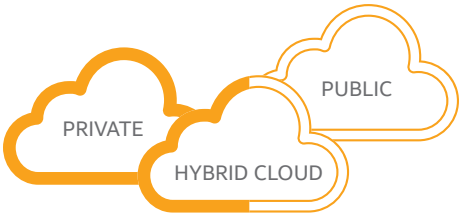
HYBRID CLOUD 101 BRIEF

Hybrid Cloud in Education

A Crash Course on Combining Private with Public Cloud Infrastructure



What is hybrid cloud? Hybrid cloud computing combines two cloud delivery models—typically private and public—to help educational systems gain more flexibility in cloud service delivery. This brief is a crash course on hybrid cloud for IT professionals in education. It covers why hybrid cloud matters to education, key architecture elements, unique technical challenges, application design considerations, and how Intel can help.

"Educational systems are embracing hybrid cloud for the same reasons as businesses."

The Path to Hybrid Cloud

Cloud technology is maturing and advancing rapidly, opening up new possibilities for more elastic private, public, and hybrid models. In education today, hybrid cloud computing is now seen as a more flexible way to use cloud computing by leveraging the complementary benefits offered by private and public clouds. These benefits include agility, cost-efficiency, security, and service availability. Hybrid clouds help balance capital and operational expenses so that budget-strapped educational systems can make optimal use of in-house resources while improving responsiveness to changing requirements.

Why Hybrid Cloud Matters to Educational Systems

Educational systems are embracing hybrid cloud computing for the same reasons as businesses.

- **Relieve burdened IT support**. There's always more work to do than there are people and funds to do it. Hybrid cloud gives schools the ability to flexibly extend or augment existing on-premises legacy systems and relieve the stress on their IT teams by moving some applications into public clouds.
- **Meet broad application needs.** A hybrid cloud lets IT optimize infrastructure to meet disparate needs and diverse workload requirements. For example, applications that require rapid deployment and/or rapid scaling may be perfect fits for public cloud. Some legacy systems such as human resources can be moved to a software-as-a-service (SaaS)[1] model. Other legacy applications may span clouds with, for example, the database layer running on premises in a private cloud and the front-end web layer running in a public cloud. With hybrid cloud, educational systems can dynamically move workloads between on- and off-premises environments based on specific performance or regulatory needs or for specific periods of time.
- **Protect sensitive student data.** Core systems containing sensitive student and school data can remain in-house and behind your firewall where you have the most control, helping you to safeguard student privacy and meet compliance regulations.

Intel: Making the Cloud Work for You

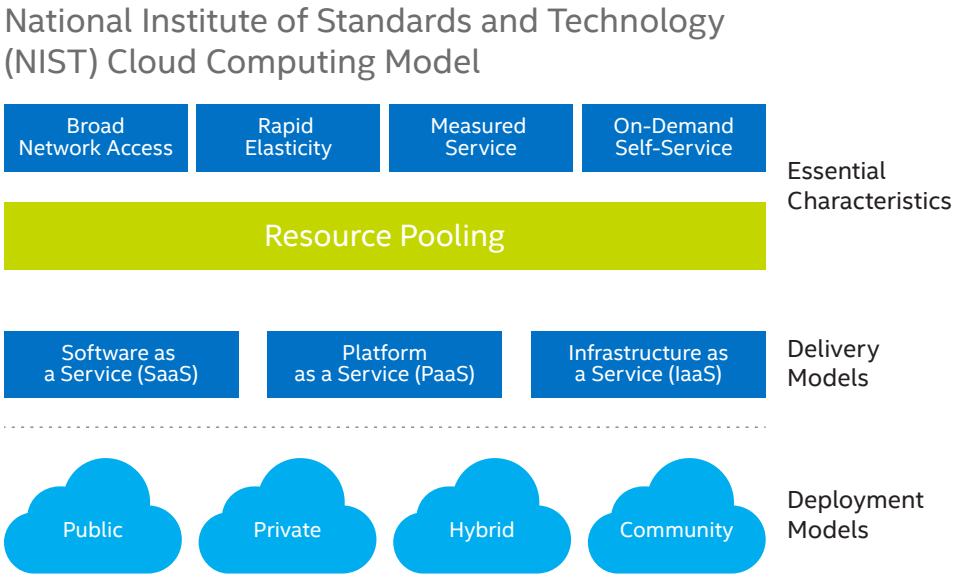
Intel wants to help you simplify delivery of cloud services so you can realize the full benefits of cloud computing in your unique education environment. As a first step, we recommend that you develop a cloud strategy that will meet your needs. Starting with your compliance requirements and educational goals, you can develop a flexible cloud environment that scales as your demand grows. Having a strategy will put you on a path to cloud maturity that enables you to expand your cloud usage to even more flexible models.

For more information on developing private cloud services, read *Ten Things IT Needs to Know about Cloud.*

- **Gain unparalleled agility**. As seen in the above examples, educational systems can use hybrid cloud computing to rapidly deploy and scale applications to meet pressing staff, student, or regulatory needs. Without the need to order and install infrastructure, school systems can often deploy applications in a matter of days or weeks and add capacity in minutes.
- **Save money.** Hybrid cloud also helps educational systems make the best use of precious budgets. By shifting certain workloads such as e-mail or collaboration sites to less-expensive public cloud environments, IT staff can pare down on-premises infrastructure costs (CapEx) and convert off-premises public cloud costs to operational expenses (OpEx) using a "build the base, rent the spike" deployment model. This helps educators achieve an optimal total cost of ownership (TCO). Public cloud environments are great ways to cost-effectively gain entirely new capabilities, such as disaster recovery facilities, that were previously out of reach for many educational systems.

Hybrid Cloud Architecture

Hybrid clouds combine two or more cloud deployment models—typically private and public—to enable data and application portability.

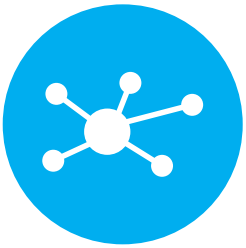


Based on *The NIST Definition of Cloud Computing.* National Institute of Standards and Technology Special Publication 800–145 (September 2011). http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

The National Institute of Standards and Technology (NIST) has described the essential characteristics of cloud computing as broad network access, rapid elasticity, measured service, on-demand self-service, and resource pooling. These characteristics can be achieved using three major cloud service delivery models: SaaS, PaaS,[2] and IaaS.[3] These delivery models can be implemented using several deployment models: public, private, hybrid, or community clouds.

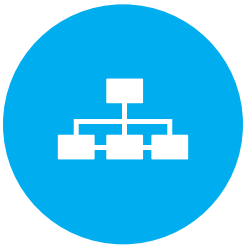
Technical Challenges Deploying and Maintaining Hybrid Cloud

While the benefits of hybrid cloud computing are appealing, the deployment models are still maturing, and combining two different cloud environments presents IT staff with a number of technical challenges.



Globally, school Internet access is growing, but remains under 10 percent in some developing countries.[4] Even the United States, where 99 percent of K–12 public schools and libraries are somehow connected to the Web, many lack high-speed connectivity.[5]

Integration of infrastructure and application environments. In a hybrid cloud, the ability to spin up virtual machines (VMs) for IaaS or combinations of IaaS and PaaS is ideally the same in both private and public cloud environments.



Infrastructure and application portability. A hybrid cloud infrastructure must be able to support the dynamic movement of VMs across both cloud environments.

Security. You must be able to maintain data security, compliance, and privacy rules when moving data into public cloud environments.

Monitoring and management across cloud environments. While monitoring is important for any cloud environment, visibility into system health across clouds and the ability to measure service availability to track against third-party service level agreements are critical.

Open, Extensible Cloud Ecosystems

The goal of hybrid cloud computing is to create an open, extensible cloud ecosystem that ties an educational system's cloud services (public and private) together to provide portability and interconnectivity. Open standards are key to creating such an ecosystem.

The Open Data Center Alliance has defined requirements for usage models in each cloud service layer for achieving interoperability and interconnectivity.

- **IaaS portability:** The ability to move physical or VM instances or images (complete with network connectivity and storage) between cloud environments over short or long distances while maintaining manageability, availability, security, and performance
- **PaaS interconnection and application portability:** The ability to move applications (and related logical data structures) between different PaaS environments—development and runtime—with cloud-aware applications that maintain attributes such as feature sets, configurability, and orchestration
- **SaaS interconnection and portability:** The ability to connect or transfer functionality and information via SaaS applications and to create mash-ups from multiple SaaS and non-SaaS applications via interfaces that exchange data smoothly

Cloud Management Platforms

A cloud management platform (CMP) is the integrated software that delivers service quality, security, and availability for workloads running in cloud environments. Your choice of platforms can simplify the management, automation, and orchestration of combined private and public clouds. CMP offerings vary widely in terms of platform maturity, architecture complexity, and capabilities.

At minimum, a CMP should provide direct user access to the system, self-service capabilities and interfaces, a workflow engine, automated provisioning, and metering and chargeback functionality.

Hybrid clouds typically offer more advanced capabilities, such as:

- Performance and capacity management
- Interoperability between private and public IaaS offerings
- Connectivity to and management of external clouds
- Application life-cycle support
- Back-end service catalogs
- Integration with external enterprise management systems

Cloud-Aware Application Design Considerations

If a hybrid cloud is in your future, you can design applications now to include capabilities that minimize portability issues down the road. Cloud-aware application development can take full advantage of underlying cloud infrastructure for improved scalability, performance, and resiliency. In designing cloud-aware applications, keep the following principles in mind:

- **Treat everything as a service.** Application capabilities should be partitioned into granular components that can be implemented, tested, and scaled separately.
- **Use representational state transfer (RESTful) APIs.** RESTful APIs enable easy reuse and scaling of application capabilities and shield applications from underlying technology implementations.
- **Separate compute and persistence.** Nothing is stored locally on the compute instance that is running the cloud application, providing deployment and scaling flexibility across environments.
- **Design for failure.** Although the goal is zero failure, in reality, components fail, services become unavailable, and latencies increase. Designing applications to gracefully survive failure enhances the user experience.
- **Architect for resilience.** An architecture designed with a focus on the mean time to recovery (MTTR) accepts imperfection and enables rapid identification and resolution of problems when they occur.
- **Operationalize everything.** All services should be easy to maintain and troubleshoot. Instrumenting, logging, and analyzing application behavior will lead to operational improvements.
- **Implement security at every layer.** A perimeter security approach is not sufficient in a public cloud. A more comprehensive approach is needed, such as encrypted transport into the cloud, secure coding and access control inside applications, and encryption at rest. The security of every API and data should be tested and analyzed.

Hybrid Cloud: Key Considerations in Protecting Student Data

Combining cloud environments brings new security challenges. This can be particularly challenging for educational systems trying to meet community and regulatory privacy demands for student data. Schools need to be able to monitor and prove that security policies are being set and enforced across cloud environments.

Below are some key considerations for designing secure hybrid clouds for schools.

- **Maintain your most sensitive workloads on premises.** Keep core systems such as those that contain personally identifiable student data behind a firewall in-house to provide the greatest control.
- **Integrate security into every layer of the cloud.** Assign security policies for infrastructure and applications to specific VMs based on their function. These policies are automatically assigned when that VM is provisioned.
- **Build security into server and client hardware.** Intel® based servers used in cloud data centers have built-in security features that enhance security by accelerating data encryption. When possible, use Intel based client devices, too, as the proliferation of client devices used to access cloud resources provides hackers with many potential access points and targets.
- **Deploy antivirus software.** Stealthy attacks on complex hybrid cloud environments are difficult to detect with traditional antivirus products. Cybercriminals use rootkit attacks to infect system components such as hypervisors, BIOS, and operating systems and can hide malware that operates in the background and spreads throughout a cloud environment. Deploy antivirus software that can protect the layers and elements unique to this environment.
- **Protect edge systems.** Edge systems that interact inside and outside the organization, such as web servers, portal servers, e-mail servers, bridges, and routers, represent a growing attack target.

How Intel Can Help

Intel makes technologies that are transforming education through the data center and the classroom. We're committed to simplifying cloud services delivery by:

- Providing guidance and resources to help you advance your cloud projects
- Helping you protect school data across cloud environments by delivering software- and hardware-assisted security capabilities

For more information on how you can implement hybrid cloud in your school system, visit **intel.com/cloud**.

Find out more about how Intel is helping educators use technology to inspire student success at **intel.com/education**.

1 SaaS: Software applications are made available through the cloud instead of installed and run locally.

2 PaaS: A cloud service model that delivers the hardware and software tools required for application development, including infrastructure and an operating system.

3 IaaS: The most basic cloud service offering, which provides virtualized computing resources (servers) on demand.

4 *Final WSIS Targets Review: Achievements, Challenges and the Way Forward.* International Telecommunications Union (2014). itu.int/en/ITU-D/Statistics/Documents/publications/wsisreview2014/WSIS2014_review.pdf

5 *When Students Can't Go Online.* The Atlantic (March 13, 2015). theatlantic.com/education/archive/2015/03/the-schools-where-kids-cant-go-online/387589/

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE. Intel disclaims all liability, including liability for infringement of any property rights, relating to use of this information. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Copyright © 2015 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

1015/MF/ME/PDF-USA

Please Recycle. 333177-001US