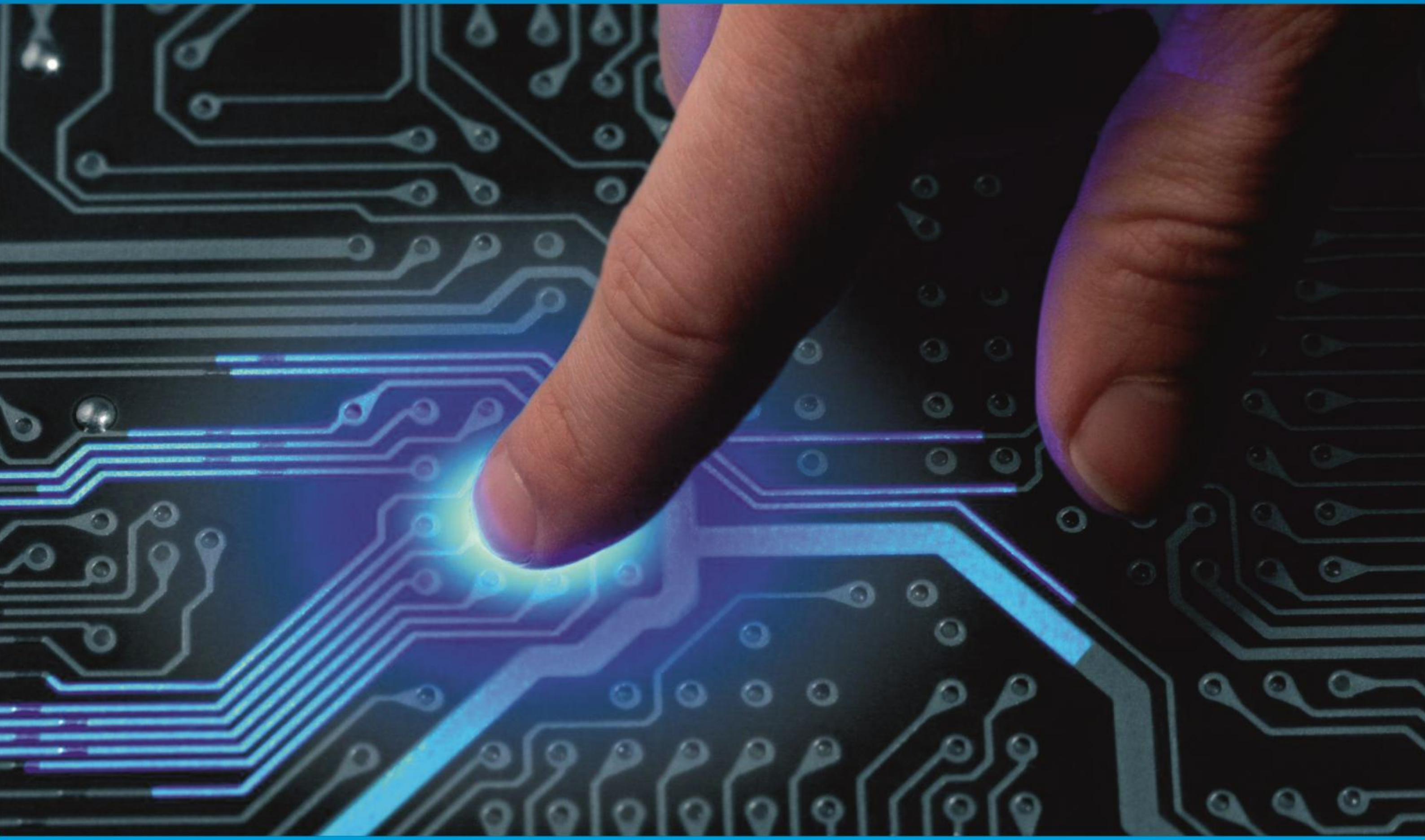
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com @ www.ijircce.com

| DOI: 10.15680/IJIRCCE.2022.1006097 |

Securing Resources Decentralized in Cloud Storage

Ms. H.SWATHI M.E., MADHUMITHA B, SAMITHA HARINI M, SRINIVASHINI M,

Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem, India

Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem, India

ABSTRACT: To reduce the computing time and response time between Token request and response, File upload or download request and results. It reduces the amount of storage space in cloud storage. To protect the confidentiality of data differential authorized duplicate check is used. It presents this authorized duplicate check in hybrid cloud architecture. The hybrid cloud architecture proposes about both the public cloud and the private cloud. In order to provide more security, the private cloud is provided with multilevel authentication. Advancements in cloud computing are leading to a promising future for Collaborative Cloud Computing (CCC). To reduce the computing time and response time between Token request and response, File upload or download request and results. Where globally- scattered distributed cloud resources belonging to different organizations or individuals (i.e., entities) are collectively used in a cooperative manner to provide services. The files are stored in the cloud. That is every client computes a data key to encrypt the data that he intends to store in the cloud. It describes a computationally cheap method for making all log entries generated. Prior to the logging machine's compromise impossible for the attacker to read and also impossible to undetectably modify or destroy. That is every client computes a data key to encrypt the data that he intends to store in the cloud.

I. INTRODUCTION

Data De-duplication with node is one of important data mining techniques for eliminating duplicate copies of repeating data. It compared the amount of storage space and save bandwidth. To protect the confidentiality of sensitive data while supporting De-duplication with node, the convergent encryption technique has been proposed to encrypt the data before outsourcing.

To decrease the registering time and reaction time between Token solicitation and reaction, File transfer or download solicitation and results. It decreases the measure of extra room in distributed storage. To protect the confidentiality of data differential authorized duplicate check is used. It present this authorized duplicate check in hybrid cloud architecture. The hybrid cloud architecture proposes about both the public cloud and the private cloud. In order to provide more security, the private cloud is provided with multilevel authentication. Advancements in cloud computing are leading to a promising future for Collaborative Cloud Computing (CCC). To reduce the computing time and response time between Token request and response, File upload or download request and results. Where globally- scattered distributed cloud resources belonging to different organizations or individuals (i.e., entities) are collectively used in a cooperative manner to provide services. The files are stored in the cloud. That is every client computes a data key to encrypt the data that he intends to store in the cloud. It describes a computationally cheap method for making all log entries generated. Prior to the logging machine's compromise impossible for the attacker to read and also impossible to undetectably modify or destroy. That is every client computes a data key to encrypt the data that he intends to store in the cloud.

Data De-duplication with node is one of important data mining techniques for eliminating duplicate copies of repeating data. It compared the amount of storage space and save bandwidth. To protect the confidentiality of sensitive data while supporting De-duplication with node, the convergent encryption technique has been proposed to encrypt the data before outsourcing. We propose another advanced duplication system supporting authorized duplicate check and compare the storage system with file contents. The hybrid cloud architecture proposes about both the public cloud and the private cloud. Thus, identical data copies of different users will lead to different cipher texts, making De-duplication with node impossible. In order to provide more security, the private cloud is provided with multilevel authentication.

II. LITERATURE SURVEY

CONFUCIOUS: A TOOL SUPPORTING COLLABORATIVE SCIENTIFIC WORKFLOW COMPOSITION: In this paper, A research is an enabling collaboration technique in the aspect of collaboration provenance management and reproducibility. Based on scientific collaboration ontology, it proposed a service-oriented collaboration model supported by a set of collaboration primitives and patterns. The collaboration protocols are then applied to support effective concurrency control in the process of collaborative workflow composition. It also reports the design and development of Confucius, a service-oriented collaborative scientific workflow composition tool that extends an open-source, single-user environment.
TECHNOLOGY **:** Floor granting algorithm, Locking Algorithm
DISADVANTAGE **:** Do not support scientific workflow application.

SECURE AND PRACTICAL OUTSOURCING OF LINEAR PROGRAMMING IN CLOUD COMPUTING: This system investigates secure outsourcing of widely applicable Linear Programming (LP) computations. In order to achieve practical efficiency, this mechanism design explicitly decomposes the LP computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer. The resulting flexibility allows us to explore appropriate security or efficiency tradeoff via higher-level abstraction of LP computations than the general circuit representation.

REAL TIME TASKS ORIENTED ENERGY-AWARE SCHEDULING IN VIRTUALIZED CLOUDS: Energy-aware scheduling algorithms developed for clouds are not real-time task oriented, thus lacking the ability of guaranteeing system schedule ability. To address this issue, this system used a novel rolling-horizon scheduling architecture for real-time task scheduling in virtualized clouds. Based on its scheduling architecture, it develop a novel energy-aware scheduling algorithm named EARH for real-time, aperiodic, independent tasks. The EARH employs a rolling-horizon optimization policy and can also be extended to integrate other energy-aware scheduling algorithms. Furthermore, it propose two strategies in terms of resource scaling up and scaling down to make a good trade-off between task's schedule ability and energy conservation.

MEETING DEADLINES OF SCIENTIFIC WORKFLOWS IN PUBLIC CLOUDS WITH TASKS REPLICATION : The elasticity of Cloud infrastructures makes them a suitable platform for execution of deadline-constrained workflow applications, because resources available to the application can be dynamically increased to enable application speed up. Existing research in execution of scientific workflows in Clouds either try to minimize the workflow execution time ignoring deadlines and budgets or focus on the minimization of cost while trying to meet the application deadline. However, they implement limited contingency strategies to correct delays caused by underestimation of tasks execution time or fluctuations in the delivered performance of leased public Cloud resources.

METHODS

1) User Registration.
2) File Upload.
3) Key Comparison.
4) Root Priority.

Log Generators

The user should ask permission to admin for user registration. When admin gives permission then OTTP will be send through User Email. Using that OTTP the user needs to register.

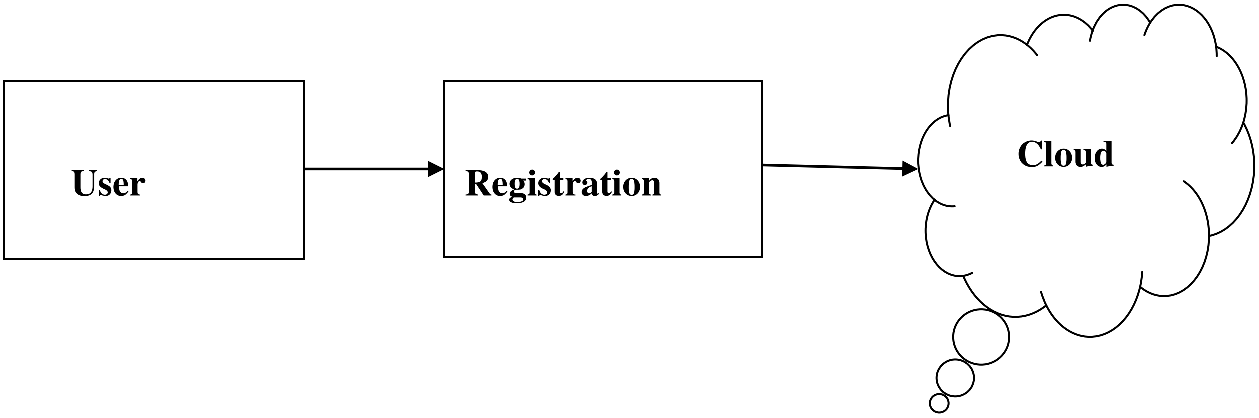


FIG 1 LOG GENERATORS

File Upload

For Storing a data file, the user can upload many files, while the file send to the server will be encrypted using AES Algorithm for Security purposes. The hacker cannot hack the file while uploading, so that it is encrypted using AES Algorithm so that no issues of hacking occur.

Key Comparison

After uploading file, for every file key will be generated using MD5 and Shah Algorithm. Keys will be stored in hash table for comparison purposes. With the Key of the file is compared to other file keys for maintain single copy of data. Such that any issue arises, single copy can be easily removed.

Root Priority

The User who first uploads a file will be the first root node, then the second who uploads the same file will the second node, third who uploads the same file will be the third node so on. Suppose the first user who uploads the file deletes the copy then the second who uploads the same file will be root of the node. The basic idea of secure De-duplication services can be implemented given additional security features insider attacker on De-duplication and outsider attacker by using the detection of masquerade activity which means unknown person stolen and damage the data. So, we confusion of the attacker and the additional costs incurred to distinguish real from fake information added, and the deterrence effect which, although hard to measure, plays a significant role in preventing from the attackers, that will harmful for our data.

III. CONCLUSION

The newly proposed system is complete system to securely outsource log records to a cloud provider. In this work, find out the challenges for a secure cloud-based log management service. The attackers use below three steps to hack. First, the attacker can intercept any message sent over the Internet. Second, the attacker can synthesize, replicate, and replay messages in his possession and the attacker can be a legitimate participant of the network or can try to impersonate legitimate hosts. It implements how to store secure log file in cloud and that file we can change read, write, delete, upload and download. It can implement AES algorithm that uses for log monitor and log generator. One of the unique challenges is the problem of log privacy that arises when we outsourced log management to the cloud. Log information in this case should not be casually linkable or traceable to their sources during storage, retrieval and deletion. It provided anonymous upload, retrieve and delete protocols on log records in the cloud using the Tor network. The protocols that it developed for this purpose have potential for usage in many different areas including anonymous publish-subscribe.

REFERENCES

[1] G. S. Aujla, R. Chaudhary, N. Kumar, A. K. Das, and J. J. P. C. Rodrigues, ‘‘SecSVA: Secure storage, verification, and auditing of big data in the cloud environment,’’ IEEE Commun. Mag., vol. 56, no. 1, pp. 78–85, Jan. 2018, doi: 10.1109/MCOM.2018.1700379.

[2] 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, doi: 10.1109/TPDS.2010.183.

[3] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, ‘‘Authentication in cloud-driven IoT-based big data environment: Survey and outlook,’’ J. Syst. Architect., vol. 97, pp. 185–196, Aug. 2019, doi: 10.1016/j.sysarc.2018.12.005.

[4] H. Hou, J. Yu, and R. Hao, ‘‘Cloud storage auditing with deduplication supporting different security levels according to data popularity,’’ J. Netw. Comput. Appl., vol. 134, pp. 26–39, May 2019, doi: 10.1016/j.jnca.2019.02.015.

[5] J. Gants and D. Reinsel. Digital Universe Decade—Are You Ready?’’ [Online]. Available: https://www.emc.com/collateral/analyst-reports/idcdigital-universe-are-you-ready.pdf

[6] X. Jia and J. Zhou, ‘‘Leakage resilient proofs of ownership in cloud storage, revisited,’’ in Applied Cryptography and Network Security. Lausanne, Switzerland: Springer, 2014, pp. 97–115, doi: 10.1007/978-3-319-07536 -5_7.

[7] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, ‘‘Dynamic-hash-table based public auditing for secure cloud storage,’’ IEEE Trans. Services Comput., vol. 10, no. 5, pp. 701–714, Sep./Oct. 2017, doi: 10.1109/TSC.2015.2512589.

[8] J. Han, Y. Li, and W. Chen, ‘‘A lightweight and privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities,’’ Comput. Stand. Interfaces, vol. 62, pp. 84–97, Feb. 2019, doi: 10.1016/j.csi.2018.08.004.

[9] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, ‘‘Proofs of ownership in remote storage systems,’’ in Proc. CCS, Chicago, IL, USA, Oct. 2011, pp. 491–500, doi: 10.1145/2046707.2046765.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. CCS, Alexandria, VA, USA, 2007, pp. 598–609, doi: 10.1145/1315245.1315318.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi cross ref

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details