Security and Privacy Enhancing Multicloud Architecture

Apeksha Mahoorkar[1] Prof. Gautam Borkar[2]
[1,2]Department of Computer Engineering
[1,2]Rajiv Gandhi Institute of Technology, Mumbai.

Abstract— In recent years use of Cloud computing in different mode like cloud storage, cloud hosting, cloud servers are increased in industries and other organizations as per requirements. The Security challenges are still among the biggest obstacles when considering the adoption of cloud services. For this a lot of research has been done. With these, security issues, the cloud paradigm comes with a new set of unique features, which open the path toward novel security approaches, techniques, and architectures.

Key words: Cloud, security, privacy, multicloud, application partitioning, tier partitioning, data partitioning, multiparty computation

I. INTRODUCTION

A number of enabling technologies contribute to Cloud computing several state-of-the-art techniques. The Virtualization technologies partition hardware thus provides flexible and scalable computing platforms. VMware and Xen are the Virtual machine techniques that offer virtualized IT-infrastructures on demand. VPN, support users with a customized network environment to access Cloud resources. Virtualization techniques are the bases of the Cloud computing since they render flexible and scalable hardware services. Cloud computing offers dynamically scalable resources provisioned as a service over the internet. The third party, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software. It will concentrate on public clouds, because these services demand for the highest security requirements. It also includes high potential for security prospects. It can provide a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects.

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. The idea of making use of multiple clouds has been proposed by Bernstein and Celeste. However, this previous work did not focus on security. Since then, other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenarios. In this paper, they introduce a model of different architectural patterns for distributing resources to multiple cloud providers. This model is used to discuss the security benefits and also to classify existing approaches. In our model, we distinguish 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, which map to different application scenarios and their security needs. Obviously, the patterns can be combined resulting in combined security merits, but also in higher deployment and runtime effort

II. RELATED WORKS

Cloud computing creates a large number of security issues and challenges. 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 we 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 and if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Therefore, there should be a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing.

An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. This can be done once, multiple times, or continuously. An attacker that also has access to the processing logic of the cloud can also modify the functions and their input and output data. Even though in the majority of cases it may be legitimate to assume a cloud provider to be honest and handling the customers' affairs in a respectful and responsible manner, there still remains a risk of malicious employees of the cloud provider, successful attacks and compromisation by third parties, or of actions ordered by a subpoena.

A major incident in a SaaS cloud happened in 2009 with Google Docs. Google Docs allows users to edit documents online and share these documents with other

users. However, this system had the following flaw: Once a document was shared with anyone, it was accessible for everyone the document owner has ever shared documents with before. For this technical glitch, not even any criminal intent was required to get unauthorized access to confidential data. Recent attacks have demonstrated that cloud systems of major cloud providers may contain severe security flaws in different types of clouds.[12]

In a flaw in the management interface of Amazon's EC2 was found. The SOAP-based interface uses XML Signature as defined in WS-Security for integrity protection and authenticity verification. Gruschka and Iacono discovered that the EC2 implementation for signature verification is vulnerable to the Signature Wrapping Attack. In this attack, the attacker—who eavesdropped a legitimate request message—can add a second arbitrary operation to the message while keeping the original signature. Due to the flaw in the EC2 framework, the modification of the message is not detected and the injected operation is executed on behalf of the legitimate user and billed to the victim's account.

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.

III. ISSUES ON MULTI CLOUD SECURITY

The Multi-cloud resource sharing scheme uses the data and application partitioning mechanism. There are Four types of architectures which are used for distributing resources to multiple cloud providers. Those architectures are Replication of applications, Partition of application System, Partition of application logic into fragments, Partition of application data into fragments. In the Replication of applications it allows receiving multiple results from one operation performed in distinct clouds. The Partition of application System into tiers allows separating the logic from the data. Partition of application logic into fragments allows distributing the application logic to distinct clouds. Partition of application data into fragments allows distributing fine-grained fragments of the data to distinct clouds. Data security and attack handling operation are managed by centralized or distributed manner in the cloud. The following drawbacks are identified from the existing system.

- Stand-alone security systems
- Malicious attacks are not handled
- Encrypted data processing is not supported
- Data integrity is not provided

IV. SECURITY PROSPECTS BY MULTICLOUD ARCHITECTURES

In this paper, we introduce a model of different architectural patterns for distributing resources to multiple clouds providers. This model is used to discuss the security benefits and also to classify existing approaches. In our model, we distinguish 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 wo 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.

Here we will discuss this four patterns in detail with their merits and flaws with respect to the stated security requirements under the assumption of one or more compromised cloud system.

A. Replication of Application

In this the first question arises that How will a cloud customer know whether his data were processed correctly within the cloud? We cannot guarantee that the operation performed in a cloud system was not tampered or it was not compromised by an attacker. The only guarantee is based on the 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 even if there is a strong bond between the two parties there always a risk of getting compromised by third parties.

B. Partition of Application System into Tiers

This section 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 and enforced effectively and that errors in the application logic do not affect the user's data?

To limit the risk of undesired data leakage due to application logic flaws, the separation of the application system's tiers and their delegation to distinct clouds is proposed. In case of an application failure, the data are not immediately at risk since it is physically separated and protected by an independent access control scheme. Moreover, the cloud user has the choice to select a particular—probably specially trusted—cloud provider for data storage services and a different cloud provider for applications.

C. Partition of Application Logic into Fragments

This section gives an answer to the following question: How can a cloud user avoid fully revealing the data or processing logic to the cloud provider? The data should not only be protected while in the persistent storage, but in particular

when it is processed. The idea is is that the application logic needs to be partitioned into fine-grained parts and these parts are distributed to distinct clouds. 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

D. Partition of Application Data into Fragments

In this 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 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, he 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.

V. SERVICE AND DATA SECURITY FOR MULTI CLOUDS

Secure Multiparty Computation (SMC) and Secret Sharing (SS) algorithm are used to improve the cloud security. Secure data exchange is handled using the Secure Multiparty Computation protocol. The Secret Sharing Algorithm is used to share key values between the users and providers. Data integrity and service integrity verification is performed using the signature models.

Intrusion detection scheme is integrated with the multi-cloud environment for malicious attack handling. Service and data management architectures are combined to provide a complete solution for security requirements. Multiparty communication based security system is used to improve the security over different clouds. Integrity is provided for data and service components sharing environment. An integrated intrusion detection system is proposed to handle malicious attacks. The multi cloud security model is used to protect service and data providers.

Different cloud resource sharing architectures are integrated in the system. Intrusion detection is performed to control malicious attackers. The system is divided into five major modules. They are resource provider, consumer, scheduling process, security process and intrusion detection process. Resource provider provides the hardware and data resources. Consumers are used to access the cloud resources. Scheduling schemes are used for the resource allocation process. Data and services are protected in the security process. Malicious attacks are handled in the intrusion detection process.

A. Resource Provider

Resource provider provides the computational resources to the consumers. Resource monitoring is performed to fetch current resource levels. Provider manages the application replication process. Data sources are also provided by the resource provider.

B. Consumer

The consumer is the resource users. Consumer submits the resource requests. Task requests are submitted resource level and time period information. Resources are allocated from multiple cloud environments.

C. Scheduling Process

The scheduling process is used to assign resources to the tasks. Application replication and fragmentation methods are used in the scheduling process. Applications are fragmented with reference to the logic and modules. Data fragmentation is used for the data distribution process.

D. Security Process

The data and services are protected with security schemes. Data values are secured with secret sharing algorithm. Multi party computations are used to protect sensitive data values. Data integrity verification is provided in the security process.

E. Intrusion Detection Process

Intrusion detection is performed to detect malicious requests. Request sources and intervals are analyzed in the intrusion detection process. Anonymous requests are detected in the intrusion detection process. Data and service providers are secured from intruders.

Sr.no	TOPIC	ALGORITHM OR TOOL	PUBLICATION YEAR	RESULTS	RESOURCES
01	Security Analysis of Cloud Management Interfaces	XML signature wrapping	2011	Results show security analysis of the amazon and eucalyptus cloud systems. Allow an adversary to gain root access to arbitrary virtual machines and Web applications hosted in these clouds, as well as gather arbitrary files and data from the Amazon S3 cloud, and the arbitrary installations of Eucalyptus clouds.	Amazon EC2 and S3 Control Interfaces Eucalyptus and Ubuntu Server Edition

02	Service and Data Security for Multi Cloud Environment	Secure Multiparty Computation (SMC) and Secret Sharing (SS) algorithm are used to improve the cloud security.	2011	1.supports data and application model to protect data and services Integrated security solution schemes are used. 2.Attack resistant resource sharing system controls the service based attacks. Risk free resource management mechanism assures service availability in all situations.	1.Replication of Application 2. Partition of Application System Into Tiers 3 Partition of Application Logic Into Fragments 4 Partition of Application Data Into Fragments
03	Security Prospects through Cloud Computing by Adopting multiple clouds	we have used RNS (Residue number system) Algorithm.	2011	1. We Have used different clouds for encryption, decryption and storage process. 2. After registration, you can able to upload and download the files from anywhere, where there is an Internet connection.	1. Secure Multiparty Computation 2.Homomorphic Encryption And Secure Multiparty Computation both use cryptographic means to secure the data while it is processed.
04	Protocols and Formats for Cloud Computing Interoperability	-	2009	1. In this paper we have shown that how technology is applies to cloud computing interoperability.	1.Most basic resources which Cloud Computing delivers is the Virtual Machine Virtual Machine Instantiation and Mobility
05	:A Securing And Sharing Data Less Cost-Effective Using Multicloud Storage	1 RSA algorithm (Ron Rivest, Adi Shamir, and Leonard Adleman) 2 Secret Sharing Algorithm	. 2012	1. Multiple clouds are adopted at the same time, the number of clouds used denotes the factor in which the costs increase. 2.IN this the customer's entities is considered with the necessary and trust building responsibility	Cloud storage Obfuscating SplittingD. Multi-party Computation
06	SECURITY AT DATA LEVEL IN CLOUD USING MULTICLOUD ARCHITECTURE	DATA ENCRYPTION ALGORITHM (DES) ELLIPTIC CURVE CRYPTOGRAPHY (ECC) SAMBA SERVER	2011	1 The cloud architecture brings convenient way to store and access files provided with confidentiality, integrity and authentication properties. 2 Data is encrypted before uploading to server storage, so message confidentiality is preserved.	Data security with encryption algorith Elliptic Curve Cryptography (ECC) with SHA-512

VI. CONCLUSION

The use of Multi-cloud systems is to share resources among different cloud environment. The resource sharing process is handled with partitioned data and service model. Secure Multiparty Computation (SMC) and Secret Sharing (SS) are the two algorithms that are used to improve the cloud security. For malicious attack handling, Intrusion detection scheme is integrated with the multi-cloud environment

The system supports data and application model. Integrated security solution schemes are used to protect data and services. Attack resistant resource sharing system controls the service based attacks. Risk free resource management mechanism assures service availability in all situations. It is expected that it should give the desired output of easy and efficient data access by the way of splitting and securing the data at multiple cloud environments without the knowledge of the end user. It should also expect that system should be capable to restore the data from remaining cloud storage in case of failure of any of the cloud storage. Another import ant expectation from the system is that it should be developer's friendly so

that vast use of the platform by number of developers and it will results into multiple implementation of the system.

REFERENCES

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing," Proc. IEEE Int'l Conf. Cloud Computing (CLOUD-II), 2009.
[2] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 199-212, 2009.
[3] Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 305-316, 2012.
[4] N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," Proc. IEEE Int'l Conf. Web Services (ICWS '09), 2009.
[5] S. Bugiel, S. Nu¨ rnberger, T. Po¨ppelmann, A.-R. Sadeghi, and T. Schneider, "AmazonIA: When Elasticity Snaps Back," Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11), pp. 389-400, 2011.
[6] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", IEEE Transactions on Dependable and Secure Computing, Vol. 10, No. 4, July/August 2013.
[7] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces," Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW '11), pp. 3-14, 2011.

