ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

A Securing And Sharing Data Less Cost-Effective Using Multicloud Storage

[I]Priyadharsshini.C, [II]SathishKumar.S, [III]Ranjidha.P
[I,III]M.E CSE, Srinivasan Engineering College, Perambalur, Tamil Nadu, India.
[II]Assistant Professor, Dept. Of IT, Srinivasan Engineering College, Perambalur, Tamil Nadu, India.
E-mail : [I]priyacs516@gmail.com, [III]ranjidha.it@gmail.com

Abstract
While using cloud services they impose new security challenges, which is the biggest obstacle. Lot of research activities has been triggered in this direction, which results in a quantity of proposals targeting the various security threats. Simultaneous usage of multiple Clouds reduce the risk for data and applications in a public cloud . Recently several approaches employing this paradigm have been proposed . They differ in partitioning and distribution patterns, technologies, cryptographic methods, and targeted scenarios as well as security levels. These developed multi cloud architectures allow to categorize the available schemes and to analyze them. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular. Besides the security issues , it also provide a new set of unique features which open the path towards novel security approaches, techniques and architectures. This project initiates this discussion by contributing a concept which achieves security merits by making use of multiple distinct clouds at the same time.

Keywords
Legal aspects,cloud paradigm.

I. Introduction

Security is the main problem in cloud storage. The cloud is general storage any one can access the service. Cloud computing opens doors to multiple unlimited venues from elastic computing to on demand provisioning to dynamic storage and computing requirement fulfillment. However, despite the potential gains achieved from the cloud computing [1] and [2].The security of an open-ended and rather freely accessible resource is still questionable which impacts the cloud adoption.

The security problem becomes amplified under the cloud model as new dimensions enter into the problem scope related to the architecture, multi-tenancy, layer dependency, and elasticity. In multi cloud computing creates a large number of security issues and challenges [3]. 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. Different services is accessed from the Multicloud user.

A more advanced, but also more complex approach comes from the distributed algorithms discipline: the Byzantine Agreement Protocol is used for increase the security and privacy in multi cloud architecture. Homomorphic Encryption and Secure Multiparty Computation in provide the more security to the user. The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. It increases the security and privacy in multi cloud.

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 leaves 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.

II. Related Work

Existing research close to our work can be found in 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 affect 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.

The main Drawback Existing research that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes.

III. Our Contributions

Main contributions. Our contributions can be summarized the main points.

The use of cloud-based platforms in the technology industry continues to evolve into more complex arrangements. It's more complex than a hybrid cloud, which is typically a paired private and public cloud. Multicloud add more clouds to the mix, perhaps two or more public IaaS providers, a private PaaS, on-demand management and security systems from public clouds, private use-based accounting.

Multi clouds require more thinking around security and governance, given their complexity and distribution.

Multi clouds may develop resiliency issues, considering the number of moving parts.

Multi clouds have value only if you select the right providers, whether on-demand or private, to meet your requirement.
It's important that you take the lessons learned from building complex distributed systems to multicloud deployments. You need to understand that integration drives complexity, which must then be managed. There is no substitute for planning and architecture.

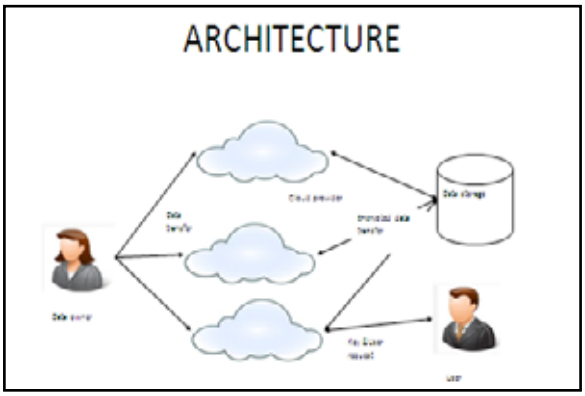

Fig. 1: Diagram of the proposed method

Fig. 1 illustrates the workflow of our proposed algorithm. Different from our previous work, in this paper the Fig.2 Multicloud is used for enables run in any platform. Multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust assumption can be lowered to an assumption of non collaborating cloud service providers. Further, this setting makes it much harder for an external attacker to retrieve or tamper hosted data or applications of a specific cloud user. Homomorphic encryption and secure multiparty computation both use cryptographic means to secure the data while it is processed.

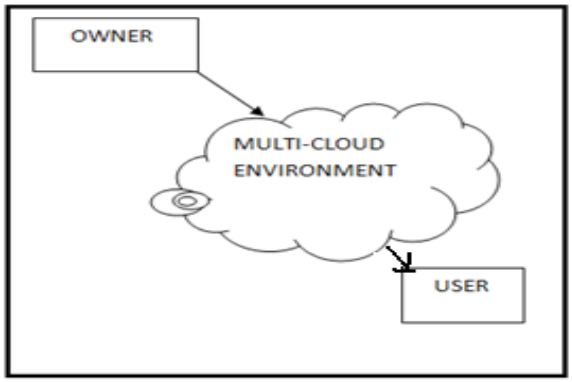

Fig. 2: Multi-cloud storage

The Multicloud Homomorphic encryption, the cloud has the main share of work, as it operates on the encrypted inputs to compute the encrypted output. Intermediate or final results need to be decrypted. This requires either interaction with the entity that holds the key (e.g., a private cloud) or the key is shared among several clouds that then assist in decrypting values that are needed in clear with a threshold encryption scheme.
The secure multiparty computation in distinct clouds guarantees the secrecy of the input data, unless the cloud providers collude to open shares or decrypt inputs. The Fig.3 a multiparty computation between clouds makes it possible to compute a function on data in a way that no cloud provider learns anything about the input or output data.

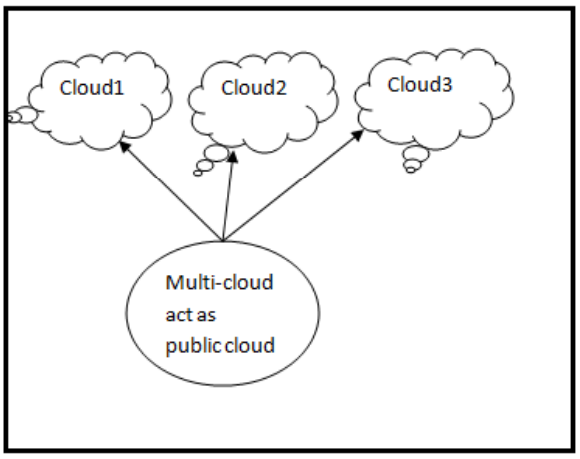

Fig. 3 : Multi-cloud splitting

A multi-party computation into the cloud, using multiple cloud services doing a multi-party computation can also is beneficial for protecting the secrecy of data of a single user. In the end, the clouds hold shares of the result which is sent back to the user who can reconstruct the result. In this case, using multiple cloud computation guarantees the secrecy of the input data, unless the cloud providers collude to open shares. A multi-party computation between clouds makes it possible to compute a function on data in a way that no cloud provider learns anything about the input or output data. As secret sharing rather than encryption is used, a collusion of all clouds would be able to reconstruct the secrets.

IV. Methods

In this project 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 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. 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. This project initiates this discussion by contributing a concept which achieves security merits by making use of multiple distinct clouds at the same time.

A. RSA Algorithm

RSA algorithm (named after its founders, Ron Rivest, Adi Shamir, and Leonard Adleman) has become almost synonymous with public key cryptography.RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

B. Key Generation

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Fig. A: Encryption

Encryption is the process of converting original plain text (data) into cipher text (data).

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Fig. B : Decryption

Decryption is the process of converting the cipher text (data) to the original plain text(data).

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

V. Implementation

These developed multi cloud architectures allow categorizing the available schemes and to analyze them according to their security benefits the implementation the design Fig4.

A. Cloud storage

Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualized the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects.

Storage availability and data protection is intrinsic to object storage architecture, so depending on the application, the additional technology, effort and cost to add availability and protection can be eliminated

Storage maintenance task, such as purchasing additional storage capacity, are offloaded to the responsibility of a service provider.

B. Attacks on cloud security

In the majority of the cases it may be legitimate to assume a cloud provider to be honest and handling the customers' affairs in a respectful and responsible manner, still there remains a risk of the own cloud system getting compromised by third parties. 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.

C. Obfuscating Splitting

The idea of obfuscating splitting is the fact that there is no general pattern for realization. Careful analysis of the splitted data and application must be performed regarding its confidentiality, i.e. checking if the information a single cloud provider receives really is "useless". A typical way of data splitting is pseudonymization: one provider receives the data with some key fields (typical personal identification data like name, address etc.) replaced by a random identifier and the second provider receives the mapping of the identifier to the original information.

D. Multi-party Computation

Multi-party computation a number of participants can compute functions on their input values without revealing any information on their individual inputs. This approach considers a multi-party computation between several clouds. Two distinct scenarios can be imagined: an application that intrinsically requires multi-party computation is outsourced to the multi-party cloud, or a single cloud user make use of a multi-party cloud for better protection of the secrecy of his data. A multi-party computation between clouds makes it possible to compute a function on data in a way that no cloud provider learns anything about the input or output data. As secret sharing rather than encryption is used, a collusion of all clouds would be able to reconstruct the secrets.

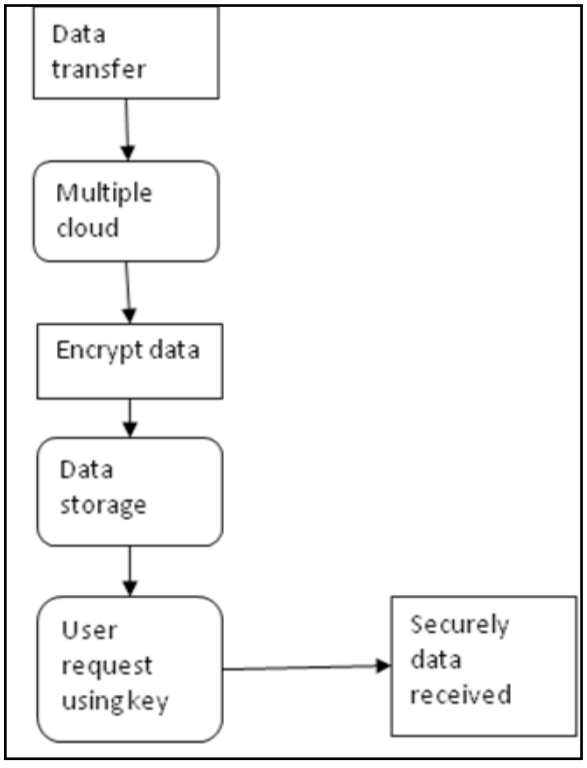

Fig. 4. Dataflow Diagram

E. Secret Sharing Algorithm

The algorithms are far from being practical, so the vision of clouds based algorithm. This requires either interaction with the entity that holds the key (e.g., a private cloud) or the key is shared among several clouds who then assist in decrypting values that are needed in clear with a threshold encryption scheme. The user will compute shares of his data using a secret sharing scheme and

distribute the shares to the different clouds. The clouds will jointly compute the function of interest on these shares, communicating with each other when necessary. In the end, the clouds hold shares of the result which is sent back to the user who can reconstruct the result. In this case, using multiple cloud computation guarantees the secrecy of the input data, unless the cloud providers collude to open shares.

F. Processor and Verifier

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

VI. RESULTS

Fig. 5: User registration and cloud storage

Fig. 6: Cloud user login and secure multi cloud storage

Fig. 7: Files are stored in cloud storage

Fig. 8: Cloud files are downloaded

VII. Conclusion

Multiple clouds are adopted at the same time, the number of clouds used denotes the factor in which the costs increase. Nevertheless, even when adopting one of the introduced approaches, the total cost might still be less than running the service in-house. The question here is what a user is willing to pay for increased assurance and security. Since no cloud service provider can absolve oneself from being vulnerable to attacks for some degree, with the adoption and support of the introduced architectures it can be explicitly confirmed, that the duty to take care of the customer's entities is considered with the necessary and trust building responsibility. RSA is, in fact, commonly used to securely transmit the keys for another less secure, but faster algorithm than RSA will continue to be developed as mathematicians discover more in the fields of number theory and cryptanalysis.

References

[1] *S. Bugiel, S. Nurnberger, 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.*

[2] *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.*

[3] *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.*

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

[5] *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.*

[6] *N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," Proc. IEEE Int'l Conf. Web Services (ICWS '09), 2009.*

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

[8] *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.*

[9] *J. Kincaid, "Google Privacy Blunder Shares Your Docs without Permission," TechCrunch, http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs- withoutpermission/, 2009.*

[10] *P. Mell and T. Grance, "The NIST Definition of Cloud*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

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.

[11] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE,Luigi Lo Iacono, and Ninja MarnauIEEE transactions on dependable and secure computing,vol.10, no.4, July/ august 2013