ISSN: 2321-7782 (Online)
Volume 2, Issue 11, November 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Methods to provide security to the data in Multi cloud architecture

G.Keerthi Reddy[1]
M.Tech Student,
Dept. of CSE, B.V. R.I.T
Medak,India

T.Satish Babu[2]
Assistant professor,
Dept. of CSE, B.V. R.I.T
Medak,India

Abstract: ***Now in this modern technology many companies and organizations are using cloud computing to store their valuable and important data as it is of low cost and we can access our data at anytime and anywhere. The main problem here is the security to that data and also the processing time to access that data. So there may be chance of getting this leakage of data outside. Even though there is an authentication such as providing username and password to the user it is not fully satisfying to provide security because of hackers are trying to get and modifying the data. So to provide more security to data, usage of Multi clouds (more than one cloud) came into picture. Here user will keep his/her data into more than one cloud. They can access their data what time they want. Based on security that needed to the data, we can use some methods to store and access that data.***

Key Words: ***Security, cloud, attacks, multi cloud.***

I. INTRODUCTION

Cloud computing is a technology, where we can store and retrieve of our data at anytime and anywhere with the use of internet. Clouds are three types: public cloud, private cloud and hybrid cloud. Generally user or any organization wills stores data in cloud because it is of low cost and we can access any where any time. But here we may face security issues at this level. Three cloud service models are available .There are Software as a service (Saas), Platform as a service (Paas), and Infrastructure as a service (Iaas). There are so many security threats to cloud computing is there in [3].An overview of security threats on cloud in [4]. So we can eliminate those security issues by using multi cloud architecture.

II. SECURITY ISSUES

Cloud computing creates so many security issues. The main problem is that user has most sensitive data. Here user must be aware that all data given to cloud provider leave the own control.

When deploying this data into clouds, cloud provider has more control on data. So there must be strong relationship between user and cloud provider first.

If an attacker has access to the cloud storage component is able to take snapshots or alter data in the storage. This might 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 not possible 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.

Some attacks techniques as per Ristenpartetal. [5], [6] 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. Then, the attacker can perform cross-VM sidechannel attacks to learn or modify the victim's data.

The authors present strategies to reach the desired victim machine with a high probability, and show how to exploitthis position for extracting confidential data, e.g., a cryptographic key, from the victim's VM. Finally, they propose the usage of blinding techniques to fend cross-VMside-channel attacks. In [7], 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 [8] discovered that the EC2 implementation for signature verification is vulnerable to the Signature Wrapping Attack[9].

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. A major incident in a SaaS cloud happened in 2009 with Google Docs [10].

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.

Recent attacks have demonstrated that cloud systems of major cloud providers may contain severe security flaws in different types of clouds (see [11], [12]).

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 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.

III. Reason For Usage of Multi Cloud Architecture

Here the idea of using multiple distinct clouds at the same time is 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.

Here by using multi clouds and with below methods we can achieve security to our data. These approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenarios.

IV. EXISTING SCENARIO

Existing system is having one cloud architecture. Means it contains Owner of the cloud provider, cloud services (where we can store user's data) and Third party Auditor. First we upload the files of information in cloud servers. Here one cloud server active cloud server and remaining are backup cloud servers.

Here first user will register in owner location then user will get secret key and this same key will be stored in to TPA. If user is ready to access the file of information from the cloud server, then user needs to enter the secrete key ,if it matches with original then user can access the data.

Here user's data may be get affected by hackers. So user may get less data .TPA takes decision to collect remaining data from any back up cloud server.

The problem here is TPA may get affected by hackers. So we cannot depend on TPA at this point.

V. PROPOSED SCENARIO

Whatever the difficulty or problem we faced with one cloud architecture will be replaced with multiple unique cloud architectures.

Here different architecture contains different security requirements. We can identify the merit based on security requirements. After identification of merit or high accuracy cloud we can apply the below methods based on our requirement.

VI. METHODS

Below are the four methods we can use in multi cloud architecture.

A. First method is by maintaining one key with the user:

whenever user wants to access their first he/she enters his credentials if they match, then user will be allowed to enter secret key to access the data and logic , when it matches then the corresponding application will be executed at each cloud to get the data. So that user can easily compare all outcomes got from clouds .So that user can easily assume the integrity of the data. For example, we can implement this by selecting the two cloud architectures and same logic and data we store in two cloud architectures. Assign the different keys for each architecture. User enters the secrete key, if it matches then user access the data and logic .As here only one key we are using so this key can easily trace by attackers. So they can easily modify the data. So less security to the data.

This method we can assign to low security needed data like movies related data.

B. Second method is by maintaining two keys with user

This second method we can assign to the data, which needs medium level security such as sports related data.

In this method, we will separate logic and data and store them in to separate clouds. Whenever user wants to access their first he/she enters his credentials, if they match, to access the content user needs to enter the two keys for logic and data. If these keys match then logic will be processed to access the data content. Here with this process we can access the data that user wants.

The problem here is even we have two keys, these keys also be traced by hackers.

C. Third Method is Splitting of user's data and placing in different clouds

This method we can apply it for data which needs more security.

Here also we will follow second method but we will split the data and store in multiple clouds.

Here we will split the user's data by using data base splitting algorithms like horizontal splitting or vertical splitting (normalization and row splitting) etc. Before applying these algorithms convert data base tables into encrypted form like cipher text using cryptographic splitting process. Data is also be in structured form like XML data [13]. Here also we can do partitioning like data bases.

if we use two cloud architecture, to access the full data user needs to enter two keys ,as we did data splitting.

If they (keys) matched then only user can access the data content.

Even though we did data splitting, this method is not fully secured one as we did not split the application logic.

D. ***Fourth method is Splitting of application logic and placing in different clouds***

With this method we can achieve full security to our data. This method is a extension of third method, here we will split the application logic with existing logic splitting algorithms.

What we do in this process is we will apply asymmetric or symmetric cryptographic algorithms [14]. Asymmetric cryptographic algorithm is public key cryptographic algorithm [15],[16].

Here logic is converted into cipher text when doing encryption with public key. While doing decrypt at user side private key will be used. Symmetric cryptographic algorithm is private key cryptographic algorithm.

Here logic is converted into cipher text [17] when doing encryption with private key. While doing decrypt at user side private key will be used.

Then we will perform partitioning for cipher text of logic .After partitioning we will store them into different cloud. If we use two clouds architecture, to access the full logic user needs to enter two keys, as we did logic splitting.

VII. CONCLUSION

Using of multi cloud architectures we can get more security to our data, compare to single cloud. Here by using fourth method we can get more security to our data.

Here the main problem is choosing relevant partitioning algorithms. We need to take partitioning algorithms in such a way that it should be faster and not complex to use.

ACKNOWLEDGEMENT

I am really thankful to my guide, Associate professor Mr. T.Satish Babu for giving such a precious guidelines in completing this paper.

References

1. Hubbard and M. Sutton, “Top Threats to Cloud Computing V1.0,” Cloud Security Alliance, http://www.cloudsecurityalliance.org/topthreats, 2010.
2. 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.
3. D. Hubbard and M. Sutton, “Top Threats to Cloud Computing V1.0,” Cloud Security Alliance, http://www.cloudsecurityalliance.org/topthreats, 2010.
4. 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.
5. 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.
6. 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.
7. N. Gruschka and L. Lo Iacono, “Vulnerable Cloud: SOAP Message Security Validation Revisited,” Proc. IEEE Int’l Conf. Web Services (ICWS ’09), 2009.
8. M. McIntosh and P. Austel, “XML Signature Element Wrapping Attacks and Countermeasures,” Proc. Workshop Secure Web Services, pp. 20-27, 2005.

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. 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.

11. 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,

12. J. Somorovsky, C. Meyer, T. Tran, M. Sbeiti, J. Schwenk, and C. Wietfeld, “SeC2: Secure Mobile Solution for Distributed Public Cloud Storages,” Proc. Second Int’l Conf. Cloud Computing and Services Science (CLOSER), pp. 555-561, 2012.

13. S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc.14th Int’l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

14. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,” Proc. 13th ACM Conf. Computer and Comm. Security, pp. 79-88, 2006.

15. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions,” Proc. 25th Ann. Int’l Conf. Advances in Cryptology (CRYPTO ’05), pp. 205-222, 2005.

16. R. Rivest, L. Adleman, and M. Dertouzos, “On Data Banks and Privacy Homomorphisms,” Foundations of Secure Computation, vol. 4, no. 11, pp. 169-180, 1978.

