

[53] Sebé, F., Domingo-Ferrer, J., Martinez-Balleste, A., Deswarte, Y., &Quisquater, J. J. (2008). Efficient remote data possession checking in critical information infrastructures. IEEE Transactions on Knowledge and Data Engineering, 20(8), 1034-1038.

[54] Butun, I., Erol-Kantarci, M., Kantarci, B., & Song, H. (2016). Cloud-centric multi-level authentication as a service for secure public safety device networks. IEEE Communications Magazine, 54(4), 47-53.

[55] Fu, A., Yu, S., Zhang, Y., Wang, H., & Huang, C. (2017). NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users. IEEE Transactions on Big Data.