Multicloud Architecture To Enhance Security And Privacy

Abstract

Security provocations are largest barrier in view of assumption of cloud services. There are set of investigation actions and amount of schemes are done on clearing those difficulties. Away from these security problems, the cloud consists of group of distinct characteristics, pro cogency and structure. It produces a survey on feasible security excellence by manufacturing utilization of numerous dentine clouds at the same time. Different dentine structures are launch and talk over as stated by their security and privacy capacity and expectation. We propose privacy and security to cloud users with less computation cost and minimum time. By using that Multicloud architecture we propose a two layer encryption and decryption method which provides double security to cloud users data. We propose Attribute based encryption to provide security to cloud users data. In propose system we take care for cloud failure which prevents data lost. So this method provides high privacy and double security to users.

1 Introduction

1.1 Detail Problem Definition

Now a day, while using cloud services we may face security challenges like hacking of private data or misuse of data by unauthorized person. Thus lots of research activities are trying to solve this. From these activities MULTICLOUD ARCHITECTURE is one of the solutions. By using Multicloud architecture we divide our data into different forms and store it onto two different clouds. If any cloud provider or unauthorized user wants to gain that data he cannot get the whole data because different parts of data are stored onto different clouds. We also have provided CRYPTOGRAPHIC MECHANISM to retrieve from and store that data onto cloud.
1.2 Justification of problem

One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple 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. This paper is an extension of and contains a survey on these different securities by Multicloud adoption approaches. It provides four distinct models in form of abstracted Multicloud architectures. These developed Multicloud architectures allow to categorize the available schemes and to analyze them according to their security benefits. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular.

1.3 Objective

The objective of this paper is to divide data into different parts and then store it onto multiple clouds which maintain privacy. To achieve data security of cloud users by using encryption and decryption cryptographic techniques.

1.4 Problem Statement

- To provide data into different parts and then store it onto multiple clouds which maintains privacy.
- To achieve data security of cloud users by using encryption and decryption cryptographic techniques.
- To achieve data security of cloud users by using Attribute Based Encryption technique.

2 Cloud security issues

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more if deploying data processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. As can be seen from this review of the related work on cloud system attacks, the cloud computing paradigm contains an implicit threat of working in a compromised cloud system. If an attacker is able to infiltrate the cloud system itself, all data and all processes of all users operating on that cloud system may become subject to malicious actions in an avalanche manner. Hence, the cloud computing paradigm requires an in-depth reconsideration on what security requirements might be affected by such an exploitation incident. For the common case of a single cloud provider hosting and processing all of its user’s data, an intrusion would immediately all security requirements: Accessibility, integrity, and confidentiality of data and processes may become violated, and further malicious actions may be performed on behalf of the cloud user’s identity. These cloud security issues and challenges triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues, the cloud paradigm comes with a
new set of unique features that open the path toward novel security approaches, techniques, and architectures. One promising concept makes use of multiple distinct clouds simultaneously.

2.1 Security prospects by Multicloud Architectures

The basic idea is to use multiple distinct clouds to vanish or overcome the risks of malicious data manipulation, and disruptions in processes. By integrating many distinct clouds, the trust assumption can be lowered to an assumption of non-collaborating cloud service providers. By introducing multi cloud it makes much harder Multicloud Architecture to enhance Security and Privacy for an external attacker to retrieve or damage the hosted data or applications of a particular cloud user. Many security techniques and methods are adopted to solve the issues in the cloud. In multi cloud, cryptographic methods such as encryption and decryption and key management are used. Database splitting is one of the other important security techniques in involving a multi cloud.

3 Major Part Of Multi Cloud Architecture

Replication of applications: Replication of applications allows receiving 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. Instead of executing a particular application on one specific cloud, the same operation is executed by distinct clouds. By comparing the obtained results, the cloud user gets evidence on the integrity of the result. In such a setting, the required trust toward the cloud service provider can be lowered dramatically. Instead of trusting one cloud service provider totally, the cloud user only needs to rely on the assumption, which the cloud providers do not collaborate maliciously against it.

Partition of application System into tiers: Partition of application System into tiers allows separating the logic from the data. This gives additional protection against data leakage due to the application logic. The architecture introduced in targets the risk of undesired data leakage. It answers the question on how a cloud user can be sure that the data access is implemented.

Multicloud Architecture to enhance Security and enforced effectively that errors in the application logic do not a fact the users data. Partition of application logic into fragments: 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: Partition of application data into fragments allows distributing ne-grained fragments of the data to distinct clouds. None of the involved cloud providers...
gains access to all the Multicloud Architecture to enhance Security and Privacy data, which safe guards the data confidentiality.

4 Need of proposed system

As can be seen from this review of the related work on cloud system attacks, the cloud computing paradigm contains an implicit threat of working in a compromised cloud system. If an attacker is able to inferate the cloud system itself, all data and all processes of all users operating on that cloud system may become subject to malicious actions in an avalanche manner. Hence, the cloud computing paradigm requires an in-depth reconsideration on what security requirements might be acted by such an exploitation incident. For the common case of a single cloud provider hosting and processing all of its users data, an intrusion would immediately a security requirements: Accessibility, integrity, and con veniality of data and processes may become violated, and further malicious actions may be performed on behalf of the cloud users identity.

These cloud security issues and challenges triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Along- side with these security issues, the cloud paradigm comes with a new set of unique features that open the path toward novel security approaches, techniques, and architectures. One promising concept makes use of multiple distinct clouds simultaneously. We propose privacy and security to cloud users with less computation cost and minimum time. By using that Multicloud architecture we propose a two layer encryption and decryption method which provides double security to cloud user’s data. We pro- pose Attribute based encryption to provide security to cloud user’s data. In Existing method there is no solution for cloud failure and there may be chances of data lost due to any one cloud failure. In propose system we take care for cloud failure which prevents data lost. So this method provides high privacy and double security to users.

5 Comparison of existing systems with proposed system & Applications

In Existing method there is no solution for cloud failure and there may be chances of data lost due to any one cloud failure. In propose system we take care for cloud failure which prevents data lost. We propose privacy and security to cloud users with less computation cost and minimum time. By using that Multicloud architecture we propose a two layer encryption and decryption method which provides double security to cloud user’s data. We propose Attribute based encryption to provide security to cloud user’s data. So this method provides high privacy and double security to users.

Applications
Following are some applications:
- To enhance the security and privacy of cloud users.
- Mostly used in Industrial Data Storage
- Also useful in Banking storage for storing the data of different branches.

6 Literature survey and problem statement

6.1 Study of existing systems

Now a day, while using cloud services we may face security challenges like hacking of private data or misuse of data by unauthorized person. Thus lots of research activities are trying to solve this. From these activities Multicloud Architecture is one of the solutions. By using Multicloud
architecture we divide our data into different forms and store it onto two different clouds. If any cloud provider or unauthorized user wants to gain that data he cannot get the whole data because different parts of data are stored onto different clouds. They have provided Cryptographic Mechanism to retrieve from and store that data onto cloud. In Existing method there is no solution for cloud failure and there may be chances of data lost due to any one cloud failure. Cloud computing creates a large number of security issues and challenges. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more, if deploying data-processing applications to the cloud, a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple 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. It is an extension of and contains a survey on this different security by multicloud adoption approaches. It provides four distinct models in form of abstracted multicloud architectures. These developed multicloud architectures allow to categorize the available schemes and to analyze them according to their security benefits. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular.

6.2 Analysis of existing systems
- O. Catrina Says Secure Multiparty Computation (SMC) protocols enable a group of parties to perform a joint computation with private inputs. To provide privacy protection they are using various e-commerce applications, e.g., benchmarking and collaborative supply chain management and planning. It could benefit from secure multiparty application. It also explores SMC approaches and research directions, aiming at providing better support for e-commerce applications.
- M.Jensen demonstrate on technical security issues arising from the usage of Cloud services and especially by the underlying technologies used to build these cross-domain Internet-connected collaborations. Cloud Computing offers dynamically scalable resources provisioned as a service over the Internet and therefore promise a lot of economic benefits to be distributed among its adopters. Depending on the type of resources provided by the Cloud of distinct layers.
- N.Gruschka aims on raising awareness of this issue while discussing vulnerability in Amazon’s Elastic Compute Cloud (EC2) services to XML wrapping attacks, which had since been resolved as a result of our findings and disclosure. They were discussed the verification steps required to effectively validate an incoming SOAP request. It reviews the available work in the light of the discovered Amazon EC2 vulnerability and provides a practical guideline for achieving a robust and effective SOAP message security validation mechanism.
- P. Mell represented important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models form a simple taxonomy that is not intended to prescribe or constrain
any particular method of deployment, service delivery, or business operation. He developed the NIST Model that is National Institute of Standard and Technology.

- Celesti represents general cloud architecture; they highlighted such limitations and propose some enhancements which add new federation capabilities. In order to address such concerns they proposed a solution based on the Cross-Cloud Federation Manager, a new component peaceable inside the cloud architectures, allowing a cloud to establish the federation with other clouds according to a three-phase model: discovery, match-making and authentication.

- J.-M. Bohli contributed a concept which achieves security merits by making use of multiple distinct clouds at the same time. Besides the security issues coming with the cloud paradigm, it can also provide a new set of unique features which open the path towards novel security approaches, techniques and architectures. They were introduced, which aims at reducing the required level of trust and which provides innovative cloud security mechanisms in form of architectural patterns.

- Yan zhu proved the security of our scheme based on multi prove zero knowledge proof system, which can satisfy completeness, knowledge soundness, and zeroknowledge properties. They articulate performance optimization mechanisms for our scheme, and in particular present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. Their experiments show that our solution introduces lower computation and communication overheads in comparison with non-cooperative approaches.

### 7 Methodology of Proposed System Architecture

![Figure 2: Architecture of Proposed System](image)

#### 7.1 Methodology

One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple 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. This paper is an extension of and contains a survey on these different securities by multicloud adoption approaches. It provides four distinct models in form of abstracted multicloud architectures. These developed multicloud architectures allow to categorize the available schemes and to analyze them according to their security benefits. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular.

We propose privacy and security to cloud users with less computation cost and minimum time. By using that Multicloud architecture we propose a two layer encryption and decryption method which provides double security to cloud user’s data. We propose Attribute based encryption to provide security to cloud users data. In Existing method there is no solution for cloud failure and there may be chances of data lost due to any one cloud failure. In propose system we take care for cloud failure which prevents data lost. So this method provides high privacy and double security to users.

There are few Modules are described below:

**7.2 N Clouds Approach**

A more advanced, but also more complex approach comes from the distributed algorithms discipline: the Byzantine Agreement Protocol. Assume the existence of n cloud providers, of which f collaborate maliciously against the cloud user, with n is greater than 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. 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 algorithm. Hence, the cloud user can determine the correct result even in presence of f malicious clouds.

**7.3 Processor and Viable**

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. For instance, Cloud A may announce intermediate results of its computations to a monitoring process run at Cloud B. This way, Cloud B can verify that Cloud A makes progress and sticks to the computation intended by the cloud customer. As an extension of this approach, Cloud B may run a model checker service that varies the execution path taken by Cloud A on-the-fly, allowing for immediate detection of irregularities.

**7.4 Cryptographic Data Splitting**

Probably, the most basic cryptographic method to store data securely is to store the data in encrypted form. While the cryptographic key could remain at the users premises, to increase edibility in cloud data processing or to enable multiuser systems it is beneficial to have the key available online when needed. This approach, therefore, distributes key material and encrypted data into different clouds. A similar approach is taken by several solutions for secure Cloud storage: The rest approach to cryptographic cloud storage is a solution for encrypted key/value storage in the cloud while maintaining the ability to easily access the data. It involves searchable encryption as the key component to achieve this. Searchable encryption allows keyword search on encrypted data if an authorized token for the keyword is provided. The keys are stored in a trusted private cloud whereas the data resides in the un trusted public cloud.
7.5 Database Splitting

For protecting information inside databases, one has to distinguish two security goals: confidentiality of data items or confidentiality of data item relationships. In the rest case, data splitting requires a scenario similar to other approaches presented before with at least one trusted provider. However, very often only the relationship shall be protected, and this can be achieved using just honest-but-curious providers. For splitting a database table, there are two general approaches: Vertical fragmentation and horizontal fragmentation. With vertical fragmentation, the columns are distributed to cloud providers in such a way that no single provider learns a confidential relationship on his own. A patient health record, for example, might be fragmented into two parts. This way, the individual providers only learn noncritical data relations. However, foreword applications, it is a nontrivial task to and such a fragmentation. First, new relations can be learned by performing transitive combination of existing ones. Second, some relations can be concluded using external knowledge. If, in the example above, the provider additionally learns about the relation, he has technically still no knowledge about the patient’s disease. However, someone with pharmaceutical background can derive the disease from the medication.

Further, new relations can also be derived by combining multiple data sets. For instance, using again the relation of (patient number, medication), the knowledge of a combination of medications can ease the guessing of the patients disease. Thus, also on a row level, database splitting might be required. This is called horizontal fragmentation. Finally, database splitting can also be combined with encryption. Using key management mechanisms like mentioned before, some database columns are encrypted. The combination of encryption and splitting protects confidential columns and still allows querying database entries using plain text columns.

8 Result Analysis

With secure multiparty computation, a number of participants can compute functions on their input values without revealing any information on their individual inputs during the computation. Here, we consider multiparty computation to be executed between several clouds. Using secure multiparty computation can be used to better protect the secrecy of the users data in online services available today, but also has the potential to make new services possible that do not exist today because of the users confidentiality requirements and the lack of a trusted third party.

9 References

[8] Taming the Two-Headed Beast, CSOonline, September 2002
[9] Security 2.0, CSOonline, April 2005
Ms. Archana V. Ugale *, Prof. K. N. Shedge **: Multicloud Architecture To Enhance Security And Privacy

Paper ID: IJIFR/ V2/ E2/ 038


[19] Justice and Home Affairs - Data Protection - Legislative documents


[22] A divided Europe wants to protect its personal data wanted by the US, Rue 89, 4 March 2008 (English)

[23] Statewatch, US changes the privacy rules to exemption access to personal data September 2007

[24] Brussels attacks new US security demands, European Observer. See also Statewatch newsletter February 2008