Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/11192
DOI URL: http://dx.doi.org/10.21474/IJAR01/11192

RESEARCH ARTICLE

AN EXTENSIVE REVIEW ON DATA INTEGRITY SCHEMES AND SECURITY ISSUES IN CLOUD PARADIGM

Hariharan R[1], Komarasamy G[2] and Daniel Madan Raja S[3]

1. Department of Information Technology, Sri Ramakrishna Institute of Technology, Coimbatore.
2. Department of Computer Science and Engineering, Jain University, Bangalore.
3. Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam.

Manuscript Info

Manuscript History
Received: 15 April 2020
Final Accepted: 18 May 2020
Published: June 2020

Key words:-
Cloud Computing, Data Integrity, Security Storage, Privacy Preserving, Security Attacks

Abstract

In recent years, Cloud computing has gained incredible recognition. Because of the massive complexities and size of the cloud there is been a threat all the time to the data from the internal and external entities. Generally, internal entities are responsible for the theft data, this leads to audit the data integrity by the third party. Whereas the sensitive information was external entities kept in the cloud throughout the intellectual query fired up on the cloud. There were several tools and methodologies presented to attain any one of them out of these two main issues and extremely few exists to deal with both data integrity and sensitive information hiding simultaneously. A consecutive study of several existing schemes is provided too with a thorough probable security attacks discussion and their mitigations. This research approach exploits the scheme of managing both techniques thereby analyzing in depth the other pastworks.

Introduction:-

Cloud computing has developed as a model for a IT businesses to enhance the abilities on the hover deprived of investing more in new set-up, licensing new software or personals training [1]. NIST expresses Cloud computing as a "model for allowing convenient, ubiquitous, network access on demand to a common configurable computing pool properties that can be provisioned and delivered rapidly with negligible executive service provider or interaction effort" [2]. It follows a modest model of "pay as you go" that permits an association to recompense service only they employ. It eradicates the necessity for preserving an internal data center through the migration of data enterprise to the remote place at a site of Cloud provider. Minimal investment, quick disposition and cost reduction are primary issues that make enterprises to use Cloud services and permit them to emphasis lying on core business and priorities concern moderately than dealingwithpracticalproblems.Accordingto [3], 91%oftheEurope and US organizations decided that decrease in rate is a foremost motive for them to migrate to framework of Cloud.

Corresponding Author:-Hariharan R
Address:- Department of Information Technology, Sri Ramakrishna Institute of Technology, Coimbatore.

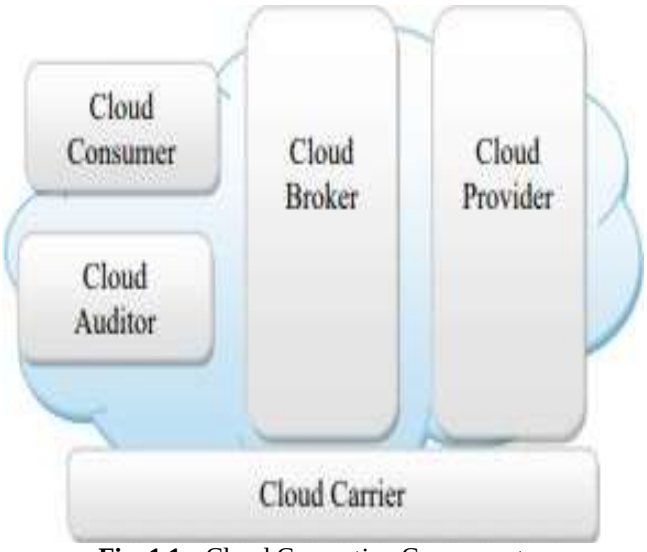

Fig. 1.1:- Cloud Computing Components.

In cloud computing there are five main components [4] depending on their contribution. Cloud auditor conduct an evaluation of cloud services in an independent manner, operations of system data, security and enactment of the implementation of cloud. A Cloud agent interacts among CSC and CSP for making business to be occurred. The carrier of Cloud offers cloud services with connectivity on behalf of CSC to CSP [5].

The size of cloud data is huge, entire file downloading to test out the integrity could be unaffordable in terms of bandwidth cost, and therefore, very unfeasible [6,7]. Furthermore, for data integrity checking conventional cryptographic primitives like authorization code (MAC), hash functions cannot be appropriate at this time directly because of the nonexistence of an original file copy for the verification purpose. In conclusion, examination of remote data integrity for the secure storage of cloud is desirable extremely in addition to a challenging topic ofresearch.

The paper is organized as follows. In Section 2, issues of cloud storage and the need of data integrity schemes are deliberated. Section 3 offers a thematic view of various data integrity models in cloud for auditing. In Section 4, privacy preserving pubic auditing for secure cloud storage was illustrated.Section 5 covers the system architecture ofdataIntegrityschemes. The conclusion and Future research directions in data integrity schemes are presented in Section 6.

Cloud storage issues and a need of data integrity schemes:

[2] Enhanced the issues of safety considerate connected with storage of cloud and highpoints the importance schemes of data integrity for the outsourced data. In this, of existing data integrity schemes taxonomy was presented to employ cloud storage. A relative investigation of present systems is provided also with a complete conversation on probable attacks of security with their mitigations. Moreover, design challenges were discussed like communication efficiency, computational efficiency, storage efficiency, and condensed I/O in these systems.

Presented a scheme with an objective to observe the state- of-the-art of PoR and afterward to recognize the problems of using PoR on cloud storage and recommend possible solutions. The available PoR schemes were analyzed. Then, the challenges and issues by using PoR exactly and cloud storage usually arelabeled.

Insisted an effectual auditing scheme of public integrity with comfortable workforce revocation of user depending on commitment vector and revocation verifier-local group signature. A concrete scheme is designed by a new structure recognized as Decrypt key, which offers reliability and effectively declaration for convergent key management on common user with sides of cloudstorage.

Proposed an identity based protected combined signatures (SIBAS) since the scheme of data integrity checking that resorts Trusted Execution Environment (TEE) as the auditor for checking the outsourced data in local side. SIBAS can not only check the outsourced data integrity, but then also attain the management of secure key in TEE over

Shamir's threshold system.

Projected a novel scheme of public verification for cloud storage with the use of in distinguishability complication, which needs a inconsequential calculation on the auditor and the envoy most computation to the cloud. Also, a scheme to support batch verification and data dynamic operations was presented, where several authentication tasks can be performed from different users efficiently by the auditor and the data of cloud-stored one can be dynamically updated. On comparing other existing works, this system reduces the auditor's computation overhead significantly. Furthermore, the overhead on batch verification of the auditor side is independent of verification tasks number in thisscheme.

Addressed the data integrity problem in Cloud computing through suggesting a system over which user are capable of checking the Cloud data integrity stored. Additionally, users can track the data integrity violation if happened. For this persistence, new concept was utilized relatively in Cloud computing termed "Provenance of Data". This system is capable of decreasing any third-party services requirement further support hardware and data items replication on consumer side for checkingintegrity.

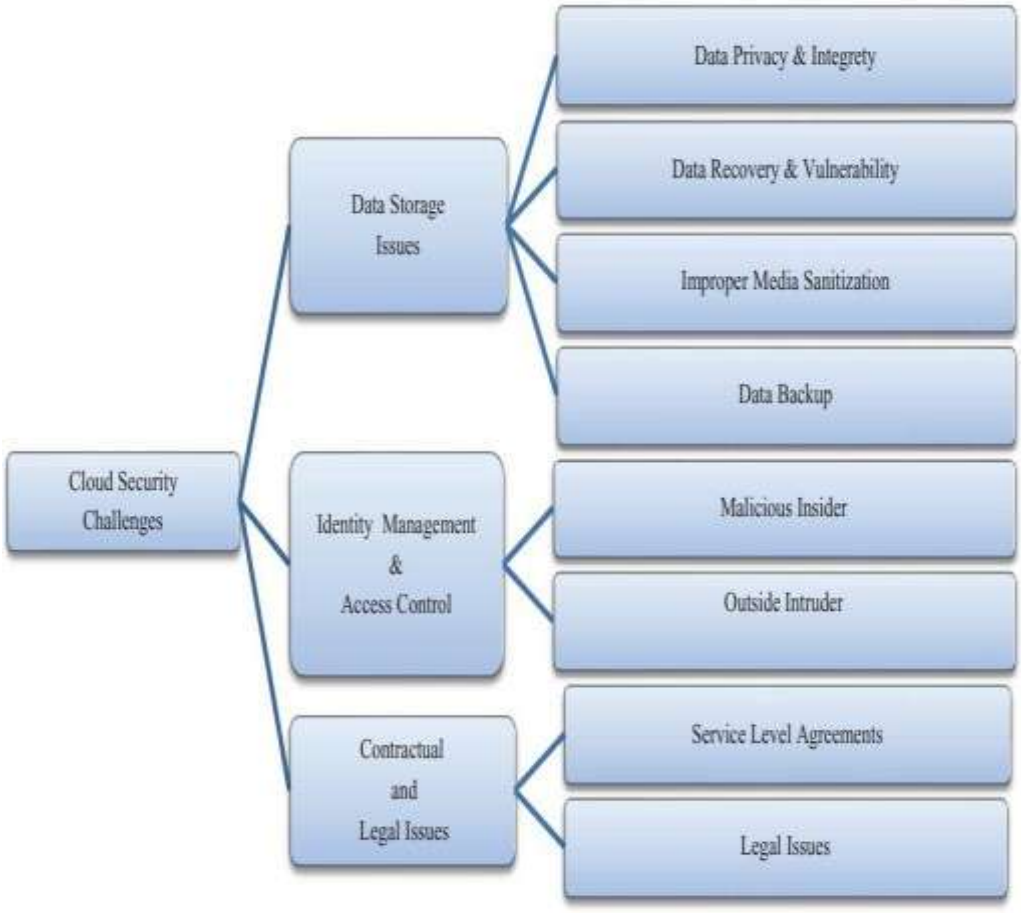

Fig 2.1:- Cloud security Challenges.

There are several kinds of attacks and threats are there in the infrastructure of cloud. The most significant cloud computing challenge is the "Security". Different security issues are as follows:

Confidentiality:
It refers to the eagerness status to depend of one party on another party to attain a intended goal. In a cloud environment, confidentiality issue is mainly based on the preferred utilization model, as data, processes, and applications control areoutsourced.

Data reliability:
Maintaining the reliability of cloud computing is considered as a major dispute to the cloud parties, as the coercion could be at the subscribers or providers level. To insure data integrity in the provider and subscriber level, a secure encryption algorithm could be used, but it could not get guaranteed that data wont changed through locating it in thecloud.

Accessibility:
The accessibility refers to the ability of the subscriber to retrieve all the information at anytime.

User authentication and authorization-Authentication refers to the procedure that will prove the users claimed exceptionality while they are trying to access any scheme. Authorization is the process of identifying the performance of the user. Loss of the authorization wills leads of cloudbreach.

Systemvulnerabilities:
Multi-tenancy-Secure sharing of the resources among theclients.

To overcome the security issues in the cloud computing several protocols are available but claiming of these protocols are very difficult. Hence in [12] an integrated model is used to ensure better Cloud security for Authentication and the multi- tenancy.

Table 1:- Possible Solutions of Data storage issues.

Authors	Proposed Scheme	Services	Privacy	Integrity	Availability	Confidentiality
L. Wei, H. Zhu	SecCloud,for Securing cloud data	EncryptionBilinear PairingSignature verification Trusted third party	Yes	Yes	No	Yes
Y. Tang, P.P. Lee, J.C.S.Lui	FADE, protocol for data privacy and integrity	Encryption Trusted third party Assured deletion Threshold secret sharing	Yes	Yes	No	Yes
Q.Liu,G.Wang	TimePRE, scheme for secure data sharingin cloud	Proxy re-encryption Attributebased encryption	Yes	No	No	Yes
Z. Tari	A methodology for security of resident data	Erasure correcting Code Data redundancy	No	Yes	Yes	Yes

Multi-tenancy depicts the sharing of virtualization and resources among the clients. As it permits several users to access similar property at the same time, there is high possibility of confidential data accessing devoid of good privileges.

Various models for data integrity auditingin cloud:
Suggested a scheme of extremely competent data integrity audit intended for cloud storage destined for applications of mobile health. The tag authentication for respective block of data produced through biosensor nodes is negligible in this system because of the hash operation use. Additionally, in stage of data integrity checking, scheme of encryption based message-locked is exploited to transport and encrypt the assessing checked data blocks information, that decreases the essential calculation and communication resources amount significantly.

Proposed an algebraic dependent signature-based data integrity auditing scheme that ensure confidentiality of cloud and integrity of data through auditing batch. Furthermore, one benefit of the system is with the aim of maintaining dynamics of data by means of employing one cloud server merely. The security analyses show that the production can attain preferred property of security. The simulation outcome of active diverse data blocks operations and numbers of sub-blocks, illustrate that this scheme is competent for real-worldapplication.

Using a sanitizer to cleanse the data blocks in proportion to the responsive file information and transform these information blocks' signature into suitable ones for the disinfected file. These signatures were employed for verifying the sanitized file integrity in the integrity auditing. Accordingly, this scheme make the stored file in the cloud phase capable of used and shared through others with condition that the susceptible information is unknown, whereas the auditing of remote data integrity is still capable of executing competently. In the meantime, the projected system depends on identity-dependent cryptography that simplifies the convoluted certificate organization. The security analysis and the performance assessment demonstrate that projected scheme was efficient andsecure.

Employed a secure and an efficient protocol auditing enable dynamics of data for influencing the consumer that information are kept correctly in the cloud. In this approach, a privacy-preserving public auditing cloud storage protocol was presented that enables data dynamics in the customary model. A auditing protocol data integrity depends on strong assumption of RSA was employed on stimulated by current Homomorphic signature of network coding scheme, and widen it to facilitate a third party auditor to review consumers data devoid of data learningcontented.

proposed a novel identity-based (ID-based structure) of RDIC procedure through making the utilization of primitive key-Homomorphic cryptographic so as to decrease the system complexity and the cost of establishment thereby handling the authentication of public key framework in PKI dependent RDIC schemes. Also, RDIC based ID and its security model including security not in favor of a cloud server that are malicious and privacy of zero knowledge alongside a third party verifier was formalized. The projected protocols ID- based RDIC leak no information regarding stored information to the verifier all through the RDICprocess.

Proposed a framework based on Data Integrity Service. In such framework, more dependable verification of data integrity might be offered for both the Data Consumers and the Data Owners, devoid of relying on some Third Party Auditor (TPA). In this, the appropriate protocols and a consequent prototype structure, which was implemented to assess the probability of these proposals, were presented. The performance assessment of the prototype system implemented was conducted, and the test consequences werediscussed.

Privacy-preserving public auditing for secure cloudstorage:
Cloud Computing has been intended as the architecture of next generation IT Initiative. It transfers the software application and database to central large data centers, wherever the data and services management might not be trustworthy entirely [19]. This exclusive model fetches about several new challenges of security that was not understood well. This work revised the confirming data storage integrity issue in Cloud Computing [20]. In specific, allowing a third-party auditor (TPA) task is considered, in support of the cloud client, to authenticate the active data integrity stored in the cloud [21]. The introduction of TPA eradicates the client participation in the course of the assessment of his data stored in the cloud is certainly complete, which can be significant in attaining scale economies for Cloud Computing [22]. The data dynamics carry through the most universal data operation forms, like deletion insertion and block modification, is also an important stage to practicality, in Cloud Computing services are not restricted to backup or archive information only in the meantime. Whereas prior works on confirming remote data

integrity frequently lack any public auditability or dynamic data support operations, this paper attains both [23]. The potential security problems and difficulties of direct extensions were recognized initially with the entire informs of dynamic data from previous works and then illustrate the way of constructing an elegant authentication system for the incorporation of these two salient features in the protocol design in a seamless manner. In specific, to attain effectual data dynamics, we can expand the present storage models verification on the classic (MHT) MerkleHashTreeconstruction deployment for block tag verification. To aid effectual multiple auditing tasks handling, the technique of bilinear aggregate signature was explored to cover ourforemost outcome into a multi-user setting, wherever TPA can accomplish several auditing tasks concurrently [24]. Extensive performance analysis and security illustrate that the proposed schemes are extremely effectual and provably protected [25]. By means of Cloud Storage, user be able to accumulate their data remotely and benefit from the high-quality applications [26].

Systemarchitecture:
The cloud data storage service architecture system connecting three different entities, as follows

1. Cloud service provider or cloud storageserver
2. Cloud user orclient
3. Third partyauditor

Cloud storage server or cloud server (CSS/CS):
The server of cloud storage is the site where consumers accumulate their data. The storage space server in cloud conserved through the cloud service provider (CSP) [5, 13].

Cloud Client/user:
This is the entity that has huge quantity of information hunger to accumulate the cloud storage server.

Third party auditor (TPA):
In support of client TPA is accountable to ensure the user integrity that is outsourced data in cloud. This is a trusted party of the client [27].

A public auditing system comprises of four processes (GenProof, KeyGen, VerifyProof and SigGen,). The functioning of a public auditing system contains of two phase, Audit and Setup [28-30]:

Setup Phase:
The user is responsible for initializing secret parameters of the system on the execution of KeyGen, and the data file F preprocesses using SigGen for the generation of metadata verification. The user in turn keeps the data file F stored and the metadata verification at the server of cloud. The consumer might modify the data file F on performing update on the data stored incloud.

Audit Phase:
The issues of audit message TPA or the cloud server challenge to confirm that the cloud server has gained the F data file correctly at the audit time. The cloud server might generate a message of response through GenProof execution with the use of F and its metadata verification as inputs. The TPA in turn verifies the cloud server response through Verify Proof.

Conclusion:-

Cloud storage was regarded as a cost effective solution that offers business continuity, pay-as-you-go, and with retention of long-term and risk mitigation in the course of adversity revival. These features were not accessible with storage on- premises. On the other hand, the model of cloud storage has intrinsic weakness; a client loses of data control outsourcing over its information. Data integrity and confidentiality were the foremost concern of user while moving information from on-premises storage to cloud storage. Several schemes on data integrity were presented so far over the years for addressing the issues related to security which in turn associated to that of the cloud storage. In this approach, cloud computing and cloud storage paradigms were deliberated along with cloud storage issues. The main motive of this approach was to enhance the security aspects understandings of the data integrity schemes. In future, there is a need to implement some effective methodologies to overcome the existing issues related to data integrity issues in cloudframework.

References:-

1. L. Zhou, A. Fu, S. Yu, M. Su, and B. Kuang, "Data integrity verification of the outsourced big data in the cloud environment: A survey," Journal of Network and Computer Applications, vol. 122, pp. 1-15, 2018.
2. F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, et al., "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends," Computers & Security, vol. 65, pp. 29-49,2017.
3. R. Ahila and S. Sivakumari, "A SURVEY: CLOUD COMPUTING SECURITY ISSUES AND TECHNIQUES," International Journal of Advanced Research in Computer Science, vol. 8, 2017.
4. N. Garg and S. Bawa, "Comparative analysis of cloud data integrity auditing protocols," Journal of network and computer applications, vol. 66, pp. 17-32, 2016.
5. T. Mohanaprakash and J. Andrews, "An examination on data integrity auditing patterns in cloud computing," International Journal of Engineering & Technology, vol. 7, pp. 200-204,2018.
6. Y. X. Yan, L. Wu, W. Y. Xu, H. Wang, and Z. M. Liu, "Integrity audit of shared cloud data with identity tracking," Security and Communication Networks, vol. 2019, 2019.
7. V. K. Devi, S. Shrenika, and N. Jyothi, "A Study on Data Integrity and Storage Efficiency Services in Cloud," International Journal of Engineering Research, vol. 5, pp. 340-346, 2016.
8. C. B. Tan, M. H. A. Hijazi, Y. Lim, and A. Gani, "A survey on Proof of Retrievability for cloud data integrity and availability: Cloud storage state-of-the- art, issues, solutions and future trends," Journal of Network and Computer Applications, vol. 110, pp. 75-86,2018.
9. B. P. Yadav, R. B. Kumar, and P. S. Rao, "Data Integrity Auditing for Secure Sharing in Cloud with Group User Revocation,"2017.
10. Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, "One secure data integrity verification scheme for cloud storage," Future Generation Computer Systems, vol. 96, pp. 376-385,2019.
11. Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 676-688,2016.
12. M. Imran, H. Hlavacs, B. J. InamUlHaq, F. A. Khan, and A. Ahmad, "Provenance based data integrity checking and verification in cloud environments," PloS one, vol. 12, 2017.
13. Y. Ren, J. Shen, Y. Zheng, J. Wang, and H.-C. Chao, "Efficient data integrity auditing for storage security in mobile health cloud," Peer-to-Peer Networking and Applications, vol. 9, pp. 854-863, 2016.
14. J. Shen, D. Liu, D. He, X. Huang, and Y. Xiang, "Algebraic signatures-based data integrity auditing for efficient data dynamics in cloud computing," IEEE Transactions on Sustainable Computing, 2017.
15. W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 14, pp. 331-346,2018.
16. M. Ma, J. Weber, and J. van den Berg, "Secure public-auditing cloud storage enabling data dynamics in the standard model," in 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), 2016, pp.170-175.
17. Y.Yu,M.H.Au,G.Ateniese,X.Huang,W.Susilo,Y. Dai, et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 767-778, 2016.
18. R. Joseph and S. Sonavane, "An in-depth survey on integrity auditing and information hiding in cloud," Asian Journal of Science and Technology, vol. 10, pp. 9642-9646, 2019.
19. H.Tian, F.Nan, C.-C.Chang, Y.Huang, J.Lu,Y.J.J. o. N. Du, et al., "Privacy-preserving publicauditing for secure data storage in fog-to-cloud computing," vol. 127, pp. 59-69, 2019.
20. L.Seth, K.Barthwal, A.Sar, A.Pokhriyal, andN.J.J. o. E. S. Aggarwal, "Privacy Preserving Auditing for Secure Cloud Storage," vol. 12052, 2017.
21. M. Salem, S. Taheri, and J.-S. J. C. Yuan, "Utilizing transfer learning and homomorphic encryption in a privacy preserving and secure biometric recognition system," vol. 8, p. 3, 2019.
22. M. B. Thakare and N. Dhande, "Privacy Preserving and Secure Data Integrity Protection security in Regenerating Coding Based Public Cloud Storage," 2017.
23. Y.Yu, M.H.Au, G.Ateniese, X.Huang, W.Susilo,Y. Dai, et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," vol. 12, pp. 767-778, 2016.
24. M. Du, Q. Wang, M. He, J. J. I. T. o. I. F. Weng, and Security, "Privacy-preserving indexing and query processing for secure dynamic cloud storage," vol. 13, pp. 2320-2332, 2018.

25. W.Shen,J.Yu,H.Xia,H.Zhang,X.Lu,R.J.J.o.N. Hao, et al., "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," vol. 82, pp. 56-64, 2017.
26. S. B. R. J. s. Prasad, "Privacy-Preserving and Regular Language Searchable Encryption Scheme For Secure Cloud Storage," vol. 65, pp. 1992-2004, 2016.
27. Y. Yu, L. Xue, M. H. Au, W. Susilo, J. Ni, Y. Zhang, et al., "Cloud data integrity checking with an identity-based auditing mechanism from RSA," Future Generation Computer Systems, vol. 62, pp. 85-91,2016.
28. Y. Yu, Y. Li, B. Yang, W. Susilo, G. Yang, and J. Bai, "Attribute-based cloud data integrity auditing for secure outsourced storage," IEEE Transactions on Emerging Topics in Computing,2017.
29. J. Zhang and Q. Dong, "Efficient ID-based public auditing for the outsourced data in cloud storage," Information Sciences, vol. 343, pp. 1-14, 2016.
30. T.-Y. Youn, K.-Y. Chang, K.-H. Rhee, and S. U. Shin, "Efficient client-side deduplication of encrypted data with public auditing in cloud storage," IEEE Access, vol. 6, pp. 26578-26587, 2018.