International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 24 Issue 05, MAY, 2024

PRIVACY PRESERVING A DATA SHARING WITH A SECURE GROUP MANGEMENT

Saba Sultana[1], Jothi kumar[2], Md Ateeq Ur Rahman[3]
Research Scholar, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086
6sabasultana@gmail.com
Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086
drjothikumarr@gmail.com
Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086
mail_to_ateeq@yahoo.com

ABSTRACT

Users can keep their data in the cloud and easily access it from anywhere at any time with cloud storage services. However, because consumers no longer have direct access to their data when it is kept in the cloud, there is a risk of data loss. Numerous cloud storage auditing techniques have been researched as a solution to this issue. A public auditing system for shared data was put up by Tian et al. in 2019 and enables data privacy, identity traceability, and group dynamics. In this work, we highlight how their scheme is vulnerable to assaults including tag fabrication or proof forgery, which means that even if the cloud server has destroyed some outsourced data, the strategy will still be insecure, It is nevertheless capable of producing reliable evidence that the server had accurately stored the data. Then, we suggest a brand-new design that offers the same features and is safe against the threats. In addition, we compare the outcomes' calculation and communication costs to those of competing systems.

1. INTRODUCTION

Users may access their saved data easily, and cloud storage offers benefits including cost savings, scalability, and a large amount of storage space. As a result, both businesses and individuals frequently use cloud storage that is managed and maintained by qualified cloud service providers (CSPs) [1]. Clients no longer have direct control over the stored files once the data is in cloud storage. Despite this, the CSPs must make sure that the client data is stored in the cloud without being altered in any way. The simplest approach to do this is to confirm the saved data's integrity after downloading. Many ways for ensuring the integrity of the data saved in the cloud without a full download have been presented [2]-[34] because it is highly inefficient when the capacity of the stored data is considerable. These methods, which go by the name of cloud storage auditing, can be divided into two categories based on the integrity verification: private auditing and public auditing. In private auditing, users who are the proprietors of the stored data carry out the verification. A third-party auditor (TPA) performs public auditing on behalf of consumers to lessen their workload, and as a result, public auditing schemes are more frequently used for cloud storage auditing. Depending on the setting, public auditing programmes offer different benefits, such as maintaining privacy. [5–9], data dynamics [10–13], and shared data [14–33] are some examples. While shielding data information from the TPA, privacy-preserving auditing is utilised to conduct an integrity verification, and dynamic data auditing allows authorised users to freely add, delete, or modify the stored data. Shared data auditing refers to the unrestricted sharing of data among authorised users. In this situation, it is important to design a legitimate user group and give serious thought to user addition and revocation. Schemes that fulfil identity traceability—a concept that can track the strange behaviour of legitimate people—have recently been developed. It has also been suggested that users participate in shared data auditing. A plan that facilitates identity traceability, data dynamics, and privacy preservation in shared data auditing was put up by Tian et al. [25]. The authors used the lazy revocation technique for effective user enrollment and cancellation. Additionally, they adopt a technique in which the group manager manages messages and tag blocks produced by the revoked user to the scheme in order to secure the design against collusion attempts between the revoked user and server. Because the method uses the lazy-revocation technique, even if a user is revoked, no further operations take place until new changes are made to the block. Using two types of attacks—a tag fabrication and a proof forgery—we demonstrate in this study that Tian et al.'s approach [25] is insecure. We then present a new technique that offers the same functionality and is secure against the aforementioned assaults. In this technique, a tag forgery is achievable by taking use of the malleability with which the tag is formed, and a proof forgery is possible by taking advantage of the secret value that is exposed to the

server when further changes to the block take place after the user's authorization has been revoked. The contributions of this study, in general, can be summed up as follows: 1. We demonstrate that Tian et al.'s approach [25] is vulnerable to both tag forgeries and proof forgeries. We demonstrate tag forgery, where an attacker can produce a legitimate tag for the altered message without being aware of any secret information. We demonstrate proof forging in which an attacker can produce a legitimate proof for a challenged message even if some cloud-stored files have been erased. 2. We create a brand-new public auditing system that is safe from the aforementioned assaults and has the same features, such identity tracing, data sharing, and privacy preservation. We modified the data proof generating approach to improve privacy preservation and the tag generation method to get rid of the malleable property. In order to safeguard the confidential information from the CSP, we also modified the lazy revocation procedure and put forth a flexible active revocation approach. 3. We formally establish the suggested scheme's security. The theorems state that the attacker is unable to produce a valid proof or tag without first knowing the secret values or the original communications, respectively. In terms of computing and communication costs, we also present comparative findings with other methods. The remainder of this essay is structured as follows.

2. RELATED WORK

First, Ateniese et al. [2] presented two provably secure PDP techniques that make use of RSA-based homomorphic authenticators. They also established a provable data possession mechanism known as PDP. As a result, public verification is supported with less expensive communication and processing. At the same time, Juels et al. [3] introduced the idea of proof of retrievability (POR), a formal security model, and a sentinel-based POR scheme with specific qualities. A new public auditing system that was based on the BLS signature [36] and is secure in the random oracle model was later proposed by Shacham et al. [4] after Shacham et al. [4] upgraded the POR scheme. Numerous studies on cloud storage auditing have been undertaken recently. enabling a range of features including shared data, data dynamics, and data privacy preservation. The PDP technique using a rank-based authenticated skip list to facilitate data dynamics was first proposed by Erway et al. [10]. High computational and transmission costs are a problem for the technique, so Wang et al. [11] suggested a new auditing scheme using the Merkle Hash Tree (MHT), which is considerably easier to use. However, this plan does not offer data privacy; in other words, it is unable to guarantee data confidentiality when being audited by a third party (TPA). Despite the fact that Wang et al.'s [5] proposed a public auditing methodology that protects privacy, their method involves significant communication and computation expenses during the audit and data updating processes. Zhu and co. [12] a novel strategy using an index hash table (IHT), another authenticated data structure, was also put out to handle data dynamics.

For shared data, Wang et al. [14] introduced Knox, an effective public auditing system. The system permits user revocation but does not provide user identity concealment based on a group signature. A ring signature is employed in Oruta [15] to conceal the identities of specific users; however, the technique also contains a flaw in that all user keys and to provide a user revocation, block tags must be produced from scratch. A strategy to achieve a user revocation utilising a proxy re-signature was also put out by Wang et al. [16]. The system makes use of a proxy for resigning in order to update the tag created by the revoked user, however it is susceptible to collusion attacks between an erroneous user and the cloud server. A new public auditing approach that combines a vector commitment [37] and a verifier-local-revocation group signature was also proposed by Jiang et al. [38].

Because it is necessary to first locate and recreate the tags created by the revoked user, the computational costs associated with the revocation step are relatively significant. A brand-new system utilising polynomial authentication tags and proxy re-signatures was also proposed by Yu et al. [18], [19]. This method can decrease the amount of communication required for verification, but it is vulnerable to a collusion attack because the revoked user still has access to a valid private key and might work in concert with the CSP. Another cloud storage auditing system based on group signatures for data sharing was then proposed. [20]–[33]. Wu et al. [24] developed a threshold privacy-preserving cloud storage auditing technique that is more effective than existing schemes utilising complex cryptographic primitives since it does not rely on a group or ring signature. A novel technique with an oblivious transfer and stateless sluggish re-encryption was also put up by Chang et al. [26] to offer an effective user revocation. The majority of these research have the issue that it is possible to obtain private data.

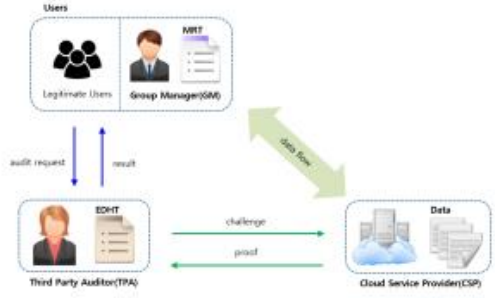


FIGURE 1. System Model.

A feasible identity-based shared data integrity auditing approach employing a sanitizable signature [39] was presented by Shen et al. [22] to address this. Since any user can access the shared data, the technique can be vulnerable because it requires a secure link between the data owner and the sanitizer. A PP-CSA approach for data sharing was developed by Xu et al. [27], in which only the authorised user may access the data and there is no requirement for between the owner of the data and the sanitizer, create a secure link. These methods have disadvantages in that they don't offer data dynamics or user renunciation, which makes it difficult to conceal critical information. A more secure auditing technique [34] that provides forward security as well as the integrity auditing scheme [35] employing keywords in encrypted data have also recently been developed, however these schemes are not appropriate for our target scenario. Only the strategy proposed by Tian et al. [25] satisfies the security among the many strategies that have been proposed. We draw attention to the security flaw in Tian et al.'s plan [25] and suggest a better one.

3.OBJECTIVE

These methods are referred to as cloud storage auditing, and they fall under the categories of private auditing and public auditing, respectively. In private auditing, users who are the proprietors of the stored data carry out the verification. A third-party auditor (TPA) performs public auditing on behalf of consumers to lessen their workload, and as a result, public auditing schemes are more frequently used for cloud storage auditing.

4. SCOPE OF THE PAPER

The paper scope allows us to concentrate primarily on security. We have a situation where consumers lose direct control over their data when they store it in the cloud, increasing the danger of data loss. We have developed a solution that offers the same functionalities and is safe from the aforementioned assaults.

5. LITERATURE SURVEY

Identity the Privacy-preserving public auditing for data storage security in cloud computing

Cloud Computing is the long-dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third-party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third-party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

Identity-preserving public auditing for shared cloud data

Cloud storage enables users to remotely store their data and share the data through the cloud. Existing integrity auditing schemes for shared data are often not identity-preserving and have high auditing cost, and hence are still far from practical application. In this work, we propose a public auditing scheme for shared data in cloud storage with identity privacy preservation. To preserve identity privacy against the auditor, we convert signatures computed by different users into signatures computed by the challenge user with proxy re-signature. Our scheme supports user revocation without re-signing signatures computed by revoked users, while the integrity of shared data can still be correctly checked. Furthermore, the auditing is efficient in the sense that the number of pairing operations during auditing is independent of the number of challenged blocks and users. We further present a batch auditing supporting multiple auditing delegations from different groups instead of only the same group. Security analysis demonstrates that our scheme is provably secure. Numeric analysis and simulation results show that both computation and communication costs of our scheme are lower than in existing schemes.

Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability

Nowadays, has been widely adopted by diverse organizations, through which users can conveniently share data with others. For security consideration, previous public auditing schemes for shared cloud the

identities of group members. However, the unconstrained identity anonymity will lead to a new problem, that is, a group member can maliciously modify shared data without being identified. Since uncontrolled malicious modifications may wreck the usability of the shared data, the identity traceability should also be retained in data sharing. In this paper, we propose an efficient public auditing solution that can preserve the identity privacy and the identity traceability for group members simultaneously. Specifically, we first design a new framework for data sharing in cloud, and formalize the definition of the public auditing scheme for shared cloud data supporting identity privacy and traceability. And then we construct such a scheme, in which a group manager is introduced to help members generate to protect the identity privacy and two lists are employed to record the members who perform the latest modification on each block to achieve the identity traceability. Besides, the scheme also achieves data privacy during authenticator generation by utilizing blind signature technique. Based on the proposed scheme, we further design an auditing system for practical scenarios. Finally, we prove the proposed scheme is secure based on several security requirements, and justify its performance by concrete implementations.

Shared dynamic data audit supporting anonymous user revocation in cloud storage

Collusion between revoked users and cloud service providers can pose a threat to the security of cloud storage data. If the original legitimate users cannot be revoked securely, it will lead to the leakage of shared data, thus affecting the security of cloud storage. In this paper, we combine vector commitment and anonymous revocation of group signature to propose an integrity audit scheme for cloud storage data that can support data modification. The anonymity of the group signature ensures that users' privacy information will not be snooped by the server. The proposed scheme supports the dynamic operation of stored data by legitimate group users besides data owners. When the user behaves improperly, the membership can be revoked by the group manager. After the user-modified data is stored in the cloud, whether the cloud server correctly stores the data can be audited by a trusted third party. Security analysis and experimental results demonstrate that our scheme is secure and efficient.

An efficient public auditing protocol with novel dynamic structure for cloud data

With the rapid development of cloud computing, cloud storage has been accepted by an increasing number of organizations and individuals, therein serving as a convenient and on-demand outsourcing application. However, upon losing local control of data, it becomes an urgent need for users to verify whether cloud service providers have stored their data securely. Hence, many researchers have devoted themselves to the design of auditing protocols directed at outsourced data. In this paper, we propose an efficient public auditing protocol with global and sampling blockless verification as well as batch auditing, where data dynamics are substantially more efficiently supported than is the case with the state of the art. Note that, the novel dynamic structure in our protocol consists of a doubly linked info table and a location array. Moreover, with such a structure, computational and communication overheads can be reduced substantially. Security analysis indicates that our protocol can achieve the desired properties. Moreover, numerical analysis and real-world experimental results demonstrate that the proposed protocol achieves a given efficiency in practice.

Identity the Privacy-preserving public auditing for shared data in the cloud

In the cloud, data is often shared by a group of users. To ensure the long-term correctness of cloud shared data, a third-party public verifier can be introduced to audit data integrity. During the auditing, protecting the privacy of the contributors of shared data from the public auditor is a fundamental issue. However, this makes it challenging to simultaneously support group membership dynamics efficiently, due to the significant amount of computation needed to update the signatures on shared data. In this paper, we propose a novel privacy-preserving public auditing mechanism for shared cloud data. With our proposed mechanism, a public verifier is able to audit the integrity of shared data without retrieving the entire data from the cloud, and also without learning private identity information of the group members. Group dynamics (user join and user revocation) are efficiently handled by outsourcing signature updating operations to the cloud via a secure proxy re-signature scheme. Experimental results show that our mechanism is highly efficient for dynamic groups.

6. PROPOSED SYSTEM

- We note that their system is vulnerable to tag forgery or proof forgery attacks in this study, which means that even if the cloud server has erased certain data, it can still produce reliable evidence that the server had correctly saved the data.
- Then, we suggest a brand-new design that offers the same features and is safe against the aforementioned threats.
- Clients no longer have direct control over their data once it is stored in the cloud. Despite this, the CSPs must make sure that the client data is stored in the cloud without being altered.

6.1 PROPOSED SYSTEM ADVANTAGE

- Stronger authentication
- Easy communication between group manager and group user.
- Any user can access the shared data

7. METHODOLOGIES

1. User Interface Design

We create the project's windows in this module. All users use these windows to log in securely. Users must provide their username and password in order to connect to the server, and only then will they be permitted to do so. If a user already has an account, they can log in directly; otherwise, they must register their username, password, and email address with the server. In order to maintain the upload and download rates, the server will create an account for each user. The user id will be set to name. Typically, logging in is required to access a particular website.

2. Group Member

Members of the group can sign up and then log in. Members of the group may also upload files. My files are visible to group members. Each group member has access to every file. Members of the group may also access requested files. The group member may also have the choice to let a user go.

3. Group Manager

The Group Manager may additionally log in. A group may be created by a group manager. A group's manager can see its members. A file is visible to the group manager. The group manager also has a delete groups option.

4. Third Party Auditor

Someone else may log in. A third party may request an audit after logging in.

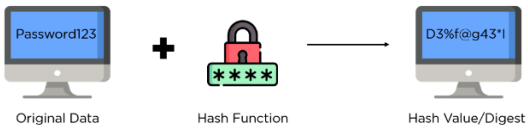
5. Cloud Storage Server

An audit-proof server for cloud storage is available. A group member may also be deleted by the cloud storage server.

8. Proposed Algorithm

SHA Algorithm

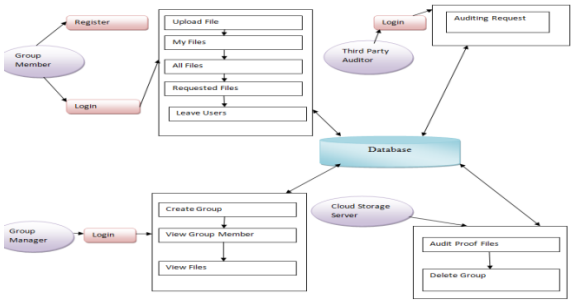
The plaintext is transformed into the appropriate hash digest using the hash function. Since they are intended to be irreversible, your digest should not, under any circumstances, provide you access to the original plaintext. No matter how many times they are used, hash functions always produce the same result when the input is left untouched.



In our project, SHA 256 is employed. The 256 in the name denotes the final hash value, which means that regardless of the size of the plaintext, the hash value will always be 256 bits.

The other SHA family algorithms are somewhat comparable to SHA 256. Look into learning a little more about their rules right now.

9. SYSTEM ARCHITECTURE



Members of this Group may register before logging in. Each group member has the ability to upload a file. All files are visible to group members. Each group member has access to all files. Each group member may request specific files. Members of the group have the option of leaving users with access to all database data. The group manager may have a login as well. He will create a group members after logging in. The group manager can see every member of the group. The group manager can see a file as well. Also capable of deletion is the group manager. Anyone may log in. Third parties can see audit requests after logging in. All cloud server information is stored in a server, and we are kept in a Mysql database.

10. RESULTS AND DISCUSSION

Fig 1 Group Member Home

Members of the group can sign up and then log in. Members of the group may also upload files. My files are visible to group members.

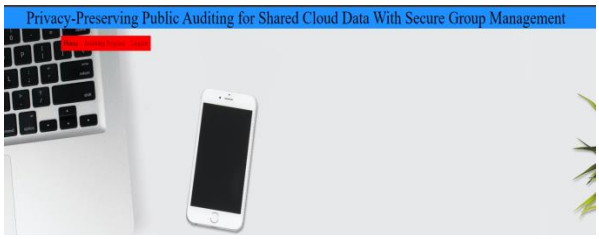


Fig 2: TPA Home

Someone else may log in. A third party may request an audit after logging in

Fig 3 Cloud Home Page

An audit-proof server for cloud storage is available. A group member may also be deleted by the cloud storage server.

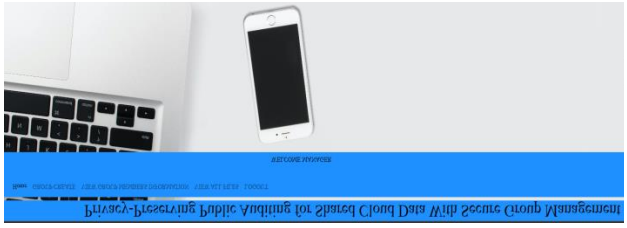


Fig 4 Manager Home page

The group manager may have a login as well. He will create a group members after logging in. The group manager can see every member of the group. The group manager can see a file as well. Also capable of deletion is the group manager.

11. CONCLUSION

An essential method for addressing the issue of guaranteeing the integrity of data saved in cloud storage is cloud storage auditing. Numerous schemes with various functionalities and security levels have been presented since there is a widespread need for the concept. In suggested a system that allows identity tracing, group dynamics, and data privacy, and they asserted that their system is secure from collusion attacks between CSPs and users who have had their access terminated. In this publication, even though some of the challenges have been omitted, we demonstrated the SHA algorithm in their scheme. Then, we suggested a brand-new design that offers the same functionality as their strategy while being safe from the aforementioned threats. Additionally, we included security justifications and a comparison of the two techniques' computation costs.

The Future Enhancement of the project is a way for us to increase security and get the group's approval. it is sufficient to demonstrate that a legitimate poof may be simulated in the random SQL attacks without any block information.

REFERENCES

[1] (Apr. 2021). Cloud Storage-Global Market Trajectory and Analytics. [Online]. Available:
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ``Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598_609.
[3] A. Juels and B. S. Kaliski, ``PORs: Proofs of retrievability for large _les," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Oct. 2007, pp. 584_597.
[4] H. Shacham and B. Waters, ``Compact proofs of retrievability," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Berlin, Germany: Springer, 2008, pp. 90_107.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, ``Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1_9.
[6] Z. Hao, S. Zhong, and N. Yu, ``A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432_1437, Sep. 2011.
[7] K. Yang and X. Jia, ``An ef_cient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717_1726, Sep. 2013.
[8] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacypreserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362_375, Feb. 2013.
[9] K. He, C. Huang, K. Yang, and J. Shi, ``Identity-preserving public auditing for shared cloud data," in Proc. IEEE 23rd Int. Symp. Quality Service (IWQoS), Jun. 2015, pp. 159_164.
[10] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, ``Dynamic provable data possession," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2009, pp. 213_222.
[11] Q.Wang, C.Wang, K. Ren,W. Lou, and J. Li, ``Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847_859, May 2011.
[12] 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 Trans. Services Comput., vol. 6, no. 2, pp. 227_238, Apr./Jun. 2013.
[13] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ``An ef_cient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402_2415, Oct. 2017.
[14] B. Wang, B. Li, and H. Li, ``Knox: Privacy-preserving auditing for shared data with large groups in the cloud," in Proc. 10th Interfaces Conf. Appl. Crypto. Netw. Secur., 2012, pp. 507_525.
[15] B. Wang, B. Li, and H. Li, ``Oruta: Privacy-preserving public auditing for shared data in the cloud," IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43_56, Jan./Mar. 2014.
[16] B. Wang, B. Li, and H. Li, ``Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92_106, Jan./Feb. 2015.
[17] T. Jiang, X. Chen, and J. Ma, ``Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Trans. Comput., vol. 65, no. 8, pp. 2363_2373, Aug. 2016.
[18] J. Yuan and S. Yu, ``Efficient public integrity checking for cloud data sharing with multi-user modi_cation," in Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM), Apr. 2014, pp. 2121_2129.
[19] J. Yuan and S. Yu, ``Public integrity auditing for dynamic data sharing with multiuser modification," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1717_1726, Aug. 2015.
[20] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ``Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, pp. 130_139, Mar. 2016.