International Journal of Latest Research in Science and Technology
Volume 12, Issue 1: Page No.1-5 (2023)
https://www.mnkjournals.com/journal/ijlrst/index.php

ISSN (Online):2278-5299

THE ADOPTION OF CLOUD COMPUTING: PROBLEMS AND SOLUTIONS

Sergio Rafael García Bravo*, Miguel Patiño Ortiz[2], Tonáhtiu Arturo Ramírez Romero[3]
[*]ESIME Zacatenco, Instituto Politécnico Nacional, srgarciabravo@gmail.com, México
[2]ESIME Zacatenco, Instituto Politécnico Nacional, mpatino2002@gmail.com, México
[3]Escuela Superior de Cómputo, Instituto Politécnico Nacional, tonahtiu@yahoo.com, México

Received: 12 May 2023; Accepted: 29 May 2023; Published :1 June 2023

Abstract: ***This document presents a general overview of the main risks and problems in cloud-computing security that the information owners face, as well as a showing of the common tools and solutions that help reduce these problems and guarantee security, confidentiality and information integrity. Finally, an architecture of the solution is proposed.***

***Keywords*:** Cloud computing, migration, security problems, attacks, solutions, cypher tools.

I. INTRODUCTION

Currently, the use of cloud computing by various companies or organizations that require storage and processing of information, as well as the use of various applications to carry out their own processes, has become a very profitable solution for those who decide to use it, since the cost incurred by hiring a Cloud Service Provider (CSP) is much lower than managing infrastructure, applications, and information. However, whenever a migration to third-party cloud services is contemplated, it is necessary to consider and analyze the impact that a possible loss, theft, or misuse of our information and/or processes carried out in this environment could have, as well as potential equipment failures, which could put the data that has been entrusted to third parties at risk. This forces organizations to seriously evaluate whether or not it is worth using cloud computing to make the decision to carry out the migration or not, and subsequently, how it would be carried out.

Once the decision to migrate has been made, the advantages, problems, and risks involved in carrying out this activity must be understood, taking into account the attacks and threats that may arise and that undermine the security of the information that is entrusted to one or more CSPs. Similarly, the methods and tools that provide an appropriate solution and allow us to maintain the privacy and confidentiality of the data or, in any case, mitigate possible damage to the outsourced information must be known. This article is organized into five sections, which are described below. Section 2 presents related work on the cloud computing migration process. Section 3 provides a general overview of the different security problems and attacks that arise in cloud computing, as well as the risks they pose to information security. Section 4 proposes tools and solution methods to mitigate security problems. Section 5 presents a proposal for a general reference framework that can serve as a guide for carrying out the cloud migration process. Finally, section 6 concludes the article.

II. RELATED WORKS

It is increasingly common for companies of different sizes and economic activities to consider using cloud computing to obtain the benefits it provides, such as cost reduction, information availability, use of technology specific to their activities, etc. In [1], benefits of migration are mentioned, such as reliability, security, scalability, recovery, collaboration, and flexibility. However, there are many inherent fears associated with cloud computing that hinder or make the decision to migrate their information systems difficult.

One of the crucial questions in an organization's decision-making process to carry out the migration of its infrastructure to the cloud or not, is the security aspects, such as how the information will be treated or the guarantee that it is always secure. In [2], it is mentioned that one of the main security problems in outsourcing data or databases sent to cloud servers is that the owner of all that information loses control of it and the CSP becomes its main administrator, becoming vulnerable to any security risks.

An analysis of different studies focused on the implementation, adoption, and acceptance of cloud computing by companies and individuals was carried out in [3], based on the Technology Acceptance Model, the Technology-Organization-Environment Framework, and the Diffusion of Innovation Theory, which are used to measure the acceptance and use of new technologies, in order to define the main factors that influence the decision to migrate or not, highlighting compatibility, security, complexity, cost, and trust. In [1], the risks associated with migration are addressed, which are mainly due to downtime and the security measures that must be adopted, not only those inherent to IT equipment but also those that involve the human capital itself, weighting the owner of the information as the main responsible for information security. Similarly, to mitigate the risks that go hand in hand with migration, it is necessary to identify the correct service provider, as well as the security protocols that it has.

Whenever companies seek to know, analyze, and assess the risks that may arise in any situation they face, a risk assessment is necessary. To determine the risks inherent in using cloud computing, a similar tool can also be used that focuses on evaluating each of the cloud service providers. A comparison of various models for evaluating risks in a cloud service provider, based on ISO/IEC and NIST standards, is carried out in [4], proposing a model composed of 3 modules: quantitative risk analysis, CSP security evaluation, and supply chain mapping, mainly focusing on the cloud service provider identifying its weak providers that represent a risk and taking corresponding actions.

There are various models that base their results on different risk aspects, each with particular characteristics that specialize in evaluating specific areas, which provide advantages and disadvantages depending on the user's needs. In [5], a cloud computing implementation model is proposed to be used in an eGovernment with the purpose of improving flaws, problems in implementation, lack of control in data, security, privacy, etc. In the implementation methodology, it begins with defining the services that want to be migrated, classifying them according to their importance, cost, and mobility, and then determining the migration order using 2 factors, impact and resource availability, which are necessary to allow the continuity of the organization's operation. Thus, this model proposes 3 types of clouds according to their size and coverage area: local, regional, and wide.

III. ATTACKS AND RISKS TO CLOUD COMPUTING

Security is one of the main, if not the main, problems that makes business owners hesitant to migrate their systems to cloud computing, due to the uncertainty that exists with privacy and data protection [6].

Once the company or organization makes the decision to migrate all or some of its services (infrastructure, applications, or storage) to the cloud, the first step is to define the level of security we want to obtain from the service provider for the handling, processing, and storage of our information. Similarly, it is important to participate and collaborate in the procurement of information security that one owns, and thus be able to take preventive and corrective measures in the event of any eventuality that may arise.

Currently, there are security standards whose purpose is to identify and generate guidelines to fight against cyber threats that originate from information losses and, consequently, large economic losses. Some of these standards are: the Federal Risk and Authorization Management Program (FedRAMP), created by the US Government in 2011 to certify cloud service providers for Federal Agencies in that country, and the ISO/IEC 27001 standard, proposed by Joint Technical Committee 1, which is used globally [7].

Despite the general picture regarding cyber threats provided by security standards, there is a great variety of problems that arise in the management of information when it needs to be stored with a CSP. Various authors mention three important properties of data, Confidentiality, Integrity, and Availability (CIA), authentication and access control, as well as broken authentication, session, and access [1] [8] [9]. Similarly, other authors establish more general problems such as lack of data control, failures in the service provider's systems and data leakage [5], attacks by the service provider itself, and even by other tenants hosted in the cloud [7].

Due to the outsourcing of information, cloud servers and networks are often the target of malicious attacks. In addition, the service provider's cloud server itself could be malicious and attempt to insert false records into the database, modify existing records, or even delete them [10]. These problems arise when data is stored in a public cloud, in a multitenant mode, meaning when our contracted provider stores information from multiple clients, since this type of configuration is the most exposed to present problems, mainly of security and privacy, as well as problems with the physical and logical location where data is stored [8].

Other security problems that arise in the use of cloud computing, both for users and service providers, and that are classified according to the resource they affect (data, applications, infrastructure, and services in general), are Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks [11], data corruption, Application Programming Interfaces (APIs), and weak Service Level Agreements (SLAs) [12].

In the search for the most common security problems and attacks to which cloud computing is exposed, which can be an obstacle for companies to decide whether or not to use this technological tool, the ones shown in Table 1 were found.

IV. SOLUTIONS TO CLOUD-COMPUTING PROBLEMS

There are various methods, procedures, and tools that help increase the security of data entrusted to third-party cloud computing service providers, thereby preserving their confidentiality and privacy and reducing the inherent risks of using cloud computing.

As a first step in defining solutions to security problems, it is necessary for the owner of the information to fully commit and be involved in finding the necessary tools, procedures, and methodologies to ensure the security of their information.

Table 1. Types of security issues and attacks to cloud computing (Own source).

No.	Security issues and attacks.	Reference
1	Confidentiality, Availability and Integrity Authentication and access control Broken authentication, session and access Other Data Related Security Issues	8, 2, 7, 9, 15
2	Attacks by other tenants Attacks by CSP	7
3	DDoS attacks	11, 12
4	System failure Access Authorization Data Leak Data privacy and security Lack of data control	5
5	Accuracy preservation	10, 16
6	Malicious server Insertion of records Modification of records.	10
7	Data corruption Weak API´s and SLA	12
8	Employees Location of servers.	1, 8
9	Data remanence Third-Party control Legal Issues and Privacy	15

IV.I. CRYPTOGRAPHY

Cryptography methods are one of the most commonly used and effective tools to provide security to information wherever it is needed, including in cloud computing. Various studies have analyzed, compared, and tested the functionality of different encryption types to understand their characteristics, benefits, drawbacks, costs, etc., for use in cloud computing [2]. Despite any functional cryptographic method being effective, homomorphic encryption has become the most advantageous due to its better security performance compared to its drawbacks. However, full homomorphic encryption can be impractical due to its high amount of operations and resources consumed [14], which reflect in processing time and cost.

Homomorphic encryption works with encrypted data, eliminating the need for constant encryption and decryption. There are two types of homomorphic encryption: simple homomorphic encryption (SHE) and fully homomorphic encryption (FHE). SHE operates on one operator (addition or multiplication), while FHE can operate on both additions and multiplications and can perform multiple operations. There are various examples of these two types of homomorphic encryption, each with its merits, limitations, and comparisons with other encryption methods [13].

Based on the existence of various homomorphic encryption algorithms, schemes and protocols have been developed to cover the security characteristics required for information and data entrusted to third parties in the cloud. These schemes aim to improve the FHE algorithm for secure database storage in the cloud [15], propose a storage protocol employing both simple and full homomorphic encryption [16], and suggest using homomorphic encryption on the client-side before sending information to the cloud [17].

The need to find a complete solution in homomorphic encryption techniques is evident to ensure the secure handling, use, and storage of information in cloud computing and reduce associated security risks, which represent the primary problem for service providers and data owners.

IV.II. OTHER SOLUTIONS

When using an encryption algorithm, the encryption process must be performed before the information is sent to the CSP (Cloud Service Provider). This way, the owner is responsible for encrypting and sending the information, which does not compromise confidentiality [2].

In addition to the use of homomorphic encryption as a solution to reduce or mitigate security issues in cloud computing, various studies have focused on finding solutions to other types of problems that pose risks to privacy, confidentiality, integrity, etc. of information and that cannot be covered solely by an encryption algorithm.

Tools and procedures can be used together and complementarity as an integral solution to provide greater security to the information. The security framework proposed in [9] is an example of this, as it employs double encryption through a genetic algorithm, stores blocks of information in various locations, and uses lists of user capabilities with access to the information, providing confidentiality, authentication of each entity, data access control, and reduced calculation time. In [18], a security architecture called Security as a Service (SaaS) is proposed, which operates based on the stepped use of an Intrusion Detection System (IDS) and Remote Advanced Attack Detection (RAAD), providing benefits such as low cost, flexibility, easy monitoring, control, and data protection.

In addition to tools and methods that seek to provide a comprehensive security solution in the handling, storage, and processing of information, there are mechanisms that focus on eliminating or reducing other types of vulnerabilities that may arise in equipment or data stored in cloud computing. For this reason, the use of a proxy with user-side data protection should always be considered as an initial security measure, which allows for data division, anonymization, and encryption (with search capacity, encrypted data computation, access control, and control of storage of data stored in the cloud) [10].

A very common threat in the IT field is Denial of Service (DoS) attacks, particularly distributed attacks (DDoS) when they are carried out on components of cloud computing. These attacks have a significant impact on the availability and functioning of cloud computing, particularly on the equipment or system under attack [18]. In [11], a taxonomy is proposed for the prevention, detection, and mitigation of this type of attack, resulting in different solution designs that will be responsible for mitigating and/or reducing the impact of such attacks.

In many cases, when the owner's information needs and the characteristics of the data make it necessary to implement a hybrid configuration, this can manifest itself in two ways: firstly, by using the company's local infrastructure and rented third-party infrastructure simultaneously, or secondly, by using infrastructure rented from various service providers. This type of configuration becomes a solution to reduce the information security risk, as if one provider's services fail, the entirety of the information is not jeopardized.

Once a hybrid configuration is in place and after adopting the necessary solutions to provide security to the information, the way in which each of the services will be effectively controlled must be considered, taking into account that each cloud service provider has different characteristics. There are models that monitor and control various services installed in different clouds, considering specific protocols for each of them [19]. This way, end-to-end control of each of the contracted services can be achieved, regardless of whether they are with different service providers.

V. Proposal for cloud migration

Along with the numerous benefits provided by cloud computing, there is also a fear among some organization executives to make use of it. In order to present a more convincing and simple way to make the decision to migrate from local IT operations to the cloud, a framework is proposed that seeks to synthesize the steps to be followed for migration. This framework is divided into 3 phases:

Phase 1

Analysis of the organization's situation: In this step, the work to be done within the organization is established, starting with understanding the characteristics and benefits of the cloud, followed by an analysis of the internal situation of systems, applications, services, and infrastructure, in order to determine the systems that can be migrated, as well as the scope and impact of migration.

Phase 2

Cloud planning and implementation: The migration plan and strategy are developed, which contain a detailed analysis of cloud service providers, their costs, as well as the characteristics provided by each one, paying special attention to the security tools integrated into the proposed solution, the activities that must be carried out in detail, the people responsible for the project and each activity, as well as the roles, possible risks, and their mitigation plans, to later carry out the implementation until its conclusion, with respective functionality tests, training, and service delivery.

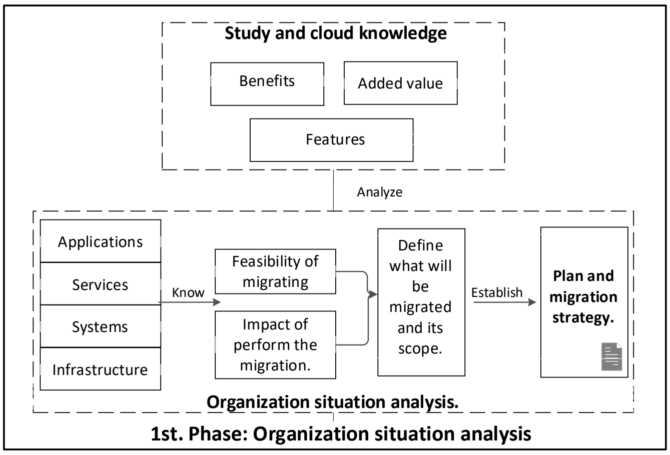
Study and cloud knowledge
Benefits
Added value
Features
Analyze
Applications
Services
Systems
Infrastructure
Know
Feasibility of migrating
Impact of perform the migration.
Define what will be migrated and its scope.
Establish
Plan and migration strategy.
Organization situation analysis.
1st. Phase: Organization situation analysis

Fig. 1 First Phase: Organization situation analysis (Own source).

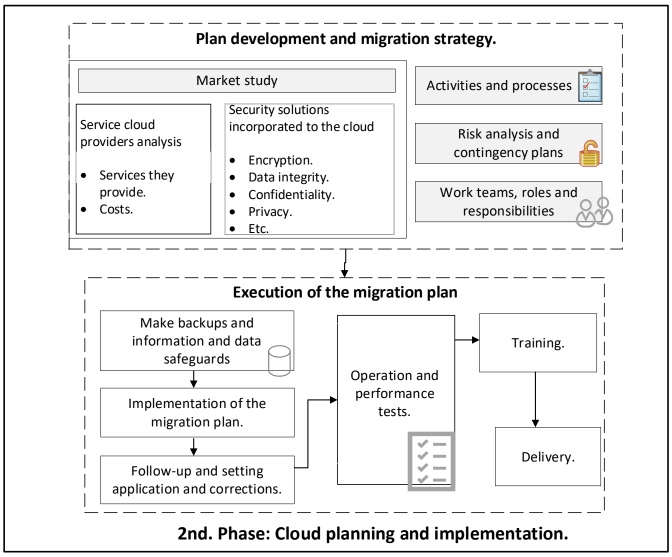
Plan development and migration strategy.
Market study
Service cloud providers analysis
Services they provide.
Costs.
Security solutions incorporated to the cloud
Encryption.
Data integrity.
Confidentiality.
Privacy.
Etc.
Activities and processes
Risk analysis and contingency plans
Work teams, roles and responsibilities
Execution of the migration plan
Make backups and information and data safeguards
Implementation of the migration plan.
Follow-up and setting application and corrections.
Operation and performance tests.
Training.
Delivery.
2nd. Phase: Cloud planning and implementation.

Fig. 2 Second Phase: Cloud planning and implementation (Own source).

Phase 3

Continuous monitoring and improvement: Once the implementation work is completed, it is necessary to monitor and evaluate the solution's performance in order to optimize processes and take advantage of the benefits provided by cloud computing. Therefore, it is proposed to establish a governance model where policies, processes, characteristics, and ways of proceeding in particular situations are defined. Once all of the above has been achieved, it is possible to fully exploit all the benefits of the cloud.

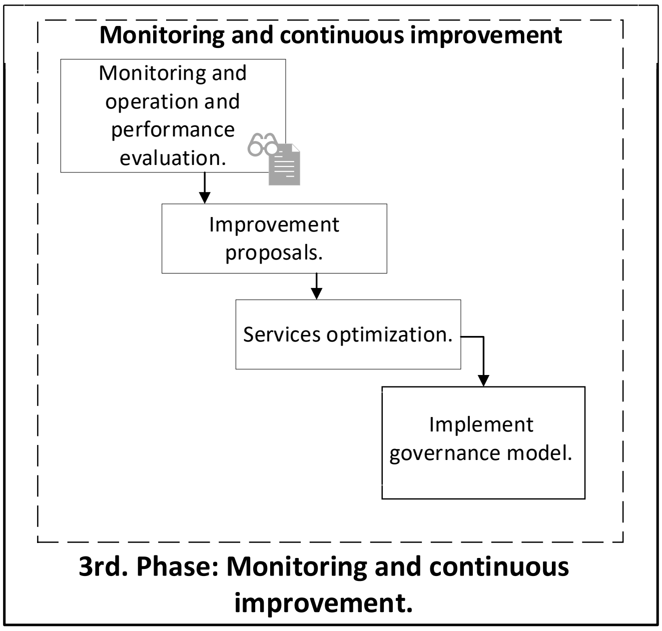
Monitoring and continuous improvement
Monitoring and operation and performance evaluation.
Improvement proposals.
Services optimization.
Implement governance model.
3rd. Phase: Monitoring and continuous improvement.

Fig. 3 Third Phase: Monitoring and continuous improvement (Own source).

VI. Conclusion

In conclusion, there are many risks and security issues that can undermine the advantages of using cloud computing to store, process, and handle data and information for an organization. However, in the same way, the existing tools and solutions were described that, individually or in combination, are capable of countering and/or mitigating the effect of such security problems, guaranteeing the confidentiality of information and allowing the processing and storage capacity provided by cloud computing to be utilized, which goes hand in hand with its economic profitability.

It is important to highlight that currently, the most commonly used tool to provide the majority of the security to the information and data stored in cloud computing is some type of cryptographic system, highlighting those cryptosystems that use homomorphic encryption, which, despite the complexity and amount of resources it consumes, provides the best security results.

References

[1] Kelf S. (2020). The security risks created by cloud migration and how to overcome them. Network Security (2020) 14-16.

[2] Mai R., Tamer A., Rasha I. (2019). Integrity and Confidentiality in Cloud Outsourced Data. Ain Shams Engineering Journal, 10, 275-285.

[3] Amron M.T., Ibrahim R., Bakar N.A.A., Chuprat S. (2019). Determining Factors Influencing the Acceptance of Cloud Computing Implementation. The Fifth Information Systems International Conference 2019, Procedia Computer Science 161 (2019) 1055-1063.

[4] Akinrolabu O., Nurse J.R.C., Marton A., New S. (2019). Cyber Risk Assessment in Cloud Provider Environments: Current Models and Future Needs. Computer & Security 87 (2019) 101600.

[5] Ali Kh. E., Mazen Sh. A., Hassanein E. E. (2018). A Proposed Hybrid Model for Adopting Cloud Computing in e-Government. Future Computing and Informatics Journal 3 (2018) 286-295.

[6] Subashini S., Kavitha V. (2011). A survey on security issues in service delivery models for cloud computing. Journal of Network and Computer Applications, 11, 1 – 11.

[7] Di Giulio C., Sprabery R., Kamhoua C., Kwiat K., Campbell R., Bashir M. (2017). Cloud Security Certifications: A Comparison to Improve Cloud Service Provider Security. ACM ICC ´17, March 22 2017, Cambridge, United Kingdom. ACM 978-1-4503-4774-7/17/03.

[8] *Kumar P.R., Raj P.H., Jelciana P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science 125 (2018) 691-697.*

[9] ShaluMall, Saroj S.K. (2018). A New Security Framework for Cloud Data. 8th International Conference on Advances in Computing and Communication (ICACC-2018), Procedia Computer Science 143 (2018) 765-775.

[10] Domingo.Ferrer J., Farràs O., Ribes-Gonzalez J., Sánchez D. (2019). Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Computer Communications 140-141 (2019) 38-60.

[11] Somani G., Singh Gaur M., Sanghi D., Conti M., Buyya R. (2017). DDoS Attacks in Cloud Computing: Issues, taxonomy, and future Directions. Computer Communications 107 (2017) 30-48.

[12] *Maniah, Abdurachman E., Lumban Gaol F., Soewito B. (2019). Survey on Threats and Risks in Cloud Computing Environment. Procedia Computer Science 161 (2019) 1325-1332.*

[13] Zhao E M., Geng Y. (2019). Homomorphic Encryption Technology for Cloud Computing. Procedia Computer Science 154 (2019) 73-83.

[14] Alaya B., Laouamer L., Msilini N. (2020). Homomorphic encryption system statement: Trends and Challenges. Computer Science Review 36 (2020) 100235 1-14.

[15] Potey M., Dhote C.A., Sharma D.H. (2016). Homomorphic Encryption for Security of Cloud Data. 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79 (2016) 175-181.

[16] Zhang J., Yang Y., Chen Y., Chen J., Zhang Q. (2017). A General Framework to Design Secure Cloud Storage Protocol Using Homomorphic Encryption Scheme. Computer Networks 129: 37 – 50.

[17] Souza S M P C., Puttini R S. (2016). Client-side encryption for privacy-sensitive applications on the Cloud. Procedia Computer Science 97 (2016) 126 – 130.

[18] Hawedi M., Talhi C., Boucheneb H. (2018). Security as a Service for Public Cloud Tenants (SaaS). Procedia Computer Science 130 (2018) 1025-1030.

[19] Copil G., Moldovan D., Truong H.L., Dustdar S. (2014). On Crontolling Cloud Services Elasticity In Heterogeneous Clouds. IEEE 7th International Conference on Utility and Cloud Computing.