NVEO
Natural Volatiles &
Essential Oils

Implementation Of Reliable Data Storage Service Within The Concept Of Metacloud

Karpov Dmitry Anatolievich[a] , **Ghassan Adnan Hammoodi Al-Bdairi** [a*1]

[a] MIREA Russian Technological University , Moscow, Russia.

Abstract. The article considers the implementation of the metacloud service allowing for the solution of blocking and/or information loss while using cloud computing due to the provider or government bodies' activities (including other countries) at information access blocking and/or its disclosure. The proposed solution enables to provide storage reliability and computerize the process of modifications synchronization introduced by the user.

Keywords: metacloud, cloud storage, data security, protection from information blockout, cloud computing.

Introduction

As it is known, cloud computing is the provision of computing services on the customer's request, from data storage and computing resources to applications. As a rule, the access is usually Internet-based and subject to payment (for general users a service paid by contextually targeted advertising can be provided).

The appearance of a multicloud is historically connected with the use of several public clouds at the rise of these services aiming to avoid both dependence on one provider and different services of arising cloud providers.

The authors developed and introduced the concept of metacloud service implementation which allows for automatic data synchronization in several independent clouds of different providers and information protection from blocking, corruption or deletion it from the provider and/or government bodies [14,15].

To verify the availability of the proposed concept a Web-service for metacloud management was developed and implemented.

The introduced web service performs data control in several clouds [1-4] and has two modes of operation: the operating mode synchronizes changes and the freezing mode stores all clouds' states at power-up time and rolls back at switching to the saved state. Operating procedure is shown in Figure 1.

At web service startup the authorization home page opens [16-19], the user enters his e-mail and password for authentication in the system. Having pressed the login button the system checks the correctness of the entered data, and if they are correct, the user is redirected to the page with the main functionality, otherwise he must enter the data again. When you hit this page [20-23], you can control the service operation using interface elements. The following commands are available:

1. Start

This command launches the main service and switches to the operating mode, connects to the clouds and generates the list of modified and new added files for each cloud [5-8]. If it is not empty, all unauthorized loaded files are deleted. The next step is to create the list of deleted files and directories based on data in other clouds. If it contains the list of deleted files, they are recovered from data in other clouds [24]. This approach also detects and cancels unauthorized files modifications, replacing them with the correct versions from other clouds unaffected by the attack.

When the initial synchronization of all clouds is completed, the control commands are returned to the standby mode.

2. Stop

The service stop procedure leads with clouds content synchronization. For this purpose, lists of files deleted by the user followed by their removal from the rest clouds of metacloud, are formed. Similarly lists of modified [9-12] and added files are generated and copied to all connected clouds.

Then the service goes into the freezing mode and the state is considered to be reference at that time [13,14].

The last step in this command processing is to return to the standby mode of the control commands.

3. Add cloud

This command enables you to connect a new cloud storage to the metacloud.

To add a new storage you must select a cloud provider from the list of supported ones, enter authentication data in the corresponding service windows. Then a new cloud will be added to the metacloud structure and will participate in processes to ensure reliable information storage.

When the procedure for adding the cloud to the system is completed, the system enters the standby mode of the control commands.

4. Delete cloud

In the current implementation the cloud delete command is limited to excluding the cloud from the metacloud structure, so that the content of the deactivated cloud stops participating in storage reliability processes. Meanwhile, user information delete from the cloud does not takes place, only authentication data is removed.

Following the completion of the cloud deletion, the transition to the standby mode of control commands occurs.

5. Time out

If the user has not shown any activity in cloud management, then the service in the freezing mode just continues expecting new commands. And if the operating mode is set, the service starts a cycle of checking clouds content in order to detect modifications and their iterations in all clouds of the metacloud immediately.

The operating cycle includes procedures of searching for files deleted by the user with further deleting from other clouds, and procedures of searching for added or changed files leading to further modifications and updates distribution to all clouds of the metacloud.

After the cloud content comparison is completed, the service returns to the control command standby mode.

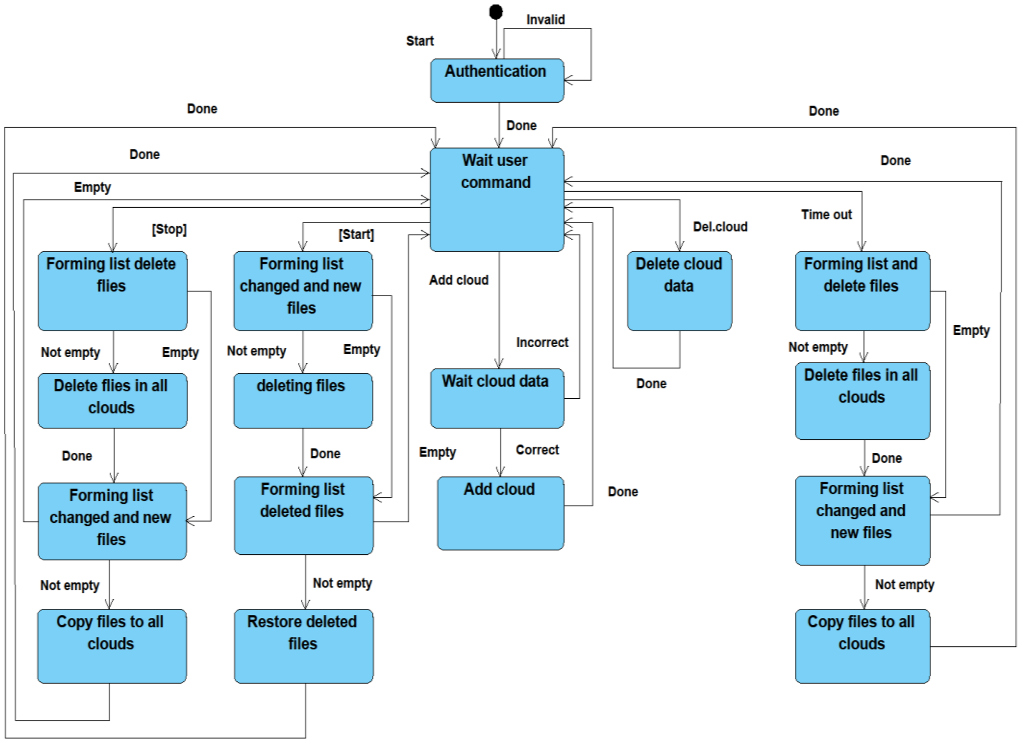

Figure 1. State chart temporary service chart when comparing clouds.

Let’s consider temporary service chart when comparing clouds’ content and modifications distribution introduced by the user in all clouds of the metacloud. The chart is shown in Figure 2.

Step 1. The user downloads a file in Cloud 1 and waits for the download’s completion.

Step 2. Metacloud management program searches for modifications in Cloud 1 and receives the answer from Cloud 1 containing information about a new file.

Step 3. Metacloud management program copies the added file from the cloud (Copying 1).

Step 4–5. Then this file is copied into all clouds of the metacloud (Copying 2 - Coping X).

Step 6–7. Modification search is repeated at a time in the rest of all clouds of the metacloud. As it is shown in Figure 2, Clouds 2 - X inform about the lack of modified files.

Step 8–9. Startup of a new search from the beginning (in a new iteration of the operating mode). There are no any modifications in clouds on these steps, that’s why the service does not perform any other operations.

Step 10. The user deletes the file in Cloud 1. While the metacloud service in the current checking cycle does not detect modifications since the considered cloud has been monitored before on step 8.

Step 11. Completion of modifications’ search in clouds of the metacloud. Cloud X also informs about lack of changes.

Step 12. At a new operating cycle metacloud management program finds the deleted file (step 10) and forms lists for the deletion in other clouds.

Step 13–14. File delete from the list in all clouds of the metacloud.

Further steps of the cycle on the chart aren't shown, but it is easy to understand that they will be similar to the above considered steps 6-7.

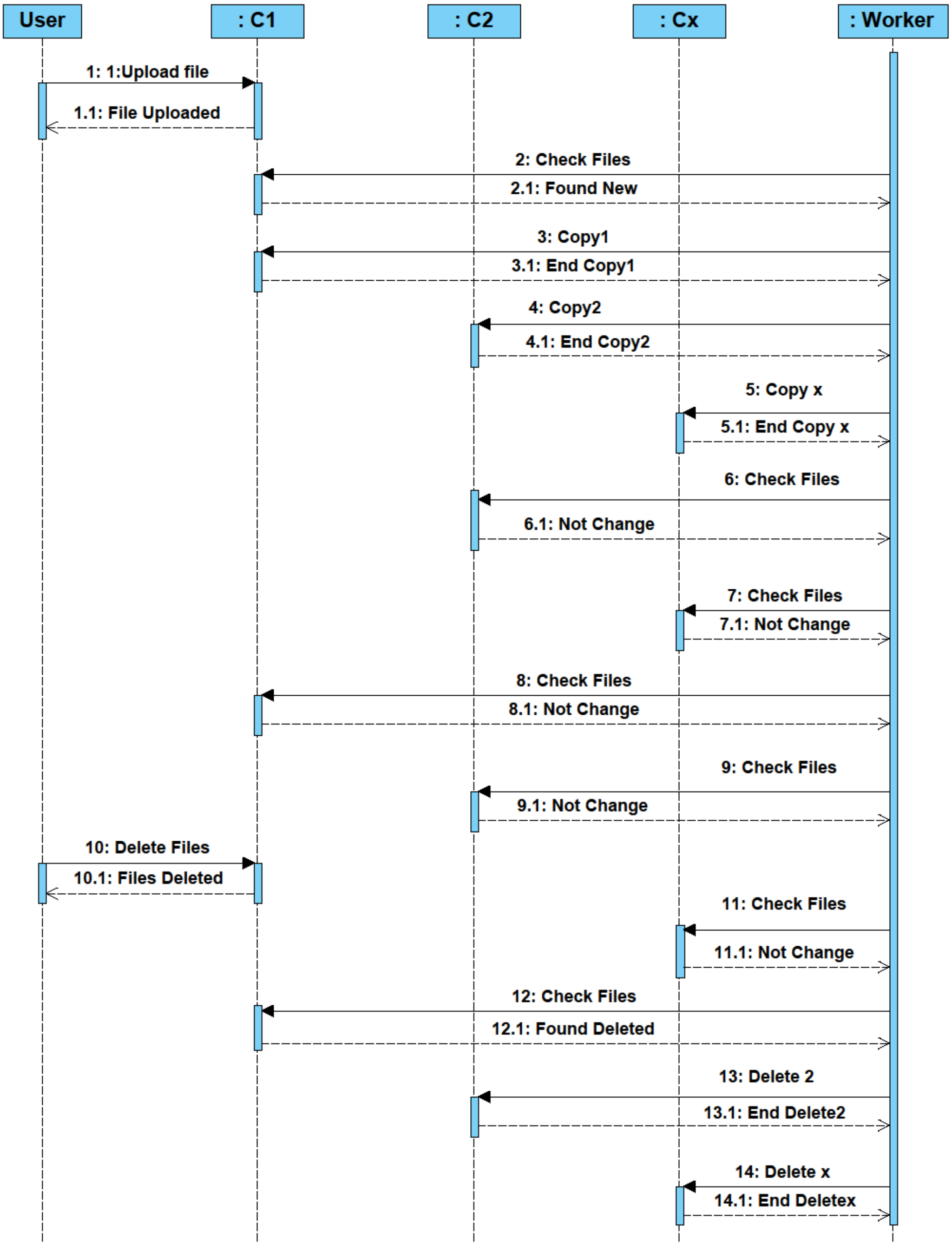

Figure 2. Workflow chart the reliable functioning of the metacloud service.

To ensure the reliable functioning of the metacloud service and prevent harm by the cloud provider and/or its country of location, it is necessary to determine the main regions for placing information and the minimum number of clouds in the metacloud structure.

Based on the analysis of the main cloud storage providers, the following regions can be distinguished:

1. The United States is characterized by great speed, good service level and the spread of mirrors around the world.
2. The EU is based on European law, but when entering the US market, accepts the requirements of United States law.

3. The Russian Federation is working over legislative initiatives to protect information from actions by foreign companies, but the risk of destroying information in teams from the owners of mirrors in case of information war aggravation is large enough. Also, the share of foreign participation in the capital of Russian cloud companies is high enough

4. Due to the domestic services implementation and isolation measures from foreign services, China provides a large share of self-sufficiency, but there are difficulties in connecting to Chinese services from other countries, and, conversely, while connecting to services of other countries from China. In particular, when traveling to China, Russians are offered to use Yandex services, not Google.

5. Regional providers work in the market of their country or region and do not claim to cover a larger territory.

The use of a large number of cloud providers with 98-99% reliability for backup is unreasonable, if they are located in various regions of influence.

Considering the original reliability of 98% and formula 1, assuming one provider destroys the data, we need minimum 3 providers to ensure 99.9% storage reliability.

$$\Delta(t) = \prod_{i=1}^{n-1}(1 - P_i(t)) - \prod_{i=1}^{n}(1 - P_i(t)) \qquad (1)$$

Therefore, the minimum list of providers should include:

– a major US cloud services provider;

– a EC average provider;

– a Russian cloud service provider.

It is worth adding a Chinese provider if you deal with APR[2] .

It is also worth including one regional provider in case of serious political differences that can lead to the blocking of other information resources.

Thus, it appears that from three to five clouds are needed to ensure the reliable metacloud functioning.

We should separately mention the reliability of the metacloud central server which ensures the data synchronization between the clouds. Similarly to an Internet provider, the metacloud server does not affect data security in the clouds, since all information can be synchronized between the clouds later. Certainly, if the main cloud is blocked at the time of temporary inoperability of the metacloud server, all the latest information will be lost, but the probability of such an event is highly possible with the operating service at the time of a pause between synchronizations. Therefore, at this stage it was decided to limit to a single metacloud server.

Conclusion

The implemented metacloud service confirmed theoretical researches and assumptions on the realization of the reliable data storage service in case of the provider's actions to destroy or block information access. At the same time the dependence of the metacloud functioning on a single control server can be referred to a minor disadvantage of the considered service. As was already mentioned in the article, the management server failure will not affect the data inside the cloud, but will only suspend the synchronization system for a while. After the service is restarted, it will continue to synchronize cloud storage. It was also found that in terms of the load reduction on the metacloud management server, it is reasonable to include from 3 to 5 cloud storage located in different countries and regions in the metacloud structure. Moreover, such amount is enough to ensure the storage reliability and availability of at least 99.9%.

References

[1] V.Yu. Shevtsov, E. S. Abramov. Analysis of modern data storage systems // Innovations in informatics. 2019.Vol. 13, No. 1. P. 25–30.

[2] I.V. Savin. Features of ensuring fault tolerance, safety and availability of data // Izvestiya TulGU. Technical science. 2019. Issue. 3.P. 118–122.

[3] Abrosimov M., Sudani K., Balance and fault tolerance in cloud computing. // Magazine "Information Security" # 4, 2018. - pp. 31–33.

[4] A.S. Vishnyakov, A.E. Makarov, A.V. Utkin, S.D. Zazhogin, A.V. Bobrov. Ensuring the protection of data presented in cloud services // Bulletin of Science and Education, 2019, No. 11-2 (65). S. 22-29.

[5] Simon Leech. Cloud Security Threats - Insecure APIs. 2017 // [Electronic resource]. - Access mode: https://community.hpe.com/t5/Grounded-in-the-Cloud/Cloud-Security-Threats-Insecure-APIs/ba-p/6871684#.WhlDqlWWbIW.

[6] Sreelekshmi S., K R Remesh Babu. Synchronized Multi-Load Balancer with Fault Tolerance in Cloud. // International Journal of Computer Information Systems and Industrial Management Applications. ISSN 2150-7988. Volume 10 (2018) pp. 107-114.

[7] Multi-cloud strategy, by Margaret Rouse 2016 https://searchcloudcomputing.techtarget.com/definition/multi-cloud-strategy#commenting

[8] Data Synchronization, By Data Integration Info Quick view on world of data http://www.dataintegration.info/data-synchronization

[9] What is multicloud? The next step in cloud computing, By David Linthicum SEP 25, 2017 https://www.infoworld.com/article/3226484/cloud-computing/what-is-multicloud-the-next-step-in-cloud-computing. html

[10] Sam Bleiberg. What are the most famous or biggest cloud security breaches events / incidents? 2018 // [Electronic resource]. - Access mode: https://www.quora.com/What-are-the-most-famous-or-biggest-cloud-security-breaches-events-incidents

[11] Fran Howarth. Identity Management in the Cloud: Top Tips for Secure Identities 2017 // [Electronic resource]. - Access mode:

https://securityintelligence.com/identity-management-cloud-tips-secure-identities-iam/

[12] Olson, John A. "Data as a Service: Are We in the Clouds?" Journal of Map & Geography Libraries. 6 (1): 76–78. doi: 10.1080 / 15420350903432739.

[13] Alhayani, B. and Abdallah, A.A. "Manufacturing intelligent Corvus corone module for a secured two way image transmission under WSN", Engineering Computations, Vol. ahead-of-print No. ahead-of-print. (2020), https://doi.org/10.1108/EC-02-2020-0107

[14] Alhayani, B.S.A., Ilhan, H. Visual sensor intelligent module based image transmission in industrial manufacturing for monitoring and manipulation problems. J Intell Manuf , 2021, 32(2), pp. 597–610 https://doi.org/10.1007/s10845-020-01590-1

[15] Alhayani, B., Abbas, S.T., Mohammed, H.J. et al. Intelligent Secured Two-Way Image Transmission Using Corvus Corone Module over WSN. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-08484-2

[16] Kwekha-Rashid, A.S., Abduljabbar, H.N. & Alhayani, B. Coronavirus disease (COVID-19) cases analysis using machine-learning applications. Appl Nanosci (2021). https://doi.org/10.1007/s13204-021-01868-7

[17] Hasan H. S., Alhayani B., et al. , "Novel unilateral dental expander appliance (udex): a compound innovative materials," Computers, Materials & Continua, vol. 68, no.3, pp. 3499–3511, 2021. https://doi:10.32604/cmc.2021.015968

[18] Abbas, S.T., Mohammed, H.J., Ahmed, J.S. et al. The optimization efficient energy cooperative communication image transmission over WSN. Appl Nanosci (2021). https://doi.org/10.1007/s13204-021-02100-2

[19] Yahya, W., Ziming, K., Juan, W. et al. Study the influence of using guide vanes blades on the performance of cross-flow wind turbine. Appl Nanosci (2021). https://doi.org/10.1007/s13204-021-01918-0

[20] B. Alhayani, S. T. Abbas, D. Z. Khutar, and H. J. Mohammed, "Best ways computation intelligent of face cyber attacks," Mater. Today Proc., 2021.

[21] B. Alhayani and H. Ilhan, "Hyper spectral image classification using dimensionality reduction techniques," Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng., vol. 5, no. 4, pp. 71–74, 2017.

[22] B. Al Hayani and H. Ilhan, "Image transmission over decode and forward based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical Internet of Things (MIoT) for remote health-care and health communication monitoring," J. Med. Imaging Heal. Informatics, vol. 10, no. 1, pp. 160–168, 2020.\

[23] Shaymaa Adnan Abdulrahman, Bilal Alhayani,A comprehensive survey on the biometric systems based on physiological and behavioural characteristics,Materials Today: Proceedings,2021,10.1016/j.matpr.2021.07.005

[24] Cisco blog. Cloud security monitoring. 2019. // [Electronic resource]. Access mode: - https://www.securitylab.ru/blog/company/cisco/346936.php