© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Enhancing Security of Multi-cloud Architecture using combination of approaches

A.Linda Alice, P. M. C Nisha, S. Sivagami
Department of Information Technology, Velammal Institute of Technology, Anna University, India

ABSTRACT

In Public cloud when it is used for the practical application which is outside the User's premises, there are several security issues are arising. These can be overcome by the use multi cloud architecture there they are using four kinds of approach like replication of application, partition application system into tiers ,partition of application logic into fragments , partition of data into fragments. In each every approach there are benefits and pitfalls. In the proposed paper we are initiating the idea of combining more than one approach so as to reach security features like integrity, confidentiality, availability, applicability, ease of use and compliance.

Keywords: cloud, web server, cloud computing, Resource pooling, IaaS, Paas

I. INTRODUCTION

The word "cloud" is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud. Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility over a network (typically the Internet).cloud offers services on demand fashion.

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. [1] The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions.

With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications. As per the National Institute of Standards and Technology's definition of cloud computing gives "five essential characteristics":

- **On-demand self-service**. A consumer can one-sidedly supply computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access**. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling**. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- **Rapid elasticity**. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

- **Measured service**. Cloud systems automatically control and optimize resource use by leveraging a metering Capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud computing offers three types of services like infrastructure as service (IAAS), software as service(SAS) and platform as service(PAS). In the IAAS it offers physical or virtual machines and other resources. SAS offers Services to the users to access application software and databases on pay per use basis. It also referred as "on demand software" service. The third service PAS delivers a computing platform, typically including operating system, programming language execution environment, database, and web server to the users.

Multi Cloud Security Aspects

Typically there three types of clouds are available such as public cloud, private cloud and hybrid cloud. Public cloud strategy the resources are outside the user's location where as in private cloud resources are available inside the user's premises. Hybrid cloud is nothing but combination of private and public cloud. Multi cloud denotes the usage of multiple independent combinations of public, private clouds by a client or a service.

In public clouds, all of the three common cloud service layers (IaaS, Paas, SaaS) share the commonality that the end-users’ digital assets are taken and processed outside the user’s premises. This creates lot of security issues, when considering cloud computing adoption [3]. The idea for reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple clouds.[4]. Several approaches employing this paradigm have been proposed recently. They are having difference in partitioning and distribution patterns, technologies, cryptographic methods and targeted scenarios as well as Security levels which is described in the paper [5]. It provides four distinct models in form of abstracted multi-cloud architectures. These Developed multi-cloud architectures allow to categorize the available schemes and to analyze them according to their security benefits. [5]

This paper is an extension of [5] and contains the idea of combining the approaches to provide strong confidentiality, availability and other security aspects in the multi cloud environment. In paper [5] it distinguishes the following four architectural patterns.

- **Replication of Applications** allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the user to get evidence on the integrity of the result.
- **Partition of Application System into Tiers** allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.
- **Partition of Application Logic into Fragments** 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. Thus, this leads to data and application confidentiality.
- **Partition of Application Data into Fragments** 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, and demerits which map to different application scenarios and their security needs. This paper initiates the idea of combining patterns that can be combined resulting in combined security Merits, but also in higher deployment and runtime effort.

Replication of Application

How does a cloud customer know whether his data was processed correctly within the cloud? There is no technical way to guarantee that an operation performed in a cloud system was not tampered with or that the cloud system was not compromised by an attacker. The guarantee is based on the level of trust between the cloud customer and the cloud provider and on the contractual regulations made between them such as SLAs, applicable laws and regulations of the involved jurisdictional domains. But there still remains a residual risk of getting compromised by third parties because the data's are taken and processed in the public clouds which is outside the user's premises.

There are several approaches are followed for the replication of application like dual execution, n-cloud approach, processor and verifier. Each and every approach is having various benefits.

II. METHODS AND MATERIAL

A. N Clouds Approach

In this approach we are assuming the existence of n clouds of which of collaborate maliciously against the cloud user, with n > 3f. In that case, each of the n clouds performs the same computational task given by the cloud user.[figure 3.1]. Then, all cloud providers collaboratively run a distributed algorithm. After that it is guaranteed that all non-malicious cloud providers know the correct result of the computation. Hence, in the final step, the result is communicated back to the cloud user via a Secure Broadcast .Hence, the cloud user can determine the correct result even in presence of f malicious clouds. The benefits of these methods are strong integrity, availability, applicability, usability [5].

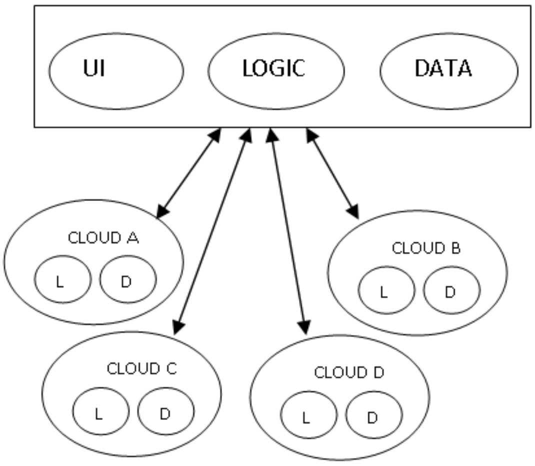

Figure 1: N-Cloud Approaches

B. Partition of Application System into Tiers

This approach provides the evidence for the integrity when the computations performed on the third party resources. It targets on the risk of undesired data leakage.

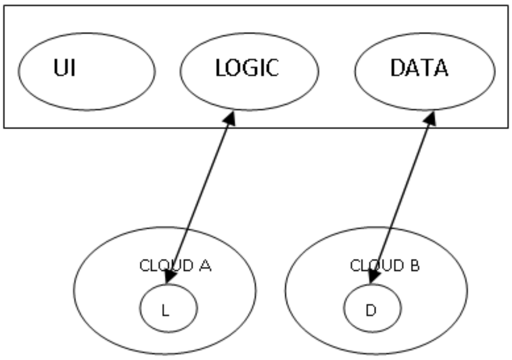

Figure 2: Partition of application system into tiers

One more thing is the cloud user has to select a particular—probably specially trusted—cloud provider for data storage services and a different cloud provider for applications. The partitioning of application systems into tiers and distributing the tiers to distinct clouds provides some coarse-grained protection against data leakage in the presence of flaws in application design or implementation.

Partition of Application Data into Fragments

In this architecture specifies that the application data is partitioned and distributed to distinct clouds. Files are common forms of data storage in databases. Files typically contain unstructured data (e.g. pictures, text documents) and do not allow for easily splitting or exchanging parts of the data.

Databases contain data in structured form organized in columns and rows. Here, data partitioning can be performed by distributing different parts of the database (tables, rows, columns) to different cloud providers. Finally, files can also contain structured data (e.g. XML data). Here, the data can be splitted using similar approaches like for databases. XML data, cryptographic data splitting etc.

C. Cryptographic Data Splitting

The basic cryptographic method to store data securely is to store the data in encrypted form. While the cryptographic key could remain at the user's premises, to increase flexibility in cloud data processing or to enable multi-user systems it is beneficial to have the key available online when needed [6].

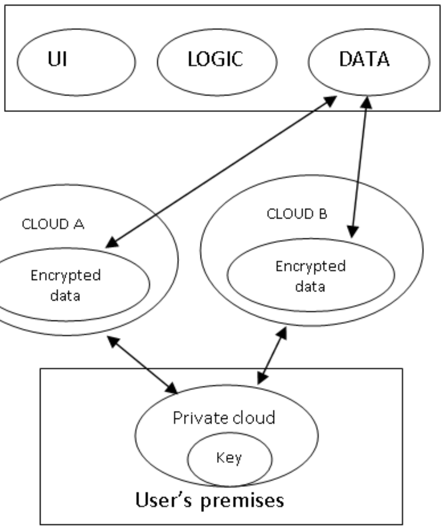

Figure 3: Cryptographic Data Splitting

This approach therefore distributes key material and encrypted data into different clouds. The best approach to cryptographic cloud storage [7] is a solution for encrypted key/value storage in the Cloud while maintaining the ability to easily access the data. It involves searchable encryption [8], [9] as the key component to achieve this. Searchable encryption allows keyword search on encrypted data if an authorized token for the keyword is provided.

III. RESULTS AND DISCUSSION

Combining Multi Cloud Architecture Approaches

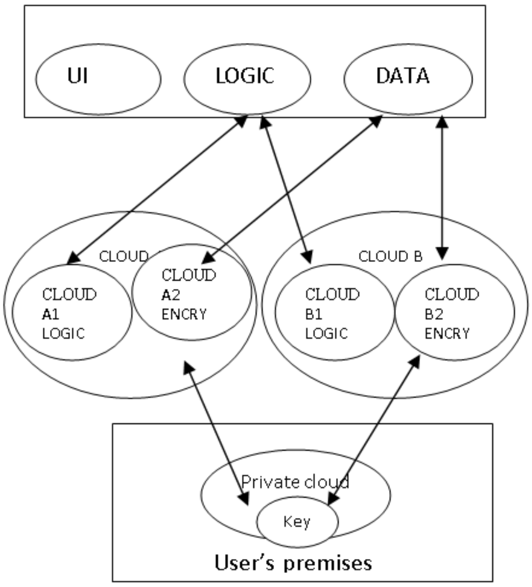

Figure 4: Combination of approaches

In the above seen approaches each and every approach provides some specific benefits and drawbacks. So by combining the approaches we can provide all the benefits like integrity, availability, confidentiality, applicability, compliance etc. For instance, the n clouds approach gives high benefits in terms of integrity, availability. The partition of application system of tiers gives benefits on applicability and ease of use. And the third approach cryptographic splitting provides strong confidentiality and compliance. So the idea is by combining these approaches will provide strong Integrity, availability, confidentiality, applicability, compliance which was described in figure.

IV. CONCLUSION

The use of multi cloud environment has the capability of processing user demand and distributing work to resources deployed across multiple clouds. In this we have combined only three approaches to avoid all the security risks in the multi cloud architecture. Likewise in the future we can combine some other approaches to get effective on demand services in the multi cloud environment.

V. REFERENCES

[1] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[2] Rouse, Margaret. "What is a multi-cloud strategy". Search Cloud Applications. Retrieved July 2014.

[3] F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits &Challenges," Blog post on IDC Survey, 2008. [Online]. Available: http://blogs.idc.com/ie/?p=210

[4] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L. L. Iacono, "Security prospects through cloud computing by adopting multiple clouds," in 4th IEEE International Conference on Cloud Computing (CLOUD). IEEE, 2011.

[5] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy Enhancing Multi-Cloud Architectures",

[6] S. Kamara and K. Lauter, Cryptographic cloud storage," Financial Cryptography and Data Security, pp. 136–149, 2010.

[7] F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud," in Proceedings of the 1st International Workshop on Securing Services on the Cloud (IWSSC), 2011.

[8] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[9] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in Advances in Cryptology–CRYPTO 2005. Springer, 2005, pp. 205–222