Asian Journal of Engineering and Applied Technology
ISSN : 2249-068X Vol. 3 No. 1, 2014, pp. 27-30

A Novel Approach for Data Storage Security in Multicloud Computing

K. Parthiban[1] and V.M.Priyadharshini[2]

University College of Engineering (BIT CAMPUS), Tiruchirappalli, Tamil Nadu, India

E-mail:

(Received on 02 March 2014 and accepted on 14 June 2014)

Abstract - **In cloud a service the main tedious problems are security and secrete maintains of the information, with the help of Multicloud services security can be enhanced and privacy can be maintained. Along with these data are encrypted by the data owner and that data are stored in cloud database. It will be more secured. For sharing the resource and information Multicloud approach can be performed. Data owner maintains the information security, The cloud is general storage any one can access the service. Many security problem raised in cloud computing. However, despite the potential gains achieved from the cloud computing freely accessible resource is still questionable which impacts the cloud adoption..Many misusing problem arise in cloud computing .To solve this problem multiple cloud approach and encrypting technique is used is proposed for enhancing security and privacy.**

Keywords: **Multicloud, security, privacy, cloud, partitioning**

I. Introduction

Security is that the main downside in cloud storage .The cloud is general storage anyone will access the service. Cloud computing opens doors to multiple unlimited venues from elastic computing to on demand provisioning to dynamic storage and computing demand fulfillment. However, despite the potential gains achieved from the cloud computing, the protection of associate degree open-ended and rather freely accessible resource continues to be questionable that impacts the cloud adoption. the protection downside becomes amplified underneath the cloud model as new dimensions enter into the matter scope associated with thedesign, multi-tenancy, layer dependency, and snap. In multi cloud computing creates an oversized variety of security problems and challenges. These problems vary from the desired trust within the cloud supplier and attacks on cloud interfaces to misusing the cloud services for attacks on alternative systems. Different services are accessed from the multicloud user.

An additional advanced, however conjointly additional advanced approach comes from the distributed algorithms discipline: the Byzantine Agreement Protocol is employed for increase the protection and privacy in multicloud design. OU secret writing and Secure Multiparty Computation in offer the additional security to the user .the employment of multiple cloud suppliers for gaining security and privacy advantages is nontrivial. It increase the protection and privacy in multicloud.The main downside that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive yet as business-critical knowledge and processes. once considering employing a cloud service, the usershould remember of the very fact that every one knowledge given to the cloud supplier leaves the own management and security sphere. Even more, if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud supplier gains full management on these processes. Hence, a powerful hope relationship between the cloud supplier and therefore the cloud user is taken into account a general necessity in cloud computing.

The use of cloud-based platforms within the technology business continues to evolve into a lot of complicated arrangements. Its a lot of complicated in hybrid cloud which usually a parried personal and public cloud .Multi cloud add a lot of clouds to the combination ,two or a lot of public cloud Iaas supplier Iaas.

Multicolud add a lot of clouds to the combination, maybe 2 or a lot of public IaaS suppliers, a personal Paas on-demand management and security systems from public clouds, personal use-based accounting. Multi cloud need a lot of thinking around security and governance ,given their complexness and distribution Multi cloud could develop resiliency problems, considering the quantity of moving elements. Its necessary that you just take lessons learned from construction distributed system to multicloud .Its necessary that you just take lessons learned from construction distributed system to multIcloud preparation .Which should be managed ,there is no substitute for arrange cloud security mechanism have limitations .There is no possible thanks to perform any reasonably knowledge dependent operation in cloud system while not breaking multi-party computation between clouds makes it attainable to calculate a perform on knowledge during a approach that no cloud supplier learns something concerning the input or output knowledge. secret sharing instead of secret writing is employed, a collusion of all clouds that may be ready to set up the secrets. For application that area unit already solved by multi party computation, no more overhead is introduced by outsourcing this computation to range of clouds. whereas addition and multiplications go along with a tiny low overhead, a lot of complicated operations have a important overhead. it's in progress analysis to cut back the overhead by multi-party computation and up to date enhancements and the standard of mensuration.

II. Problem Statement

Cloud user can access the data from other clouds, many partition breakdown in the cloud system. There is no security and confidentiality in cloud system. Cloud computing means Internet computing, many security issues cloud system. Most sophisticated data security systems possible as they want your business and realize that data security is a big concern.Third access is mainly possible in the cloud system One idea on decreasing the risk for data and applications in a public cloud is the simultaneous usage of multiple Clouds. Data leakage has been solved here. Privacy has been achieved here. Malicious attack has been solved here.

III. Existing Systems and Their Drawbacks

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 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.

The problem with the idea of obfuscating splitting is the fact that there is no general pattern for realization. Careful analysis of the splitter data and application must be performed regarding its confidentiality, i.e. checking if the information a single cloud provider receives really is "useless.

IV. Proposed Solution

Multi cloud is proposed for enhance the privacy of the system. Multiple distinct cloud is proposed for provide the more security. It provide the more integrity of result. Different type approach has been proposed for enhance security. It can compare with distinct clouds it can identify the data leakages. It provide the more security between cloud provider and cloud customer. Same copies of multiple information are transferred to multiple clouds. Multiple clouds are simultaneously transferring the information. Every cloud can monitor the execution of other cloud computations. But it does not show the output of other cloud executions. For enhance the security of data in the clouds data base splitting the data in the cloud data base. It provides the more confidentiality for cloud system. The typical encryption scheme provides the more security data transferring. OU (Okamoto–Uchiyama) encryption is proposed for provide the more security. The user encrypts the data with his public key and uploads the cipher texts to the Cloud. The benefits of cloud computing are easy to identify. It will lead to more capacity and flexibility, and particularly reducing costs. All these benefits are needed to help growing a successful business. Clouds distinct advantages attract the attention of many organizations, but the aspect that makes many organizations to retreat against this technology is How to secure data in the cloud and ensure the safety of environment.

Advantages

1. The Data generated by various people and institutions (such as email, medical records, photos, financial transactions, etc.) has been increasing rapidly and management of these data by the cloud will bring flexibility and economic saving.

2. To protect information privacy and fight against unwanted access in the cloud, the owners of data before outsourcing sensitive data encrypt them.

3. Stored data encryption schema Access control to prevent unauthorized access data backup plan Secure storage of data on backup media

V. Methodologies

OU (Okamoto–Uchiyama) encryption is widely used Public-Key algorithm. By using OU (Okamoto–Uchiyama) encryption to encrypted the data to provide security so that only the concerned user can access it. By Securing the data, We using unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required , user places a request for the data for the Cloud provider, Cloud provider authenticate the user and delivers the data. OU is a block cipher, in which every message is grouping to the integer . OU (Okamoto–Uchiyama) encryption consists of public key and Private key . In cloud environment , Public key is analyzed to all whereas Private-Key is known only to the user who originally owns the data. T cloud provider and decryption is done by the Cloud user,. Once the data is encrypted with the Public-Key, it can be encrypted with the corresponding Private-Key only.

Secure Multiparty computation use cryptographic means to secure the data while it is processed. In Okamoto–Uchiyama the user encrypts the data with his public key and uploads the cipher texts to the Cloud. The cloud can independently compute on the encrypteddata to obtain an encrypted result, which only the user can decrypt. Therefore in this scenario, Okamoto–Uchiyama encryption uses an asymmetric fragmentation where the user (or a small trusted private cloud) manages the keys and performs the encryption and decryption operations, while the massive computation on encrypted data is done by an entrusted public cloud.

VI.Conclusion

Since multiple clouds are adopted at the same time, many of the 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 cloud. A user is willing to pay for increased assurance and security .Since thereare numerousanalogies in other disciplines where the replication of resource is common practice despite the fact of additional costs coming this approach ,the provided security Benefits might wait out the additional costs. Some common practice despite additional weights .Besides an increased fee for enhanced security service, The cloud provider might find

the proposed architecture fee for enhanced security issues, The cloud provider might willingness to provider might find the proposed system. And since no cloud service can provide can absolve oneself form being vulnerable it cab explicitly confirmed ,that duty cycle to take care of customer entities is consider with the necessary and trust building responsibility.

VII. Future Work

In previous work in nature the project has covered almost all the requirements further requirements and improvements can easily be done since the structured or modular in nature. changing the existing concepts or adding the new concepts can append the improvements. Further improvements can be made to the application, so that the project functions very attractive and useful manner than the present one. In future, try to present a simulation for cloud computing in security purpose. Clouds are used for access the data form bigserver.

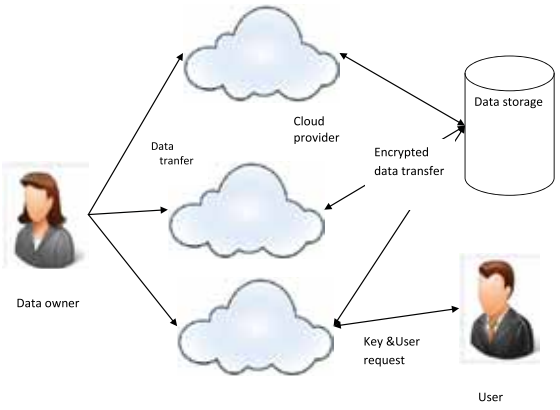

Fig.1Proposed System Design

References

[1] 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.

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

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

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

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.