Journal of Practical
Management Information Systems

J. Practical MIS, 2(6): 17-20, 2021

Research Paper

Security and Privacy in Cloud Computing

Z. Lashkaripour

Department of Computer, Faculty of Engineering, Velayat University, Iranshahr, Iran

Received: 20 October 2021 Revised: 21 November 2021 Accepted: 19 December 2021

Abstract

Various reasons such as maintaining security or even financial and technological resource limitations might be the objective of organizations or individuals to shift to the cloud computing environment. After that the main burden of preserving the security of the data and privacy of the consumer is on the service provider. Due to the variety of technologies used in a cloud environment a broad range of challenges exist that are threats for the security and privacy of the whole environment. For this reason, after presenting the features of a cloud computing environment we have introduced the security and privacy challenges and their possible solutions. Therefore, this paper could be a very good starting point since each side-consumer and provider-would be aware of their rights and responsibilities.

Keywords: Cloud computing, security, privacy, policy.

How to cite the article:

Z. Lashkaripour, Security and Privacy in Cloud Computing, J. Practical MIS, 2021; 2(6): 17-20,

Introduction

The name cloud computing was inspired by the cloud symbol that is usually used to illustrate the internet in diagrams [1]. Although migrating to the cloud can significantly reduce the infrastructure cost; but, it does raise the cost of data communication. Thereby a tradeoff between the requirements and expenditures is always essential especially when security requirements are the case. Furthermore, consumers need to ensure the quality, availability, reliability, and performance of the resources and this is provided through Service Level Agreements (SLAs) negotiated between them and the providers [2]. However, arranging the SLA would need a very close attention since everything is based on this agreement and all the rights and responsibilities are specified in it.

This paper contains the following sections. At first cloud computing and its basic characteristics are introduced, and then the challenges and remedies of security and privacy in a cloud computing environment as an essential requirement are given and finally, the results and conclusion are respectively given in the last sections.

Features of Cloud Computing

The definition of National Institute of Standards and Technology (NIST) for cloud computing is [3]: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". This definition indicates the specifications and advantages of using this novel information system.

The main service models used in cloud computing as shown in Figure 1 [4] are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). On the other hand, references like [2, 5] add Data storage as a Service (DaaS) to the mentioned models however, DaaS could be seen as a special type of IaaS therefore, we will consider the services as in Figure 1. This reference architecture is based on the work of the University of California, Los Angeles, and IBM [6].

According to this architecture the main service components—computation, storage, and communication—are explicit for the cloud software infrastructure (IaaS) and cloud software environment (PaaS) layers. In this model services of the top layers such as cloud Web application could be implemented and operated in the traditional way—that is, running on top of a standard Operating System (OS) without using dedicated cloud software infrastructure and environment components. Beside the original model, authors in [4] have added vertical spans based on the functions relevant to the services.

The three main parts of the architecture given in Figure 1 are:

- Supporting Information Technology (IT) infrastructure: This includes facilities and services common in IT systems. They are included due to the fact that any component of a cloud service even the non-cloud ones should be secured.
- Cloud-specific infrastructure: The heart of a cloud service lies in the components that form this part of the model. Therefore, cloud-specific vulnerabilities are related to these components.
- Cloud service consumer: The network that separates the consumer from the cloud infrastructure is made explicit; one of cloud computing's main characteristics is that usually an untrusted network provides access to cloud resources.

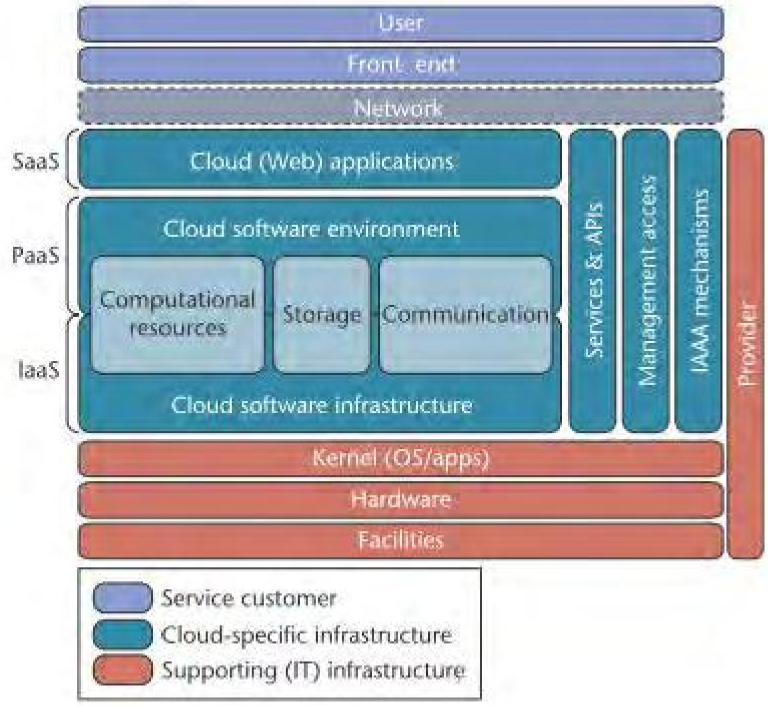

Fig 1: Cloud computing architecture

Security and Privacy Challenges and Possible Solutions

From the consumer's point of view preserving the security and privacy of confidential data might require splitting them up on different cloud computing environments. In this way the probability of losing the whole data in case of compromise is zero but, expenditure and time cost are intensively affected. Thereby a tradeoff between security requirements and expenditures is always essential. On the other hand, from the provider's point of view various challenges exist in a cloud environment which need careful consideration and that is due to the variety of technologies used.

The challenges mentioned in this section do also exist in non-cloud environments but regarding the characteristics of cloud, overcoming them could be more sophisticated (for more information refer to [7]).

A. Authentication

It is important to properly authenticate the consumers and grant them their license to access the demanded service and data if authenticated. Consumer authentication can be done by means of an IDentity Management (IDM) mechanism. An IDM should protect the sensitive information of the cloud parties while using different identity tokens and identity negotiation protocols could be an issue. In addition, the multi-tenancy characteristic of cloud would add more complexity and the provider should also be capable of protecting identity and authentication information of not only one consumer but a group of them simultaneously.

Recently user-centric IDM has received attention that will take away the complexity of IDM from the enterprises and allow them to focus on their own functions.

B. Access Control

Fine -grained access control policies are essential due to heterogeneity and diversity of services and also diversity of access requirements in different domains. Furthermore, generic access control interfaces are needed for interoperability between domains but it should be considered that the least privilege policy is of importance.

Role-Based Access Control (RBAC) is a simple and flexible model for managing dynamic requirements. But due to insufficient knowledge regarding the users, assigning them directly to roles is difficult for service providers. Thereby, using credential-or attribute-based models might enhance this capability.

C. Trust Management and Policy Integration

In a cloud environment services might be delivered by multiple providers with different security and privacy policies that integrating them without any suitable access control could lead to a security breach. Therefore, a trust framework is required to manage interaction and sharing between different service domains.

According to [7] "One possible approach is to develop a comprehensive trust-based policy integration framework that facilitates policy integration and evolution based on interdomain- and service-access requirements. Because service composition dynamics in the cloud can be complex, trust and access control frameworks should include delegation primitives. Efficient cryptographic mechanisms for trust delegation involve complex trust-chain verification and revocation issues, raising significant key management issues".

D. Secure-Service Management

It might be necessary to integrate services and provide a service that meets consumer's protection needs. In this condition, despite issues such as Quality of Service (QoS), cost and SLA, an automatic and systematic service provisioning and composition framework with respect to security and privacy issues is crucial.

The Open Services Gateway initiative (OSGi) service platform helps service providers, developers, software vendors, gateway operators, and equipment vendors to cooperatively develop, deploy, and manage services by means of an open and common architecture. This service platform could be a suitable choice for managing secure services.

E. Privacy and Data Protection

Consumers have to outsource their data to the cloud which has the potential risk of unauthorized access either by the provider or by other consumers. Therefore, cloud providers must assure the privacy of the consumer and transparency in the operations performed on the data.

To be able to control user rights and specify the allowed operations in the cloud, a standard-based heterogeneous data-centric security approach is an essential element. Furthermore, cryptographic approaches, usage policy rules that provide access to data only when the policies are satisfied, Virtual Local Area Networks (VLAN), and network middle boxes (e.g. firewalls, packet filters) [8] should also be considered.

Conclusions

Important organizations such as banks and hospitals or even individuals might be motivated to switch to a cloud environment. A variety of reasons such as limited resources, expenditure and security requirements could be the cause of this shift. Although a cloud system provides an on demand and elastic service on a pay-as-you-go manner but there are a number of issues that need close attention. One of the main issues in any system either automatic or bureaucratic is security and a cloud computing system is no exception. Hence, this paper is organized to indicate the security and privacy issues of a cloud environment. Authentication, access control and data protection are just part of the concerns of this innovative information system that after introducing these challenges we have given some possible solution. Due to the significance of data and protecting them against unauthorized access, as a future work we will perform a thorough investigation in this context.

References

[1] Zissis, D. and Lekkas, D., 2012. "Addressing cloud computing security issues". Future Generation computer systems, 28(3), pp.583-592.

[2] Dillon, T., Wu, C. and Chang, E., 2010, April. "Cloud computing: issues and challenges". In 2010 24th IEEE international conference on advanced information networking and applications pp. 27-33. Ieee.

[3] Mell, P. and Grance, T., 2011. "The NIST definition of cloud computing".

[4] Grobauer, B., Walloschek, T. and Stocker, E., 2011. "Understanding cloud computing vulnerabilities". IEEE Security & Privacy, 9(2), pp.50-57.

[5] Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J. and Fu, C., 2010. "Cloud computing: a perspective study. New Generation Computing", 28(2), pp.137-146.

[6] Youseff, L., Butrico, M. and Da Silva, D., 2008. "Toward a unified ontology of cloud computing". In 2008 Grid Computing Environments Workshop pp. 1-10. IEEE.

[7] James, BD., 2010. "Security and privacy challenges in cloud computing environments".

[8] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. "A view of cloud computing". Communications of the ACM, 53(4), pp.50-58.