CHALLENGES OF IT INFRASTRUCTURE MANAGEMENT ON CLOUD COMPUTING

Marius-Ioan TODERICI[1], Aurel Mihail ȚÎȚU[2,3], Camelia Cristina DRAGOMIR-PÂNZARU[4,2], Maria POPA[5]

Abstract: *As more and more organizations move from on-premises infrastructure to cloud infrastructure the complexity is growing. Managing the hybrid infrastructure has become challenging for many organizations technically, economically and humanly. There are several challenges that organizations moving from on-premises to cloud infrastructure need to address such as: security, internet connectivity, regulatory compliance, performance, integration of software solutions, cost management, technical staff. The organization needs to define very well what data it uploads to the cloud and what policies it adopts in case it is unavailable for a period of time or what methods it uses for data recovery. Organizations need to make an analysis of their current and long-term storage capacity needs in order to take advantage of the benefits of the cloud, in particular the possibility of dynamic allocation of processing resources. These can be allocated when needed and withdrawn when no longer needed to reduce costs.*

Keywords: *Cloud computing management, IT infrastructure management, cloud computing management.*

JEL Classification: *L92, O10, R40*

[1] National University of Science and Technology Politehnica Bucharest, marius@toderici.ro
[2] Lucian Blaga University of Sibiu, Faculty of Engineering, mihail.titu@ulbsibiu.ro
[3] Academy of Romanian Scientists, 3 Ilfov Street, 050044
[4] Transilvania University of Braşov, camelia.dragomir@unitbv.ro
[5] University of Alba Iulia, mpopa@uab.ro

1. Introduction

Due to technological advancement, the IT domain has become indispensable for organizations, IT infrastructure is the core engine of any modern management enterprise organization. Modern network infrastructure is one of the basic pillars of information technology. Modern telecommunications involve the fast and accurate transmission of large volumes of data. With the transition from telecommunications using analog signals to digital transmissions, telecommunications has moved to a new level with an exponential increase in usage. Today digital information is transmitted using different propagation media, we have copper network (utp/ftp cable network or telephony), fiber optics, radio networks, GSM networks, 5G networks, satellite communications or we even use power grids on which we modulate the digital signal.

The diversity of data transmitted through communications media has contributed to the development of today's modern communications. So today we have in an organization several types of networks, we have business networks, industrial networks, networks that manage confidential information, all of them being interconnected, exchanging data according to clear, precise rules at well determined time intervals have changed the way organizations use information. Access to information from anywhere is a reality of today's personal and professional life, the lack of access to the organization's data by users or the impossibility of quick access translates into decisions with negative consequences for the organization. The complexity of the IT infrastructure of enterprise organizations is very high, the staff of these organizations is large in the level of thousands, tens or hundreds of thousands of employees who have access to the organization's data and services through various IT equipment fixed and mobile workstations, phones, tablets or different "gadgets" such as smart watches or bracelets.

As more and more cultured organizations move from on-premises infrastructure to Cloud infrastructure the complexity is growing. Hybrid infrastructure management (Figure 1) has become challenging for many organizations both technically, economically and humanly. There are

several challenges that organizations moving from on-premises infrastructure to cloud infrastructure have to solve such as: security, internet connectivity, regulatory compliance, performance, integration of software solutions, cost management, technical staff.

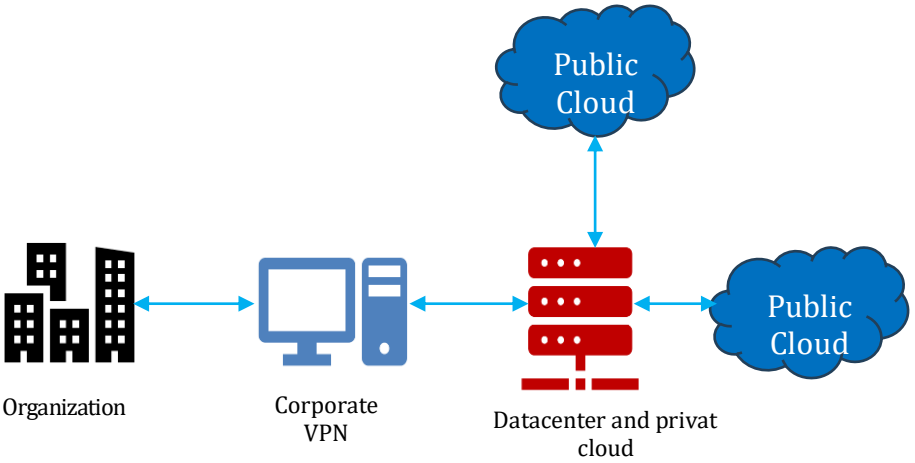

Figure 1. *Hybrid Cloud*

2. Security and data protection

Security is one of the main challenges of moving from on-premises infrastructure to the cloud. Moving to cloud or hybrid cloud infrastructure greatly increases the attack surface. Security teams must ensure constant monitoring of cloud environments to ensure their protection. This requires tools that ensure constant monitoring of hardware resources and alerting systems or solutions that ensure automatic and prompt intervention in the event of threat detection. The use of firewall protection equipment protects the organization against unauthorized access, it is also important to use antivirus solutions on workstations to ensure security.

Security risks are also reduced by updating all security equipment based on recent vulnerability patches known to the equipment vendors. Another necessary and mandatory measure is the use of communications that use encrypted end-to-end protocols so that data is secure both in transit and at

the end. In addition to the use of encrypted communication protocols, it is necessary to use a multi-factor authentication method such as MFA (Figure 2). The use of multi-factor authentication (MFA) or two-factor authentication (2FA) provides added security for organizations and user accounts because this method requires in addition to a password something that only the user has: a smart card, token or fingerprint. By using two components of different categories on the authentication side, security is ensured. This minimizes the risk of password theft and compromise of the user's accounts and therefore the organization's

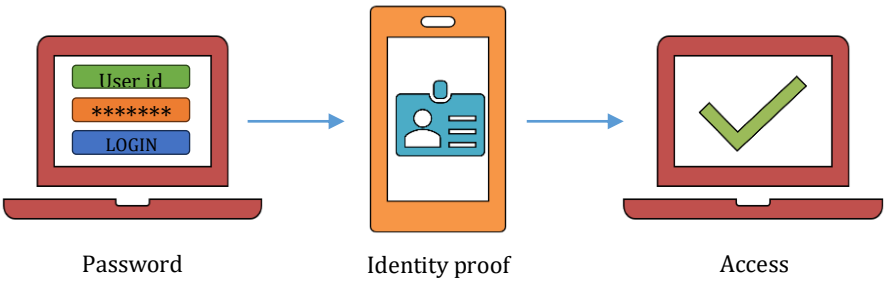

Figure 2. *Multi-factor authentication (MFA)*

Organizations that use only complex password policies for authentication are at risk of password theft because it is known that users generally use the same password for different accounts or sites out of convenience and because it is easier to remember. A password once stolen can create big security breaches and big losses for organizations.

From an IT management point of view, there is a need to create policies to regularly manage security updates for equipment. A proactive approach greatly reduces the risk of security breaches or data loss, so it is mandatory to install regularly scheduled firmware updates as well as to update the operating systems on the equipment, whether servers, firewall equipment or antivirus solutions.

Regular security audits and risk assessments are also mandatory. Auditing security systems on a regular basis allows you to quickly identify

vulnerabilities and weaknesses in your organization's Cloud infrastructure. Risk assessment is another necessary step to be taken by IT teams to evaluate potential threats and their impact on the infrastructure and the organization. Another management action that can be taken is to promote security awareness measures in the organization. Through these threat awareness measures, a culture of the importance of ensuring security is promoted as well as the responsibility for the necessary security measures such as using strong passwords, changing passwords at intervals, etc.

A mandatory security measure is the provision of a user identity management solution within the organization. Identity management is a framework of processes, policies and technologies that facilitate electronic or digital identity management. Using IAM technologies, IT administrators can control user access to essential data and information in their organization. Modern IAM (figure 3) systems include the option of single sign-on, two-factor authentication and multi-factor authentication and even privileged account management. These systems offer the possibility to store user identity and profile data securely and ensure that only necessary data is shared.

Figure 3. *IAM service components*

"The Identity Management System is responsible for managing user accounts and how users access the organization's systems. The main purpose of identity management systems is to ensure the user's identity and to secure the user's identity on the network and in the organization's systems. Any user who wishes to log on to a particular website or email has to provide an identifier (e.g. email address) and authentication and authorization data after which he/she has access to the system and the data." (M. A. Thakur, 2015)

Digital identities are not just for human users; IAMs also manage the digital identities of devices, applications and services to govern access to digital resources or to run other services and applications on on-premises or cloud infrastructure.

3. Capacity management, scalability and management of data compliance

One of the big challenges of cloud systems for organisations is capacity management. Data is the most precious asset of organisations, nowadays data is quickly collected from across different services like SCADA, IoT, accounting data, emails, logs which are then stored for different further processing, analytical reporting, analytics etc.. Most of the time we need more powerful systems to analyze large capacities of data that is stored for long periods of time, which often leads to the need for larger and faster storage systems to meet the requirements. Storing and processing large amounts of data in the cloud is very expensive both in terms of storage and machine cost. Another important issue that comes with storing and processing large amounts of data in the cloud is bandwidth management and internet connectivity. Keeping data in the cloud involves uploading it to the cloud over an internet connection which needs to be managed so that it does not cause disruption to the organization's IT services.

For these reasons it is very important for organisations to be aware of the costs associated with storing, processing and traffic of this data and

the choice of which data to store in the cloud should be made after a rigorous business analysis of current and future needs. As part of this analysis, patterns of data to be stored and processed, trends and growth moments need to be identified so that the purchase of storage services and computing resource requirements are optimized. In this case the ability to dynamically allocate processing resources and withdraw them when not needed is very useful. Dynamic management of these resources can bring serious cost savings with cloud service expenses. The scalability and processing power of cloud systems is very good but resource management is the prerogative of the IT team so optimizing the data that is stored in the cloud as well as managing the computing resources is very important and necessary to ensure service efficiency and performance. Otherwise the high costs of storing data in the cloud can quickly become a factor that unbalances organizations' budgets.

Another issue to be managed by organisations is regulatory compliance and regulatory requirements. Depending on the business domain or industry not all data can be uploaded to the cloud or depending on legislative requirements some data can only be uploaded to regional cloud systems (Europe or America) so these compliance policies need to be well analyzed and created by organisations. These policies also need to be exposed to cloud service providers to ensure that they are also compliant as most of the time cloud service providers back up data from a site (location) to other locations out of a desire to provide secure backups for customers and may be unknowingly breaking the law. All major cloud service providers offer tools to control and manage data in cloud systems.

4. Management of Internet connectivity

With the shift from on-premises infrastructure to the use of cloud services, the impact on internet connections is very high, especially if applications are used that need high bandwidth for data transfer or low latency for fast data processing. In all cases the move to cloud services requires high-speed internet connections. If we add to these one of the

above security requirements, secure communications it is very important to ensure the capacity of the equipment that provides end to end communications between the organization's systems and the cloud, this means ensuring the capacity of the equipment that is on-premises as well as the acquisition of secure cloud communications services. Analyzing the data traffic and the data that is transmitted to the cloud, processed and used is very important to ensure the capacity of the communication systems as well as to prevent outages.

Without careful analysis of the data travelling to and from cloud systems, the exponential increase in data traffic that needs to be handled by the equipment can easily result. For these reasons and for redundancy reasons it is essential to segregate data and services and provide multiple broadband communication paths. It is ideal to use a communication path for email separate from web browsing or the communication path used for various business services. At the same time, an analysis needs to be done on applications and services that need low latency and fast response as for these services a different path needs to be found for integration into local or edge systems.

In all cases, to ensure communication redundancy, all systems must be redundant and ideally, communication service providers should also be redundant for organisations that cannot have interruptions in the use of cloud systems.

5. Systems integration and migration

Moving from on-premises IT infrastructure to the cloud often means migrating applications and services from on-premises infrastructure to the cloud. This creates challenges on the migration and assurance side of cloud systems. An organization's systems are interconnected, they exchange data and interoperability can be an issue and migrating systems without losing data or disrupting communications is a significant challenge for any organization. To prevent these problems, it is very important to use communication standards between applications and services and to

eliminate customization. The adoption of standard communication protocols and APIs enables rapid migration of systems as all cloud service providers provide standard APIs and communication protocols. The migration and testing of systems should be done gradually so that in the testing phase all integration issues of the solutions are resolved so that there are no compatibility issues or disruptions.

6. Lack of expertise and skills

By migrating systems to the cloud, it may seem at first that not as many IT staff are needed, which is often presented by cloud providers themselves as one of the benefits of cloud migration, as a reduction in IT staff costs. In reality, organisations often quickly find out that IT staff does not need to be reduced but needs to be trained to maintain and operate the cloud systems and services that are interconnected with on-premises equipment and services and keep the organization's services running smoothly. This means that there is a need to train and upskill existing IT staff and provide tools/applications with which they can manage the organization's systems both in the cloud and on-premises. However, by migrating systems to the cloud various maintenance services can be outsourced which can lead to reductions in in-house IT staff.

7. Conclusions

Moving from on-premises IT infrastructure management to the cloud is a challenge for organisations, data and applications need to be migrated to the cloud, with access to data and applications dependent on internet connectivity and its management.

The organization needs to define very well what data it uploads to the cloud and what policies it adopts in case it is unavailable for a period of time or what methods it uses to recover data.

Organisations need to make an analysis of their current and long-term storage capacity needs in order to take advantage of the benefits of the

cloud, in particular the possibility of dynamic allocation of processing resources.

These can be allocated when needed and withdrawn when they are no longer utilized to reduce costs. It is very useful to constantly monitor the computing resources in use because in the cloud any allocated resource (test or development environments), even if unused, generates costs that can quickly escalate.

Another very important aspect is ensuring data security and legal compliance; organisations need to define their procedures and work scenarios in order to be as resilient as possible.

Ensuring redundant high-speed communications paths is another important aspect of successful migration of services to the cloud being just as important as training the IT staff who need to manage the organization's IT systems.

References

1. Ranjan, F. G. (2021). Convergence of Edge Services & Edge Infrastructure. IEEE Conference on Network Function Virtualization and Software Defined Networks (pg. 96-99). Heraklion: IEEE.
2. Santoyo-González, C. C.-P. (2020). Network-Aware Placement Optimization for Edge Computing Infrastructure Under 5G. IEEE Access, vol. 8, 56015-56028.
3. Anjos, J. C. (2020). Data Processing Model to Perform Big Data Analytics in Hybrid Infrastructures. IEEE Access, vol. 8, 170281-170294.
4. Aradi, S. (2022). Survey of Deep Reinforcement Learning for Motion Planning of Autonomous Vehicles. IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 2, 740-759.
5. Bhowmik, S. (2017). Cloud Computing. Cambridge: Cambridge University Press.

6. Ke, Z. H. (2017). Privacy Disclosure Checking Method Applied on Collaboration Interactions Among SaaS Services. IEEE Access, vol. 5, 15080-15092.
7. Pöhn, W. H. (2022). Reference Service Model Framework for Identity Management. Reference Service Model Framework for Identity Management, IEEE Access, vol. 10, 120984-121009.
8. Das, R. (2024). The Zero Trust Framework and Privileged Access Management (PAM). CRC Press.
9. Benkhelifa, A. B. (2019). Virtual Environments Testing as a Cloud Service: A Methodology for Protecting and Securing Virtual Infrastructures. IEEE Access, vol. 7, 108660-108676.
10. Ghazizadeh, M. Z.-l. (2012). A survey on security issues of federated identity in the cloud computing. 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings (pg. 532-565). Taipei, Taiwan: IEEE.
11. Fanti, M. (2023). Implementing Multifactor Authentication: Protect Your Applications from Cyberattacks with the Help of MFA. United Kingdom: Packt Publishing.
12. H. J. Syed, A. G. (2018). CloudProcMon: A Non-Intrusive Cloud Monitoring Framework. IEEE Access, vol. 6, 44591-44606.
13. J. Carretero, G. I.-M.-C.-B. (2018). Federated Identity Architecture of the European eID System. IEEE Access, vol. 6, 75302-75326.
14. J. Gedeon, F. B. (2019). What the Fog? Edge Computing Revisited: Promises, Applications and Future Challenges. IEEE Access, vol. 7, 152847-152878.
15. M. A. Thakur, R. G. (2015). User identity & lifecycle management using LDAP directory server on distributed network. International Conference on Pervasive Computing (ICPC) (pp. 1-3). Pune: India.
16. M. A. Thakur, R. G. (2015). User identity and Access Management trends in IT infrastructure- an overview. International Conference on Pervasive Computing (ICPC) (pg. 1-4). Pune, India: IEEE.

17. M. Alrashoud, L. A. (2014). Binary linear programming-based release planning for multi-tenant business SaaS. Conference on Computer Science & Software Engineering, (pg. 1-8).

18. M. I. Sarwar, Q. A. (2023). Digital Transformation of Public Sector Governance With IT Service Management–A Pilot Study. IEEE Access, vol. 11, 6490-6512.

19. Matko, V., Brezovec, B., & Milanovic, M. (2019). Intelligent Monitoring of Data Center Physical Infrastructure. Applied Sciences 9(23):4998.

20. Matt, S. (2015). Migrating to Cloud-Native. O'Reilly Media.

21. Oracle, C. (2023). Oracle IaaS, Infrastructura ca serviciu. Preluat de pe oracle.com: https://www.oracle.com/ro/cloud/what-is-iaas/

22. R. T. Moreno, J. G.-R. (2021). A Trusted Approach for Decentralised and Privacy-Preserving Identity Management. IEEE Access, vol. 9, 105788-105804.

23. Y. Gao, S. Z. (2019). A Hybrid Algorithm for Multi-Objective Scientific Workflow Scheduling in IaaS Cloud. IEEE Access, vol. 7, 125783-125795.

24. Z. Li, Y. Z. (2017). Towards a full-stack devops environment (platform-as-a-service) for cloud-hosted applications. Tsinghua Science and Technology, vol. 22, 1-9.