RESEARCH PAPER | Computer Science | Volume : 5 | Issue : 5 | May 2015 | ISSN - 2249-555X

Multicloud Architectures for Integrity and Confidentiality of Application and Data

KEYWORDS: Cloud, security, privacy, multicloud, application partitioning, tier partitioning, data partitioning

Anju Peeter
M.tech in CSE , Marian Engineering College, Trivandrum, Kerala

G.P.Simi Margaret
Asst.Professor in CSE, Marian Engineering College,Trivandrum,Kerala

ABSTRACT *The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Cloud computing creates a large number of security issues and challenges.Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple clouds .The basic underlying idea is to use multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering.Multicloud Architectures provide integrity and confidentiality for application and data.*

1 Introduction

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud computing model consists of five characteristics, three delivery models, and four deployment models [1]. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service.The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

Cloud computing creates a large number of security issues and challenges.Cloud providers should address privacy and security issues as a matter of high and urgent priority. using "single cloud" for deploying application and data is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds".Several approaches employing this paradigm have been proposed recently. They differ in partitioning and distribution patterns, technologies, cryptographic methods, and targeted scenarios as well as security levels.

2 Security prospects by multicloud architectures

The issues related to cloud security is integrity and confidentiality of application and data. The data stored in single cloud may suffer from damage during transition operations from or to the cloud storage provider. The idea of making use of multiple clouds has been proposed by Bernstein and Celesti. The basic idea is to integrate multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. Different architectural patterns like Replication of applications, Partition of application system into tiers, Partition of application logic into fragments and Partition of application data into fragments are used.

3 Replication of application

The main issues faced by application and data when stored in a single cloud provider are privacy preservation and integrity of the ressult obtained. Replication of applications allows to receive multiple results by executing multiple copies of the same application on multiple distinct clouds. By comparing the obtained results, the cloud user gets evidence on the integrity of the result.

4 Partition of application system into tiers

This architecture targets the risk of undesired data leakage by the separation of the application system's tiers and their delegation to distinct clouds.The logic and the data is stored in two different clouds sothat any flaws in the application logic does not affect data.

5 Partition of application logic into fragments

This architecture variant targets the confidentiality of data and processing logic.Data should be protected when it is processed.Instead of using single cloud for entire application logic,the logic is partitioned into fine-grained parts and these parts are distributed to distinct clouds. This approach can be instantiated in different ways depending on how the partitioning is performed. The clouds participating in the fragmented applications can be symmetric or asymmetric in terms of computing power and trust.Two concepts are common. The first involves a trusted private cloud that takes a small critical share of the computation,and a untrusted public cloud that takes most of the computational load. The second distributes the computation among several untrusted public clouds, with the assumption that these clouds will not collude to break the security. 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.

6 Partition of application data into fragments

This multicloud architecture specifies that the application data is partitioned and distributed to distinct clouds. The most common forms of data storage are files and databases. Files typically contain unstructured data and do not allow for easily splitting or exchanging parts of the data. This kind of data can only be partitioned using cryptographic

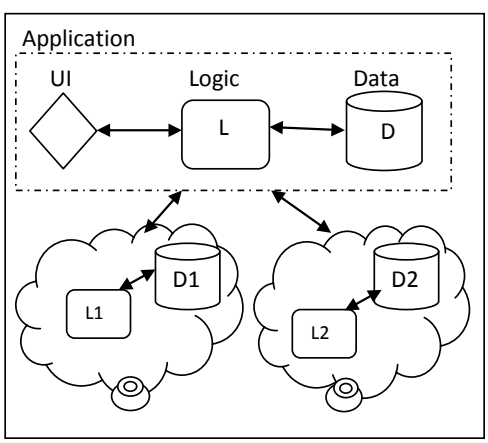
Volume : 5 | Issue : 5 | May 2015 | ISSN - 2249-555X

methods.Databases contain data in structured form organized in columns and rows. Here, data partitioning can be performed by distributing different parts of the database to different cloud providers. Finally, files can also contain structured data. Here, the data can be splitted using similar approaches like for databases. XML data, for example, can be partitioned on XML element level. However, such operations are very costly. Thus, this data are commonly rather treated using cryptographic data splitting.

7 Partition of application logic and data into fragments.

Proposed system aims to provide integrity and confidentiality for application logic and data(Fig.1)Here the application logic and data will be fragmented and distributed to distinct clouds.This approach have many advantages.Considering the application logic , no cloud provider learn the complete application logic and no cloud provider learns the over all calculated result of the application.

Fig. 1.Partition of application logic and data into fragments.



It also allows distributing fine-grained fragments of the data to distinct clouds.None of the involved cloud provider gains access to all the data,which safe guards data's confidentiality.Databases contains data in structured form organized in columns and rows.Here, data partitioning can be performed by distributing different parts of the database to to different cloud providers.Data encryption scheme also improves the confidentiality of data. To provide integrity multiple distinct clouds executing multiple copies of the same application can be deployed.Application logic can be deployed into multiple distinct clouds where same operation is performed by distinct clouds. By comparing the obtained result ,the cloud user gets evidence on the integrity of the result.

Communication Architecture

Communication architecture (Fig 2) specifies how the communication between different cloud providers and client is established. It consist of follwowing parts.

1.Service Client

It is used to access a service made available by a server. when user requests a logic to be executed, service client direct the service request to correct service provider.

2.Service Interface

Services expose their capabilities via well-defined ,standars service interfaces. Program logic is seperated from underlying technologies through the use of Interfaces each of which defines a contract between a service consumer and a service provider.Service interface helps the client to know about the data to be send to the service,input parameters,return values etc.it publish the functionalities implemented in the cloud.

3.Integration Layer

It consolidate and show the result obtained by executing the logic in the cloud.Logic will be executed on multiple distinct clouds and compare the result to get evidence on the integrity of the result and show the correct result to the user.

4.Data Security Layer

This layer is used for handling application data.Data will be encrypted by suitable encryption scheme and encrypted data will be stored in cloud.When user requests to retrieve data, encrypted data will be taken from cloud and decryption is performed by data security layer and result is shown to the user. Homomorphic encryption can be used to secure the data while it is processed.In homomorphic encryption, the user encrypts the data with his public key and uploads the ciphertexts to the Cloud. The cloud can independently compute on the encrypted data to obtain an encrypted result, which only the user can decrypt.Therefore homomorphic encryption uses an asymmetric fragmentation, where the user manages the keys and performs the encryption and decryption operations, while the massive computation on encrypted data is done by an untrusted public cloud. Pailier cryptosystem can be used for implementing homomorphic encryption.It include keygeneration,encryption and decryption.A simpler variant of key generation is used here.

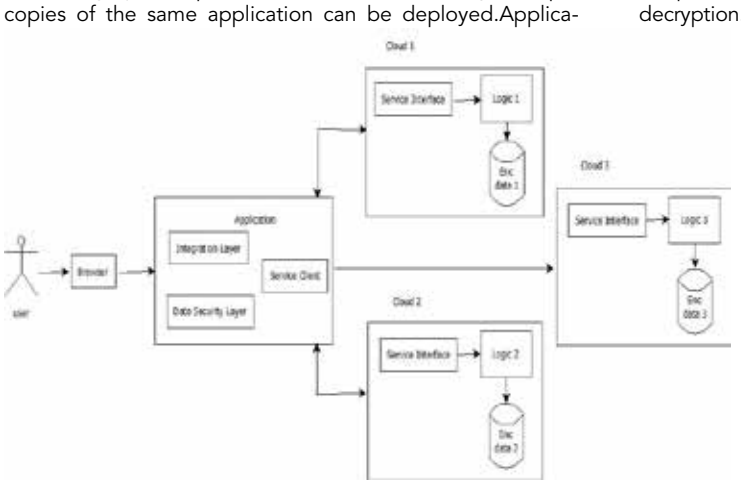


Fig. 2.Communication Architecture

Volume : 5 | Issue : 5 | May 2015 | ISSN - 2249-555X

Key generation
1.Choose two large prime numbers *p* and *q* of equivalent length gcd(pq,(p-1)(q-1)=12 .Compute n=pq and λ=(p-1)(q-1)

3 .Select random integer g where g=n+1

4.Compute $\mu=[(p-1)(q-1)]^{-1} \bmod n$

Public key (n,g)

Private key (λ, μ)

Encryption
1.Let m be a message to be encrypted where

$m \lambda Z_n$

2.Select random r where $\lambda\lambda Z_\lambda^*$

3.Compute ciphertext as $c=g^m r^n \bmod n^2$

Decryption
1. Ciphertext $\lambda \lambda Z_\lambda^{2*}$

2. Compute message:

$\lambda = ((\lambda^\lambda \bmod \lambda^2) - 1)/n) \ \lambda \bmod n)$

Homomorphic properties
A notable feature of the Paillier cryptosystem is its homomorphic properties. As the encryption function is additively homomorphic, the following identities can be described:

Homomorphic addition of plaintexts
1.The product of two ciphertexts will decrypt to the sum of their corresponding plaintexts,

$D(E(m_1,r_1).E(m_2,r_2) \bmod n^2)=m_1+m_2 \bmod n$

2.The product of a ciphertext with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,

$D(E(m_1,r_1).g^{m2} \bmod n^2)=m_1+m_2 \bmod n$

Homomorphic multiplication of plaintexts
1.An encrypted plaintext raised to the power of another plaintext will decrypt to the product of the two plaintexts,

$D(E(m_1,r_1)^{m2} \bmod n^2)=m_1m_2 \bmod n$

$D(E(m_2,r_2)^{m1} \bmod n^2)=m_1m_2 \bmod n$

2.More generally, an encrypted plaintext raised to a constant *k* will decrypt to the product of the plaintext and the constant,

$D(E(m_1,r_1)^{k} \bmod n^2)=k\ m_1m_2 \bmod n$

However, given the Paillier encryptions of two messages there is no known way to compute an encryption of the product of these messages without knowing the private key.

8 Conclusion
This paper focus on integrity and confidentiality of application logic and data. By Partitioning and deploying the application logic and data into multiple clouds, confidentiality of logic and data can be improved. Homomorphic encryption allows to store and process the encrypted data in the cloud.Use of multiple distinct clouds to execute multiple copies of the same application provides integrity for the result.

REFERENCE [1]. P. Mell and T. Grance(2010), "The NIST Definition of Cloud Computing, Version 15," Nat'l Inst. of Standards and Technology, Information Technology Laboratory, vol. 53, p. 50, http://csrc.nist.gov/groups/ SNS/cloud-computing/. | [2]. J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L.Iacono(2011),"Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing(CLOUD). | [3] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen(2013, july/august), Member, IEEE,Luigi Lo Iacono, and Ninja Marnau," Security and Privacy-Enhancing Multicloud Architectures" ieee transactions on dependable and secure computing, vol. 10, no. 4. | [4]. M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono(2009), "On Technical Security Issues in Cloud Computing," Proc. IEEE Int'l Conf. Cloud Computing(CLOUD- II),. | [5].S.Kamara and K. Lauter(2010), "Cryptographic Cloud Storage," Proc.14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149. | [6]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky(2006), "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13thACM Conf. Computer and Comm. Security, pp. 79-88. | [7]. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone Lee, G. Neven, P. Paillier, and H. Shi(2005), "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions," Proc. 25th Ann. Int'l Conf. Advances in Cryptology (CRYPTO '05), pp. 205-222. | [8]. R. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan(2009), "CryptDB: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp. Operating Systems Principles, pp. 85-100, 2011. [44] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order- Preserving Symmetric Encryption," Proc. 28th Ann. Int'l Conf. Advances in Cryptology: The Theory and Applications of Cryptology (EUROCRYPT '09), pp. 224-241. | [9]. R. Rivest, A. Shamir, and L. Adleman(1978), "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126. | [10]. A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill(2009), "Order-Preserving Symmetric Encryption," Proc. 28th Ann. Int'l Conf. Advances in Cryptology: The Theory and Applications of Cryptology (EUROCRYPT '09), pp. 224-241. | [11]. L. Wiese(2010), "Horizontal Fragmentation for Data Outsourcing with Formula-Based Confidentiality Constraints," Proc. Fifth Int'l Workshop Security (IWSEC '10), pp. 101-116. |