Research Article Impact Factor: 0.621 ISSN: 2319-507X
Samreen Shaikh, IJPRET, 2014; Volume 2 (9): 213- 219 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

TITLE: SECURITY AND PRIVACY- ENHANCEMENT BY MULTI- CLOUD ARCHITECTURES

SAMREEN M. SHAIKH A[1], PRANJALI P. DESHMUKH[2]

1. M. E. Scholar, department of CSE, P. R. Pote (Patil) College of Engineering, Amravati, Maharashtra, India.
2. HOD, P. R.Pote(Patil), College of Engineering & Technology, dept. of CSE Amravati, Maharashtra, India.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

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.

Keywords: Cloud, security, privacy, multi cloud, application partitioning, tier partitioning, data partitioning, multiparty computation

Corresponding Author: MR. SAMREEN M. SHAIKH A

Access Online On:

www.ijpret.com

How to Cite This Article:

Samreen Shaikh, IJPRET, 2014; Volume 2 (9): 213- 219

PAPER-QR CODE

INTRODUCTION

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. 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—include high potential for security prospects.

2. CLOUD SECURITY ISSUES

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. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing.

3. SECURITY PROSPECTS BY MULTICLOUD ARCHITECTURES

The basic underlying idea is to use 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 no 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.

4. REPLICATION OF APPLICATION

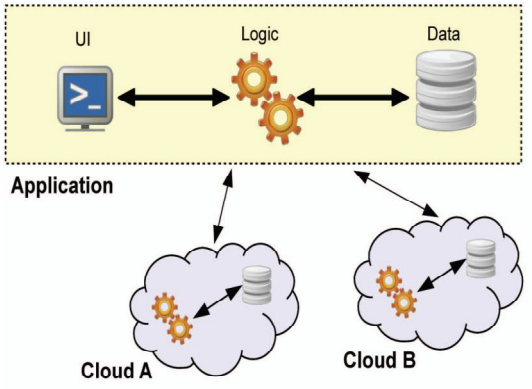

Fig. 1. Replication of application systems.

Assume that n > 1 clouds are available (like, e.g., Clouds A and B in Fig. 1). All of the n adopted clouds perform the same task. Assume further that f denotes the number of malicious clouds

and that n _f > f the majority of the clouds are honest. There are other methods of deriving the correct result, for instance using the TurpinCoan algorithm [3] for solving the General Byzantine Agreement problem.

4.1 Dual Execution

In such a situation, a first and trivial approach for verification might be that a cloud customer triggers the creation of its annual accounting report more than once.

For instance, instead of giving the same request to one cloud provider only (called Cloud A hereafter), a second cloud provider (called Cloud B) that offers an equivalent type of service is invoked in parallel. By placing the same request at Clouds A and B, a cloud user can immediately identify whether his request was processed differently in Clouds A andB.

4.2 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.

5. PARTITION OF APPLICATION SYSTEM INTO TIERS

The architecture introduced in this section targets the risk of undesired data leakage. It answers the question on how a cloud user can be sure that the data access is implemented and enforced effectively and that errors in the application logic do not affect the user's data? To limit the risk of undesired data leakage due to application logic flaws, the separation of the application system's tiers and their delegation to distinct clouds is proposed (see Fig. 2).

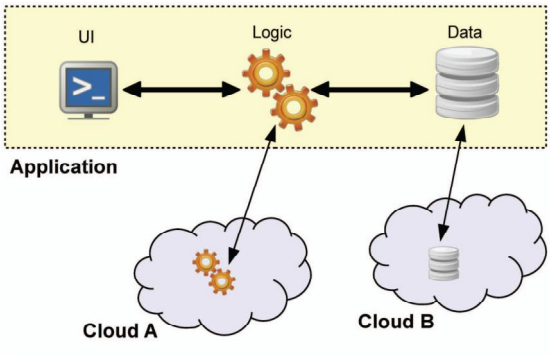

Fig. 2. Partition of application system into tiers.

6. PARTITION OF APPLICATION LOGIC INTO FRAGMENTS

This architecture variant targets the confidentiality of data and processing logic. It gives an answer to the following question: How can a cloud user avoid fully revealing the data or processing logic to the cloud provider?

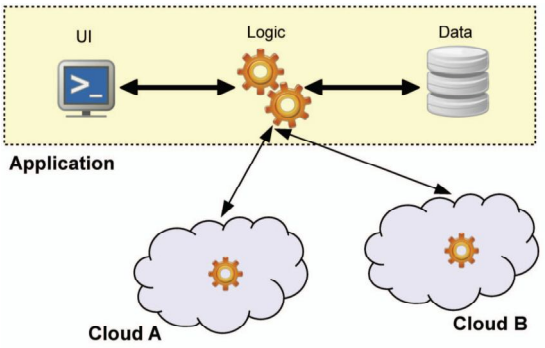

Fig. 3. Partition of application logic into fragments.

6. 1 Obfuscating Splitting

By this approach, application parts are distributed to different clouds in such a way, that every single cloud has only a partial view on the application and gains only limited knowledge. An approach by Danezis and Livshits [7]

The application is split in the following way: The service sends the function to be evaluated to the client. The client retrieves his necessary raw data and processes it according to the service needs. The result and a proof of correctness is given back to the service providing public cloud. In the cloud, the remaining functionality of the service is offered based on the aggregated input of the clients. This architecture protects the detailed user data, and reveals only what the cloud needs to know to provide the service.

6. 2 Homomorphic Encryption and Secure

Multiparty Computation Homomorphic encryption and secure multiparty computation both use cryptographic means to secure the data while it is processed. In homomorphic encryption, the user encrypts the data with his public key and uploads the cipher texts to the Cloud. The cloud can independently compute on the encrypted data to obtain an encrypted result, which only the user can decrypt. Therefore, in our scenario, homomorphic 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 un trusted public cloud.

7. PARTITION OF APPLICATION DATA INTO FRAGMENT

This multi cloud architecture specifies that the application data is partitioned and distributed to distinct clouds (see Fig. 4). The most common forms of data storage are files and databases. Files typically contain unstructured data (e.g., pictures, text documents) and do not allow for easily splitting or exchanging parts of the data. This kind of data can only be partitioned using cryptographic methods.

Databases contain data in structured form organized in columns and rows. Here, data partitioning can be performed by distributing different parts of the database (tables, rows, columns) to different cloud provider. Finally, files can also contain structured data (e.g., XML data). Here, the data can be splitted using similar approaches like for databases. XML data, for example, can be partitioned on XML element level. However, such operations are very costly. Thus, this data are commonly rather treated using cryptographic data splitting.

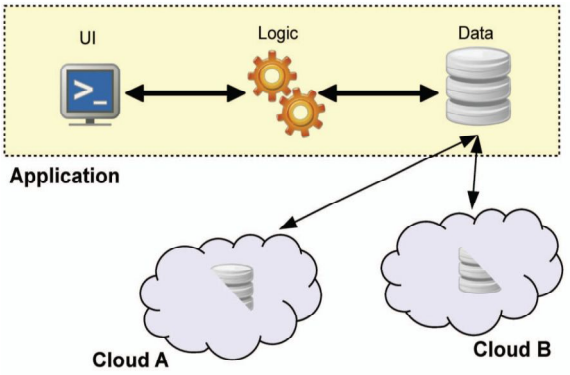

Fig. 4. Partition of application data into fragments.

7.1 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 [9]. This approach, therefore, distributes key material and encrypted data into different clouds. For instance, with XML data, this can, e.g., be done inside the XML document by using XML encryption [10].

7. 2 Database Splitting

For protecting information inside databases, one has to distinguish two security goals: confidentiality of data items (e.g., a credit card number) or confidentiality of data item relationships (e.g., the items "Peter" and "AIDS" are not confidential, but their relationship is).

In the first case, data splitting requires a scenario—similar to other approaches presented before—with a least one trusted provider (or additional encryption; see below). However, very often only the relationship shall be protected, and this can be achieved using just honest-but-curious providers.

8. CONCLUSION

The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. As the approached investigated in this paper clearly show, there is no single optimal approach to foster both security and legal compliance in an omniapplicable manner. Moreover, the approaches that are favorable from a technical perspective appear less appealing from a regulatory point of view, and vice versa.

However, two major indications for improvement can be taken from the examinations performed in this paper. First of all, given that for each type of security problem there exists at least one technical solution approach, a highly interesting field for future research lies in combining the approaches presented here. For instance, using the n clouds approach (and its integrity guarantees) in combination with sound data encryption (and its confidentiality guarantees) may result in approaches that suffice for both technical and regulatory requirements.

Second, we identified the fields of homomorphic 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.

ACKNOWLEDGMENTS

We would like to thank P. P. Deshmukh madam, specifically who provided helpful information about this topic and helped to quickly resolve issues that I encountered.

REFERENCES

1. 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, 2011.

2. P. Mell and T. Grance, “The NIST Definition of Cloud Computing, Version 15,” Nat’l Inst. of Standards and Technology, Information Technology Laboratory, , 2010.

3. R. Turpin and B.A. Coan, "Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement," Information Processing Letters, vol. 18, no. 2, pp. 73-76, 1984.

4. I. Koren and C.M.C. Krishna, Fault-Tolerant Systems. Morgan Kaufmann.

5. J.D.J. Wisner, G.K.G. Leong, and K.-C. Tan, Principles of Supply Chain Management: A Balanced Approach. South-Western, 2011.

6. N.A.N. Lynch, Distributed Algorithms. Morgan Kaufmann, 1996.

7. G. Danezis and B. Livshits, "Towards Ensuring Client-Side Computational Integrity (Position Paper)," Proc. ACM Cloud Computing Security Workshop (CCSW '11), pp. 125-130, 2011.

8. S. Groß and A. Schill, "Towards User Centric Data Governance and Control in the Cloud," Proc. IFIP WG 11.4 Int'l Conf. Open Problems in Network Security (iNetSeC), pp. 132-144, 2011.

9. F. Pagano and D. Pagano, "Using In-Memory Encrypted Databases on the Cloud," Proc. First Int'l Workshop Securing Services on the Cloud (IWSSC), pp. 30-37, 2011.

10. J. Somorovsky, C. Meyer, T. Tran, M. Sbeiti, J. Schwenk, and C. Wietfeld, "SeC2: Secure Mobile Solution for Distributed Public Cloud Storages,"

11. J. Vijayan, "Vendors Tap into Cloud Security Concerns with New Encryption Tools,"

12. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen," Security and Privacy-Enhancing Multicloud Architectures" IEEE.