ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# Security and Privacy-Enhancing Multicloud Architectures

**P.Aswini**
**M.Tech Student**
**Dept. of CSE**
**Avanthi Institute of Engineering and Technology, Vizianagaram.**

**K.Ravindra, M.Tech, (Ph.D)**
**Associate Professor**
**Dept. of CSE**
**Avanthi Institute of Engineering and Technology, Vizianagaram.**

## ABSTRACT

***Security challenges are still among the biggest obstacles when considering the adoption of cloud services. This 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, which open the path toward novel security approaches, techniques, and architectures. This paper provides 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.***

## INTRODUCTION

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. These services have long been referred to as Software as a Service (SaaS). Some terms such as PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) are used by vendors to describe their roducts, but we avoid these because accepted definitions for them still vary widely. There is no crisp line between “low-level “infrastructure and a gher-level “platform “. We believe both of these are more alike than different, and we do consider them together. Similarly, some related term such as “gridcomputing,” from the high-performance computing community, suggests protocols to offer storage over long distances and shared computation; however those protocols did not lead to a software environment that grew beyond its own community. The data center hardware and software is what we will call a cloud.

Cloud computing offers dynamically scalable resources provisioned as a service over the Internet. The thirdparty, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the loud paradigm promise to reduce capital as well as operational expenditures for hardware and software. Clouds can be categorized taking the physical location from the viewpoint of the user into account [2]. 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 premise—usually in the own data center—this setup is called private cloud. A hybrid approach is denoted as hybrid cloud. This paper will concentrate on public clouds, because these services demand for the highest security requirements but also— as this paper will start arguing—includes high potential for security prospects. 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 from an intraorganizational to an interorganizational context. This creates a number of issues, among which security aspects are regarded as the most critical factors when considering cloud computing adoption [3]. Legislation and compliance frameworks raise further challenges on the outsourcing of data, applications, and processes. The high privacy standards in the European Union, e.g., and their legal variations between the continent’s countries give rise to specific technical and organizational challenges [4]. 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 [5] and contains a survey on these 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. The rest of this paper is organized as follows: Section 2 motivates the need for effective cloud security countermeasures by briefly reviewing the current state of play. The observations further lead to the fact that most of the research and development work is currently devoted to dedicated security schemes, which do not consider the specific properties of the cloud itself. Only recently some proposals on making use of multiple distinct clouds at the same time to realize security goals started to appear. To provide a formal ground to categorize and analyze these proposals, we propose a set of four distinct multicloud architectures. These multicloud architectures are introduced in Section 3 and each of them is further discussed in Sections 4, 5, 6, and 7, including case studies. Section 8 provides a consideration of legal and compliance aspects. Finally, in Section 9, an assessment and comparison of the presented approaches is given. Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in [6]. 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. In [7], an overview of security flaws and attacks on cloud infrastructures is given. Some examples and more recent advances are briefly discussed in the following. Risten part et al. [8], [9] presented some attack techniques for the virtualization of the Amazon EC2 IaaS service. In their approach, the attacker allocates new virtual machines until one runs on the same physical machine as the victim's machine. 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 [10] discovered that the EC2 implementation for signature verification is vulnerable to the Signature Wrapping Attack [11]. A major incident in a SaaS cloud happened in 2009 with Google Docs [12]. Google Docs allows users to edit documents (e.g., text, spreadsheet, presentation) 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 (see [13], [14]). The idea of making use of multiple clouds has been proposed by Bernstein and Celesti [15].

## EXISTING SYSTEM

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. How does a cloud customer know whether his data were 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 only kind of 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 even if the relation and agreements are perfectly respected by all participants, there still remains a residual risk of getting compromised by third parties.

## DISADVANTAGES:

1. Cost is high related to operational expenditures (hardware, software)
2. Third party auditors are not control the all security risks.
3. Misuse the cloud services
4. Attackers are going to alter and manipulations of data.

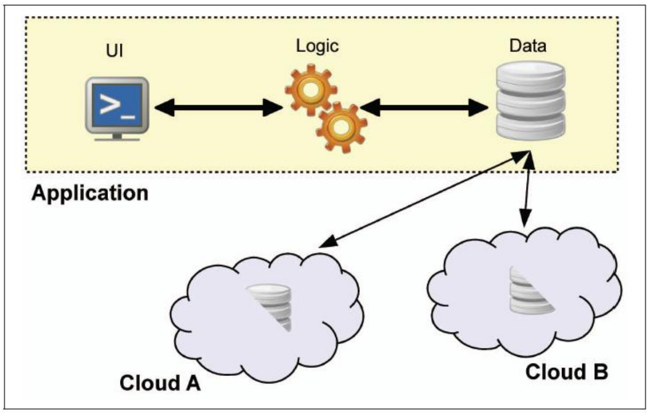
## PROPOSED SYSTEM:

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 multi cloud adoption approaches. 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. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular. The rest of this paper is organized as follows: motivates the need for effective cloud security countermeasures by briefly reviewing the current state of play. The observations further lead to the fact that most of the research and development work is currently devoted to dedicated security schemes, which do not consider the specific properties of the cloud itself. Only recently some proposals on making use of multiple distinct clouds at the same time to realize security goals started to appear.

## ADVANTAGES:

1. Reduce the capital and expenditure.
2. Reduce the attacker risks
3. Its gives the confidentiality and mitigate the attacks

## ARCHITECTURE:



## MODULES

- n Clouds Approach.
- Processor and Verifier
- Cryptographic Data Splitting
- Database Splitting.

## MODULES DESCRIPTION

## PROCESSOR AND VERIFIER

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 verifies the execution path taken by Cloud A on-the-fly, allowing for immediate detection of irregularities.

## 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 > 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 nonmalicious 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.

## 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 user's premises, to increase flexibility 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 first 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 untrusted public cloud.

## 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 first case, data splitting requires a scenario—similar to other approaches presented before—with a 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, for real-world applications, it is a nontrivial task to find 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 first 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 set. For instance, using again the relation of (patient number, medication), the knowledge of a combination of medications can ease the guessing of the patient's 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.

## CONCLUSION

We explicitly do not investigate this field here due to space restrictions; however we encourage the research community to explore these combinations, and assess their capabilities in terms of the given evaluation dimensions. Second, we identified the fields of homomorphism encryption and secure multiparty computation protocols to be highly promising in terms of both technical security and regulatory compliance.

As of now, the limitations of these approaches only stem from their narrow applicability and high complexity in use. However, given their excellent properties in terms of security and compliance in multi cloud architectures, we envision these fields to become the major building blocks for future generations of the multi cloud computing paradigm.

## FUTURE SCOPE

Sharing data flexibly and securely is the main issue in cloud computing. Users prefer cloud to upload their data with different users. Uploading of data to server may lead to leakage of private data of user to everyone. In the future we can provide distributed and independent concurrent access to all the users.

## REFERENCES

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, 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, JULY/AUGUST 2013

[2] P. Mell and T. Grance, “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/, 2010.

[3] F. Gens, “IT Cloud Services User Survey, pt.2: Top Benefits & Challenges,” blog, http://blogs.idc.com/ie/?p=210, 2008.

[4] Gartner, “Gartner Says Cloud Adoption in Europe Will Trail U.S. by at Least Two Years,” http://www.gartner.com/it/page. jsp?id=2032215, May 2012.

[5] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L. Iacono, “Security Prospects through Cloud Computing by Adopting Multiple Clouds,” Proc. IEEE Fourth Int’l Conf. Cloud Computing (CLOUD), 2011.

[6] D. Hubbard and M. Sutton, “Top Threats to Cloud Computing V1.0,” Cloud Security Alliance, http://www. cloudsecurityalliance.org/topthreats, 2010.

[7] 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.

[8] 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.

[9] 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.

[10] N. Gruschka and L. Lo Iacono, “Vulnerable Cloud: SOAP Message Security Validation Revisited,” Proc. IEEE Int’l Conf. Web Services (ICWS ’09), 2009.

[11] M. McIntosh and P. Austel, “XML Signature Element Wrapping Attacks and Countermeasures,” Proc. Workshop Secure Web Services, pp. 20-27, 2005.

[12] J. Kincaid, “Google Privacy Blunder Shares Your Docs without Permission,” TechCrunch, http://techcrunch.com /2009/03/07/ huge-googleprivacy- blunder-shares-your-docs-withoutpermission /, 2009.

[13] 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.

[14] 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.

[15] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, “Blueprint for the Intercloud—Protocols and Formats for Cloud Computing Interoperability,” Proc. Int’l Conf. Internet and Web Applications and Services, pp. 328-336, 2009.

## AUTHOR DETAILS

**P.Aswini**
M.Tech Student
Dept. of CSE
Avanthi Institute of Engineering and Technology,
Vizianagaram.

**K.Ravindra, M.Tech, (Ph.D)**
Associate Professor
Dept. of CSE
Avanthi Institute of Engineering and Technology,
Vizianagaram.