Division And Replication of Data in Cloud for Optimal Performance and Security

[1] Ms.R.Nithya,[2] S.Samrin Nisha
[1] *Assistant Professor, Department of Computer Science, Bon Secours College for Women, Thanjavur*
[2] *Scholar, Department of Computer Science, Bon Secours College for Women, Thanjavur*

***Abstract*— Security issues arise when data is outsourced to a third party for administrative control, as is the case with cloud computing. Attacks by other users and cloud nodes might result in data vulnerability. Therefore, to safeguard data that jointly addresses security and performance challenges, strong security measures are needed. We split the file into pieces and spread the pieces of data among the cloud nodes. Only a single fragment of a specific file is stored on each node, ensuring that even in the event of a successful attack, the attacker is not exposed to any important information. We demonstrate that it is very unlikely to find and compromise every node holding the pieces of a single file.**

***Keywords*— administrative control, attacker, fragments of a single file.**

I. INTRODUCTION

On-demand self-services, pervasive network connectivity, resource pooling, flexibility, and measurable services are characteristics of cloud computing. Cloud computing is a compelling choice for adoption by companies, organisations, and individual users due of the aforementioned features. One of the most important factors preventing the widespread use of cloud computing is security. Every participating entity needs to be secure for a cloud to be considered secure. It is necessary to safeguard the data that is outsourced to a public cloud. It is necessary to stop unauthorised individuals and processes from accessing data, whether on purpose or by mistake. In order to address the security and performance concerns jointly, we suggest in this project that data be divided and replicated on the cloud for optimal performance and security. The DROPS approach, We split a file into pieces and spread the pieces of data among the cloud nodes. Only one piece of information is stored on each node, ensuring that even in the event of a successful attack, the attackers won't be able to access any sensitive information. The purpose of this project is to design the application which implements DROPS to offer protection to the file saved in public cloud from the attackers. The goal of this project is to protect files stored on public cloud servers from hackers. Users of the off-site data storage cloud utility must transfer data within the shared and virtualised cloud environment, which raises a number of security issues. Many users can share physical resources thanks to the cloud's flexibility and pooling. Additionally, the shared resources could occasionally be redistributed to other users, which might endanger data using data recovery techniques. Moreover, a virtual machine (VM) may transcend the limitations of a virtual machine monitor (VMM) in a multi-tenant virtualised environment. Other VMs may be able to obtain unofficial data due to interference from the fugitive virtual machine. Similarly, data integrity and privacy may be jeopardised by cross-tenant virtualised network access. Inadequate media sanitisation might potentially cause leaks.

II. LITERATURE SURVEY

Every mentoring program is built on top of Performance Analysis Systems. Without a doubt, a person will progress with the guidance and assistance of statistical data, which will also help the business where he works succeed. A background inquiry is carried out in order to look at similar contemporary approaches that are utilised to analyse student performance. Before starting our literature research, we first learn about three existing systems that are comparable to the suggested system.

Cloud computing data enters: energy-efficient data replication

We examine data replication in cloud computing data centres in this work. Unlike previous methodologies available in the literature, we evaluate both energy efficiency and bandwidth usage of the system, in addition to the increased Quality of Service as a result of the decreased communication delays. A new paradigm called

cloud computing uses a network to deliver computer resources as a service. For many cloud applications, communication resources frequently represent a bottleneck in the service providing process. Therefore, data replication, which delivers data closer to data users, is considered as a possible option. It makes it possible to reduce bandwidth consumption and network latency.

Problems with data security in cloud computing

Combining several current technologies, including distributed computing, grid computing, parallel computing, and others, cloud computing is an alluring concept. Businesses are saving millions of dollars by implementing cloud computing because of its pay-as-you-go pricing model. Because more and more people and businesses are depending on the cloud for their data. Through the internet, it provides its users with low-cost services including data storage, processing power, and shared resources at any time and from any location.

This raises the question of how safe the cloud environment is, even while cloud computing offers numerous benefits but also some security issues.

Description of Data Centre Networks' Structural Robustness

Examine the resilience of the most advanced DCNs in this research. Our main contributions include: (a) presenting multi-layered graph modelling of different DCNs; (b) conducting a comparative analysis by studying the classical robustness metrics with different failure scenarios; (c) demonstrating the insufficiency of the classical network robustness metrics to accurately assess the DCN robustness; and (d) proposing new methods to quantify the DCN robustness. There isn't a thorough investigation focussing on the DCN resilience at the moment. As a result, we think that this work will provide a solid basis for further DCN robustness research. inspired by the issue of cloud storage access management.

Access control and assured deletion for secure overlay cloud storage

This article explains how to save data management expenses by outsourcing off-site data backups to third-party cloud storage providers. However, since the data is being held by third parties, we must offer security guarantees for it. We create and deploy FADE, a secure overlay cloud storage solution that provides file guaranteed destruction and fine-grained, policy-based access control. FADE is based on a set of cryptographic key operations that are self-maintained by a quorum of key managers and are not dependent on third-party clouds in order to accomplish such security objectives. Specifically, FADE functions as a seamless overlay system on top of the cloud storage systems available today. It links outsourced files to file access policies and, in the event that file access policies are revoked, deletes the files to prevent anyone from recovering them. FADE's proof-of-concept prototype is implemented on top of Amazon S3, a modern cloud storage service.

Privacy and security problems in the cloud computing environment

A potent architecture for carrying out complicated and large-scale computation is cloud computing. From the standpoint of the user, the two main issues with the cloud are privacy and information security. The architecture, data security, and privacy concerns of cloud computing, including data confidentiality, integrity, authentication, trust, service level agreements, and regulatory challenges, are surveyed and evaluated in this study. This paper's goal is to critically examine and thoroughly explore the present privacy and data security difficulties that cloud computing faces. It increases the capabilities of information technology (IT) by offering devoted users on-demand access to computer resources. obstacles that cloud computing faces in terms of data security and privacy, and evaluate these problems critically.

III. System Implementation

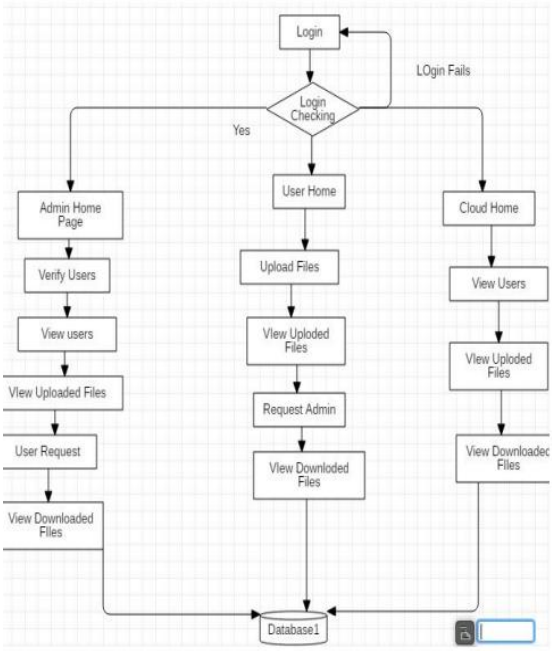
Existing System

A cloud computing paradigm known as "cloud storage" stores data on distant computers that may be accessed online. A cloud storage service provider maintains, runs, and oversees it on a storage server that uses virtualisation methods. This cloud is public; the user may store the file in the cloud storage and also offer the protection to the file by encrypting the file.

Proposed System

We introduce DROPS, which judiciously splits user files into fragments and stores them in key cloud locations. A file can be divided into pieces based on user-specified criteria as long as each fragment doesn't include any important information. The whereabouts of several cloud pieces should not be made public by a successful assault on a single node. We choose the nodes such that they are

not next to each other and are spaced a specific distance apart in order to further enhance security and keep an attacker guessing about where the file fragments are. The information file is fragmented and replicated between cloud nodes by the intended theme. Even if an attack is successful, the suggested DROPS technique makes sure that the attacker doesn't learn any important information. For data security, we don't use conventional encryption methods. The suggested scheme's non-cryptographic nature speeds up the necessary information insertion and retrieval processes. To increase security, we ensure that the file pieces are reproduced in a controlled manner, with each fragment being replicated only once.



Proposed Architecture

Methodology

1) Cloud Client: This person should be either the owner or the user of the data.

Data Owner: The data owner is in charge of uploading files to the cloud and seeing files that have been posted by others or by himself. Information on the fragment that was deposited and its replicas, together with their cloud node numbers, are available to the data owner.

The person in charge of downloading or viewing material uploaded by others is known as the data user. He must be an authorised user in order to download anything from the cloud; otherwise, he will be viewed as an attacker.

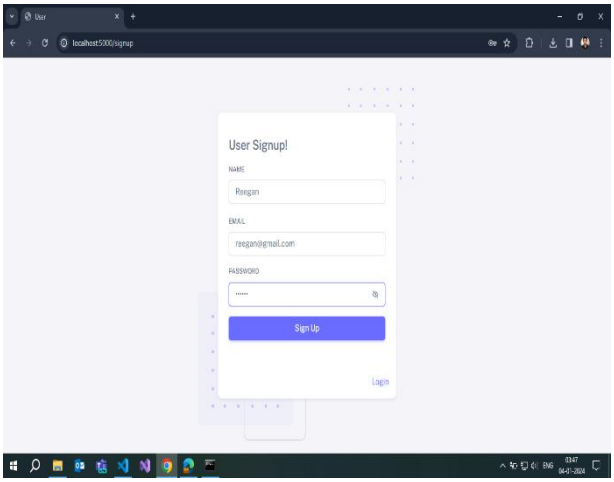
Admin: - Admin is an authorised individual with the authority to verify authorised users and data owners. Along with maintaining information and authentication, he is also in charge of block allocation.

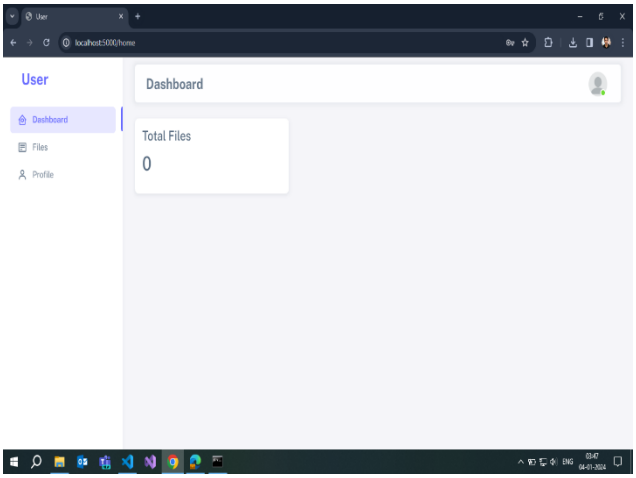
2) Cloud Server:-Fragmentation: This method is employed to divide the file for server-side security. The Fragmentation algorithm is used in this method. It takes a file as input and outputs file fragments.

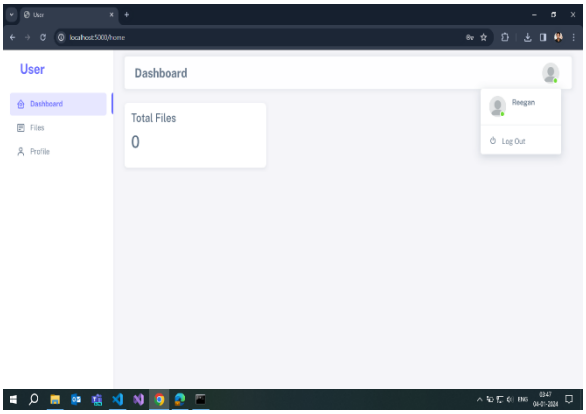
Replication: This method makes duplicate copies of the pieces. These replicas are helpful in the event that an attacker corrupts one of the pieces. The administrator may then replace the replica there, join all of the fragments, and transmit the file to the authorised user or data owner. This method creates replicas of file fragments by using a replication algorithm that receives fragments as input and outputs replicas.

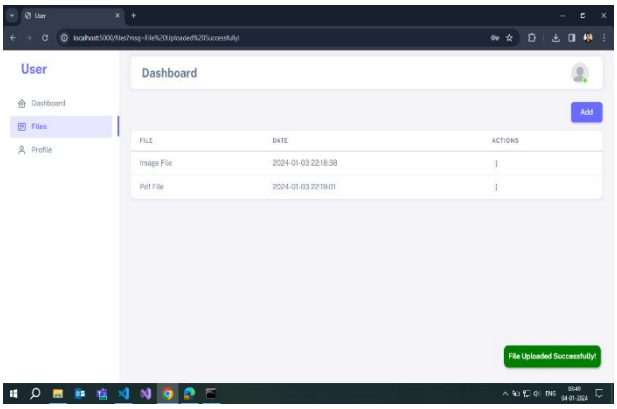
Allocation: We must assign those pieces to a cloud server for data storage when the file is spit out and replicas are created. We must take security concerns into account while allocating or storing such parts.

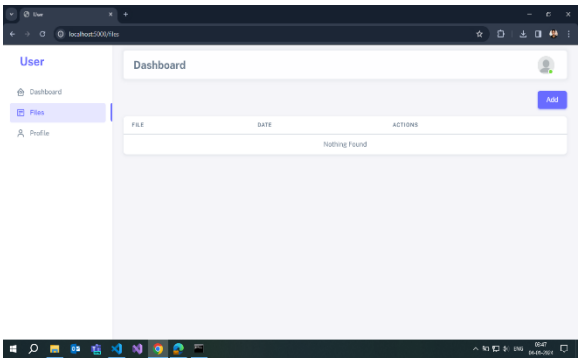
Experimental Results

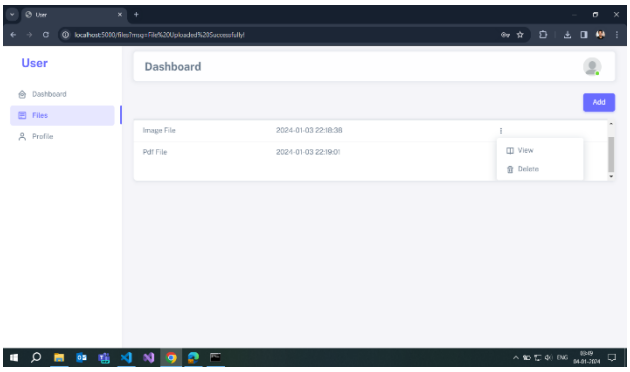


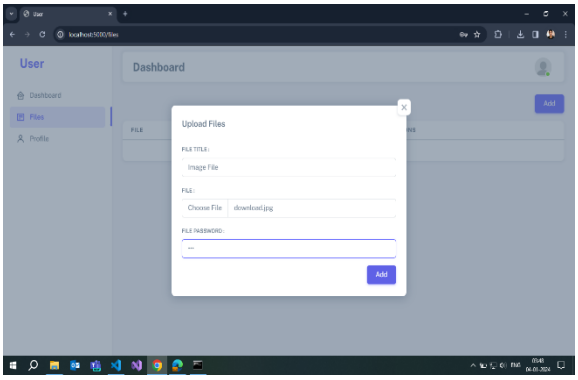


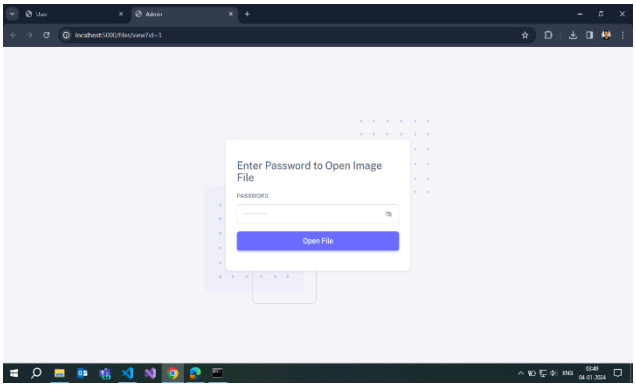

User
Dashboard
Total Files
0
Reegan
Log Out

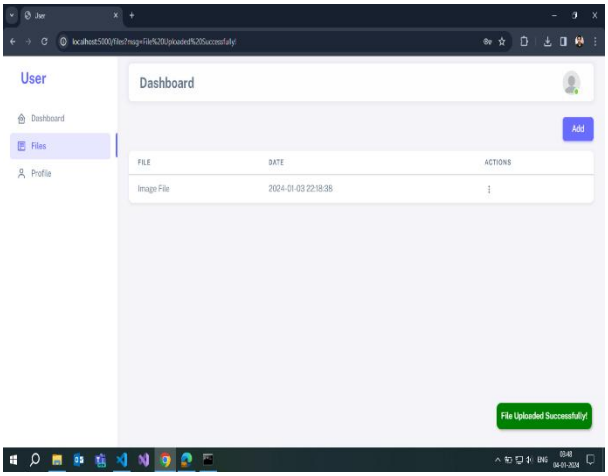

User
Dashboard
Add
FILE
DATE
ACTIONS
Image File
2024-01-03 22:18:38
Pdf File
2024-01-03 22:19:01
File Uploaded Successfully!

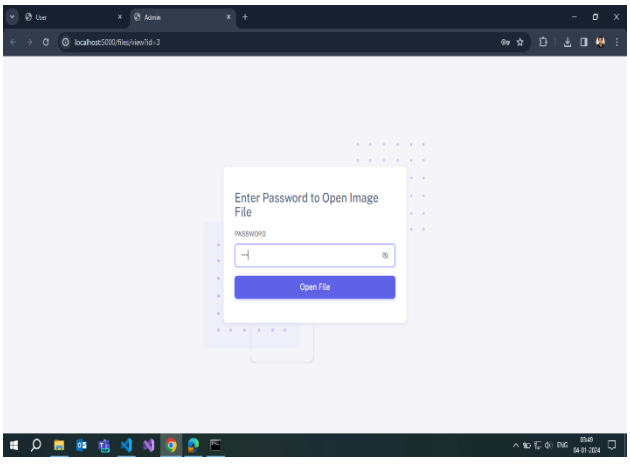

User
Dashboard
Add
FILE
DATE
ACTIONS
Nothing Found


User
Dashboard
Add
Image File
2024-01-03 22:18:38
Pdf File
2024-01-03 22:19:01
View
Delete


User
Dashboard
Add
Upload Files
FILE TITLE :
Image File
FILE :
Choose File
download.jpg
FILE PASSWORD :
Add


Enter Password to Open Image File
PASSWORD
Open File


User
Dashboard
Add
FILE
DATE
ACTIONS
Image File
2024-01-03 22:18:38
File Uploaded Successfully!


Enter Password to Open Image File
PASSWORD
Open File

IV. CONCLUSIONS

The Division and Replication of Data in Cloud, a novel methodology put forward in this study, addresses both security and retrieval time concerns. The information record was split up, and its components are dispersed among several nodes. The T-coloring approach was used to separate the nodes. In the event of a successful attack, the fragmentation and dispersion guarantee that no vast amounts of data are accessible to an adversary. No cloud node stored more than a single section of a comparable document. Compared to full-scale replication solutions, our Division and Replication of Data in Cloud methodology performed better. The results of the reenactments showed that the simultaneous focus on security and execution resulted in a somewhat lower execution level and a higher degree of information security.

At the moment, a user must download the file, update its contents, and then submit it again using the DROPS process. Creating an automated update system that will only create and update the designated fragments is a wise move.

REFERENCES

[1] "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security," Mazhar Ali, Samee U. Khan, IEEE 2023.

[2] In their May 2023 Technical Report CMU-CS-01-120, J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla discuss how to choose the best data distribution plan for a long-lasting storage system.

[3] S. U. Khan and I. Ahmad, "Evaluation and comparison of ten Internet data replication methods based on static heuristics," Journal of Parallel and Distributed Computing, Vol. 68, No. 2, pp. 113–136,2022.

[4] "Energy-efficient data replication in cloud computing datacenters," by D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, in IEEE GlobecomWorkshops,pp. 446-451,2022.

[5] Loukopoulos and I. Ahmad, "Genetic algorithms for static and adaptive distributed data replication," Journal of Parallel and networked Computing, Vol. 64, No. 11, pp. 1270-1285, 2021.

[6] Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, pp. 1771-1783,2021, "Quantitative comparisons of the state of the art data centre architectures," by K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya.

[7] Journal of Internet Services and Applications, Vol. 4, No. 1, pp. 1–13, 2020; K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing."

[8] "Incentives for cooperation in peer-to-peer networks," by K. Lai, M. Feldman, I. Stoica, and J. Chuang, in Proceedings of the First Workshop on Economics of Peer-to-Peer Systems, pp. 631660, 2020.

[9] The International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2019, Manisha Kalkal and Sona Malhotra, "Replication for Improving Availability and Balancing Load in Cloud Data Centres."

[10] In the Proceedings of the 5th International Conference on Cloud Computing, Hatman, S. M. Khan and K. W. Hamlen, "Intra-cloud trust management for Hadoop,"

[11] Privacy, "security and trust issues arising from cloud computing," in Proceedings of the 2nd International Conference on Cloud Computing, pp. 693702, 2018 by S. Pearson and A. Benameur.

[12] "Privacy-preserving digital identity management for cloud computing," IEEE Data Eng. Bull, vol. 32, no. 1, pp. 2127, March 2018. E. Bertino, F. Paci, R. Ferrini, and N. Shang.

[13] In Proc. 10th Int. Conf. Web Inf. Syst. Eng., pp. 275289, 2017, F. Skopik, D. Schall, and S. Dustdar, "Start trusting strangers bootstrapping and prediction of trust."

[14] H. Guo, J. Huai, Y. Li, and T. Deng, "KAF: Kalman filter based adaptive maintenance for dependability of composite services," in Proceedings of the 20th International Conference on Advanced Information Systems, pp. 328342, 2016.

[15] Y. Wei et al., "Cloud computing and service-oriented computing: Opportunities and Challenges," IEEE Internet Comput., vol. 14, no. 6, pp. 7275, Nov./Dec. 2015.