A SECURE AND PRIVACY ASSURED MULTI CLOUD ARCHITECTURE

Shaik Lalmahammad[1], Boppudi Swanth[2], Betam Suresh[3]

[1]M.Tech (CSE) Scholar, Vikas Group of Institutions, Nunna, Vijayawada, A.P, (India)

[2]Asst. Professor, Department of CSE, Vikas Group of Institutions, Nunna, Vijayawada, A.P, (India)

[3]HOD, Vikas Group of Institutions, Nunna, Vijayawada, A.P, (India)

ABSTRACT

Security threats are one of the major problems when seeing the acceptance of cloud services. This caused a lot of investigation activities and its resulting in a amount of suggestions pointing the various cloud security problems. Along with these security problems, the cloud prototype comes with a different new set of features, which shows the way toward novel security methods, techniques, and designs. In this paper we provide a review on the realisable security advantages by making use of multiple clouds simultaneously. Different architectures are presented and discussed about their security and privacy abilities and predictions.

***Keywords**: Security, Cloud, Privacy, Data Partitioning, Multi-Cloud, Application Partitioning, Tier Partitioning*

I. INTRODUCTION

Cloud computing provides dynamically accessible resources as a service over the Internet. The third-party, self-service, on-demand, pay-per-use and seamlessly accessible computing resources and facilities offered by the cloud prototype promise to decrease the capital as well as functioning costs for software and hardware. Clouds can be categorized considering the physical position from the lookout of the user into the account. A public cloud is accessible by third-party service providers and contains properties outside the user's properties. In case the cloud system is may be installed on the user's location generally in the own data center this is called private cloud and a hybrid method is indicated as hybrid cloud. In this paper we concentrated on public clouds because these services request for the more security requirements. In public clouds, three common cloud service layers (Infrastructure as a Service, Public as a Service, and Software as a Service) share the unity to the end users, ordinal assets are occupied from an intra-organizational to an inter-organizational context. This produces a number of problems, among which security phases are observed as the most serious factors when considering the cloud computing acceptance and compliance structures raise additional challenges on the outsourced data, processes and applications. To reducing the risk for applications and data in a public cloud service, is the simultaneous usage of multiple clouds. Many approaches employing this prototype have been suggested recently. They vary in separating and distribution technologies, designs, cryptographic methods, and directed scenarios as well as security heights. In this paper we provide four different models in the form of inattentive multi-cloud architectures. These developed a multi-cloud architectures allow to group the available structures and to analyse them according to their security advantages. A valuation of the different approaches with regards to legal features and compliance suggestions is given in particular.

1.1 Cloud Security Issues

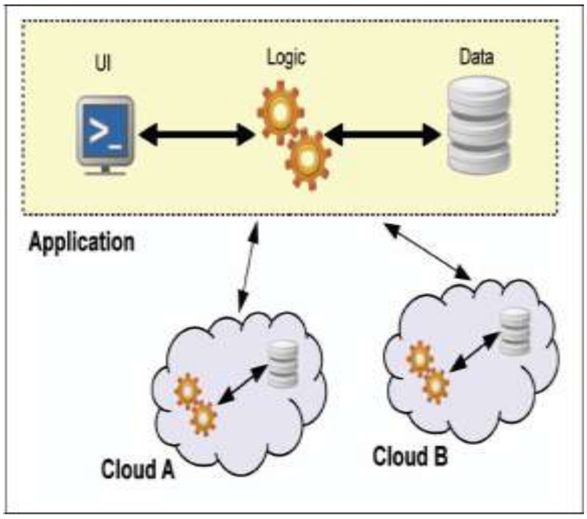
Cloud computing faces many security issues and challenges. These issues collection from the required trust in the cloud service provider and attacks on cloud interfaces to misusing the cloud data for attacks on other cloud systems. One of the main difficulties that the cloud computing prototype indirectly contains is that of secure outsourcing of sensitive data and business-critical data. When seeing usage of a cloud service, user must need be aware of the detail that all his data given to the cloud service provider and leave the own control. Especially, if deploying the data-processing applications to the cloud service via Infrastructure as a Service or Public as a Service, a cloud service provider gains the full access control on these processes. Later, a faith relationship between the cloud service provider and the cloud service user is considered a normal necessity in cloud computing. An attacker that has gain access to the cloud storage And also able to download data or alter data in the storage. This might be done may be one time or multiple times and an attacker can also has access to the business logic of the cloud and can also modify the operations like input and output data. Although in many common cases it may be genuine to accept a cloud service provider to be truthful and manage the customers' activities in a responsible and respectful manner, and there still leftovers a risk of malicious staffs of the cloud service provider.

II. PROPOSED WORK

In this paper, we proposed a model of various architectural designs for distributing assets to multiple cloud service providers. This model is used to deliberate the security advantages and also to categorize previous methods. In our model, we differentiate four architectural designs:

Replication of application systems allows to accept multiple results from one process made in distinct clouds and to compare both of them within the own premise. This allows the user to get proof on the honesty of the result. There is no official way to assurance that and process performed in a cloud system was not interfered with or the cloud system was not attacked by an attacker. The only way of assurance is based on the trust between the cloud service provider and cloud customer and on the contractual rules made between both of them such as service level agreements, appropriate laws, and rules of the involved organizational domains. And even if the relation and contracts are perfectly appreciated by all contributors, there is still some outstanding risks of those are compromised by third parties. To solve this basic problem, different multiple clouds performing multiple copies of the single same application can be deployed (Fig. 1). Instead of performing a specific application on one specific cloud and the same process is executed by different clouds. By comparing the achieved results the cloud user gets proof on the honesty of the result. In such scenery, the necessary trust toward the cloud service provider can be dropped dramatically. Instead of believing one cloud service provider completely, the cloud user only requires trusting on the assumption and that the cloud service providers do not work together with maliciously against her.

Partition of application System into tiers allows separating the logic from the user's data. This gives additional security against data leakage due to faults in the application logic. The architectural design defined in the previous Replication of applications enables the cloud user to get some proof on the honesty of the calculations performed on third-party services. The architecture presented in this partition of application system into tires aims the risk of undesired data leakage and it will give answer to the question in what way a cloud user can be assured that the data access is applied and imposed effectively and the errors in the application logic do not disturb the users' data? And to reduce the risk of data leakage because of application logic faults, the parting of the application system tiers and their allocation to different clouds are proposed (Fig. 2). In situation of an application failure, that the data is not immediately at risk meanwhile it is physically divided and secured by an independent access control pattern. Furthermore the cloud user has choice to choose a particular trusted cloud service provider for data storage and a various cloud provider for applications. It requests to be noted, the security service provided by this architecture can only be completely exploited, if the execution of the application logic on the users data is performed on the cloud user system, only in these types of cases, the application earner does not learn anything about the user data. Therefore, the Software as a Service based distribution of an application, to the user side in combination with the measured access to the user's data performed from the same user system is the maximum far reaching instantiation.



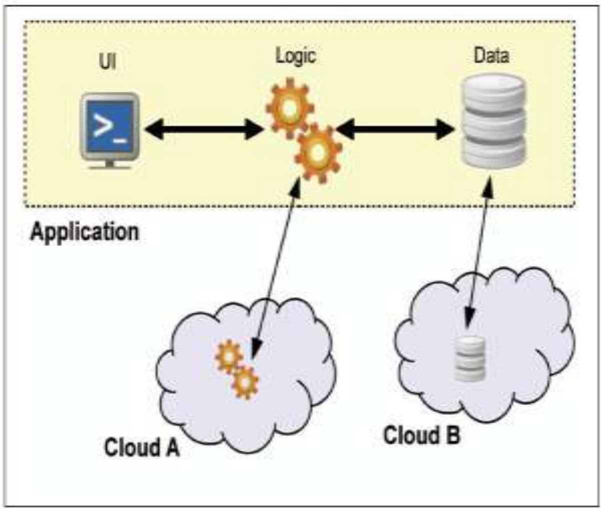
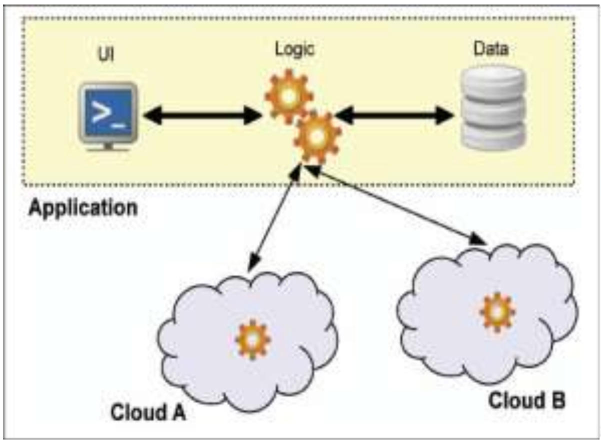


Fig.1 Replications of application systems **Fig.2 Partition of application System into tiers**

Partition of application logic into fragments allows allocating the application logic to different clouds. It has two benefits. (i) No cloud service provider learns the whole application logic. (ii) No cloud service provider learns the complete calculated end result of the application and this leads to application confidentiality and data confidentiality. The impression of this architecture is that the application logic requests to be separated into fine grained fragments and these parts are distributed to different clouds (Fig. 3). This method can be instantiated in various ways based on how the separating is performed. The clouds contributing in the fragmented applications can be asymmetric or symmetric in terms of computing trust and performance. The two common concepts are. The first encompasses a reliable private cloud that takes a minor critical share of the computation and after that a untrusted public cloud that takes maximum of the computational capacity. The second allocates the computation among different untrusted public clouds with an assumption that these public clouds will not collude to break the security rules.

Partition of application data into fragments allows allocating fine-grained fragments of the data to different clouds. None of the involved cloud service providers gains contact to all the data, which protects the data confidentiality. Each of the presented architectural designs provides distinct security merits, which plot to various application situations and their security requirements. Clearly, the designs can be mutual resulting in mutual security merits and but also in advanced deployment and runtime effort. This multi-cloud architecture tells that the application data is divided and distributed to different clouds (Fig. 4). Mutual forms of data storage are databases and files. Files normally contain unstructured data like pictures, text documents and do not allow for simply exchanging or splitting parts of the data. These types of data can only be divided using cryptographic techniques. Databases have data in structured format like organized rows and columns. Now, data partitioning can be performed by allocating different parts of the database like tables, columns, and rows to different cloud service providers. Some files can also contain structured data like XML data. At this point, the data can be split using related approaches like for databases.



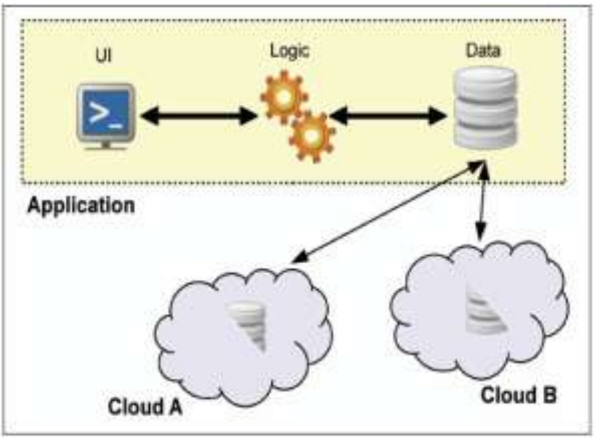


Fig.3 Partition of application logic into fragments **Fig.4 Partition of application data into fragments**

III. CONCLUSIONS

The use of various cloud service providers for gaining privacy and security benefits. As the methods explored in this paper clearly demonstrate, there is no single ideal approach to foster both legal and security compliance in a relevant manner. Furthermore, the methodologies that are favourable from a practical perspective seem less attractive from a controlling point of view, and vice versa. There are few approaches that score appropriately in both these scopes lack adaptability and ease of use, later can be used in very rare conditions only. As can be seen from the deliberations of the four main multi-cloud methodologies, each of them has its drawbacks and weak spots, either in terms of security assurances, in terms of compliance to legal responsibilities, or in terms of possibility and given that each type of multi-cloud approach comes under any one of these four types, this suggests a state of the art that is slightly dissatisfying. Nevertheless, two main notices for development can be taken from the inspections implemented in this paper and given that for every type of security difficult there happens at least one nominal solution approach, a highly exciting field for future research lies in uniting the methodologies presented here. For occurrence, using the n clouds approach in grouping with complete data encryption may result in methodologies that suffice for both practical and monitoring requirements.

REFERENCES

[1] D. 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] 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.

[4] 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.

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

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

[7] J. Kincaid, “Google Privacy Blunder Shares Your Docs without Permission,” TechCrunch, 2009.

[8] 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.

[9] 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.

[10] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M.

[11] 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.

AUTHORS PROFILE

Shaik Lalmahammad, pursuing M.Tech(CSE) from Vikas Group of Institutions, Nunna, Vijayawada. Affiliated to JNTU-Kakinada, A.P., India

Boppudi Swanth, working as an Asst. Professor of CSE department at Vikas Group of Institutions, Nunna, Vijayawada, Affiliated to JNTU-Kakinada, A.P., India

Betam Suresh, is working as an HOD, Department of Computer science Engineering at Vikas Group of Institutions, Nunna, Vijayawada, Affiliated to JNTU-Kakinada, A.P., India