IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 11, November 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 11, November 2022||

| DOI:10.15680/IJIRSET.2022.111149 |

Efficient Data Integrity with Provable Data Possession Based Cryptographic Technique for Cloud Storage

[1]Dr.S.GOKULRAJ, [2]A.MONIKA

[1]Professor, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Thindal, Erode, Tamilnadu, India.

[2]PG Student, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Thindal, Erode, Tamilnadu, India.

ABSTRACT: Cloud storage, an economically attractive service offered by cloud service providers (CSPs), has attracted a large number of tenants. However, because the ownership and management of outsourced data are separated, outsourced data faces a lot of security challenges, for instance, data security, data integrity, data update, and so on. In this article, we primarily investigate the problem of efficient data integrity auditing supporting provable data update in cloud computing environment. Subsequently, on the basis of the Merkel sum hash tree (MSHT), we introduce an efficient outsourced data integrity auditing scheme. Our designed scheme could synchronously meet the requirements of provable data update and data confidentiality without dependency on a third authority. At the same time, the numerical analysis shows that the computing complexity logarithmically grows with the number of outsourced subfiles. The paper proposed the scheme for Data Integrity is Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server, can be used to realize audit services.

I. INTRODUCTION

With the fast development of computer and network technology, the total volume of digital data shows an exponential growth tendency . The investigation report shows that there were 5200GB digital data for everyone on average in 2020 . However, the storage resources of tenants are so limited that cannot preserve such large-scale data. Therefore, massive data storage would become a challenging problem for resource constrained tenants. Fortunately, cloud storage offers a potential solution to handle the issue of massive data storage and management.

By embracing cloud storage services, tenants could upload their data to the cloud data center, thus efficaciously reducing the local memory space and computational cost . Because of these attractive advantages, a growing number of tenants prefer to employ cloud storage services. According to the report of Cisco, there were 3.6 billion Internet consumers at the beginning of 2020. At the same time, about 55% of Internet consumers embraced cloud storage . In cloud storage, the management of outsourced data is separated from its ownership . Therefore, tenants would lose the physical management of their outsourced data, thus cannot directly perform any operations over the outsourced data . In other words, the cloud data center performs all operations over the outsourced data. Nevertheless, the cloud data center is not fully reliable, and it might not honestly perform these operations according to the tenant's commands. As a result, although cloud storage has huge advantages, it inevitably faces plenty of serious problems, for instance, data confidentiality, data integrity, data update, etc. If these problems, especially data integrity, are not solved well, it will greatly prevent the public from accepting and employing cloud storage services.

II. LITERATURE SURVEY

Auditing Cache Data Integrity in the Edge Computing Environment [1]

Edge computing allows app vendors to deploy their applications and relevant data on distributed edge servers to serve nearby users. Caching data on edge servers can minimize users' data retrieval latency. However, such cache data are subject to both intentional and accidental corruption in the highly distributed, dynamic, and volatile edge computing

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 11, November 2022||

| DOI:10.15680/IJIRSET.2022.111149 |

environment. Given a large number of edge servers and their limited computing resources, how to effectively and efficiently audit the integrity of app vendors' cache data is a critical and challenging problem.To propose a new data structure named **variable Merkle hash tree (VMHT)** for generating the integrity proofs of those data replicas during the audit. VMHT can ensure the audit accuracy of EDI-V by maintaining sampling uniformity. EDI-V allows app vendors to inspect their cache data and locate the corrupted ones efficiently and effectively. Both theoretical analysis and comprehensively experimental evaluation demonstrate the efficiency and effectiveness of EDI-V.

Efficient Data Storage Security with Multiple Batch Auditing in Cloud Computing [2]
Cloud Computing has been visualized as the next generation architecture of IT endeavor. It moves the storage databases to the centralized large data centers, where the direction of the data and services may not be trustworthy. This fetches many new security challenges, which have not been well understood properly.

The problem is to find efficient protocol which avoids unnecessary overhead to the user in checking the integrity of their own data and also it should support dynamic data operations instead of just achieve and back up the data files in the cloud.In the proposed system, we consider the task of allowing a third party auditor to verify the integrity of the data stored in the cloud on behalf of the client. The entry of third party auditor eliminates the participation of the client through the auditing of whether his/her data stored in the cloud are indeed not damaged, which can be important in cloud computing for achieving economies of scale. The support for data dynamic operations such as block modification, insertion, and deletion are also a significant step toward practicality, since services in cloud computing are not restrict to file away or backup data only. To attain effective data dynamics we improved the existing system of storage models by manipulating the classic Merkle Hash Tree building for block tag authentication.

Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage", Volume XIV [3]
Outsourced data auditing protocols enable a verifier to efficiently check the integrity of the outsourced files without downloading the entire file from the cloud, which can dramatically reduce the communication overhead between the cloud server and the verifier. Existing protocols are mostly based on public key infrastructure or an exact identity, which lacks flexibility of key management.Proposed system to address the complex key management challenge in cloud data integrity checking by introducing attribute-based cloud data auditing, where users can upload files to cloud through some customized attribute set and specify some designated auditor set to check the integrity of the outsourced data. To formalize the system model and the security model for this new primitive, and describe a concrete construction of attribute-based cloud data integrity auditing protocol. The new protocol offers desirable properties namely attribute privacy preserving and collusion-resistance. To prove soundness of our protocol based on the computational Diffie-Hellman assumption and the discrete logarithm assumption. The proposed attribute-based cloud data integrity auditing protocol consists of three procedures, namely Enroll, Store and Audit.

Efficient Verification of Edge Data Integrity in Edge Computing Environment [4]
Edge computing, as a new computing paradigm that extends cloud computing, allows a service vendor to deploy its services on distributed edge servers to serve its service users in close geographic proximity to those edge servers.

Caching edge data on edge servers can minimize service users' data retrieval latency. However, such edge data are subject to intentional and accidental corruption in the highly distributed and dynamic edge computing environment. Verifying the integrity of service vendors' edge data accurately and efficiently is a critical security problem. Given a potentially large number of edge servers and their limited computing capacities, verifying the integrity of the edge data on each edge server individually is computation expensive.Edge Data Integrity (EDI) problem from the service vendor's perspective by proposing an inspection and corruption localization scheme for EDI named ICL-EDI. This scheme allows a service vendor to inspect its edge data and localize corrupted edge data on multiple edge servers accurately and efficiently. To evaluate its performance, we implement ICL-EDI and conduct extensive experiments to demonstrate its effectiveness and efficiency. An efficient EDI scheme must not pose high computational overheads on edge servers. efficient EDI scheme must allow a service vendor to verify the integrity of a potentially large number of edge data replicas with low computational overheads. This is the second design objective of ICL-EDI.

Dynamic Proof of Data Possession and Replication with Tree Sharing and Batch Verification in the Cloud [5]
Cloud storage attracts a lot of clients to join the paradise. For a high data availability, some clients require their files to be replicated and stored on multiple servers. Because clients are generally charged based on the redundancy level required by them, it is critical for clients to obtain convincing evidence that all replicas are stored correctly and are

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 11, November 2022||

| DOI:10.15680/IJIRSET.2022.111149 |

updated to the up-to-date version.Proposed system is developed a dynamic proof of data possession and replication (DPDPR) scheme, which is proved to be secure in the defined security model. This scheme shares a single authenticated tree across multiple replicas, which reduces the tree's storage cost significantly. It allows for batch verification for multiple challenged leaves and can verify multiple replicas in a single batch way, which considerably save bandwidth and computation resources during audit process. And also evaluate the DPDPR's performance and compare it with the most related scheme.

III. SYSTEM METHODOLOGY

First, most of the previous solutions are based on proof of retrievability (PoR) technology or provable data possession (PDP) technology, whose computing complexity grows approximatively linearly with the scale of outsourced files. Hence, the efficiency is not attractive if the scale of outsourced file keeps growing .

Second, lots of the previous works require to depend on a third authority (TA), whose security and stability are particularly troubling. On the one hand, because of the expensive overhead, the third authority would refuse to provide services, which will cause service interruption. On the other hand, the third authority might be attacked by the adversary, and it cannot resist the commands of the government, which both would trigger privacy leakage. Last but not least, although some of the previous solutions concurrently accomplish data confidentiality, data integrity, and data update in some special scenarios, the practicability and universality are so limited that they cannot be applied to large-scale data outsourcing scenarios.

DRAWBACKS

- Massive data storage would become a challenging problem for resourceconstrained tenants.
- In cloud storage, the management of outsourced data is separated from its ownership

The paper proposed the scheme for Data Integrity is Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server, can be used to realize audit services. The profiting from the interactive zero-knowledge proof system, address the construction of an interactive PDP protocol to prevent the fraudulence of prover (soundness property) and the leakage of verified data (zero-knowledge property). There prove that our construction holds these properties based on the computation Diffie–Hellman assumption and the rewind able black-box knowledge extractor and also propose an efficient mechanism with respect to probabilistic queries and periodic verification to reduce the audit costs per verification and implement abnormal detection timely. In addition, present an efficient method for selecting an optimal parameter value to minimize computational overheads of cloud audit services.

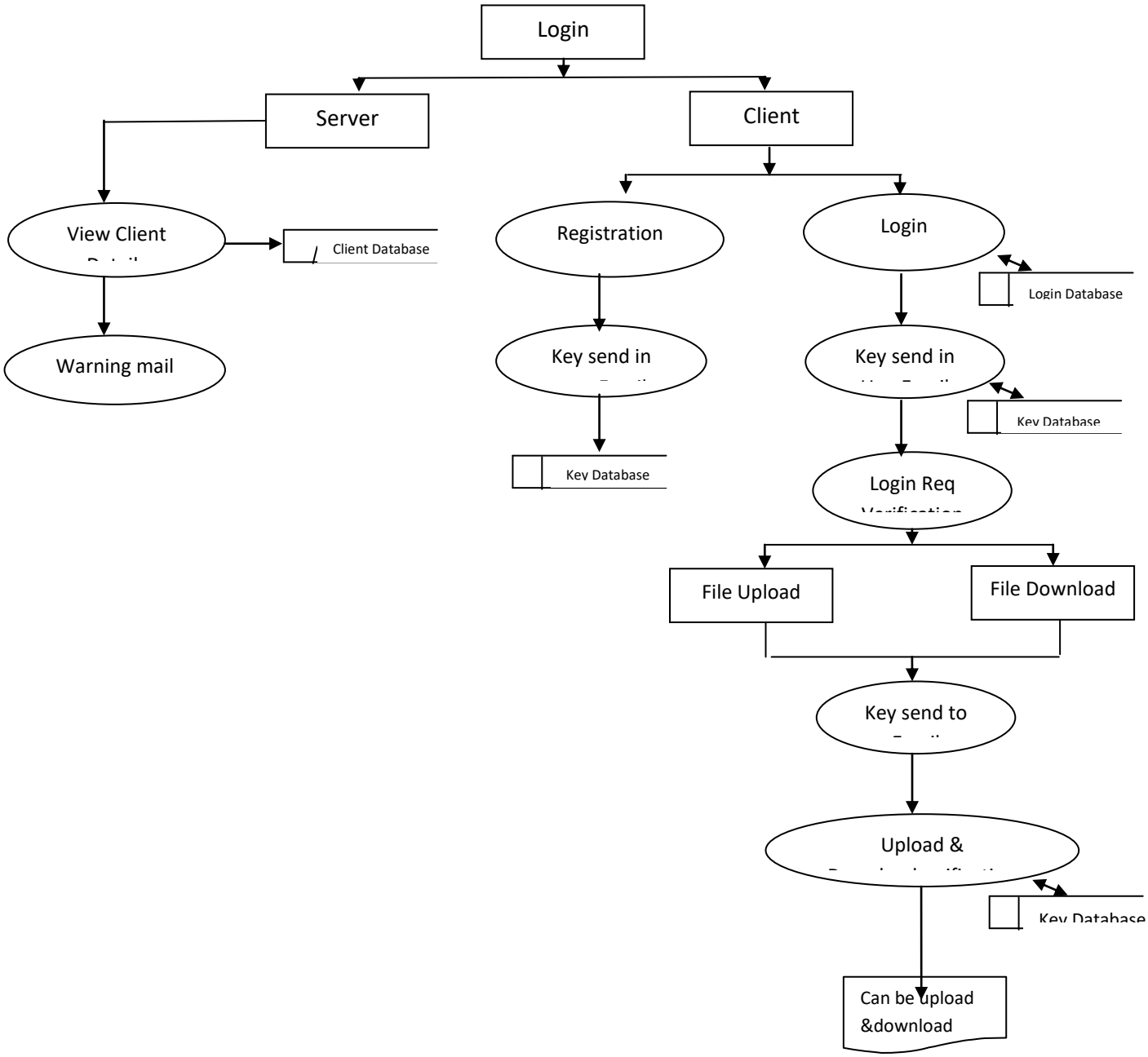
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 11, November 2022||

| DOI:10.15680/IJIRSET.2022.111149 |

IV. SYSTEM ARCHITECTURE

This section shows the all architecture diagrams which are used in this proposed system design.



V. CONCLUSION

It addressed the construction of an efficient audit service for data integrity in clouds.Profiting from the standard interactive proof system, to propose an interactive audit protocol to implement the audit service based on a third party auditor. In this audit service, the third party auditor, known as an agent of data owners, can issue a periodic verification to monitor the change of outsourced data by providing an optimized schedule. To realize the audit model, we only need to maintain the security of the third party auditor and deploy a lightweight daemon to execute the verification protocol.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 11, November 2022||

| DOI:10.15680/IJIRSET.2022.111149 |

Hence, our technology can be easily adopted in a cloud computing environment to replace the traditional Hash-based solution. More importantly, it proposed and quantified a new audit approach based on probabilistic queries and periodic verification, as well as an optimization method of parameters of cloud audit services. This approach greatly reduces the workload on the storage servers, while still achieves the detection of servers' misbehavior with a high probability. Our experiments clearly showed that our approach could minimize computation and communication overheads.

REFERENCES

1. H. Tian et al., "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Trans. Services Comput., vol. 10, no. 5, pp. 701–714, Sep./Oct. 2017.
2. F. Guo, H. Zhang, H. Ji, X. Li, and V. C. Leung, "An efficient computation offloading management scheme in the densely deployed small cell networks with mobile edge computing," IEEE/ACM Trans. Netw., vol. 26, no. 6, pp. 2651–2664, Dec. 2018.
3. W. Tong, B. Jiang, F. Xu, Q. Li, and S. Zhong, "Privacy-preserving data integrity verification in mobile edge computing," in Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst., 2019, pp. 1007–1018.
4. R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Gener. Comput. Syst., vol. 78, pp. 680–698, 2018.
5. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.
6. W. Tong, B. Jiang, F. Xu, Q. Li, and S. Zhong, "Privacy-preserving data integrity verfication in mobile edge computing," in International Conference on Distributed Computing System. IEEE, 2019, pp. 1007–1018.
7. H. Wang, D. He, A. Fu, Q. Li, and Q. Wang, "Provable data possession with outsourced data transfer," IEEE Transactions on Services Computing, 2019.
8. T. Wang, J. Zhou, X. Chen, G. Wang, A. Liu, and Y. Liu, "A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 3–12, 2018.
9. C. Yang, Y. Liu, F. Zhao, and S. Zhang, "Provable data deletion from efficient data integrity auditing and insertion in cloud storage," Computer Standards & Interfaces, vol. 82, 2022.
10. B. Li, Q. He, F. Chen, H. Jin, Y. Xiang, and Y. Yang, "Auditing cache data integrity in the edge computing environment," IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 5, pp. 1210–1223, 2021.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details