International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:5, 2015

New Security Approach of Confidential Resources in Hybrid Clouds

Haythem Yahyaoui, Samir Moalla, Mounir Bouden, Skander Ghorbel

Abstract**—**Nowadays, cloud environments are becoming a need for companies, this new technology gives the opportunities to access to the data anywhere and anytime. It also provides an optimized and secured access to the resources and gives more security for the data which is stored in the platform. However, some companies do not trust Cloud providers, they think that providers can access and modify some confidential data such as bank accounts. Many works have been done in this context, they conclude that encryption methods realized by providers ensure the confidentiality, but, they forgot that Cloud providers can decrypt the confidential resources. The best solution here is to apply some operations on the data before sending them to the provider Cloud in the objective to make them unreadable. The principal idea is to allow user how it can protect his data with his own methods. In this paper, we are going to demonstrate our approach and prove that is more efficient in term of execution time than some existing methods. This work aims at enhancing the quality of service of providers and ensuring the trust of the customers.

Keywords**—**Confidentiality, cryptography, security issues, trust issues.

I. Introduction

CLOUD Computing is a set of hardware and software, offering an easy access to shared computing resources such as: servers, storage infrastructure, applications and network devices [1], [2]. Nowadays this technology is becoming a need for companies, because it gives them an easier way to manage their resources and especially their confidential resources.

When talking about confidential resources, many companies prefer to use their own platform, because they are afraid of internet attacks and also of Cloud providers.

To encourage these companies, and according to some studies in [3]-[5], Cloud providers encrypt data before storing them, using two types of encryption algorithm, thus we distinguish:

- Symmetric algorithms such as: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES and Blowfish for customer data encryption.
- Asymmetric algorithms such as: Rivest-Shamir-Adleman (RSA) to encrypt exchanged keys between clients and Cloud Platform.

In cloud environment, the encryption process and file storage are presented in Fig. 1.

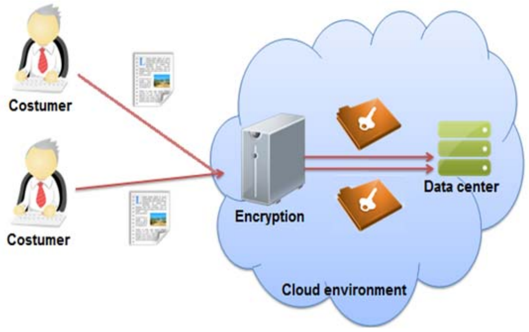

Fig. 1 Encryption and Storage process

Many organizations have problems in the trust relationship with cloud providers. Indeed, Cloud providers can manage confidential resources such as: personal resources.

Many works have been done in order to protect the confidential customer’s data, and there are many techniques such as: protection by the provider side [6]-[8], or by the customer side [9], [10]. But also there are many limitations such as: trust issues, when talking about provider side, or a waste of time when talking about customer side.

In this paper we are trying to propose, implement, and evaluate a new approach of the security of confidential resources, based on splitting and combining data randomly, before sending them to different cloud providers.

This paper is organized as follows. Section II presents some existing methods and their limitations. We introduce our approach in Section III before implementing it in Section IV, and evaluating it in Section V. Finally we conclude the paper and discuss future works in Section VI.

II. Related Work

In this section we will present the results from other studies; we have two kinds of customer data security: the provider side and the customer side.

A. Provider Side

Drop Box [6], the famous cloud provider; use the AES-256 bits encryption method and Secure Sockets Layer (SSL) Protocol. Thus this cloud provider analyzes the applications and infrastructure to identify vulnerabilities with the aim of improving and protecting customer data against attacks.

Google [7], the dominant of the cloud market, says that customer data is distributed across multiple machines on

Haythem Yahyaoui and SamirMoalla are with the Faculty of Sciences of Tunis, Tunisia, University of Tunis el Manar (e-mail: haythem.yahyaoui@gmail.com, sam_moalla@yahoo.fr).

Mounir Bouden is with the Research Department of Smart HOST Tunisia (e-mail: mounirb@smarthost.tn).

Skander Ghorbel is with the Higher Institute of Computer Science and Multimedia of Sfax, Tunisia (e-mail: skander.ghorbel@gmail.com).

several sites. Then it will be cut out and replicated on different systems, to avoid producing points of failure. Finally, these data blocks are randomly appointed which generates an additional security, therefore unreadable customer data.

Unlike Google and DropBox, Microsoft Windows Azure [8] offers several encryption methods, to propose to the customers the freedom to choose the method that meets their needs. This environment also uses segregation that gives the opportunity to store customer deployments and virtual machines in the same physical device and offers economic benefits.

We can conclude then that confidential resources stored in the cloud are very well secured against attacks from some users of this new technology. However, cloud providers can have access to the confidential resources before the encryption process or also after the encryption process by decrypting the customer's data.

In this perspective we are led to propose a new approach that makes it possible for customers to secure their data before storing them in public cloud.

B. Customer Side

New approaches are proposed in [9] and [10], based on the symmetric algorithms such as: AES, DES, 3DES, RC4, RC6 and Blowfish to encrypt resources in the customer machine, before sending them to the cloud.

A limitation of these approaches is due to the characteristics of symmetric encryption algorithms; indeed they are very costly in terms of time, mainly when the data is large. This limit could be a constraint to the customer, because he doesn't want to lose time, and therefore he can be forced to leave the cloud environments.

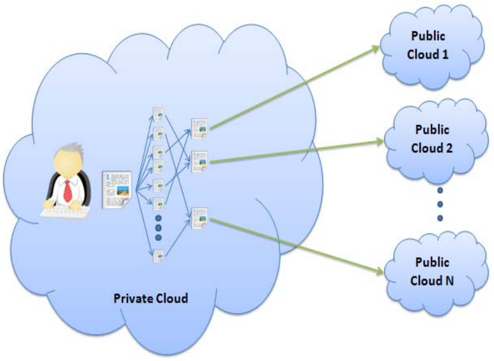

Fig. 2 Approach process

III. Proposed Approach

In this section we present our new approach for the security of confidential resources. Our method is based on splitting the file to send into several parts, and then generating some sub files from a combination of the parts using a fingerprint key, before sending them to different cloud providers.

If there is an unwanted access to one of sub files, the customer will be always protected.

Our approach process is presented in Fig. 2.

Here is a presentation of the different phases of our approach:

- **Phase 1**:*Signature and Fragmentation*
  - Generation of the electronic fingerprint using the hash function MD5.
  - Generation of the Finger Key using the generated Fingerprint.
  - Splitting the file to send into several parts.
- **Phase 2**: *Combination and regrouping*
  - Generation of sub files by the combination of the generated parts using the Finger Key.
  - Regrouping the sub files in the case when they are much than the cloud providers
- **Phase 3**: *Upload*
  - Sending the sub files to different Cloud providers.

The upload process is described in Fig. 3.

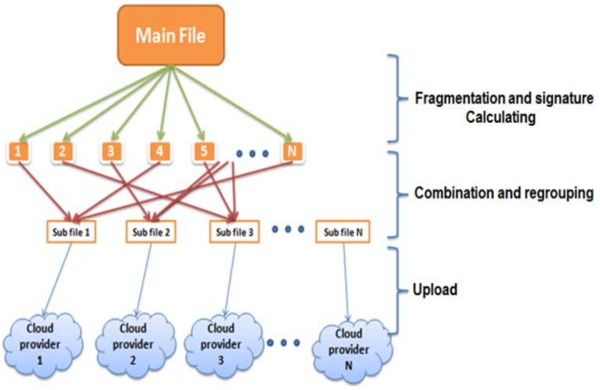

Fig. 3 Upload process

In the download phase, our approach is based on, downloading the sub files, splitting them, and finally applying the inverse of the combination that was done in the upload phase.

Here are the proposed phases:

- **Phase 1**: *Download*
  - Downloading the sub files from the different cloud providers
- **Phase 2**: *Fragmentation*
  - Splitting thesub files into several parts.
- **Phase 3**: *Generation of the main file and checking the data integrity*
  - Generation of the main file using the reverse of the combination used in the upload process.
  - Generation of the electronic fingerprint using the hash function MD5.
  - Comparing the fingerprint with the generated fingerprint during the upload process, in order to check the integrity of the main file.

The download process is described in Fig. 4. The integrity of hosted data in the cloud is a constraint that should be respected, for that reason we applied the MD5 hash function on the main file in the first phase of the upload process, and also in the final phase of the download process, to generate the electronic Fingerprints and finally comparing them. If they are equals we can conclude that the integrity constraint is respected. This option is described in Fig. 5.

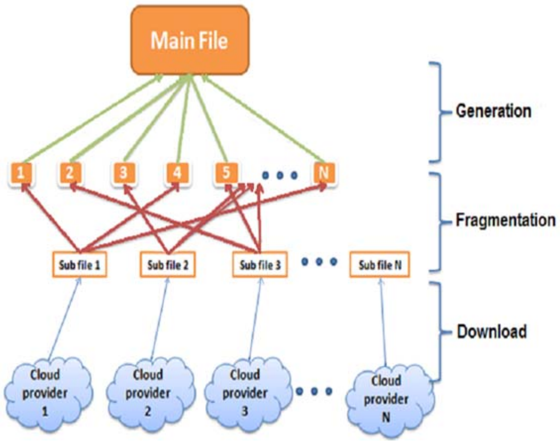

Fig. 4 Download process

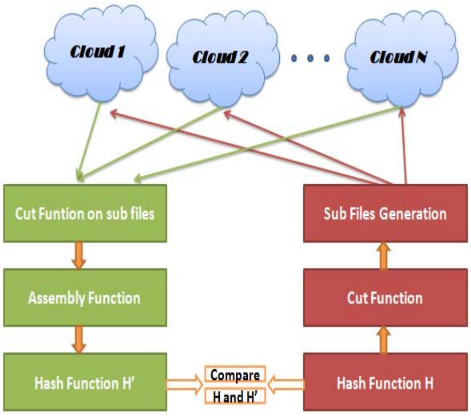

Fig. 5 Integrity check

IV. Implementation

Until now, we do not know into how many parts we will split the main file, also the number of sub files generated. For that reason we are going to apply our method using some different values in order to find out on what value our method is more efficient.

Evaluating our solution was performed on a virtual machine VMware, with 2 GB of RAM and only one CPU 1,6 GHz running OpenSUSE 13.2.

We have to mention that the number of sub files generated depends on the number of providers chosen by the customer. In our tests we supposed that the number of providers is three in order to make the comparison easier.

TABLE I
Evaluation Results

Parts\size (MB)	32	64	128	256	512
6 Parts	1,83	3,78	18,19	29,02	53,04
9 Parts	1,64	4,92	16,23	27,6	52,14
12 Parts	2,09	4,62	14,72	40,19	67,23

Table I is a summary of the obtained results evaluated in second (S). In the left column we find the number of parts and in the first line we find the size in Megabytes (MB) of the tested files.

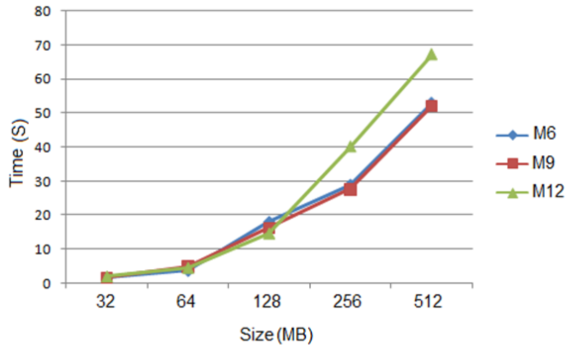

Fig. 6 Response time of M6, M9, and M12

Previous results are shown in Fig. 6. From Fig. 6, we can conclude that the green curve (M12) seems to be the best until 128, however, from 128 it is the worst in term of time, the curve M9 compared to M6 and M12, seems to be the best, specially form 128.We can also calculate the speed from the evaluation results using:

$$\text{Speed}=\frac{\text{File size}}{Execution\ time}$$

TABLE II
Speed of M6, M9, and M12

Parts\size(MB)	32	64	128	256	512
M6	17,49	16,93	7,04	8,22	9,65
M9	19,51	13,01	7,89	9,28	9,82
M12	15,31	13,85	8,70	6,37	7,62

Previous results are shown in Fig. 7. From all the previous results, we can conclude that M9 is the most effective method in term of time. So we will split the main file into 9 parts when comparing with the existing methods.

V.Evaluation

In this section, we try to deploy some existing methods in order to compare between them and our proposed method.

We implemented some symmetric algorithms such as: AES with cbc mode and 256 bits key length and DES with cbc mode. The obtained results are classified by the Fig. 7.

TABLE III
Response Time of AES, DES, and M9

Method\size (MB)	32	64	128	256	512
AES	2,49	5,34	16,17	28,21	42,59
DES	5,33	9,02	24,70	37,29	55,54
M9	1,64	4,92	16,23	27,6	52,14

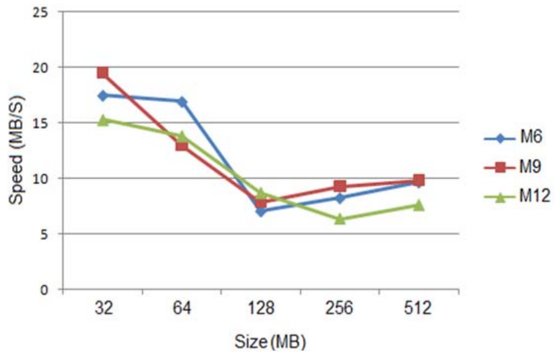

Fig. 7 Speed of M6, M9, and M12

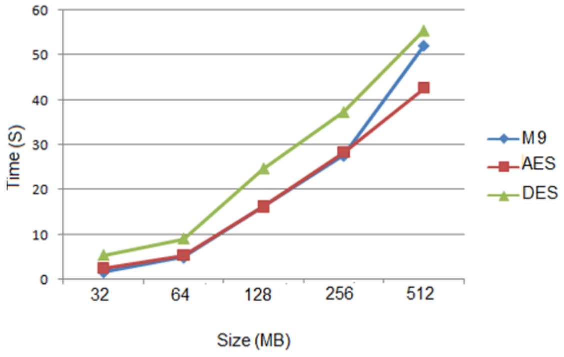

Fig. 8 Response time of AES, DES and M9

Previous results are shown in Fig. 8. From Fig. 8 we can conclude that the blue curve (M9) seems to be the best in the interval [32, 256], but form 256 the red curve (AES) is the best in term of time. We can also calculate the speed of the different algorithms in order to clarify the obtained results:

TABLE IV
SPEED OF AES, DES, AND M9

Method\Size (MB)	32	64	128	256	512
AES	12,85	11,99	7,92	9,07	12,02
DES	6,00	7,10	5,18	6,77	9,21
M9	19,51	13,01	7,89	9,28	9,82

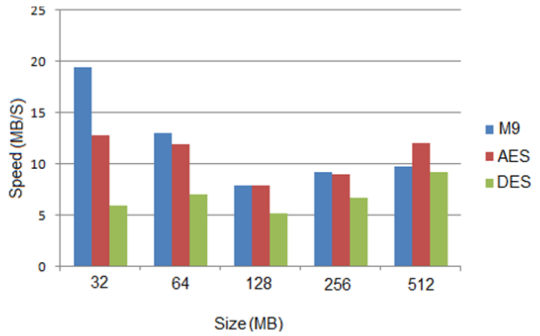

Fig. 9 Speed results of AES, DES and M9

We compare the different speeds using Fig. 9. Figs. 7-9 are virtualization of the obtained results during the experimental phase; from that phase we can conclude that our proposed method is more efficient than the existing methods in the interval [32, 256]. However, from 256 MB file's size, the AES encryption method is the best. We have to mention that our comparison is based on execution time and speed.

VI. Conclusion

In this research paper we proposed a new approach of security of confidential resources in hybrids clouds. Our proposed method was evaluated and compared with the existing security methods in the same environment and configurations. The comparison phase is based on speed calculated from the execution time.

In the future work we will analyze some optimization techniques, and we will apply the best of them on our method in the order to make it more efficient and speedier. Our challenge will be focused on the high file's size.

References

[1] J. Liu, Q. Zhang, and H. Chen, "The Characteristics of Cloud Computing," IEEE 39th International conf. Parallel Processing Workshops. San Diego CA, pp. 275-279, September 2010.

[2] M. Zhou, R. Zhang, D.Zeng, and W. Qian, "Services in the Cloud Computing era: A survey," IEEE 4th International Universal Communication Symposium. Beijing CHINA, pp. 40-46, October 2010.

[3] K. Jasem Mohammad Omar, S. Abbas, M. El-Sayed El-Horbaty, and M. Abdel-Badeeh Salem, "A comparative study between modern encryption algorithms based on cloud computing environment," IEEE 8th International Conference for Internet Technology and Secured Transactions. London, United Kingdom, pp. 531-535, December 2013.

[4] C.P. Gupta, and I. Sharma, "A fully homomorphic encryption scheme with symmetric keys with application to private data processing in clouds," IEEE Fourth International Conference on the Network of the Future. Pohang, p. 1-4, October 2013.

[5] M. Zhou, R. Zhang, W. Xie, W. Qian, and A.Zhou, "Security and Privacy in Cloud Computing: A Survey," IEEE Sixth International Conference on Semantics Knowledge and Grid. Beijing, pp. 105-112, November 2010.

[6] DropBox, "Privacy Policy" https://www.dropbox.com/en/privacy published 2015-02-13.

[7] D. Sheng, D. Kondo, and F. Cappello, "Characterizing Cloud Applications on a Google Data Center," IEEE 42nd International Conference on Parallel Processing. Lyon, pp. 468-473, October 2013.

[8] Microsoft, "Windows Azure Privacy Overview" http://download.microsoft.com/download/1/6/0/160216AA-8445-480B-B60F-5C8EC8067FCA/WindowsAzure-SecurityPrivacyCompliance.pdf

[9] M. Mohamed. Eman, H. S. Abdelkader, S. El-Etriby, "Data Security Model For Cloud Computing," The Twelfth International Conference on Networks. Seville, pp. 66-74, January 2013.

[10] A.S.R. Armel, and V. Thavavel, "Ghost encryption: Mobile data security model encrypting data before moving it to the cloud service provider," IEEE Fifth International Conference on Advanced Computing. Chennai, pp. 512-516, December 2013.