Manufacturing Science and Education 2025

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineerin
Vol. 68, Issue Special III, August, 2025

HYBRID CLOUD IT INFRASTRUCTURE MAINTENANCE USING ARTIFICIAL INTELLIGENCE

Marius Ioan TODERICI, Aurel Mihail TITU, Nicoleta Madalina STAN

Abstract*: IT infrastructure maintenance must be carried out in such a way as to have the least possible impact on the processes in the organization. Any infrastructure needs maintenance to update systems, apply security patches or simply to perform scheduled or unscheduled maintenance operations in the event of interventions necessary to ensure the proper functioning of the equipment. Hybrid cloud IT infrastructure has a great advantage in that it is mostly a redundant infrastructure that allows maintenance processes to be carried out with the least possible impact on the processes in the organization. By using virtualization and distributed systems in most situations, it is not necessary to completely stop the systems under maintenance, this is most often done hot with the systems in production, totally transparent to users. Redundant storage systems, redundant network and security infrastructure, systems that use redundant virtual machines allow maintenance to be carried out by allowing the other systems or equipment with the same role in the system to take over the functions of the equipment/system under maintenance. From this point of view, the maintenance of these systems can be automated and optimized so that it is carried out during less busy periods of time to have minimal impact on the organization's business processes.*

Keywords: *Infrastructure maintenance, hybrid cloud, management processes, artificial intelligence, hardware, backup*

1. INTRODUCTION

IT infrastructure maintenance should be done in a way that has the least impact on the processes in the organization. Any infrastructure needs maintenance to update systems, apply security patches or simply to perform scheduled or unscheduled maintenance operations in case of interventions necessary to ensure the proper functioning of equipment.

Hybrid cloud IT infrastructure has a great advantage in that it is mostly a redundant infrastructure that allows maintenance processes to be carried out with minimal impact on the organization's processes. By using virtualization and distributed systems, in most situations it is not necessary to completely shut down systems under maintenance, as this is often done hot with systems in production, completely transparent for users. Redundant storage systems, redundant network and security infrastructure, and systems using redundant virtual machines allow maintenance to be performed by allowing other systems or equipment with the same role in the system to take over the functions of the equipment/system under maintenance.

From this point of view, the maintenance of these systems can be automated and optimized so that it can be performed in less busy periods of time in order to have minimal impact on the organization's business processes.

2. PREVENTIVE AND PROACTIVE MAINTENANCE OF HYBRID CLOUD IT INFRASTRUCTURE

Hybrid cloud infrastructure management must contain a framework of policies and processes to ensure effective control of the hardware resources and services hosted in the hybrid infrastructure.

Proactive and predictive infrastructure maintenance includes several processes:

- ensuring backup processes for virtual machines;

- cloning virtual machines;
- upgrading operating systems and application maintenance;
- log monitoring and log archiving;
- maintenance of hardware servers, storage systems, etc.;
- network infrastructure and security equipment maintenance.

IT infrastructure maintenance should be carefully scheduled and executed to minimize disruption to organizational operations. To streamline administrative tasks and reduce the likelihood of errors, these maintenance processes should be proceduralized and, where possible, automated. By incorporating artificial intelligence into the system, tasks such as testing and verifying data integrity can be autonomously handled, ensuring that systems remain secure and efficient with minimal manual oversight. This approach not only enhances operational efficiency but also allows IT teams to focus on more strategic tasks, improving overall productivity and system reliability.

2.1 Backup processes for virtual machines

The process of creating backups is one of the core processes of systems maintenance and one of the core processes that ensures continuity in the event of a disaster or problems such as data loss or corruption. Backup processes should be scheduled with a granularity that allows data to be restored as quickly as possible if needed. Retention of backups should be done in such a way as to allow data to be restored and recovered when needed. The granularity of backup and retention shall be determined by internal procedures for each individual system.

Modern virtualization systems have several facilities through which different backup processes can be provided, and these concepts are essential for securing the organization's data and creating backup procedures (Fig. 1.):

- Differential backup - Only files that have changed since the last full backup are backed up;
- File-level backup - Backup that is defined at the file and directory level;
- Full backup - A backup of all files;
- Full Virtual Machine Backup - Creates a backup of all the files that make up an entire virtual machine, including disk images, configuration files and more;
- Image-level backup - Creates a backup of the entire storage volume;
- Incremental (Snapshot)- Backs up only the files that have changed since the last backup, either full or incremental.

Depending on the specifics of each application or IT service the backup procedure will be determined. If the application or IT service is not based on databases but uses a more file-based system, the virtual machine-based system can be used as a process and such a procedure can be realized as follows:

- Daily - differential or incremental backup (the machine will be unavailable for a very short time of the order of seconds);
- Weekly - full backup of the virtual machine (the machine must be shut down);
- Monthly or Quarterly - Image level backup (the whole system will be unavailable).

If the IT application or service includes databases then a backup procedure will be approached that relies on an agent that is installed on the virtual machine:

- Daily - the agent creates backups in a manner similar to file-level incremental backup, this method is indicated to ensure the consistency of database information (virtual machine is available);
- Weekly - full backup of the virtual machine (the virtual machine must be powered off);
- Monthly or quarterly - Image-level backup (the entire system will be unavailable).

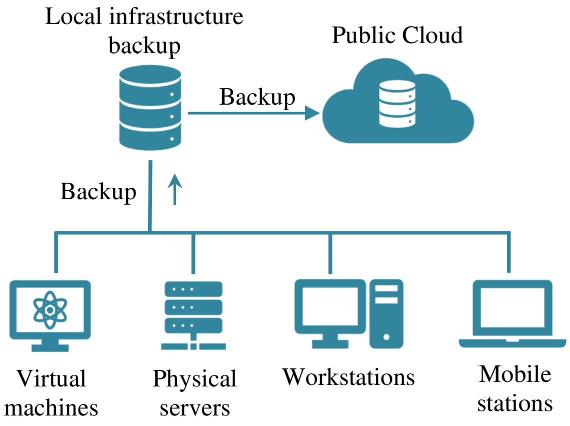

Fig. 2. Backup model in hybrid cloud infrastructure

(source nakivo.com)

For each backup, a retention period will be set for daily backups of at least 7 days and for weekly backups of at least 30 days. Within the backup procedures an important section must be dedicated to testing the backup copies. These should be restored on test media to ensure data quality and integrity. Testing backup copies is a mandatory process in backup procedures and are good exercises for restoring data when necessary.

Backup procedures can be easily automated based on scripts and run automatically by machines or by artificial intelligence-based systems that can also test the backup copies created simplifying the work of IT staff.

2.2 Cloning virtual machines

Cloning virtual machines is a process by which development environments or test environments from production environments are generally realized. By cloning a virtual machine, we basically back up one virtual machine at a time and start it in another environment. We can make two types of clones depending on the source we start from. If the source is a virtual machine or a full backup then the clone is a standalone to which we only need to change a few features to access it. The machine can't be started/accessed in the same environment unless you change a few characteristics such as IP and name. Another way of cloning is to create a clone from an incremental copy, and then you have a linking clone that is dependent on the original machine.

The cloning system is widely used in development and testing environments. Public cloud systems have automated this process by being able to schedule clones and the environments in which they will be hosted. This enables clone management, optimizes costs because they will be started when needed for as long as needed. Virtual machines must be carefully managed in the cloud because each resource started in the public cloud is charged even if not used and in the private cloud each virtual machine consumes resources from the physical computing system.

2.3 Updating operating systems and maintaining applications

Updating operating systems on virtual machines, updating applications, databases or components used within the IT systems in the organization are mandatory maintenance operations that install the latest versions of applications or operating systems on the machines used within the organization.

The update of these systems or applications is done periodically as part of the planned maintenance of systems, applications or components or when manufacturers release different security patches as part of unplanned maintenance.

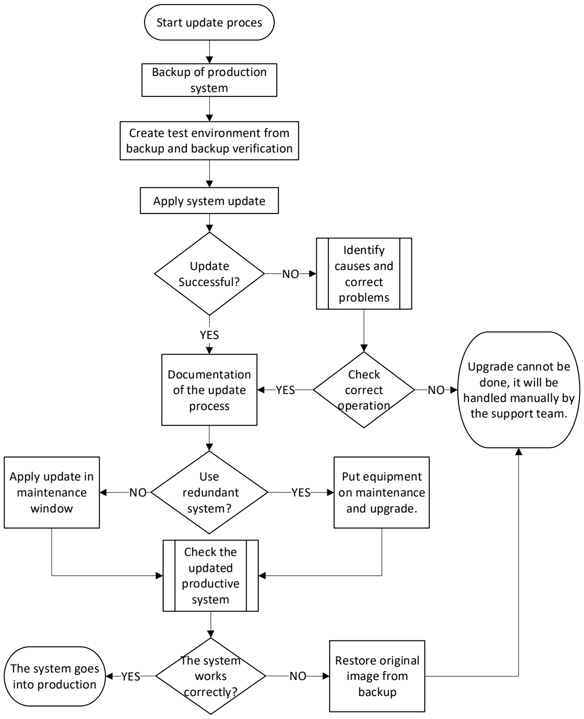
Start update proces
Backup of production system
Create test environment from backup and backup verification
Apply system update
Update Successful?
NO
Identify causes and correct problems
YES
Documentation of the update process
YES
Check correct operation
NO
Upgrade cannot be done, it will be handled manually by the support team.
Apply update in maintenance window
NO
Use redundant system?
YES
Put equipment on maintenance and upgrade.
Check the updated productive system
The system goes into production
YES
The system works correctly?
NO
Restore original image from backup

Fig. 2. Process procedure for applying updates on productive systems

In both cases the production systems upgrade procedure (Fig. 2.) should include at least the following steps:

1. Perform backup of the productive system;
2. Create test environment from the created backup - by this step the backup is verified if needed;
3. Apply updates to the test environment and verify it;
4. If the updated test environment meets the functional requirements and it is

considered that they can be applied to the production environment, proceed to the next step, otherwise attempt to debug the test system to identify and resolve the problems encountered;

5. Schedule the timing of the update so that the impact on the production system is minimized. If necessary, an updated copy of the production system will be made;
6. Perform maintenance on the production system. If the system is redundant, i.e. consists of multiple machines then they will be upgraded one at a time so that system downtime is minimized;
7. Testing of the upgraded productive system and then moving to production.

2.4 Log monitoring and log archiving

Log monitoring is a mandatory process for the IT team. By monitoring logs one can observe the behavior of the entire hybrid cloud system. The logs in the hybrid cloud system are multiple and to monitor the logs it is useful to use some log monitoring and log interpretation solutions. There are several solutions in the market that facilitate the monitoring of logs and various metrics in the system. These solutions are used both in the cloud and on-premises. Both versions make use of different agents that help collect the information, standardize it and send it to the centralized solution. In the cloud solution the information is uploaded to the cloud where it is interpreted and users have access to it in the form of reports, alerts, etc. In the on-premises solution the logs are interpreted locally in the same centralized dashboard form.

Solutions that are used in the cloud often have costs that are directly proportional to the number and size of logs processed so it is good that they are filtered and correlated as much as possible to optimize costs and streamline the process.

Log files have a defined retention period for the information they contain. Proper maintenance is essential, as unregulated growth can cause them to consume significant system storage, leading to unnecessary resource usage and increased operational costs. Once the relevant data has been processed, logs should be archived and retained for a period sufficient to allow the reconstruction of events or incidents. After this period, logs should be deleted and the system cleaned to free up resources. As a best practice, it is advisable to separate infrastructure and hybrid cloud logs from application and service logs, ensuring clearer organization, easier troubleshooting, and more effective log management.

2.5 Hardware maintenance servers, storage systems

The hardware used in hybrid cloud infrastructure is usually dedicated data center hardware so it is designed to run 24/7. However, this equipment also needs maintenance such as changing power supplies, swapping disks or memories, adding memory or new storage. Dedicated data center and 24/7 equipment enables most operations without shutting down, which makes maintaining it much simpler in terms of its impact on the organization's business processes. After changing defective parts or adding additional components, the system immediately recognizes the new components or signals the problem without affecting the smooth operation of the system. The fact that these machines have redundant facilities is a big advantage, the dual power supplies allow the faulty ones to be changed without shutting down the systems, if a server in a cluster system has a fault the hypervisor (cluster management system) will automatically move the virtual machines to the rest of the servers in the cluster or in the cloud so the impact in case of physical faults is minimized. Maintenance of physical systems should be scheduled and done periodically at least once a year, and to be proactive components that may fail should be purchased or have a service contract in place so that they can be serviced and changed as soon as a potential failure is flagged to minimize data loss or degradation in IT service quality.

2.6 Network infrastructure and security equipment maintenance

Network infrastructure and security equipment play a critical role in ensuring reliable communications and safeguarding data. These systems require regular physical and software maintenance to remain effective and secure. In particular, security updates are essential to address emerging threats and vulnerabilities, and are typically aligned with the update cycles provided by equipment manufacturers. To minimize the operational impact of maintenance activities, it is recommended that critical communication and security components be deployed in a redundant configuration. This allows one unit to undergo updates or maintenance while the other continues to handle network operations, thereby ensuring continuous service availability and reducing the risk of downtime.

The maintenance process of the communication and security equipment shall also include backing up the image of the equipment to be upgraded, routing traffic to the other equipment in the network, applying the upgrades, testing the upgraded equipment in the system, validating it and putting it into production or reverting to the original image if the upgraded equipment is not successfully validated. If the upgrade process is successfully completed, this shall be documented and the next equipment shall be upgraded. If we have communication and security equipment management tools, different automations can be established through the maintenance policies to facilitate the maintenance process and if the system has an artificial intelligence component, it can be used for installing updates, testing the system and monitoring it.

The maintenance of communication and security equipment should follow a structured and reliable process to ensure system stability and minimize service disruption.

This process typically includes the following key steps:

- Backup:
  Create a full backup image of the device prior to any upgrade. This serves as a rollback point in case the upgrade fails or causes issues.
- Traffic Rerouting:
  Temporarily redirect network traffic to redundant or backup systems to ensure uninterrupted service during the maintenance window.
- Upgrade Deployment:
  Apply the necessary firmware or software updates to the equipment.
- **Testing and Validation:**
  After the upgrade, test the device in the live system environment to verify functionality and performance. If validation is successful, the equipment is returned to production. If not, the system is rolled back using the previously saved image.
- Documentation and Progression:
  Once the upgrade is successfully completed and validated, the process should be documented thoroughly. The same procedure can then be applied to the next device in the upgrade queue.

When communication and security equipment management tools are in place, this workflow can be significantly optimized through automation. Maintenance policies can automate tasks such as image backup, traffic failover, upgrade execution, and system validation.

Additionally, if artificial intelligence components are integrated into the infrastructure, they can further enhance the process by:

- Automating the installation of updates based on system readiness and low-usage periods.
- Performing intelligent testing and anomaly detection during and after upgrades.
- Continuously monitoring system health to identify issues before they affect operations.

This structured and intelligent approach to maintenance ensures that security infrastructure remains robust, up-to-date, and resilient with minimal manual intervention and risk.

3. METHODS AND TECHNIQUES FOR USING ARTIFICIAL INTELLIGENCE FOR HYBRID IT INFRASTRUCTURE MANAGEMENT

Artificial intelligence is rapidly penetrating cloud systems management as well, and they are becoming increasingly popular as they make their presence felt. Large cloud service providers such as Google, Amazon and Microsoft have started to offer artificial intelligence modules.

Efficient resource allocation is key to maintaining optimal performance in hybrid cloud environments. AI algorithms, especially those based on machine learning (ML), can analyze historical data and predict future resource requirements. This proactive allocation ensures that resources are allocated in a way that prevents bottlenecks and minimizes underutilization. Consolidation learning, for example, can dynamically adapt to changing workloads, making decisions that continuously improve over time. [3]

The main ways in which artificial intelligence is being used in hybrid cloud systems are:

- Task automation: Artificial intelligence is used to automate tasks that will be performed in the public cloud and here we have resource management in particular the addition of compute or storage resources needed in particular for application development and security management. Artificial intelligence especially through learning algorithms can quickly detect malicious code sequences or patterns that are a threat from a security point of view. By using artificial intelligence on the side of provisioning resources, creating the machines needed for different tests, managing the lifecycle of these resources we make significant savings in time, financial and human resources.

  An effective example of using AI to automate backup tasks is its application in managing routine, repetitive backup operations. AI can identify tasks that are typically performed manually and automate them, enabling IT teams to focus on more strategic and complex activities. In addition, AI can run various automated routines, such as testing backup copies in isolated environments, verifying data integrity, and scanning for potential malware or infections in saved copies.

  While these tasks - data backup, copy testing, and verification - may appear routine, they are often time-consuming and slow. However, they are essential for ensuring the security and reliability of an organization’s data. By automating these processes, AI significantly enhances both efficiency and data protection.

- Performance optimization: Artificial intelligence is used to optimize the performance of applications running in a hybrid cloud environment. The test patterns are done by setting different predefined data sets and tasks and the result will be analyzed by artificial intelligence. The advantage is that it has much higher analysis capability and speed, it can quickly analyze test batteries and can identify the best performing patterns or identify bottlenecks, including making recommendations for improving systems.

  A strong example of optimizing backup system management is the use of artificial intelligence to streamline and enhance backup processes. These processes can be scheduled to run at different times based on a variety of parameters, including: system utilization levels, permissible backup start times, required system uptime, the volume of data to be backed up, the average duration of backup operations, the target storage system, the number of systems that can be backed up simultaneously on a storage device, the total number of systems requiring backup, the type of backup (snapshot, full, or incremental), the retention policy for backup copies, and the level of network traffic generated at any given time within the organization.

  All of these factors must be considered when developing an effective backup plan for an organization. AI can significantly improve this process by analyzing these complex parameters and optimizing backup schedules and resource usage. Moreover, it can detect overloaded resources, enabling better distribution and more efficient use of the infrastructure involved in backup operations.

- Real-time monitoring and detection: Artificial intelligence is used to collect data from the logs of applications and systems running in the organization's hybrid cloud. The number of logs that are generated by the applications and systems in the hybrid cloud is very large and vast which makes it virtually impossible for the organization's IT staff to track and interpret them. Artificial intelligence through the technique of learning and identifying patterns or repetitive sequences, trends and patterns enables quick identification of problems by providing insight into the data generated by applications running in a hybrid cloud environment. Using artificial intelligence to analyze logs helps improve the performance and security of hybrid cloud environments.

Log monitoring is a complex task due to the vast volume of data generated across an organization's infrastructure. With most systems now operating online continuously, users and customers interact with them both during and outside of standard working hours. Detecting suspicious or unauthorized activity is critical to maintaining data security.

Artificial intelligence is highly effective in this context, leveraging its learning capabilities to monitor infrastructure logs over time and detect anomalies or irregular patterns that may indicate security threats. AI's ability to analyze large datasets and identify patterns far exceeds that of human analysts. Moreover, AI can respond to detected anomalies by automatically executing predefined actions to mitigate risks, operating continuously, 24/7, without interruption.

- Predictive Analysis to Prevent Data Loss: Artificial intelligence enables proactive identification of hardware issues or vulnerabilities in storage systems through the analysis of historical data. Storage systems operate continuously and rely on disks that, while highly reliable, are still subject to eventual failure. By continuously analyzing operational data, AI can identify early indicators of hardware degradation or potential vulnerabilities within the storage infrastructure. This capability allows organizations to proactively address issues by predicting failures before they occur, enabling timely maintenance or replacement of at-risk components. As a result, not only is the risk of unexpected data loss significantly reduced, but inventory management is also optimized—ensuring that only parts with a high probability of failure are replaced or stocked. This strategic approach improves overall system reliability, minimizes downtime, and reduces unnecessary expenditures on spare components.
- Security Assurance: By using artificial intelligence, we can improve the security of the IT infrastructure in the organization's hybrid cloud. Through machine learning technique the artificial intelligence algorithms can quickly identify any abnormal network traffic within the network, inside the infrastructure or to the outside which allows to quickly isolate the security breach reducing the risk of propagation. Furthermore, AI enhances threat detection by performing intelligent log analysis to uncover unusual patterns of user behavior that may indicate compromised accounts, insider threats, or unauthorized access attempts. These capabilities (*Table 1*) allow for faster incident response, greater situational awareness, and a proactive approach to threat mitigation. As a result, organizations benefit from a more resilient and adaptive security framework across their hybrid environments.

Table 1

Key capabilities and comparative advantages

Traditional security approach	**AI Powerd security**
Manual log reviews and predefined rules	Real-time anomaly detection through machine learning
Delayed response to threats due to limited monitoring	Instant alerting and automated containment of suspicious activity
Static policies with limited adaptability	Adaptive learning that evolves with infrastructure behavior
Focus on known threat signatures	Ability to detect unknown (zero-day) threats and user anomalies

Some examples services which are using artificial intelligence in hybrid cloud systems would be:

- Amazon SageMaker - is a platform that enables the creation, training and deployment of machine learning models. The platform can be used to automate many of the tasks involved in machine learning, such as data preparation, training and deployment of models. With built-in tools for labeling, debugging, and monitoring, SageMaker enables developers and data scientists to accelerate the development lifecycle while maintaining high model performance and operational efficiency. Amazon SageMaker is a fully managed platform that streamlines the process of building, training, and deploying machine learning models at scale. It simplifies and automates many of the complex and time-consuming tasks traditionally associated with machine learning, including data preparation, model training, tuning, and deployment.

- Microsoft Azure Machine Learning Studio: is a platform for creating, training and deploying machine learning models. The platform can be used to automate many of the tasks involved in machine learning, such as data preparation, training and deployment of models. By automating key processes such as data preprocessing, algorithm selection, and hyperparameter tuning, Azure Machine Learning Studio enables faster development and more efficient operationalization of machine learning solutions in both experimental and production environments. Microsoft Azure Machine Learning Studio is a cloud-based platform designed for building, training, and deploying machine learning models. It offers an intuitive interface and a suite of powerful tools that support the entire machine learning lifecycle—from data preparation and model training to evaluation and deployment.
- Google Cloud AutoML: can be used to automate the process of creating and deploying machine learning models. This can be useful for organizations that want to use machine learning to improve the performance or security of their hybrid cloud environment, but don't have the knowledge to do this on their own. Designed for users who may not have deep data science or ML engineering backgrounds, AutoML simplifies complex tasks such as model selection, training, and tuning through an intuitive interface and automated workflows. This makes it especially valuable for organizations seeking to leverage machine learning to enhance performance, security, or operations within hybrid cloud environments—without requiring extensive in-house AI expertise. Google Cloud AutoML is a suite of machine learning tools that allows organizations to automatically build and deploy high-quality machine learning models with minimal expertise.

By leveraging machine learning techniques, artificial intelligence algorithms require an initial learning phase to analyze data from within the hybrid cloud environment—such as network traffic patterns, application behavior, user activity, and system resource usage. Once trained, these AI-driven models can be effectively utilized to automate a wide range of tasks, including resource allocation, virtual machine provisioning, application deployment, and performance tuning. Additionally, AI significantly contributes to strengthening the security posture of hybrid IT infrastructures by detecting anomalies, optimizing threat response, and ensuring continuous system resilience.

4. CONCLUSIONS

The management of hybrid IT infrastructure systems is a complex process due to the interconnection of on-premises and cloud systems that host the organization's IT applications and services. Maintaining systems is necessary to keep them running smoothly, ensure security and add new functionality. At the same time, the maintenance processes of hybrid IT infrastructure systems need to be as efficient as possible, with minimal impact on the organization's processes (minimal downtime). Regular updating is an essential part of the organization's security assurance process. Lack of security updates increases the risk of service interruption and data loss in the event of an attack. Artificial intelligence has the potential to revolutionize hybrid cloud management by automating essential backup tasks and performance monitoring.

Implementing artificial intelligence in the management of hybrid IT infrastructures brings several significant benefits that contribute to improved performance, reliability, and security:

- Automation of routine operations: AI can handle essential, repetitive tasks such as equipment updates, backup automation, and performance monitoring. This reduces the workload for IT staff, increases efficiency, and lowers the risk of human error.

- Predictive analytics: By examining historical data and monitoring infrastructure behavior, AI can anticipate issues like system slowdowns or hardware failures. This allows teams to take preventive action before problems affect system performance or availability.
- Optimized resource and task management: AI enables smarter allocation of hardware resources and efficient scheduling of maintenance activities. This helps minimize downtime and ensures continuous availability of the organization's services.
- Enhanced security through continuous monitoring: With 24/7 monitoring capabilities, AI strengthens security by detecting potential threats and applying updates automatically. As described in this article (Fig. 2), this leads to a more secure and resilient infrastructure with minimal manual intervention.

Disadvantages of using AI in hybrid IT infrastructure management:

- Implementation complexity: Integrating AI tools into existing hybrid IT environments can be technically demanding, often requiring substantial time, expertise, and infrastructure adjustments.
- High initial investment: Deploying AI-driven solutions typically involves considerable upfront costs for software, hardware, and workforce training.
- Data privacy and compliance risks: AI systems require access to vast volumes of organizational data, which, if not properly governed, may raise significant privacy concerns and compliance challenges.
- Risk of overreliance: Excessive dependence on AI can diminish the expertise of human teams and lead to operational vulnerabilities if AI systems malfunction or produce inaccurate outputs.

While AI-powered systems hold the potential to transform hybrid cloud management by improving efficiency and automation, their successful implementation hinges on strategic planning, strong governance, and a well-balanced integration of human oversight and machine intelligence.

5. REFERENCES

[1] Majumdar, S., Madi, T., Wang, Y., Jarraya, Y., Pourzandi, M., Wang, L., Debbabi, M., *Security Compliance Auditing of Identity and Access Management in the Cloud: Application to OpenStack*. International Conference on Cloud Computing Technology and Science (CloudCom) (pg. 58-65). Canada, Vancouver: IEEE, 2015.

[2] Miller, L. *Secure Access Service Edge (SASE).* Palo Alto Ntetworks 2nd Special Edition, 2022.

[3] Segeč, P., M. M. *SD-WAN - architecture, functions and benefits.* 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), (pg. 593-599). Košice, 2020.

[4] Thopalle, P. K., *Hybrid cloud management using AI.* International Journal of Management IT and Engineering. vol 4, 2018.

[5] Moreno, R. T., J. G.-R., *A Trusted Approach for Decentralised and Privacy-Preserving Identity Management.* IEEE Access, vol. 9, 105788-105804, 2021.

[6] Rose S., Borchert, O., *Zero Trust Architecture.* National Institute of Standards and Technology, 2020.

[7] Eiers, W., Sankaran, G., *Quantifying Permissiveness of Access Control Policies.* 2022 IEEE/ACM 44th International Conference on Software Engineering (ICSE) (pg. 1805-1817). Pittsburgh, USA: IEEE, 2022.

[8] Miliano, I. S., *Machine Learning-based Automated Problem Categorization in a Helpdesk Ticketing Application*. 8th International Conference on Orange Technology (ICOT), (pg. 1-6). Daegu, 2020.

[9] Agarwal, S. B., *Automated Assignment of Helpdesk Email Tickets: An Artificial Intelligence Life-Cycle Case Study*. AI Magazine, Volume 41, 2020.

[10] Asma, A., Badr, B., *Intelligent Network Management and Control: Intelligent Security, Multi-criteria Optimization, Cloud Computing, Internet of Vehicles, Intelligent Radio*. Willey, 2021.

[11] Gooley, J., Y. D., *Cisco Software-Defined*. Cisco Press, 2021.

[12] Leng, T., *SD-WAN Solution*. Huawei Technologies Co, 2024.

[13] Sagi, S., *Hybrid AI: Harnessing the Power of Cloud and On-Premise Datacenter for Enterprise AI Use Cases*. Journal of Artificial Intelligence & Cloud Computing, SRC/JAICC-246, 2024.

[14] Sarwar, M. I., Abbas, Q., *Digital Transformation of Public Sector Governance with IT Service Management–A Pilot Study*. IEEE Access, vol. 11, 6490-6512, 2023.

[15] Kumar, R., Singh, V., *AI-driven Optimization Techniques for Cloud Resource Management*. Cloud Computing and Big Data, vol. 9, no. 4, pp. 21–33, 2020.

[16] Smith, H. E., Patel, D. M., *Implementing Zero Trust Architecture with AI in Hybrid Cloud Systems.* Journal of Cybersecurity and Cloud Technologies, vol. 3, no. 2, pp. 45–57, 2021.

[17] Zhao, L., Liu, W., *Enhancing Network Security in Hybrid Cloud Environments Using Machine Learning Algorithms.* IEEE Transactions on Cloud Computing, vol. 13, no. 6, pp. 1078–1090, 2021.

[18] Park, J., Kim, S., *Automated Network Traffic Management in SD-WAN with AI Integration.* International Journal of Network Management, vol. 32, no. 3, pp. 299–310, 2022.

[19] Zhang, X., Zhang, Y., *AI-based Anomaly Detection in Hybrid Cloud Architectures.* Future Internet, vol. 13, no. 7, pp. 168–182, 2021.

[20] Zhao, Q., Yang, H., *Smart Cloud Infrastructure Monitoring Using Machine Learning for Anomaly Detection.* Journal of Cloud Computing: Advances, Systems and Applications, vol. 9, no. 1, pp. 75–88, 2020.

[21] Tan, J., Lee, M., *AI-powered Cloud-native Applications for Dynamic Scaling in Hybrid Cloud Environments.* International Journal of Cloud Computing and Services Science, vol. 10, no. 3, pp. 221–235, 2021.

[22] Wang, Y., Lin, F., *AI and Machine Learning Techniques for Optimizing Cloud Storage in Hybrid Cloud Systems.* Journal of Cloud Computing Research, vol. 8, no. 4, pp. 115–126, 2022.

Mentenanța infrastructurii IT cloud hibride utilizând inteligența artificială

Mentenanța infrastructurii IT trebuie realizată astfel încât să aibă un impact cât mai mic asupra proceselor din organizație. Orice infrastructură are nevoie de mentenanță pentru actualizare sisteme, aplicarea de patch-uri de securitate sau pur și simplu pentru efectuarea de operații de întreținere programate sau neprogramate în cazul unor intervenții necesare pentru asigurarea bunei funcționări a echipamentelor. Infrastructura IT de tip cloud hibrid are un mare avantaj prin faptul că este în cea mai mare parte o infrastructură redundantă care permite realizarea proceselor de mentenanță cu un impact cât mai mic asupra proceselor din organizație. Prin utilizarea virtualizării și a sistemelor distribuite în cele mai multe situații nu este necesară oprirea completă a sistemelor aflate în mentenanță, aceasta făcându-se de cele mai multe ori la cald cu sistemele aflate în producție, total transparent pentru utilizatori. Sistemele redundate de stocare, infrastructura redundată de rețea și de securitate, sistemele care folosesc mașini virtuale redundate permit realizarea de mentenanță prin posibilitatea preluării funcțiilor echipamentului/sistemului aflat în mentenanță de către celelalte sisteme sau echipamente cu același rol din sistem. Din acest punct de vedere mentenanța acestor sisteme poate fi automatizată și optimizată astfel încât aceasta să se realizeze în perioade de timp mai puțin aglomerate pentru a avea impact minim asupra proceselor de business ale organizației.

Marius Ioan TODERICI, Doctoral Candidate, National University of Science and Technology Politehnica Bucharest, Faculty of Industrial Engineering and Robotics, Bucharest, Romania, marius@toderici.ro

Aurel Mihail TITU, Professor, Corresponding Author, "Lucian Blaga" University of Sibiu, 10 Victoriei Street, Sibiu, Romania, e-mail: mihail.titu@ulbsibiu.ro; Academy of Romanian Scientist, 3 Ilfov Street, Bucharest, Romania

Nicoleta Madalina STAN, Doctoral Candidate, National University of Science and Technology Politehnica Bucharest, Faculty of Industrial Engineering and Robotics, Bucharest, Romania, madalina.nita12@yahoo.com