Towards securing cloud data in the multi-cloud scenario

Firas Qays Kamal [1], Ahlam Abbas Betti[2]
[1]Directorate General of Education Al Qadisiyah, Iraq
[2]Technical Institute of Al-Diwaniyah, Al-Furat Al-Awsat Technical University (ATU), Iraq

ABSTRACT

Cloud computing has emerged to be the accepted computing model which provides services on-demand. The most used service layer is infrastructure as a Service (IaaS) to outsource data to the cloud. With this service, organizations and individuals can avail of cloud services in pay as you use fashion instead of investing money for such infrastructure. Cloud provides many such benefits to its users. However, as the cloud servers are remote and assumed to be untrusted, users are worried about data security. Initially, a single cloud was used to store data. With the advancements in technologies and for reliability reasons, the concept of multi-cloud has emerged. The security and reliability issues with a single cloud can be overcome with multi-cloud systems. The rationale behind this is that a single cloud might have malicious insiders. When two or more clouds collaborate and provide services to end-users, it is expected to have more reliability and possible reduction in malicious insiders. This paper focuses on studying the potential security of data that is stored in multi-cloud. We built an algorithm and prototype application that demonstrates the concept of securing data in a multi-cloud environment. The empirical results revealed that the proposed system could ensure the data outsourced to cloud computing where a multi-cloud scenario prevails.

Keywords: Insider threat, CERT dataset, Cybersecurity, Attacker's psychology, IT sabotage

Corresponding Author:

Firas Qays Kamal
Directorate General of Education, Al Qadisiyah, Iraq
E-mail: faris_qais2001@yahoo.com

1. Introduction

Cloud computing has been around for some years. It has revolutionized the way data is stored, and the way computing takes place. As a pool of computing resources, the cloud can cater to the needs of organizations concerning outsourcing data and computing in pay per use fashion. This outsourcing is that the cloud provides a massive amount of storage place that cannot be possible with small organizations and individuals. Without capital investment, businesses can have a plethora of cloud services on-demand. The services are provided with affordable pricing, and thus cloud became popular these days. The essential services rendered by the cloud are infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), as shown in Figure 1. These service layers provide respective services to end-users. However, in this paper, we deal with infrastructure as a Service where the cloud data is stored. Traditionally single cloud concept is used. Right from the inception of the cloud, there has been the concept of a single cloud where data is stored, and other services are rendered.

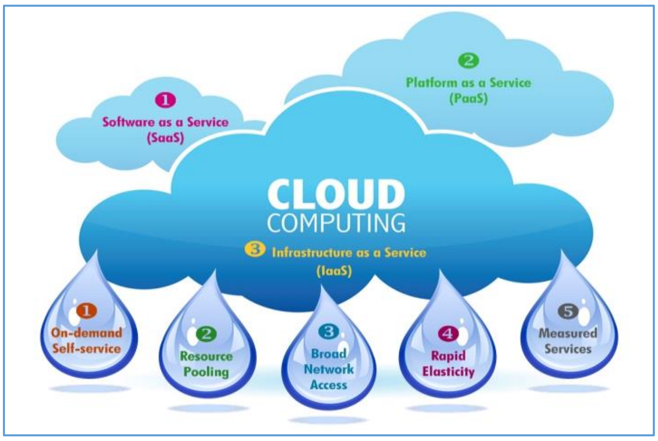


Figure 1. Cloud computing and its services

With a single cloud, there is a possibility of having reliability problems. This can be avoided by using multiple clouds working together. The single cloud may be subjected to insider attacks on the data, while the multi-cloud is subjected to business rules, and it can avoid the possibility of such attacks. Moreover, multi-cloud can improve the quality of service, scalability, and reliability besides 100% availability. Recently there has been increased research in the multi-cloud environment. In this paper, we focused on the security of data in multi-cloud environments. We proposed an algorithm that takes care of secure data dynamics in multi-cloud.

Our contributions in the paper are described here. We investigated the present state of the art on the multi-cloud environment concerning the security of cloud data. Then we proposed and implemented an algorithm to ensure that the data storage and retrieval take place in the multi-cloud environment with complete security. Afterward, we built a prototype application that uses the proposed mechanism to secure cloud data dynamics. The outcome revealed that the system could secure data in the multi-cloud environment. The rest of the paper is set out as follows. Section II allows for literature review. The proposed schema is discussed in detail in section III. Section IV presents experimental findings, while the paper is completed in section V.

2. Related works

Many solutions came into existence to reduce the risk of security to outsourced data in the cloud. The solutions are of different varieties. For instance, public auditing, provable data possession, proof of retrievability, attribute-based encryption, and improvements in the single cloud are examples of the research carried out. This section provides a review of literature that reflects the current academic thinking. Simple cryptographic methods are used in [1] for secure data storage in a single cloud. The concept of the hash function is explored in [2]. In [3] and [4] provable data possession concept was introduced to ensure that data integrity is not lost. The concept of fault-tolerant protocols was introduced in [5] and [6]. In all the approaches, cloud computing resources are required, and experiments are done with the cloud in storage security.

Auditing is one of the solutions provided in the literature. Many researchers contributed to improving the public auditing concept. As explored in [7], the cloud service providers are to ensure secure cloud data operations. They need to take care of infrastructure-related issues and other security problems in the cloud. Reliability and availability are other vital factors that are to be addressed in cloud computing [8]. There are many issues associated with cloud storage. There are many domains whose data is outsourced. For instance, medical data is outsourced, and securing such data is indispensable. In the same fashion, banks and other financial institutions outsource their data. Therefore, such data is susceptible and needs to be protected without fail.

As opined in [9], security risks are critical things to be addressed in cloud computing. According to a survey conducted and presented in [10], security is one of the top challenges in cloud computing. Many security issues are involved when extensive data from databases are moved to cloud data centers [11]. As shown in [12], many delivery models are to be protected from malicious attacks. It is the responsibility of the cloud service provider to ensure the security of the outsourced data. In [13], different levels of security for IaaS service layer of could computing. These levels of security are to safeguard the interests of data owners. It also needs to take care of security issues resulting from hardware or software failures in the cloud. Hacked password and data intrusion are the security risks identified and explored in [14] in an environment like Amazon. In [15], multi-cloud is analyzed and its utility in the real world. In [16], two security layers in the multi-cloud were identified. They are intra-cloud and inter-cloud layers concerning providing scalable and secure solutions with 100% availability. In [17], the concept of readers and writers in the context of cloud computing is explored. Here architecture is proposed for a multi-cloud environment. The name of the architecture is DepSky. It addresses many security issues such as confidentiality besides availability and scalability.

3. Proposed system

The proposed framework aims to model a multi-cloud environment and test data protection. We proposed and implemented an algorithm to check the security of stored data. We built a prototype application to run the algorithm and demonstrate how data is encrypted and split into multiple parts, and stored in various clouds. The concept of using multiple clouds is to ensure availability, reliability, and scalability. Our proposed algorithm is concerned with data integrity within the multi-cloud environment. As the multi-cloud concept has prevailed in the real world, it is essential to have a security evaluation of multi-cloud. This paper threw light on this, and the empirical study focused on the secure data dynamics in the multi-cloud environment.

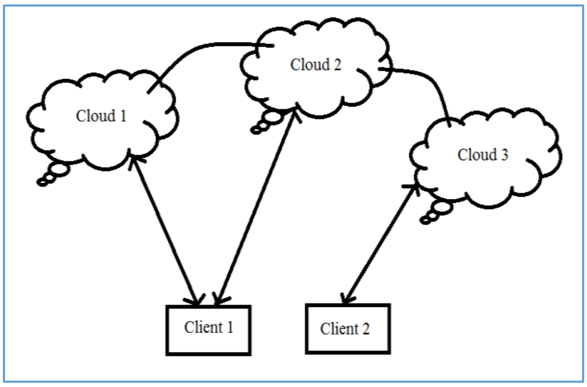


Figure 2. Multi-cloud environment

As shown in Figure 2, it is evident that multiple clouds collaborated to provide reliable and scalable services. The proposed algorithm takes care of data integrity in the context of multi-cloud. Due to the ability of the algorithm to cater to the needs of storage in multi-cloud, it is tested with a prototype application that simulates the multi-cloud environment and secures data dynamics.

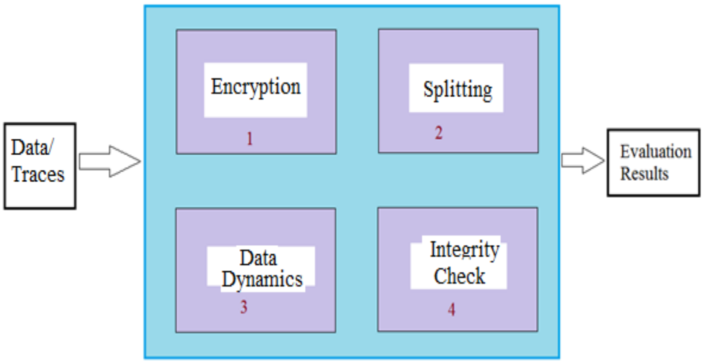


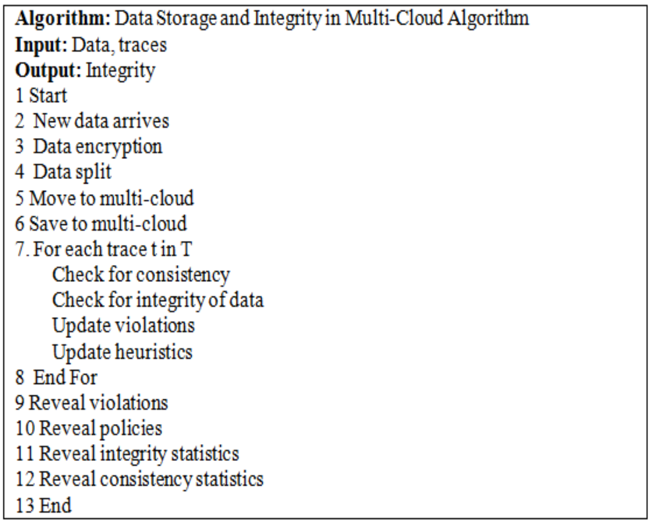
Figure 3. Necessary modules in the proposed system

As can be seen in Figure 3, there are four essential models in the proposed system. The first module takes care of the encryption of data. It makes use of standard cryptographic primitives supported by the Microsoft.NET platform. Then the second module takes care of splitting data to get stored into different clouds. Afterward, the third module takes care of data dynamics in the multi-cloud environment, while the last module performs an integrity check. For integrity checking, the following algorithm is used.

4. Proposed algorithm

We proposed an algorithm that takes care of data integrity in a multi-cloud environment. It makes use of data and traces to have an integrity check. It also saves the heuristics it understands in the process. This know-how is used later to ensure that the data integrity is not lost.

Algorithm 1 – Algorithm for data storage and integrity in multi-cloud



```
Algorithm: Data Storage and Integrity in Multi-Cloud Algorithm
Input: Data, traces
Output: Integrity
Start
New data arrives
Data encryption
Data split
Move to multi-cloud
Save to multi-cloud
For each trace t in T
    Check for consistency
    Check for integrity of data
    Update violations
    Update heuristics
End For
Reveal violations
Reveal policies
Reveal integrity statistics
Reveal consistency statistics
End
```

As is evident in algorithm 1, the proposed algorithm takes both data and traces as input. Concerning new data, it performs encryption and splitting to send data to a multi-cloud environment. In the case of data integrity, it checks traces to find any inconsistencies or violations. It updates heuristics and will be in a better position to work in the future with the help of knowledge gained.

5. Experimental results

To show design proof, we developed a prototype application. The application is created using Microsoft.NET to simulate the cloud environment and has experimented on it. The observations we made are related to security in the context of multi-cloud. We captured the number of executions, true positives, and false positives. We also provided the research dynamics in the recent past about single and multi-cloud environments on secure data storage and retrieval.

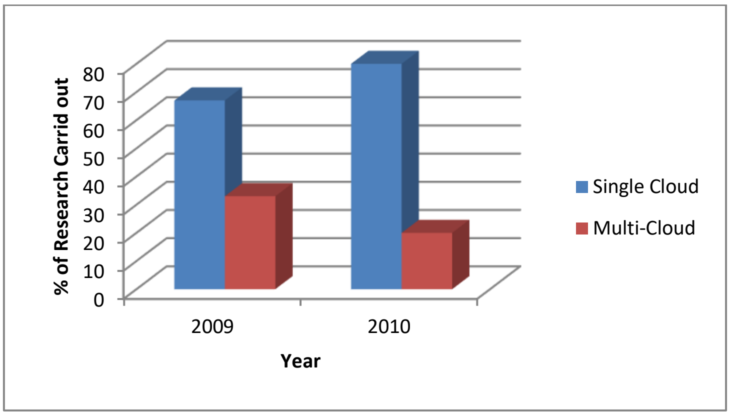


Figure 4. Research dynamics on the single and multi-cloud

As shown in Figure, more research on the multi-cloud was carried out in 2009. It is 33% while the same is 20% in 2010. The single cloud research is more in both the years, and in 2010 it is highest. These results reveal the trend in the study in cloud computing.

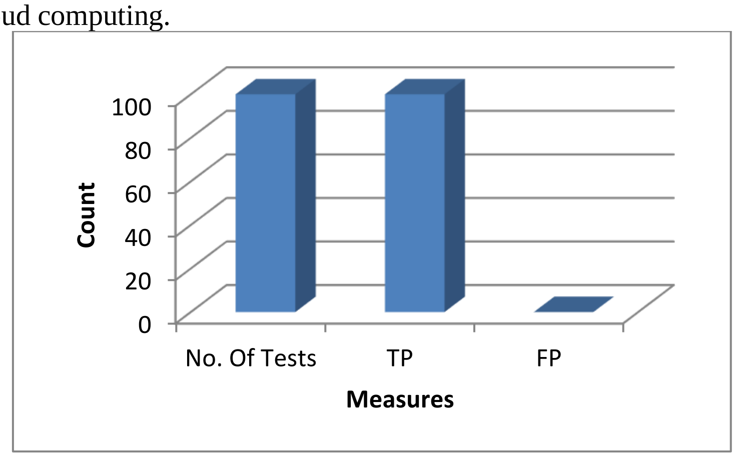


Figure 5. Evaluation results

We evaluated the proposed system with data and traces. The results revealed that the system is working as per the expectations. The security provided to data is tested 100 times. It resulted in 100% true positives and 0% false positives. This reflects the usefulness of the proposed scheme for protecting data outsourced to a multi-cloud environment.

6. Conclusions and future work

In this paper, we studied the security of cloud data. Mainly we found the difference between single cloud and multi-cloud environments. It is believed that multi-cloud can provide more reliability and security. Many schemes came into existence to deal with the security of outsourced data. However, they were designed and implemented, keeping a single cloud in mind. However, there is the possibility that the data is outsourced to multi-cloud for reliability and security reasons. When multiple clouds are involved, and when they are from different service providers, it is believed that they improve the quality and security of services. We suggested and implemented in this paper a security mechanism that caters to the needs of the users of the cloud. In other words, the proposed solution can secure data stored in multi-cloud environments. We evaluated the system with a prototype application. The empirical findings showed our application helped deal with secure storage and retrieval in the context of multi-cloud. This research can be further expanded to enhance data protection in multi-cloud by proposing new schemes to operate on encrypted data and support data dynamics.

References

[1] C. Cachin, I. Keidar, and A. Shraer, "Trusting the cloud", *ACM SIGACT News*, vol.40, pp. 81-86, 2009.

[2] R.C. Merkle, "Protocols for public keycryptosystems", *IEEE Symposium on Security and Privacy*, pp. 122-134, 1980.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", *Proc. 14th ACM Conf. on Computer and communications security*, pp. 598-609, 2007.

[4] A. Juels and B.S. Kaliski Jr, "PORs: Proofs of retrievability for large files", *14th ACM Conference on Computer and communications security*, pp. 584-597, 2007.

[5] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", *Operating Systems Review*, vol.33, pp. 173-186, 1998.

[6] J. Hendricks, G.R. Ganger, and M.K. Reiter, "Low overhead byzantine fault-tolerant storage," *21st ACM SIGOPS symposium on Operating systems principles*, pp. 73-86, 2007.

[7] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, vol.34, no.1, pp 1-11, 2011.

[8] S. Kamara and K. Lauter, "Cryptographic cloud storage", *14th International Conference on Financial Cryptography and Data Security*, pp. 136-149, 2010.

[9] J. Viega, "Cloud computing and the common man", *Computer*, vol. 42, pp. 106-108, 2009.

[10] Clavister, "Security in the cloud", Clavister White Paper, 2008.

[11] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing", *International Conference on Advances in Recent Technologies in Communication and Computing*, pp. 1-9, 2010.

[12] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", *IEEE Security & Privacy*, vol.8, no.6, pp. 24-31, 2010.

[13] T.ristenpart, E. Tromer , H. Shacham, and S. Savage, "Hey, you, get off my cloud: exploring information leakage in the third-party compute clouds ", *ACM Conference on computer and communication security*, pp.199-212, 2009.

[14] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", *Technical Report TR-08-07*, Computer Science Group, Harvard University, pp. 1-15, 2007.

[15] M. Vukolic, "The Byzantine empire in the intercloud," *ACM SIGACT News*, vol.41, pp. 105-111, 2010.

[16] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud," *Research Report RZ*, 3783, 2010.

[17] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", *6th Conference on Computer systems*, pp. 31-46, 2011.