Azerbaijan Journal of High Performance Computing, Vol 5, Issue 1, 2022, pp. 52-56
https://doi.org/10.32010/26166127.2022.5.1.52.56

Cloud Security: A Review of Current Issues and Proposed Solutions

Elviz Ismayilov

Azerbaijan State Oil and Industry University, Baku, Azerbaijan, elviz.ismailov@asoiu.edu.az

*Correspondence: Elviz Ismayilov, Azerbaijan State Oil and Industry University, Baku, Azerbaijan, elviz.ismailov@asoiu.edu.az

Abstract

Cloud technologies are currently one of the fastest growing directions in the IT field. This architecture uses virtualization technology in several computing paradigms (distributed systems, grid and service computing, etc.). It is possible to reach the goal using the unlimited possibilities of the Internet. It should be noted that most companies have transferred their resources and capabilities to cloud technology. According to Check Point Software Technologies Ltd 2020 statistics, 39% of enterprises said that security is important in cloud technology, and 52% said that public and hybrid cloud technologies have become more critical in the direction of security over the past two years. Enterprises are concerned about personal data storage and using special software enabled by cloud technologies. They are considering these points.

This paper also discusses the various benefits of the cloud with its challenges and applications.

Keyword: Cloud Technologies, Paas, Saas, Iaas, DraaS, Baas.

1. Introduction

Before considering particular security in cloud technology, it is essential to know its types and architectures and how enterprises integrate that technology into the business process. According to statistics, 66% of companies use cloud technologies; it should be noted that this number continues to grow faster every year. Here, 33% of users are more advanced, 33% are currently integrated into cloud technology, 7% are laggards, 13% are just followers, and 14% are beginners (Diaby, T., & Rad, B. B., 2017).

Cloud services are separated clearly by the type of services provided and the service deployment on different infrastructures (Subramanian, N., & Jeyaraj, A., 2018; Xu, X., 2012).

According to the type of services provided, cloud services can be divided into the following types:

- app as a service (SaaS): The software platform developer provides the client with remote access to it. For example, it is in the SaaS model that Microsoft provides customers with the use of MS Office Suite (Office Web Apps) along with SharePoint Server, Exchange Server, and other services and applications.

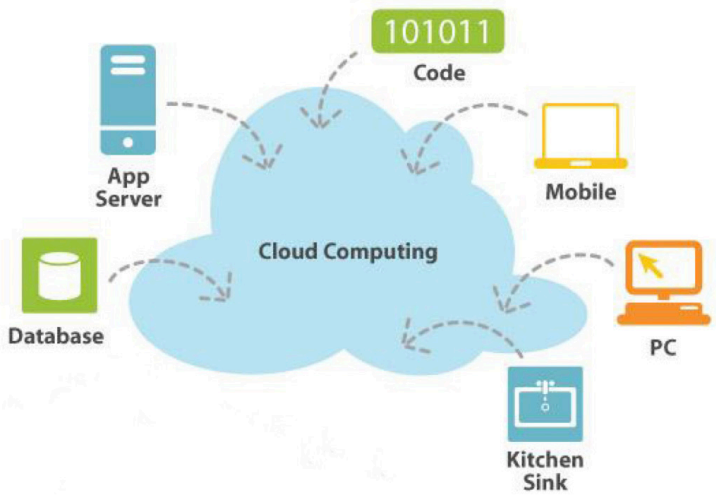

Fig. 1. Some services that can be integrated into the cloud

- platform as a service (PaaS): The cloud service provider provides the customer with a ready-made software environment and tools for setting it up. PaaS elements are hardware, operating system, DBMS, middleware, testing, and development tools. The client can customize such a platform to suit his needs, making it a platform for software testing or, for example, a system for automating a control system. This type of service is especially popular with software developers.

- Infrastructure as a service (IaaS): IaaS providers provide customers with computing infrastructure (servers, data storage, operating systems, and network resources) for deploying and running their own software solutions. The option is suitable for companies whose need for resources is not the same at different points in time - there are surges in demand, but they gradually subside (or the organization is growing rapidly, and the problem of constantly scaling the infrastructure arises). Also, IaaS will be the best solution when a company does not have enough funds to create its infrastructure.

Disaster Recovery as a Service (DraaS): An option to provide disaster recovery solutions with the help of a provider's cloud. When client services fail, they are restarted within a few minutes but are already in the cloud. Data from the client's leading site is replicated to the cloud solution provider's site. Such solutions are of particular interest to companies with a large number of business-critical applications.

Backup as a service (BaaS): Following decoding the abbreviation, we are talking about backing up customer data to the provider's cloud. The provider provides a place to store information and tools for fast and reliable copying.

Cloud technology follows according to its type (Kaur, R., 2015; Jadeja, Y., & Modi, K., 2012, March).

A single company owns a private cloud. This company is responsible for all aspects of cloud security: the organization's sole responsibility is the cloud infrastructure, availability, and information security incidents.

Public cloud (Community cloud) infrastructure is intended for a specific community of organizations with common problems and tasks. The cloud infrastructure's owners ensure security, availability, and responsibility for data safety. One or more organizations in a given society may own the cloud infrastructure.

A public cloud is an infrastructure available for unrestricted use, and the service provider is responsible for security and availability.

A hybrid cloud is an infrastructure composed of the cloud services described above. The components of such a combination of cloud services are independent platforms.

2. Paradigma of Security

In cloud technology, privacy must be protected throughout the chain, including the provider of the "cloud" solution, the consumer, and the communications connecting them.

It is the responsibility of the cloud technology service provider to ensure both physical and software integrity of data from third-party intrusions. It is no coincidence that "cloud" data centers are usually designed based on the most modern security standards (including encryption issues, as well as the anti-virus, as mentioned earlier, protection, and protection against hacker attacks) (Khalil, I. M., Khreishah, A., & Azeem, M., 2014).

The consumer must implement appropriate policies and procedures "in its territory" to prevent the transfer of access to third parties. In this sense, the objective advantages of "clouds" should not be confused with saving the client from any attempt to ensure the security of his information perimeter.

Solving security problems includes traditional and well-known solutions. It consists of several unique solutions that must be optimized to maintain the virtual environment's performance by adding security in executing standard tasks (Shaikh, F. B., & Haider, S., 2011, December).

In the global "cloud" computing experience, there are cases where the consumer cannot access programs for a long time. Serious failures are already occurring in equipment operation, even in large providers of "cloud" services. An unusual "Internet shutdown" due to the fault of the provider (not necessarily the provider providing direct service to the customer, but the trunk operator may be to blame) can make it impossible to work with "cloud" resources in principle (Ryan, M. D., 2013).

It is clear that before starting projects related to the transfer of specific IT services to the "cloud," customers should assess such risks, conduct a comprehensive inventory of applications (determine the list of business-critical ones), and only then make decisions on how to proceed (Indu, I., Anand, P. R., & Bhaskar, V., 2018; Mohit, P., & Biswas, G. P., 2017; Khan, S. I., & Hoque, A. S. L., 2016, January).

After researching the security of cloud types, the most common risks are data leaks, insufficient management of access, user accounts and authorization, insecure use of ports and APIs, exploits and vulnerabilities of the software used, account hacking, insiders attackers, irretrievable data loss, insufficient provider due diligence, use of cloud services for criminal purposes, DoS and DDoS problems and Risks of using shared resources.

Conclusion

The issues listed above are very important. Considering that all companies provide software, services, etc., since it is moved to the cloud, its security is the most important issue. If a mistake is made here in any section, companies will not only lose data but also suffer material damage

Securing cloud services is one of the industry's top priorities. Security issues in cloud services are relevant because more and more users and organizations store essential data, run business processes in the cloud, and transfer or connect business processes with cloud technologies.

Most of the information security problems of cloud services can be solved by applying for cryptographic protection (Kamara, S., & Lauter, K., 2010) and by competent administrative measures by the supplier and service provider. These measures should take into account the individual requirements of the client. It is also essential to implement international standards for the security of cloud services and to monitor how customers and service providers implement these standards.

A complete description and accounting of creating a secure REST API for microservices deployed in the cloud can be distinguished from software tools and methods.

The threat of insider information leakage - the most severe threat, if not prevented, can be solved if the client's cloud services or the provider itself ensures the registration of all user actions in the system.

Reference

Diaby, T., & Rad, B. B. (2017). Cloud computing: a review of the concepts and deployment models. *International Journal of Information Technology and Computer Science, 9*(6), 50-58.

Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal, 21*(4), 574-588.

Jadeja, Y., & Modi, K. (2012, March). Cloud computing-concepts, architecture and challenges. In *2012 international conference on computing, electronics and electrical technologies (ICCEET)* (pp. 877-880). IEEE.

Kamara, S., & Lauter, K. (2010). Cryptographic Cloud Storage, Microsoft Research.

Kaur, R. (2015). A review of computing technologies: distributed, utility, cluster,

grid and cloud computing. *International Journal of Advanced Research in Computer Science and Software Engineering, 5*(2), 144-148.

Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers, 3*(1), 1-35.

Khan, S. I., & Hoque, A. S. L. (2016, January). Privacy and security problems of national health data warehouse: a convenient solution for developing countries. In *2016 International Conference on Networking Systems and Security (NSysS)* (pp. 1-6). IEEE.

Mohit, P., & Biswas, G. P. (2017). Confidentiality and storage of data in cloud environment. In *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications* (pp. 289-295). Springer, Singapore.

Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software, 86*(9), 2263-2268.

Shaikh, F. B., & Haider, S. (2011, December). Security threats in cloud computing. In *2011 International conference for Internet technology and secured transactions* (pp. 214-219). IEEE.

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering, 71,* 28-42.

Xu, X. (2012). From cloud computing to cloud manufacturing. *Robotics and computer-integrated manufacturing, 28*(1), 75-86.

Submitted: 28.12.2021
Accepted: 17.05.2022