Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 406-408, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.ssps.212

Securing Data in Multi Cloud Using Data Access Control

G. Sulthana Begam, B. Shanthini and S. Rajeswari

St.Peter's College of Engineering and technology, Avadi, Chennai, India

Abstract: Cloud Computing is a new paradigm in which Infrastructure resources, application platform and software are delivered as an Utility Service over the internet for the costomer on pay per use basis. The multi-cloud approach is an extended version of the hybrid cloud idea which integrates n-clouds.The applications can use different infrastructures or services provided by different cloud service provider in parallel or on demand.To develop a framework to provide secure interoperation in the multi cloud architecture and to address Specific security issues like trust, policy, and privacy.

Key words: Multi Cloud · Security Issues · Trust · Confidentiality

INTRODUCTION

Cloud mashups are a recent trend mashups combine services from multiple clouds into a single service or application, offer more-sophisticated services today, cloud mashups require pre established agreements among providers as well as the use of custom-built, proprietary tools that combine services through low-level, tightly controlled and constraining integration techniques.

Clouds can be classified considering the physical location into account [1]. A public cloud is offered by third-party service providers and involves resources outside the user's premises. In case the cloud system is installed on the user's siteusually in the own data center—this setup is called private cloud. Different applications may have different business requirements that influence the choice of public or private clouds. hybrid cloud connects a private cloud or an on-premise IT infrastructure with a public cloud to add the additional resources on-demand. The multi-cloud approach is an extended version of hybrid cloud which integrates N-Clouds used in SaaS and IaaS service model..

At present multi-cloud used in the IaaS Service model connects cloud infrastructures provided by different cloud service provider that applications can use different infrastructures or services in parallel or on demand. Multi-cloud has a special importance in the SaaS area. The amount of new SaaS applications is growing from day to day and with that the demand to integrate this varying solutions and let exchange the data.

Multi Cloud Architectures: There are different types of architectural patterns for multi clouds[2][3].

Replication of Applications in Distinct Clouds: It 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 verify the integrity of the result deployed to the cloud. On the other hand, it needs to be noted that it does not provide any protection in respect to the confidentiality of data or processes. On the contrary, this approach might have a negative impact on the confidentiality because—due to the deployment of multiple clouds—the risk rises that one of them is malicious or compromised. It need to implement protection against an unauthorized access to data. This architectural concept can be applied to SaaS- service model.

Partition of Application System into Tiers: It allows to separate the application logic from the data. This gives additional protection against data leakage due to flaws in the application logic. The architecture targets the risk of undesired data leakage. 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 errors in application design or implementation. This architectural concept can be applied to all three cloud services. This architecture requires standardized interfaces to couple applications with data services provided by distinct CSP.

Corresponding Author: G. Sulthana Begam, St.Peter's College of Engineering and technology, Avadi, Chennai, India.

Partition of Application Logic into Fragments: It allows distributing the application logic to distinct clouds. The advantage of this pattern are

- Cloud provider can not learn the complete application logic.
- Cloud provider may not know the overall calculated result of the application. Which leads to data and application confidentiality.

Multi Cloud Needs and Challenges:

- Support for of breed' approach where customers can choose modular solutions that best suited their needs from a wide range of different vendors.
- To eliminate single point of failures
- Establishing trust among different cloud providers
- The integration of the many different and usually independent operating cloud services and their interfaces to each other which increases system complexity
- Loss of client's control over resources and data.
- Threats that target exposed interfaces due to data storage in public domains
- Data privacy concerns due to multi-tenancy

Specific Risks in Multi-Cloud Environments:

- Security breaches.
- Risk of costs unpredictability.

Comparison of Multicloud Architectures: Since there are many possible multi cloud architectures, it is not feasible o perform a general evaluation adequately covering all of them. However, in this section we perform a high-level comparison of all multi cloud approaches presented above, based on their capabilities in terms of security, feasibility and compliance. Therein, the security considerations indicate an approach's general improvements and aggravations in terms of integrity, confidentiality and availability of application logic or data, respectively. These Multi cloud approachs is highly beneficial in terms of integrity (every deviation in execution that occurs at a single cloud provider only can immediately be detected and The feasibility aspect covers issues of applicability, business readyness and ease of use. Herein, applicability means the degree of flexibility of using one approach to solve different types of problems. Business-readyness evaluates how far the research on a multi cloud approach has progressed and if it is ready for real-world applications, whereas ease of use indicates the complexity of implementing the particular approach. As an example, the approaches of secure multiparty computation may be of high benefits in terms of security, but only solve a very specific type of computation problem and are quite complex to implement even if they can be applied reasonably[4].

The compliance dimension provides a high-level indication of the impact of each approach to the legal obligations implied to the cloud customer when utilizing that approach. Application of the dual execution approach, for instance, maybe favorable in terms of security and feasibility, but requires complex contractual negotiations between the cloud customer and two different cloud providers, doubling the workload and legal obligations for the whole cloud application. Equivalently, the use of more than two different cloud providers (n clouds approach) improves on integrity and availability, but also requires n contract negotiations and risk assessments, amplified by the necessity to assess the risks associated with automated detection and correction of irregularities within then parallel executions [5].

Proposed Work: The issue of securing data and interoperation in multi-cloud environment was addressed. To develop a framework that allows Partition of application System into tiers of application logic and application data distributing to distinct clouds. The cloud user has the choice to select specially trusted-cloud provider for data storage services and a different cloud provider for applications.

Outsourced data introduces new security challenges, importantly ensuring the integrity of data. we consider the task of allowing a Third Party Auditor (TPA) on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud making use of its independent computing resources. public auditability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information.

The proposed scheme has four important features:

- It enables indirect mutual trust between the owner and the CSP (Cloud Service Provider).
- It allows the owner to outsource data to a CSP and perform dynamic operations on the outsourced data, i.e., modification, insertion, deletion and append.

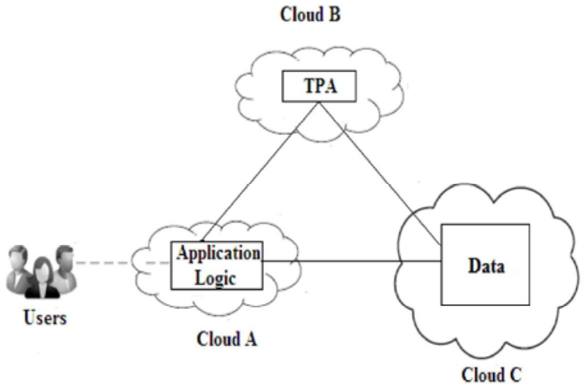

Fig. 1: Partition of application system into tiers.

- It allows owner to grant right to authorized users to access the remote data
- It ensures that authorized users receives the latest version of the outsourced data.
- It allows the owner to grant or revoke access to the outsourced data.

Implementation: The cloud computing storage model considered in this work consists of four main components as illustrated in Fig. 1:

- data owner that can be an organization or individual generating sensitive data to be stored in the cloud and made available for controlled external use for authorized users.
- CSP who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users.
- Authorized users—a set of owner's clients who have the right to access the remote data and
- Trusted Third Party (TTP), an entity who is trusted by all other system components and has capabilities to find unauthorized users and malicious intruders.

Homomorphic Encryption: The data owner has a File F consisting of m blocks. For confidentiality, the owner encrypts the data before sending to cloud servers. After data outsourcing, the owner can interact with the CSP to perform block-level operations on the file. In addition, the owner enforces access control by granting or revoking access rights to the outsourced data [6].

To access the data, the authorized user sends a data-access request to the CSP and receives the data file in an encrypted form that can be decrypted using a secret key generated by the authorized user. The TTP is an independent entity, however, any possible leakage of data toward the TTP must be prevented to keep the outsourced data private. The TTP and the CSP are always online, while the owner is intermittently online. The authorized users are able to access the data file from the CSP even when the owner is offline.

CONCLUSION

To develop a framework that allows Partition of application System into tiers of application logic and application data distributing to distinct clouds and to secure the data was proposed. Three are some important issues which are relevant in multi-cloud environments: interoperability issues between services offered by different providers, the ease of migration from a current service to a new equivalent service and the security issues for different types of multi cloud architecture were discussed

REFERENCES

1. Mell, P. and T. Grance, "The NIST Definition of Cloud Computing, Version 15," Nat'l Inst. of Standards and Technology, Information TechnologyLaboratory, 53: 50, http://csrc.nist.gov/groups/
2. Bernstein, D., E. Ludvigson, K. Sankar, S. Diamond and M. Morrow, 2009. "Blueprint for the Intercloud-Protocols and Formats for Cloud Computing Interoperability," Proc. Int'l Conf. Internet and Web Applications and Services, pp: 328-336.
3. Celesti, V.A., F. Tusa, M. Villari and A. Puliafito, 2010. "How to Enhance Cloud Architectures to Enable Cross-Federation," Proc. IEEE Third Int'l Conf. Cloud Computing (CLOUD), pp: 337-345.
4. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono and Ninja Marnau, 2013. "Security and Privacy-Enhancing Multicloud Architectures," IEEE Transaction on Dependable and Secure Computing, 10(4): 212-223.
5. Groß, S. and A. Schill, 2011. "Towards User Centric Data Governance and Control in the Cloud," Proc. IFIP WG 11.4 Int'l Conf. Open Problems in Network Security (iNetSeC), pp: 132-144.
6. Groß, S. and A. Schill, 2013. "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Transactions on Parallel and Distributed Systems, 24(12): 2375-2385.