Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-625-6_8

DeepScience
Open Access Books

Chapter 8: Building Resilient Cloud-Based Infrastructure for Intelligent Control Systems

8.1. Introduction

Distributed control systems constitute an important area of application for smart technology, particularly when information and communication technology are involved in control actions. In this regard, smart technology must address outstanding design problems that concern the optimization of control systems resources and communication networks, the integration of control systems within IEC 61499 design standards, as well as the evaluation of their operation conditions in real-time. Networked control systems are a particular cyber-physical class in which the control system is assisted by data transport networks, considering the natural constraints that arise from the scenario. For instance, one of the major current control systems problems is the joint optimization of networked control systems communications and control actions, since each one of those systems independently has optimization targets that considerably improve their respective performance as well as the information that these systems provide to each other. However, implementing such a joint optimization process introduces a conflict of interest with distinct cost or utility functions for each control system, alongside reliability and fault-tolerance issues that generally remain unaddressed when executing the control or communications actions.

Cloud technologies represent key support for network control system applications and evolution, especially in scenarios that include interest-based control, such as automated driving and intelligent transportation systems. The interconnection of vehicular systems interactions through cloud resources enables support for cooperative control processes of complex events, for example, the request of priority traffic signals for emergency vehicles. However, driven by an interest-centric network model, new challenges emerge, including optimization processes at every stage of the control actions, given the associated costs of each action—both control and communications. Intelligent control systems are enabling technologies, considering the push that artificial intelligence has been given for the interconnection and joint coordination of multiple CPSs. The progress

of artificial intelligence for control lies in the interconnection and joint operation of multiple cyber-physical systems, engineers of optimization policies using intelligent control systems, and the amalgamation of the power and capability of cloud technologies to bring Internet of Things devices to market and provide scalability for future needs.

8.1.1. Overview of the Study's Objectives and Scope

Within the context of a changing world, the resilience of energy and environmental systems has been a key issue that nations must respond to in order to mitigate the effects of climate change. These issues are addressed from different perspectives and produce a large amount of data related to the environment and energy. For this reason, the acquisition, processing, and analysis of large volumes of data play a fundamental role in solving complex problems and optimizing decision-making. It is possible to process and analyze large data archives quickly by combining cloud storage with the use of artificial intelligence in the control of complex physical systems, such as those used in buildings. This framework permits the generation of intelligent control systems that can optimally implement effective energy-saving strategies, thus guaranteeing the desired level of service.

Based on these considerations, the aim has been to propose and develop a cloud framework for the implementation of artificial intelligence algorithms aimed at the intelligent control of complex physical systems. In particular, a cloud-based architecture that combines high availability, redundancy, fault tolerance, and resource elasticity has been described. This architecture has been validated with an AI-based control system through the implementation of intelligent control strategies in an electrical microgrid. Experiments were performed using significantly different computing clusters to show that the methodology can be transferred to the control of other complex physical systems. Finally, the proposed architecture makes it possible to connect a SCADA system with a real physical environment and cloud-based AI algorithms, where real-time operation and optimization functionalities are implemented.

8.2. Understanding Intelligent Control Systems

Modern advances in technologies, such as the Internet of Things (IoT), Cyber-Physical Systems (CPSs), data analytics, and artificial intelligence (AI), have enabled new systems with high levels of performance and intelligence. An example application domain is intelligent infrastructure control systems in simple and complex environments, also known as smart systems or smart grids. In the latter, an environment supports the logic and operation of one or several physical infrastructures that are controlled dynamically, optimally, and often globally[1-3].

In a CPS, the control intelligence is distributed, but in smart grids, a global control and supervision intelligence is often used. The control infrastructure is accessed and executed on through a cloud and sets operational constraints, conditions, configurations, and actions for the operated and managed physical infrastructures.

8.2.1. Definition and Overview

An intelligent control system (ICS) can be characterized by different aspects, such as its performance, flexibility, and robustness against changes and disturbances during operation. The system must be designed such that it is able to solve the targeted control problem. Flexibility in the design reduces the effort of reconfiguring or redesigning the system after its initial implementation. Robustness denotes the ability of the system to adapt to changes in the operational environment while still fulfilling the design criteria or tolerating a certain degradation in its performance.

Fig 8 . 1 : Intelligent Control System: Characteristics and Implementation

From an implementation point of view, an intelligent control system can further be characterized by the employed components (hardware and software). Mainly, the objectives of the system influence the choice of the components. The implementation may suffer from a lack of resilience, despite an intelligent design of the system. Different aspects play a role when examining the resilience of the system: e.g., redundancy of resources, dependability (failure-free operation), network properties (latency and speed), security aspects of resources (secrecy, integrity, and authentication), and privacy of

users. Building an ICS for a safety-critical application, therefore, requires taking all aspects into account. Distributing resources may solve some points, whereas certain requirements impose restrictions on the distribution, particularly when there are also latency requirements (i.e., placing resources physically close to the controlled process).

8.2.2. Applications in Industry

Low-cost self-organizing systems based on the focus of control technology on system modeling and knowledge representation were introduced. They needed to be tailored to allow usage by specialized users, regardless of a lack of knowledge of control theory. The proposed approach enables the quick setup and deployment of an automation system.

The cloud-service-based architecture for knowledge-intensive manufacturing systems consisted of two core parts: a manufacturing service platform hosted by a cloud-service center and a knowledge base of production methods. The service platform held domain knowledge and information about the production capability and production status of the enterprise and workshop. The knowledge base contained information on how to produce an item.

8.3. Cloud Computing Fundamentals

Cloud computing has attracted tremendous attention in recent years as the next generation of information technology. By shifting computing and storage resources outward from an enterprise to the third-party data centre, essential components of an intelligent control system can be provided as services to subscribers on an on-demand basis. Rich resources and economic features are thereby provided as the core values of cloud computing. In particular, the concept of a cloud provides a high-quality intelligent control system into which all data processing in the control system can be shifted. As a result, data can be analysed in the cloud, and the cloud can intelligently send individual commands for the desired outcome to any intelligent control system. Several implementations of this concept have been proposed: Lotus Notes, Spreadsheets, and database options in the cloud.

Infrastructure represents a foundational level that underpins other areas of architecture and focuses on delivering shared IT services to enable and support both operational processing and change [2,4,5]. Infrastructure can be provided in terms of physical devices, logical devices, facilities, services, and service components. These are grouped into categories to ensure that common infrastructure areas can be managed collectively (e.g., Availability Management, Backup, and Recovery, part of the Business Continuity

group). Infrastructure must be resilient to ensure the ongoing availability and continuity of services. It must therefore be designed, implemented, and operated to provide resilience against all forms of disruption, whether malicious or accidental.

8.3.1. Cloud Service Models

A deployed control system implementation can be part of a much larger environment that utilizes resources within a cloud. These resources can comprise hardware, applications, or platforms. Hardware resources can be virtualized servers, physical storage devices, or hosts behind the firewall.

Cloud service models depend on the level of shared resources. These models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Network as a Service (NaaS). IaaS involves sharing hardware resources. PaaS shares development frameworks and toolkits. SaaS involves sharing application software. NaaS pertains to sharing network resources.

Cloud service models depend on the level of resources shared. IaaS involves sharing hardware resources. PaaS shares development frameworks and toolkits. SaaS involves sharing application software. NaaS pertains to sharing network resources.

8.3.2. Deployment Models

The diversity of consumer needs in intelligent control systems is reflected in the breadth of solutions provided by the cloud service, deployment, and management models. The main cloud deployment models are private cloud, community cloud, public cloud, and hybrid cloud, also referred to as the internal cloud, external cloud, and mixed cloud.

The private cloud provides services to an organization within an intranet. The infrastructure is owned, built, and managed by the company itself, an alternative company, or a combination, and it can be located either within or outside the organization's premises. In providing a cloud, the environment must address issues such as cloud and firewall security and implementation of failover and load balancing mechanisms. This ensures resilience against failures and security threats. The community cloud provides services to multiple organisations through the public network. Ownership can be an association of organisations, a company, a combination, or a third party. The public cloud offers services to the general public on the Internet, with the infrastructure owned and managed by a service provider company. The hybrid cloud is a composition of two or more deployment models linked by technology that allows data and application portability. While the corporate servers operate in the

organization's private cloud, public cloud services support extended markets, high scalability, and computing power.

8.3.3. Benefits of Cloud Computing

Cloud computing offers many potential benefits to companies deploying intelligent control systems and associated applications—a fraction of which is described here. The pay-per-use model shifts from upfront capital expenditure (capex) to operating expenditure (opex). The time to deploy is reduced from months or years to hours or minutes. Pay-as-you-grow eliminates the need to plan capacity in the light of future demand, and the delivery of a service by someone else with the appropriate skills means that the bar of technical knowledge and investment is lowered considerably.

The various service models offer different levels of abstraction suitable for different types of organisations and IT workload. Organisations can choose between the different service models based on their security, control, and cost requirements. The SPSM section discusses each cloud model in more detail. The different deployment models provide organisations with a choice about how and when to use public cloud and private cloud. Organisations can therefore balance the benefits of public cloud with the control and security of private cloud.

8.4. Designing Resilient Infrastructure

Digital infrastructure in the cloud offers a truly distributed and scalable platform. Infrastructure-as-a-service platforms such as Amazon, Microsoft, and Google provide advanced API-driven capabilities, including programmatic deployment of virtual machine instances, bandwidth provisioning, elastic scaling of load balancers, and object and block storage. Collectively, these capabilities ease the deployment of large-scale control workloads and provide resiliency and reliability in the event of faults and failures.

Cloud platforms provide resilience through the concept of a region, designed to be a fault-isolated location through one or more availability zones. An availability zone consists of one or more discrete data centers, each with separate power, networking, and connectivity, housed in separate facilities. The availability zones within a region are interconnected with high-speed, private links with low-latency networking. Colocations ensure independence of availability zones while allowing for synchronous replication of data across zones.

8.4.1. Key Design Principles

With the pervasive integration of smart agents into a myriad of critical systems, robust intelligence guarantees during crises and hazards have become indispensable. The Cloud Intelligence paradigm offers substantial scalability and cost-effectiveness in training, testing, and deploying resilient intelligence that can adeptly manage failures in field agents.

The design of a robust and resilient Cloud Intelligence system for critical applications must embody three essential principles. Firstly, it must be fault-tolerant to mitigate the effects of natural disasters, cyber attacks, and other failures [4-6]. Secondly, it must ensure adequate capacity to accommodate high demand and the influx of requests for assistance. Thirdly, it must be intelligent, enabling proactive analysis of intelligence and early hazard prediction in areas susceptible to natural disasters and other hazards.

These principles ensure that all associated agents are supplied with a fault-tolerant intelligence service that supports corresponding intelligent and cognizant control. The following sections delineate the design of the Cloud Intelligence system by these guiding principles.

Fig 8 . 2 : Cloud Intelligence for Critical Systems: Principles and Resilience

8.4.2. Redundancy and Failover Mechanisms

Cloud computing impacts on reliability and fault tolerance have been treated largely as a side-effect of performance improvements and cost-reduction opportunities. Indeed, the setup typically involves VMs replicated into pairs. Primary VMs perform operations, while the secondary ones usually reside powered off and are then activated in the event of a failure of the primary VM. At first, this approach might look wasteful; however, operation-oriented companies such as banking, healthcare, or aeronautics cannot afford prolonged service outages. Moreover, in these types of applications, the key performance indicators are the system's availability, fault tolerance, and reliability rather than profit.

On the other hand, AI-based systems often show an unusually high computational footprint. This means that they typically cannot afford a powered-off system, as such a system would never be able to meet the expected QoS. Thus, a load of up to 50% needs to be tolerated at each VM, and the replicas must not be powered off. This load requirement spoils the usual resilience plans underpinning the brainy services implemented through a public-cloud solution. Accordingly, some fault and/or failure scenarios are not protected or considered. In more detail, no redundancy is present to mirror a primary VM or service when the other one is under a heavy load or when routine maintenance operations are to be conducted.

8.5. Security Considerations

Cloud computing or cloud operations are internet-based computing where shared resources, data, software, and information are provided to computers and other devices on demand, anytime and anywhere. The common cloud applications are web e-mail, online document-editing tools, and data storage services. The business or end user software requirements are raised on the cloud, including the provisioning of various types of resources as a service on demand. The common name that is often used is utility computing, by analogy to water, electricity, and telephony, where a client just has to pay for the utility consumed. Cloud providers are poised to become a full-fledged operating system and marketplace for many third-party web applications. Cloud computing is poised to become a serious alternative for information technology organizations and outsourcing companies to implement internal and external services.

Companies like Google, Yahoo, and Amazon already are using cloud computing to improve the performance of their existing applications. A well-known company like Clarinet is in the process of implementing a software test hosting platform, ARES, using cloud computing. Presidential Information Technology advisor Vivek Kundra, in his paper ‘‘Towards an Effective Revolution in Tools, Education, and Methods for Achieving National Security, Protecting Privacy, and Ensuring Public Safety in the 21st

Century'' proposed a government-based cloud named Apps.gov that will host more than 100 applications. Based on this application development framework, various government organizations propose to develop applications and host them on the cloud, reducing considerable costs and depending on other agencies for their infrastructure.

8.5.1. Data Protection Strategies

Intelligent control systems rely on data collected from various physical and virtual sensors that monitor different parts, regions, or scopes. Multiple levels of cyber-physical-cloud computing and intelligence extend the scope and focus of control operations and processes. Fair and open access to the data is ensured for authorized personnel assigned the relevant roles and tasks within an organization.

The volumes, variety, veracity, and velocity of the data are immense and increasing rapidly. Suitable mechanisms and models are necessary for protecting data, handling redundancy, ensuring data availability under attack by eliminating single points of failure, and balancing costs with performance. Data protection involves the replication of data across different storage devices or locations to address these concerns.

8.5.2. Access Control Mechanisms

Several approaches enable end users to define access control policies for their resources either directly or indirectly. For instance, aspects of the model in Section 3.3, such as the visibility of projects, can be controlled using the Cloud Control Backup feature through the Azure portal. Defined roles allow various ports to be opened dynamically on resources, providing a form of indirect access control over icids-sb resources. Adopting the attribute-based access control (ABAC) paradigm, which utilizes attributes for both subjects and resources, gives the cloud consumer fine-grained access control to an entire environment of resources [6-8].

The information landscape for decision-makers is augmented by intelligent control systems. They gain increased self-understanding through the integration of mechanisms that facilitate the reverse flow of information from control components to the contextual level, in addition to the conventional forward flow for hosting reactions. Closely linked to understanding is the concept of self-sustaining — the system's ability to initiate and control processes that regenerate its internal structures and operational resources, thus maintaining both the specification and the application of policies. These capabilities form a feedback network that continuously updates the set of policies. Intelligent control systems exhibit constancy in behavior, even when internal or external changes alter their evaluation criteria or the set of policies.

8.5.3. Compliance and Regulatory Issues

Data destinations, actions, controls, and compliance business processes require the highest level of security. Certain demanding business areas may have to conform to the Sarbanes–Oxley Act, HIPAA, Gramm–Leach–Bliley, or European Union Law. If operational, qualitative, or quantitative performance information is available within the proposed station-keeping and emergency station-keeping control process, then this information should be stored and presented alongside the information for compliance purposes.

No regulatory approvals are necessary. However, the process has been designed actively to support the compliance business process operation.

8.6. Performance Optimization Techniques

With the growing adoption of the Internet of Things (IoT) paradigm in cyber-physical systems and control applications, the demand for computing infrastructure with enhanced capabilities has increased exponentially. Cloud computing has responded to this demand by offering service models that optimize costs, increase scalability, support virtualization, and consolidate resources. The platform-as-a-service cloud paradigm facilitates the evolution of intelligent control applications by integrating foundational data from sensors, the capacity of control operation software, and the resilient actuating functions of connected devices. However, achieving complete service-chain resilience requires ongoing monitoring of underlying components to ensure fault-free execution.

The concept of fault-tolerant-related resiliency lies at the core of fault-tolerant system design. Despite the promise of cloud computing for many real-time applications, its high susceptibility to failures and faults poses a significant challenge, and the services provided may not be highly resilient. Resiliency-oriented optimization methods have been proposed for resource provisioning in service-grids; nevertheless, resiliency and fault-tolerant models along with their optimization techniques for intelligent control operations in PaaS cloud environments remain largely unexplored. As a consequence, resource allocation in cloud-assisted intelligent control applications calls for the design and implementation of resiliency-oriented optimizations to guarantee fault-tolerant provisioning of real-time intelligent control services.

8.6.1. Load Balancing Strategies

One of the widely used methods of workload balancing is feature-based load balancing. In this method, the elements of a feature vector can be mapped to a set of agents/nodes to perform a set of actions. As a result, an agent is allowed to select a particular type of

feature for performing a task. For instance, in a hotel room service application, the server requests consist of a feature vector with two features, i.e., "food" and "items for the room". If a feature-based distribution is performed, then server requests may be distributed to a restaurant or concierge agent depending on the features of the request. The feature-based load balancing approach is suitable for social agent interactions where the agents are designed to handle such situations. However, apart from the task load, the overall remaining capacity is not taken into account. As a result, real-time systems may face a deadlock when a misplaced task is allocated to a server with insufficient capacity.

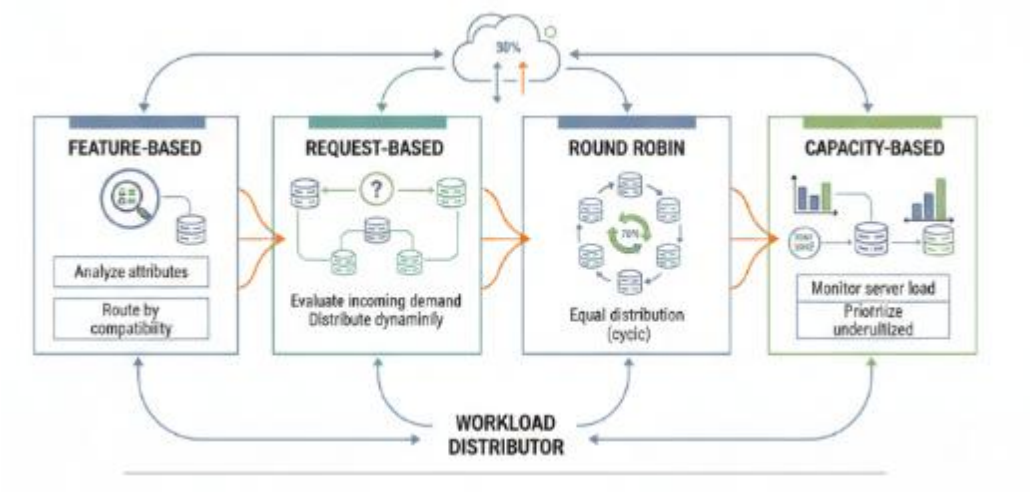

Fig 8 . 3 : Workload Balancing Methods: Feature-Based, Request-Based, Round Robin, and Capacity-Based

Another approach is the request-based load balancing, where a set of tasks or requests in a queue needs to be performed by an agent. Agents that are capable of handling such a request have to make requests to the server to allocate the task. The requests are granted to an agent only when the task allocation to the agent does not create a deadlock or a safety condition violation. Another widely used approach for workload balancing is the round robin approach, in which a sequence-based distribution of requests to the server is performed [5,7,9]. It is one of the fair and simple approaches that ensures equal allocation of requests to all servers with equal capacity. However, it finds less use in real-time distributed systems because of the risk of task deadlock and overlooking of the server's load conditions.

An alternative approach, referred to as a capacity-based approach, is presented here. This approach takes into account the load and remaining capacity of the servers when performing the request allocation.

8.6.2. Resource Allocation and Management

The optimal allocation of resources, both in terms of the number of virtual instances and overall resource capacities, is of paramount importance for the performance of a cloud-based control platform. Contemporarily, the majority of cloud-service providers focus on minimizing cost while fulfilling functional and non-functional requirements, so as to be able to provide profit-driven pricing schemes. However, this perspective often leads to underpayment and can ultimately negatively impact revenue and performance, as resources can be oversold, resulting in overutilised physical machines. To better balance the objectives of both cloud-service providers and cloud-service clients, researchers therefore focus on economic models that couple the client and provider costs. However, the introduction of multiple conflicting requirements inherently leads to optimization problems with several objectives.

In addition to the task of optimally selecting resource capacities, another control-related aspect constitutes the scheduling of cloud-based control tasks. Service providers can draw upon a wealth of literature in scheduling that deals with the alleviation of resource contention, which is a crucial problem in heterogeneous virtualized environments. However, methods that allocate applications to virtual machines, such as NBA, do not allow for the scheduling of IaaS-level tasks to properly consider differences in application task properties, such as timing properties, with the needs of time-sensitive control applications in mind.

8.7. Case Studies

Several Scenarios in the Dispatching System of the Freight Hub

Wind-storage-hydrogen-electricity complementary utilization is an advanced technology. Xining city is located in the east–north of the Qinghai-Tibet Plateau. It belongs to the Qinghai-Xizang Plateau (Plateau) climate zone, which has a unique geographical location and abundant natural resources. Its favorable natural and climatic conditions are suitable for the development of clean energy. Longshan Mountains are rich in wind resources. The hydropower in the Huangshui River Basin is abundant, rich in solar energy resources, and suitable for the development of pumped-storage power stations and conventional hydropower stations. Huangditan Hydropower Station, Liujiaxia Pumped Storage Power Station, and Longyangxia Pumped Storage Power Station have been planned and designed. The role of the complementary utilization of water and coal is also more prominent.

The combination of water and coal will play an important role in relieving the problem of 'water shortage' and other related problems in the power system in the future. The new energy complementary system composed of wind, solar, and hydrogen demonstrated

here will play a very positive role in further improving new energy consumption and optimizing energy structure.

8.7.1. Successful Implementations

Critical communications present some of the most demanding applications for modern communications technology. When designing and developing communications systems for critical communications, resiliency is paramount. Services must continue functioning without interruption or failure in the face of any single failure in the underlying communications infrastructure. For the Super Wi-Fi network, services must be resilient to any single failure of the physical channel, the radio equipment, and the core data-networking equipment.

Using multiple physical connections to the cloud is a key design consideration for maintaining critical communication services over the Super Wi-Fi network. Utilizing two separate networks minimizes any single point of failure between the BSC and a service’s corresponding cloud controller function. Since most of these networks rely on fiber-optic connectivity, multiple physical providers provide diverse routes underground. These diverse routes minimize the probability that a service will lose connectivity due to natural or unintentional events such as flooding, earthquakes, tornadoes, or accidental cutting of an underground cable.

8.7.2. Lessons Learned

OpenStack bears a large footprint that can hinder responsiveness during outages and periods of rapid change. Inexperienced or under-trained staff responsible for responding to failures will require additional liaisons and advisers to assist them with root cause analysis and corrective action procedures. Operators inexperienced with cloud concepts may not immediately understand or recognize that outdated or improperly configured resource monitors may be the ultimate cause. Lack of prioritized action lists and scheduled change windows increases the frequency of unsynchronized configuration changes to network, storage, and compute components. Miscommunication between individual cloud component stakeholders can lead to the order of changing resources in cascading failure events.

The application of intelligent control in a cloud environment is global in scope. Incident response information can be found in numerous public mailing lists, bug patches in various online repositories, as well as in individual blogs and message boards. Outbound communication from the organization must appear as internal as possible with respect to the OpenStack ecosystem, to receive proper cooperation regarding identifying root

causes and developing solutions. Inbound communication destined for the cloud system must also be resilient against other cloud failures by being distributed in both the geographical and logical hosting space. Additional care must be taken during service events to ensure that this communication path is available to internal operators.

8.8. Future Trends in Cloud-Based Control Systems

The relationship between controllers and controlled systems should be rethought and re-engineered due to the increased capabilities and changed roles introduced by cloud infrastructure. The nature of intracloud communications, with a generic delay from the controller to the controlled system being constantly available, needs to be considered together with the fact that the cloud is available only for fast equipment or parts within the individual physical machines.

A possible evolution for control systems that could make use of benefits such as higher computational power via an increased number of possible nodes is the implementation of the proposed hierarchical structure. Each controlled system (e.g., a mobile robot) could be managed by its own Agent Controller implemented in the cloud. At a higher level, the Agent Controller on a physical machine could communicate with other M-SCADA instances, analyzing the environment and optimizing the tasks of the mobile robot group. At an even higher level, a supervisory controller could be introduced, managing and controlling all the services for the different physical machines.

8.8.1. Emerging Technologies

The convenience, efficiency, and cost-effectiveness of Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) are driving many enterprises to migrate their existing services or business operations to the cloud. Cloud computing enables consumers to pay only for the resources they want. Cloud resources can be elastically provisioned and released in an adaptable manner, allowing enterprises to be more scalable and respond flexibly to dynamic circumstances with resources on demand. However, if an organization places its critical systems and data on a cloud. The organization will lose direct control and delegate responsibility to the cloud provider party for the availability and security of the sensitive information and artifacts. Moreover, most of the cloud resources are shared equally among multiple tenants. Any failure at the Cloud Service Provider side can impact the business operations and workloads of multiple tenants running on that cloud service node. Cloud outages may result from different factors such as software errors, hardware failure, common input/output problems, resource depletion, and connectivity. For example, as a result of a software update, the Google Docs team experienced a cloud outage in 2012. In 2014,

a cloud outage occurred at Verizon due to an environmental control system (air conditioning) failure. In 2015, AWS experienced a cloud outage due to a network hardware failure. In 2016, a major Windows Azure cloud outage was caused by resource depletion.

These cloud outages will undoubtedly hurt business operations and result in the loss of a company's reputation. Ultimately, the company may even suffer financial losses. For example, the Amazon AWS outage in 2015 led to a financial loss of $150 million. Likewise, the same cloud outage resulted in a loss of $12 million for Vice Media and $5.7 million for Netflix [1,9-10]. Other factors, such as human error, infrastructure, or natural disasters, can also cause such outages. Considering these challenges, Alibaba Cloud proposed a non-cloud service model implemented based on a hybrid cloud. This hybrid cloud-based approach focuses on setting up a passive cloud resource in the web service that can react to an outage by redirecting traffic to the real workload until the main Cloud Service Provider resource recovers. The hybrid cloud approach will be discussed in more detail in Chap. 10.

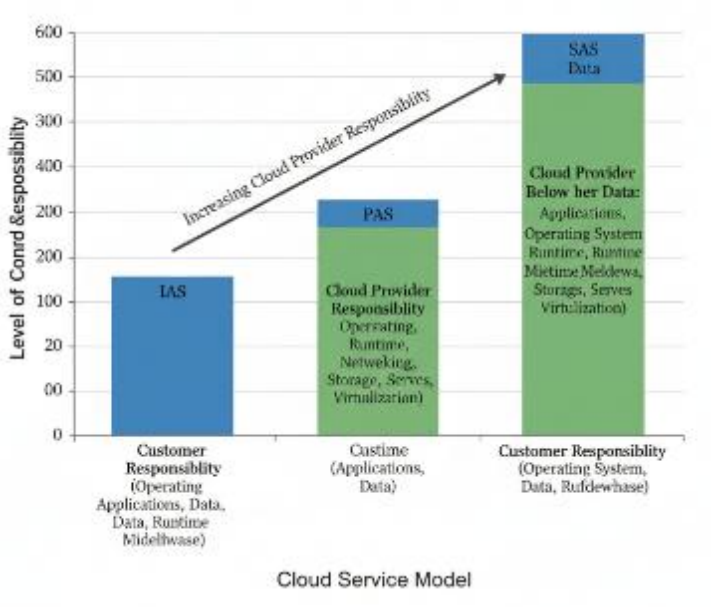

Fig 8 . 4 : Delegation of Control & Responsibility across Cloud Service Models

8.8.2. Potential Challenges

Despite the clear benefits associated, migrating the control system layers to a Cloudcation environment would still pose some challenges that the designers of such systems should consider carefully before deciding, such as:—

Privacy, security, and trust: transferred control systems should connect to the Cloudcation provider exclusively, with encrypted links to ensure that unauthorized parties cannot gain access to sensitive information and protect the users' privacy. The Cloudcation provider should also strictly control communications with services inside the Cloudcation to mitigate the potential risk of services attacking each other. Moreover, users' trust in the Cloudcation provider is necessary for accepting the new structure. Cloudcation providers should therefore fulfill the promised SLAs and behave fairly to win the trust of their customers.

High availability: physical machines and the links connecting them must be highly available to satisfy the SLA for cloud service. Less time for failover might cause data loss. However, low-cost service cannot provide high availability. It might be necessary to disintegrate the SLA components for services in the Cloudcation so that users can use different services to meet their SLA of high availability.

Latency: the connection between the control system and the functional components running inside the Cloudcation might delay the reaction of the control system. However, the physical locations of a control system should be recognised and a distributed scene should be considered where functions related to real-time procedures run in a local Cloudcation to reduce the latency.\

Response time: the time that the control system takes to invoke the functional components running inside the Cloudcation might increase to a point where the bandwidth requirements of the control system are beyond that of the migration.

8.9. Conclusion

The emergence of NCSs as an alternative to PDVFCSs for operating applications has inspired interest in developing fault-tolerant structures for such systems. This study analyzed the FT control of an NCS in an ADS to address sensor and actuator fault occurrence, considering network fault occurrence via a representation of the data transmission paths as a conditional DTMC. By constructing a hierarchical FT controller, the closed-loop ADS system was shown to maintain stability with a certain probability when both controller and network faults were present. Unlike previous studies, two-dimensional faults were considered concurrently, enabling the system to tolerate one kind of fault occurring together as well as separately. Simulation results confirmed the functionality of this design. Moreover, a demonstration system was designed to show the feasibility of the proposed solution in a practical application, and the experimental results coincided with the simulation results.

These preliminary studies provide a direct direction for further FT work on NCSs. As the fault models become more realistic, the HFT control of NCSs for ADSs will be

examined systematically. Considering that practical NCS fault modes fit the faults of the proposed models well, the design methods for HFT controllers will therefore be extended to other NCS applications.

8.9.1. Final Thoughts and Future Directions

The ability to build a cloud-based infrastructure capable of implementing the resilient execution of intelligent control systems is a significant step toward more advanced cloud control. Improvements to Zoneaware would also enhance our approach. For example, zone awareness could be integrated into a formal migration algorithm for minimizing system downtime. With some additional programmability, Zoneaware could support additional resilience-related use cases—such as allowing one to specify the quality-of-service support expected from a given zone placement. Moving beyond Zoneaware, an improved realization of the broader Fog of everything concept would provide automated decisions concerning workload placement across both multiple clouds and private infrastructure—enabling workloads to operate as resiliently as possible, while simultaneously considering budget, latency, security, or other concerns.

Looking ahead, the emergence of platform-as-a-service and software-as-a-service cloud products can provide even greater opportunities—and challenges—in achieving resilient execution. On one hand, these products allow the implementation of more advanced systems without the requirement that a team implement and maintain the lower-level building blocks. On the other hand, the lack of control over the placement of execution environments—provided by these services—limits a system's ability to consider resilience in placement. Solutions to this issue must rely upon cross-service-level mechanisms and approaches highly similar to those introduced here.

References

[1] Diez O. (2014). Resilience of Cloud Computing in Critical Systems. Quality and Reliability Engineering International, 30(3), 397–412. https://doi.org/10.1002/qre.1579

[2] Meda, R. (2025). Integrated Sales Performance Management Platforms: Leveraging AI for Quota Allocation, Demand Forecasting, and Zone-Based Sales Optimization. Advances in Consumer Research, 2(4).

[3] Tärneberg W, Skarin P, Årzén K-E, Kihl M. (2023). Resilient Cloud Control System: Realizing Resilient Cloud-Based Optimal Control for Cyber-Physical Systems. arXiv, 2304.00857. https://doi.org/10.48550/arXiv.2304.00857

[4] Kalisetty, S., & Inala, R. (2025). Designing Scalable Data Product Architectures With Agentic AI And ML: A Cross-Industry Study Of Cloud-Enabled Intelligence In Supply Chain, Insurance, Retail, Manufacturing, And Financial Services. Metallurgical and Materials Engineering, 86-98.

[5] Wijaya S, Ramadhan A, Andhika A. (2023). Cloud-Based Control Systems: A Systematic Literature Review. International Journal of Reconfigurable and Embedded Systems, 12(1), 135–148. https://doi.org/10.11591/ijres.v12.i1.pp135-148

[6] Kalisetty, S., Preethish Nanan, B., Annapareddy, V. N., Gadi, A. L., & Kommaragiri, V. B. (2022). Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital Infrastructure, Secure Networks, and Intelligent Manufacturing. Venkata Narasareddy and Gadi, Anil Lokesh and Kommaragiri, Venkata Bhardwaj, Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital Infrastructure, Secure Networks, and Intelligent Manufacturing (December 15, 2022).

[7] Shirazi N-u-h, Simpson S, Oechsner S, Mauthe A, Hutchison D. (2015). A Framework for Resilience Management in the Cloud. Elektrotechnik und Informationstechnik, 132, 122–132. https://doi.org/10.1007/s00502-015-0290-9

[8] Gadi, A. L. (2020). Evaluating Cloud Adoption Models in Automotive Manufacturing and Global Distribution Networks. Global Research Development (GRD) ISSN: 2455-5703, 5(12), 171-190.

[9] Konaganti S.D.P. (2023). Intelligent Resilience in Multi-Cloud Systems. International Journal of Scientific Research in Science and Technology, 8(6), 431–440. https://doi.org/10.32628/IJSRST251222708

[10] AI-Enabled Predictive Modeling for Flood and Mobile Home Insurance Claims Management. (2025). MSW Management Journal, 34(2), 1295-1316.