International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

A Secure Multi Copy Dynamic Data Posession Using Proxy Server in Cloud Computing

N.Sravya & G.Vijay Kumar

1 M.Tech Student, Dept. of CSE, SKU College of Engineering, Anantapur, India.
2 Lecturer,Dept. of CSE, SKU College of Engineering, Anantapur, India.

ABSTRACT:

Now-a-days organizations are moving towards storing their knowledge in cloud servers provided by the cloud service suppliers (CSPs) thus on cut back the strain placed on their company servers. During this paper, we have a tendency to propose storing the info in cloud by cacophonous the file into totally different components and storing them in several servers. The value required in storing the info move into multiple components is low compared to storing multiple copies of information file. This fashion of storing multiple components of a file additionally ensures that associate offender doesn't get his hands on the entire file. The file cacophonous technique is employed for cacophonous the file into multiple components. Throughout the retrieval of the file it's rejoined by the merging the split file components. Within the planned system, file sharing is additionally created safe by verification of the file requestor before the file is shared. For associate redoubled level of quantitative, convenience, and sturdiness, some customers might want their knowledge to be replicated on multiple servers across multiple knowledge centers. during this paper, we have a tendency to propose a map-based demonstrable multi copy dynamic knowledge possession (MB-PMDDP) theme that has the subsequent features: 1) it provides associate proof to the shoppers that the CSP isn't cheating by storing fewer copies; 2) it supports outsourcing of dynamic knowledge, i.e., it supports block-level operations, like block modification, insertion, deletion, and append 3) it permits licensed users to seamlessly access the file copies keep by the CSP. in addition we have a tendency to show the safety against colluding servers, and discuss a way to determine corrupted copies by slightly modifying the planned theme.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

KEY WORDS: Cloud computing, dynamic environment, data duplication, outsourcing data storage.

INTRODUCTION:

The confidentiality issue will be feeling by encrypting confidential knowledge before outsourcing to remote servers. As such, it's an important demand of consumers to possess robust proofs that the cloud servers still have their knowledge and it's not being corrupt with or partly deleted over time. As a result, several researchers have payee attention on the matter of demonstrable knowledge possession (PDP) and projected completely different systems to review the information hold on remote servers. PDP could be a methodology for authenticating knowledge integrity over remote servers. In an exceedingly typical PDP model, the information house owners manufacture some information for an information file to be used later for verification functions through a challenge-response protocol with the remote/cloud server. The owner sends the file to be held on an overseas server which can be untrusted, and erases the native copy of the file. One in every of the core style ethics of outsourcing knowledge is to produce dynamic behavior of information for a spread of applications. this implies that the marginally hold on knowledge will be not solely accessed by the approved users, however conjointly economical and scaled samples of PDP constructions that contend with dynamic knowledge. The ultimate are how-ever for one copy of the information file. PDP methodology has been procurable for multiple copies of static knowledge. PDP system directly deals with multiple copies of dynamic knowledge. once proving multiple knowledge copies, typically system integrity check fails if there's one or additional corrupted copies were gift.

LITERATURE SURVEY:

1.“ Z. Hao, S. Zhong, and N. Yu”, A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability , Remote knowledge integrity checking may be a crucial technology in cloud computing. Recently, several works concentrate on providing knowledge dynamics and/or public verifiability to the present variety of protocols. Existing protocols will support

each options with the assistance of a third-party auditor. In an exceedingly previous work, Sebé et al. propose a distant knowledge integrity checking protocol that supports knowledge dynamics. During this paper, we tend to adapt Sebé et al.'s protocol to support public verifiability. The projected protocol supports public verifiability while not facilitate of a third-party auditor. Additionally, the projected protocol doesn't leak any non-public info to third-party verifiers. Through a proper analysis, we tend to show the correctness and security of the protocol. After that, through theoretical analysis and experimental results, we tend to demonstrate that the projected protocol features a sensible performance.

2. " Z. Hao and N. Yu", A multiple-replica remote data possession checking protocol with public verifiability", several cloud storage suppliers declare that they store multiple replicas of clients' knowledge so as to forestall knowledge loss. However, presently there's no guarantee that they really pay storage for multiple replicas. Recently a multiple-replica demonstrable knowledge possession (MR-PDP) protocol is projected, that provides shoppers with the power to examine whether or not multiple replicas area unit very keep at the cloud storage servers. However, in MR-PDP, solely non-public verifiability is achieved. during this paper, we tend to propose a multiple-replica remote knowledge possession checking protocol that has public verifiability. the general public verifiability will increase the protocol's flexibility therein a third-party auditor will perform the info checking on behalf of the shoppers. Homomorphic authentication tags supported BLS signature area unit utilized in the projected protocol. By security analysis and performance analysis, the projected protocol is shown to be secure and economical, that makes it terribly appropriate in cloud storage systems.

3." Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau", Efficient provable data possession for hybrid clouds, demonstrable knowledge possession may be a technique for guaranteeing the integrity of knowledge in outsourcing storage service. during this paper, we tend to propose a cooperative demonstrable knowledge possession theme in hybrid clouds to support

measurability of service and knowledge migration, within which we tend to take into account the existence of multiple cloud service suppliers to hand and glove store and maintain the clients' knowledge. Our experiments show that the verification of our theme needs a tiny low, constant quantity of overhead, which minimizes communication complexness.

4. " A. F. Barsoum and M. A. Hasan", Provable possession and replication of data over cloud servers, additional and more organizations area unit choosing outsourcing knowledge to remote cloud service suppliers (CSPs). Customers will rent the CSPs storage infrastructure to store and retrieve virtually unlimited quantity of knowledge by paying fees metered in gigabyte/month. For associate degree raised level of measurability, accessibility, and sturdiness, some customers might want their knowledge to be replicated on multiple servers across multiple knowledge centers. The additional copies the CSP is asked to store, the additional fees the purchasers area unit charged. Therefore, customers ought to have a robust guarantee that the CSP is storing all knowledge copies that area unit set within the contract, and every one these copies area unit in line with the foremost recent modifications issued by the purchasers. during this paper, we tend to propose a map-based demonstrable multicopy dynamic knowledge possession (MB-PMDDP) theme that has the subsequent features: 1) it provides associate degree proof to the purchasers that the CSP isn't cheating by storing fewer copies; 2) it supports outsourcing of dynamic knowledge, i.e., it supports block-level operations, like block modification, insertion, deletion, and append; and 3) it permits licensed users to seamlessly access the file copies keep by the CSP. we tend to provides a comparative analysis of the projected MB-PMDDP theme with a reference model obtained by extending existing demonstrable possession of dynamic single-copy schemes. The theoretical analysis is valid through experimental results on an advertisement cloud platform. additionally, we tend to show the safety against colluding servers, and discuss a way to establish corrupted copies by slightly modifying the projected theme.

5. " C. Wang, Q. Wang, K. Ren, and W. Lou", Ensuring data storage security in

cloud computing, Cloud computing has been visualized because the next-generation design of IT enterprise. In distinction to ancient solutions, wherever the IT services area unit underneath correct physical, logical and personnel controls, cloud computing moves the applying code and knowledgebase's to the massive data centers, wherever the management of the info and services might not be absolutely trustworthy. This distinctive attribute, however, poses several new security challenges that haven't been well understood. during this article, we tend to concentrate on cloud knowledge storage security, that has forever been a vital side of quality of service. to make sure the correctness of users' knowledge within the cloud, we tend to propose a good and versatile distributed theme with 2 salient options, opposing to its predecessors. By utilizing the homomorphism token with distributed verification of erasure-coded knowledge, our theme achieves the combination of storage correctness insurance and knowledge error localization, i.e., the identification of misbehaving server (s). in contrast to most previous works, the new theme any supports secure and economical dynamic operations on knowledge blocks, including: knowledge update, delete and append. in depth security and performance analysis shows that the projected theme is very economical and resilient against Byzantine failure, malicious knowledge modification attack, and even server colluding attacks

RELATED WORK:

EXISTING SYSTEM:

Once the data has been outsourced to a remote CSP which may not be trustworthy, the data owners lose the direct control over their sensitive data. This lack of control raises new formidable and challenging tasks related to data confidentiality and integrity protection in cloud computing. The confidentiality issue can be handled by encrypting sensitive data before outsourcing to remote servers. As such, it is a crucial demand of customers to have strong evidence that the cloud servers still possess their data and it is not being tampered with or partially deleted over time. Consequently, many researchers have focused on the problem of provable data possession (PDP) and proposed different schemes to audit the data stored on remote servers.

One of the core design principles of outsourcing data is to provide dynamic behavior of data for various applications. This means that the remotely stored data can be not only accessed by the authorized users, but also updated and scaled (through block level operations) by the data owner. PDP schemes presented focus on only *static* or warehoused data, where the outsourced data is kept unchanged over remote servers. The latter are however for a *single* copy of the data file.

DISADVANTAGES OF EXISTING SYSTEM:

Once the data has been outsourced to a remote CSP which may not be trustworthy, the data owners lose the direct control over their sensitive data. This lack of control raises new formidable and challenging tasks related to data confidentiality and integrity protection in cloud computing.

PROPOSED SYSTEM:

When verifying multiple data copies, the overall system integrity check fails if there is one or more corrupted copies. To address this issue and recognize which copies have been corrupted, we discuss a slight modification to be applied to the proposed scheme.

We propose a map-based provable multi-copy dynamic data possession (MB-PMDDP) scheme. This scheme provides an adequate guarantee that the CSP stores all copies that are agreed upon in the service contract. Moreover, the scheme supports outsourcing of dynamic data, *i.e.*, it supports block-level operations such as block modification, insertion, deletion, and append. The authorized users, who have the right to access the owner's file, can seamlessly access the copies received from the CSP.

We give a thorough comparison of MB-PMDDP with a reference scheme, which one can obtain by extending existing PDP models for dynamic single-copy data. We show the security of our scheme against colluding servers, and discuss a slight modification of the proposed scheme to identify corrupted copies. In this work, we do not encode the data to be outsourced for the following reasons.

First, we are dealing with dynamic data, and hence if the data file is encoded before

outsourcing, modifying a portion of the file require re-encoding the data file which may not be acceptable in practical applications due to high computation overhead.

Second, we are considering economically-motivated CSPs that may attempt to use less storage than required by the service contract through deletion of a few copies of the file. The CSPs have almost no financial benefit by deleting only a small portion of a copy of the file.

Third, and more importantly, unlike erasure codes, duplicating data files across multiple servers achieves scalability which is a fundamental customer requirement in CC systems. A file that is duplicated and stored strategically on multiple servers – located at various geographic locations

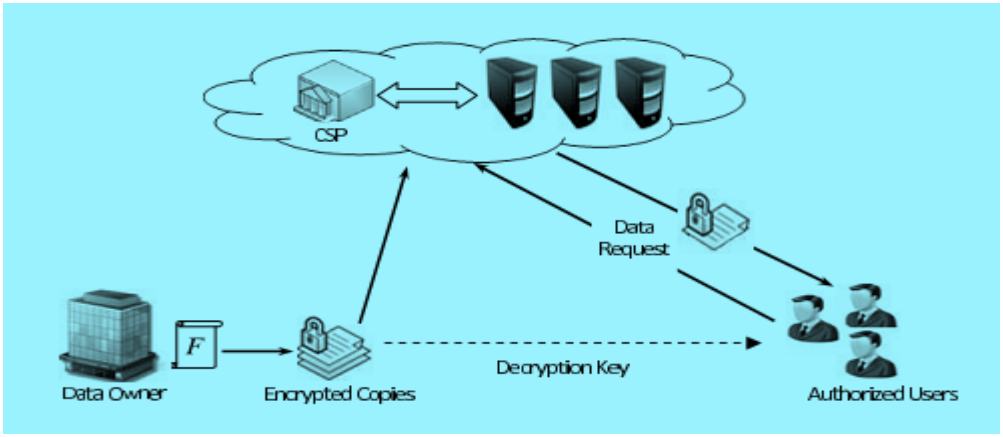
ADVANTAGES OF PROPOSED SYSTEM:

IMPLEMENTATION:

Although PDP schemes have been presented for *multiple* copies of *static* data, to the best of our knowledge, this work is the first PDP scheme directly dealing with *multiple* copies of *dynamic* data.

The storage model used in this work can be adopted by many practical applications. For example, e-Health applications can be envisioned by this model where the patients' database that contains large and sensitive information can be stored on the cloud servers. In these types of applications, the e-Health organization can be considered as the data owner, and the physicians as the authorized users who have the right to access the patients' medical history. Many other practical applications like financial, scientific, and educational applications can be viewed in similar settings.

SYSTEM ARCHITECTURE:



The knowledge owner outsources knowledge to the cloud for convenient and reliable data access to the corresponding users. to shield the information privacy, the information owner encrypts the first data through encoding method. To boost the potency, the information owner generates some keywords for every outsourced document. After that, the information owner sends the encrypted documents and therefore the corresponding indexes to the cloud, and sends to cloud server. The cloud server is associate degree intermediate entity that stores the encrypted documents and corresponding indexes that square measure received from the information owner, and provides knowledge access and search services to look users. Once a quest user sends a keyword to the cloud server, it might come a set of matching documents supported sure operations. A search user queries the outsourced documents from the cloud server with following 3 steps. First, the search user receives each the key and parallel key from the information owner. Second, consistent with the search keywords, the search user uses the key to come up with trapdoor and sends it to the cloud server. Last, she receives the matching document assortment from the cloud server and decrypts them with the parallel key. The outsourced documents provided by the information owner square measure keep within the cloud server. If they match the search keywords, they're sent to the search user. Attributable to the privacy of documents, they must not be diagnosable except by the information owner and therefore the approved search users.

CONCLUSION:

Outsourcing knowledge to remote servers has become a growing trend for several organizations to alleviate the burden of native knowledge storage and maintenance. During this work, we've studied drawback the matter of making multiple copies of dynamic record and the way to resolve this problem by storing the enter totally different servers once rending it into multiple components. We've additionally projected however file sharing is created secured by confirmatory the file requestor and solely then permitting him access to the file. During this work we've studied the matter of making multiple copies of dynamic record and confirmatory those copies hold on international organization sure cloud servers. To the simplest of our information, the projected theme is that the 1st to deal with multiple copies of dynamic knowledge. The interaction between the licensed users and also the CSP is taken into account in our theme, wherever the licensed users will seamlessly access a knowledge copy received from the CSP employing a single secret key shared with the information owner. Moreover, the projected theme supports public verifiability, permits arbitrary variety of auditing, and permits possession-free verification wherever the friend has the flexibility to verify the information integrity even supposing he neither possesses nor retrieves the file blocks from the server. The dynamic block operations of the map-based approach area unit through with less communication price than that of the tree-based approach. a small modification is done on the projected theme to support the feature of distinguishing the indices of corrupted copies. The corrupted knowledge copy is reconstructed even from an entire harm victimization duplicated copies on alternative servers. Through security analysis, we've shown that the projected theme is demonstrably secure.

REFERENCES:

[1] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.

[2] Y. Deswarte, J.-J. Quisquater, and A. Saïdane, "Remote integrity checking," in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS), 2003, pp. 1–11.

[3] F. Sebé, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034–1038, Aug. 2008.

[4] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," IACR Cryptology ePrint Archive, Tech. Rep. 2008/186, 2008.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou. (2009). "Ensuring data storage security in cloud computing," IACR Cryptology ePrint Archive, Tech. Rep. 2009/081. [Online]. Available: http://eprint.iacr.org/

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. 14th Eur. Symp. Res. Comput. Secur. (ESORICS), Berlin, Germany, 2009, pp. 355–370.

[7] 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.

[8] Z. Hao and N. Yu, "A multiple-replica remote data possession checking protocol with public verifiability," in Proc. 2nd Int. Symp. Data, Privacy, E-Commerce, Sep. 2010, pp. 84–89.

[9] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. 14th Int. Conf. Theory Appl. Cryptol. Inf. Secur., 2008, pp. 90–107.

[10] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Efficient provable data possession for hybrid clouds," in Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS), 2010, pp. 756–758.

1 N.SRAVYA has received the B. Tech (Information Technology) degree from Gates institute of technology, Anantapur,A.P in 2014, and pursuing M.Tech(Computer science and Engineering) in Srikrishna Devaraya University College of Engineering and Technology, Anantapuramu district (AP).

2. Goddumarri Vijay Kumar received his B.Tech Degree in Computer Science and Information Technology from Jawaharlal Nehru Technological University, Hyderabad, India, in 2008; M.Tech in Computer Science & Engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 2012. He has experience of 8 years in teaching graduate level and 4 years in teaching postgraduate level and he presently working as Lecturer in Department of CSE Srikrishna Devaraya University College of Engineering,. Anantapuramu district (AP).