Multicloud Architecture to Enhance Security and Privacy

Ware Sayali¹, Jadhav Varsha², Sayyed Almas³, Junnare Bhagyashri⁴, Prof. M. T. Jagtap⁵

¹,²,³,⁴,⁵PVGCOE, Nashik. University of Pune.

Abstract: In today’s life the security issues and challenges are widely increases. Because, now all the data are stored on clouds. The cloud provides the security and privacy features. But, the major incident in a SaaS cloud happened in 2009 with Google Docs. It allows users to edit documents (e.g. Text’s, spreadsheet’s, presentation’s) online and share these documents with other users. So, the data which is stored on public cloud is not secure. The existing most of data storing activities are done on the single cloud system. So, the security and privacy issues are the biggest commonly occurring problem that are phasing today. The proposed system is based on Multi-Cloud feature. The data stored on Multi-Cloud is in splitted format. The homomorphic Encryption and Decryption techniques are used to provide more features to proposed system. The splitting of data is in segments. The proposed system keeps the backup of that data on multiple clouds like the RAID system.

Keywords: Multi-Cloud, SaaS, Security, Privacy, Encryption, Decryption

1. Introduction

The use of cloud computing has increased rapidly in many organizations small and medium companies use cloud computing services for different reasons because these services provide fast access to their application and reduce their infrastructure cost. Cloud provider should address privacy and security issues as a matter of high priority. Dealing with single cloud provider is becoming less popular with customer’s.

This system focuses on the issues related to the data security and privacy aspects of cloud computing. As data and information will be shared with a third party, cloud computing client’s want to avoid an untrusted cloud providers. Protecting private and important information, such as credit card details or a patient’s medical record from attacker’s is of critical importance. In addition, the potential for migration from a single cloud to multi-cloud environment is examined and research related to security issues in multi-cloud in cloud computing is surveyed.

2. Security issues in Cloud

The Security and privacy challenges are still amongst the largest obstacles when considering the adaption of cloud services. This triggered a lot of research activities, resulting in quantity of proposals targeting the different cloud security threats. In 2009, a major incident with a SaaS cloud happened with “Google Docs”.

There are following drawbacks of the existing system:
1. Standalone security and privacy system
2. Malicious attacks are not handled by single cloud
3. Data encryption is not supported
4. Data integrity and confidentiality is not provided.

Fig 1. Key Challenges in Cloud Computing.

3. Proposed System Architectures

The proposed system architecture describes the flow of overall system like encryption, decryption, cloud connectivity, splitting and merging the file, uploading & downloading the file these are various activities that are performed.

The basic idea is to use multiple different clouds at the same time to overcome the risk
of malicious data manipulation, disclosure and process tampering.

Fig2. System Architecture.

4. Architectural Patterns

Architectural patterns are used for distributing resources to multiple cloud providers. This model is used to discuss the security and privacy benefits.

In proposed system the following four architectural patterns are discuss:

4.1 Replication of applications:

Instead of executing a single application on specific cloud, the same operation is executed by multiple distinct clouds. It allows to receive multiple results from one operation performed in distinct clouds and to compare them.

Fig3. Replication of application systems.

4.1.1 Dual Execution

In such a situation, a first approach for verification might be that a cloud customer triggers the creation of its annual accounting report more than once. For instance, instead of giving the same request to one cloud provider only, a second cloud provider that provides an equivalent type of service is invoked in parallel.

4.1.2 n Clouds Approach

A more complex, but also more advanced approach comes from the distributed algorithms discipline: The Byzantine Agreement Protocol. Assume the existence of n cloud provider, of which f collaborate maliciously against the cloud user, with n > 3f. In that case, each of the n clouds performs the computational task given by the cloud user. Then, all cloud providers collaboratively run a distributed algorithm that solves the General Byzantine Agreement problem.

4.1.3 Processor and Verifier

Instead of having Clouds A and B perform the very same request, another viable approach consists in having one cloud provider “monitor” the execution of the other cloud provider.

4.2 Partition of Application System into Tiers:

System into tiers allows to separate the logic from the data object. It gives additional protection against data leakage due to flaws in the application logic.

Fig4. Partition of Application System into Tiers.

4.3 Partition of Application Logic into Fragments:

It allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application.
4.3.1 Obfuscating Splitting

By this approach, application parts are distributed to different clouds in such a way, that every single cloud has only a partial view on the application and gains only limited knowledge. Therefore, this method can also hide parts of the application logic from the clouds. For application splitting, a first approach is using the existing sequential or parallel logic separation. Thus, depending on the application, every cloud provider just performs subtasks on a subset of data.

A difficult challenge of obfuscating splitting in general is the fact that there is no generic pattern for the realization.

4.3.2 Homomorphic Encryption Technique and Secure Multiparty Computation

Homomorphic encryption and secure multiparty computation both use cryptographic means to secure the data while it is processed. In homomorphic encryption, the user encrypts the data with his public key and uploads the cipher texts to the Cloud. The cloud can independently compute on the encrypted data to obtain an encrypted result, which only the user can decrypt. Therefore, in our scenario, homomorphic encryption uses an asymmetric fragmentation, where the user (or a small trusted private cloud) manages the keys and performs the encryption and decryption operations, while the massive computation on encrypted data is done by an untrusted public cloud.

4.4 Partition of Application Data into Fragments:

It allows distributing fine grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

Each of the introduced architectural patterns provides individual security merits, which map to different application scenarios and their security needs.

5. Conclusion

The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. As the approaches investigated in this paper clearly show, there is no single optimal approach to foster both security and legal compliance in an Omni applicable manner. Moreover, the approaches that are favourable from a technical perspective appear less appealing from a regulatory point of view, and vice versa. The few approaches that score...
sufficiently in both these dimensions lack versatility and ease of use, hence can be used in very rare circumstances only.

As can be seen from the discussions of the four major multicloud approaches, each of them has its pitfalls and weak spots, either in terms of security guarantees, in terms of compliance to legal obligations, or in terms of feasibility. The every type of multi cloud approach falls into one of these four categories; this implies a state of the art that is somewhat dissatisfying.

6. References


4. Maha TEBAA,"SecureCloud Computing through Homomorphic Encryption",aboratory of Mathematics, Computer and Applications, University Mohammed VAgdal, Faculty of Science, Rabat Morocco, maha.tebaa@gmail.co.


9. R. Shobana,"SECURITY AND PRIVACYHANCING MULTI CLOUD ARCHITECTURES", Vinayaka Missions University Chennai, Tamil Nadu, India.