Cutter IT Journal

The Journal of Information Technology Management

Vol. 26, No. 3
March 2013

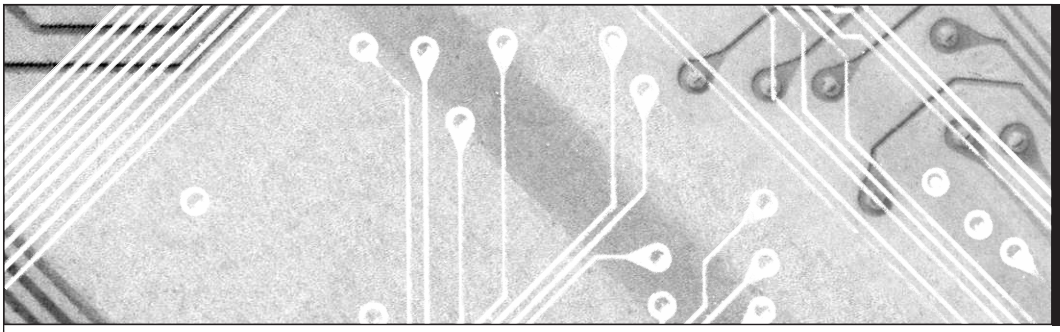
"Cloud service providers, the IT industry, professional and industry associations, governments, and IT professionals all have a role to play in shaping, fostering, and harnessing the full potential of the emerging cloud ecosystem."

— San Murugesan, Guest Editor

The Emerging Cloud Ecosystem:

Innovative New Services and Business Models

CUTTER CONSORTIUM



Cutter IT Journal

About Cutter IT Journal

Part of Cutter Consortium's mission is to foster debate and dialogue on the business technology issues challenging enterprises today, helping organizations leverage IT for competitive advantage and business success. Cutter's philosophy is that most of the issues that managers face are complex enough to merit examination that goes beyond simple pronouncements. Founded in 1987 as *American Programmer* by Ed Yourdon, *Cutter IT Journal* is one of Cutter's key venues for debate.

The monthly *Cutter IT Journal* and its companion *Cutter IT Advisor* offer a variety of perspectives on the issues you're dealing with today. Armed with opinion, data, and advice, you'll be able to make the best decisions, employ the best practices, and choose the right strategies for your organization.

Unlike academic journals, *Cutter IT Journal* doesn't water down or delay its coverage of timely issues with lengthy peer reviews. Each month, our expert Guest Editor delivers articles by internationally known IT practitioners that include case studies, research findings, and experience-based opinion on the IT topics enterprises face today — not issues you were dealing with six months ago, or those that are so esoteric you might not ever need to learn from others' experiences. No other journal brings together so many cutting-edge thinkers or lets them speak so bluntly.

Cutter IT Journal subscribers consider the *Journal* a "consultancy in print" and liken each month's issue to the impassioned debates they participate in at the end of a day at a conference.

Every facet of IT — application integration, security, portfolio management, and testing, to name a few — plays a role in the success or failure of your organization's IT efforts. Only *Cutter IT Journal* and *Cutter IT Advisor* deliver a comprehensive treatment of these critical issues and help you make informed decisions about the strategies that can improve IT's performance.

Cutter IT Journal is unique in that it is written by IT professionals — people like you who face the same challenges and are under the same pressures to get the job done. *Cutter IT Journal* brings you frank, honest accounts of what works, what doesn't, and why.

Put your IT concerns in a business context. Discover the best ways to pitch new ideas to executive management. Ensure the success of your IT organization in an economy that encourages outsourcing and intense international competition. Avoid the common pitfalls and work smarter while under tighter constraints. You'll learn how to do all this and more when you subscribe to *Cutter IT Journal*.

Cutter IT Journal®

Cutter Business Technology Council: Rob Austin, Ron Blitstein, Tom DeMarco, Lynne Ellyn, Israel Gat, Vince Kellen, Tim Lister, Lou Mazzucchelli, Ken Orr, and Robert D. Scott

Editor Emeritus: Ed Yourdon
Publisher: Karen Fine Coburn
Group Publisher: Chris Generali
Managing Editor: Karen Pasley
Production Editor: Linda M. Dias
Client Services: service@cutter.com

Cutter IT Journal® is published 12 times a year by Cutter Information LLC, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA (Tel: +1 781 648 8700; Fax: +1 781 648 8707; Email: citjeditorial@cutter.com; Website: www.cutter.com; Twitter: @cuttertweets; Facebook: Cutter Consortium). Print ISSN: 1522-7383; online/electronic ISSN: 1554-5946.

Subscription rates are US $485 a year in North America, US $585 elsewhere, payable to Cutter Information LLC. Reprints, bulk purchases, past issues, and multiple subscription and site license rates are available on request.

Opening Statement

by San Murugesan, Guest Editor

Driven by several converging and complementary factors, cloud computing is advancing as an IT service delivery model at a staggering pace. It is also causing a paradigm shift in the way we deliver and use IT. Its transformational potential is huge and impressive, and consequently cloud computing is being adopted by a spectrum of stakeholders — individual users, businesses, educational institutions, governments, and community organizations. It is also helping to close the digital (information) divide.

In order to successfully and fully embrace the promise of clouds, adopters must, of course, use one or more of the three foundational cloud services — software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS). But they must also address several other related factors, including security, privacy, user access management, compliance requirements, business continuity, and more. Furthermore, would-be adopters may have to use services from more than one service provider, aggregate those services, and integrate them with each other and with the organization's legacy applications/systems. Thus they need to architect a cloud-based system to meet their specific requirements. But special skills and experience are needed to do all this — skills that many cloud adopters wouldn't have.

To assist them in their transition to clouds and to allow them to focus on their core business, a cloud ecosystem is emerging that aims to offer a spectrum of new cloud services, including support services that augment, complement, and assist the popular SaaS, IaaS, and PaaS offerings. Investors, corporations, and startups are eagerly investing in promising cloud computing technologies and services in both developed and developing economies.

What are these new cloud services, and what are their business models? Who is offering them, and how do we evaluate them? How can cloud adopters leverage and benefit from these services? How will the cloud ecosystem emerge in the next five years? These are some of the key questions facing IT professionals, cloud adopters, and business executives.

A BIGGER CLOUD ECOSYSTEM IS ON ITS WAY

The cloud ecosystem has begun to evolve to provide a vast array of services that support and aid in deployment of cloud-based solutions for a variety of applications across many different domains. Further new types of cloud deployment, new models that deliver value-added services, and new costing and business models are on the horizon. Besides cloud service providers and users, many new players that perform niche roles are getting into the cloud arena. Cloud-based applications are being widely adopted by individuals and businesses in developed countries, and even more so in developing economies such as India, South Africa, and China.[1] Governments in many countries are promoting adoption of clouds by businesses, particularly micro, small, and medium enterprises, as well as individuals. As a result, a new bigger cloud ecosystem is emerging.

Besides cloud service providers and users, many new players that perform niche roles are getting into the cloud arena.

A current snapshot of the cloud ecosystem reveals:

- **Cloud services.** Besides the three foundational cloud services (SaaS, IaaS, and PaaS), new services include data as a service, desktop as a service, security as a service, APIs as a service, backup as a service, disaster recovery as a service, storage as a service, test environment as a service, testing as a service, data analytics as a service, and science as a service.
- **Cloud delivery models.** These models include public clouds, private clouds, hybrid clouds, community clouds, personal clouds, multi-tiered clouds, mega clouds (clouds of clouds), and microclouds.
- **Cloud players.** Among these players are cloud service providers, cloud service users, cloud enablers, cloud aggregators, cloud brokers, cloud auditors, cloud regulators, professional and industry

associations promoting and developing cloud standards, governments, cloud training providers, and educators and researchers.

The cloud ecosystem is poised to become bigger, more powerful, and more versatile. Clouds are becoming the "new normal."[2]

Invariably, the terms and conditions of cloud services are enforced (dictated) by the service providers and are distinctly provider-centric.

IN THIS ISSUE

To provide a glimpse of the emerging cloud ecosystem and the issues surrounding it, we present four articles in this issue that focus, in turn, on PaaS-IaaS integration, intrusion detection as a service (IDaaS), user-centric cloud service agreements, and the realization of an interoperable cloud ecosystem.

Integrated PaaS: A Game Changer?

Our first author, Beth Cohen, leads a consulting practice in IT infrastructure strategy. In her article, Cohen highlights the role of PaaS in developing and delivering applications better, faster, and cheaper and discusses the need for — and the benefits of — integrating PaaS with underlying IaaS cloud infrastructures. She also presents a good overview of the PaaS market, compares the key features of popular PaaS platforms, and outlines currently available integrated PaaS/IaaS tools. As development tools become easier to deploy and use on the clouds, Cohen argues, a bright future awaits for PaaS, with widespread adoption by both established enterprises and startups. Will integrated PaaS be a game changer for many businesses that need to maximize the benefits of cloud architectures? She believes it is likely.

Securing the Clouds: Intrusion Detection as a Service

Security of data and applications in the clouds continues to be a key concern for cloud users and regulatory agencies, and intrusion detection within the cloud environment is a major challenge for security analysts and cloud users. Intrusion detection systems (IDSs) have come to the rescue in many attacks, and our second article addresses the challenges involved in deploying an IDS. In their article, John P Veigas and K Chandra Sekaran of the National Institute of Technology Karnataka, India, present a brief overview of IDSs in general and in the cloud. They highlight major ongoing developments in this area, as well as their limitations. They then introduce "a framework for an intrusion detection and reporting service for cloud consumers based on the type of application and consumer's security needs" and walk us through their proof-of-concept.

The User-Centered Cloud SLA: Making It a Reality

When organizations consider adopting cloud services, they have legitimate concerns relating to performance, availability, privacy, disaster recovery, and notification of failures, and they want to know how they can ensure that these aspects are adequately addressed. Invariably, the terms and conditions of cloud services are enforced (dictated) by the service providers and are distinctly provider-centric. Users typically have very little say on these terms and conditions and must simply take them as given. Cutter Senior Consultant Claude Baudoin discusses this important and often neglected facet of cloud computing in our third article, "Cloud Ecology: Surviving in the Jungle." Briefly outlining the roles of the five key actors in the cloud ecosystem (as defined in the NIST Cloud Computing Reference Architecture), Baudoin highlights the drawbacks of current provider-biased contractual agreements. In an effort to achieve a better balance, and drawing on the findings of a Cloud Standards Customer Council (CSCC) working group,

UPCOMING TOPICS IN CUTTER IT JOURNAL

APRIL

Jim Sutton

Is Lean the Path to Releasing the Competitive Business Potential in Knowledge Work?

MAY

Lynne Ellyn

The Role of Coaching, Mentoring, and Team Building in High-Performance Teams

JUNE

Simon Woodworth

Mobile Security Challenges

JULY

Rebecca Herold

Big Data Privacy

he discusses what cloud users must request from providers. These needs range from clear document names and unambiguous expression of commitments to mutual agreement about auditing mechanisms. Baudoin's recommendations will help ensure that cloud consumers "don't get eaten alive, or at least [can] put up a good fight."

Enabling an Interoperable Cloud Ecosystem

As we begin to use clouds for a variety of applications across many different domains, their seamless use and transparent integration become essential requirements. To realize such an ecosystem, of course, much work remains to be done by ecosystem participants, and this demands good will, collaboration, and coordination among them. In our final article, Kathy Grise, Future Directions Senior Program Director with IEEE, offers recommendations to industry participants on what approaches and steps they must take to facilitate the cloud ecosystem's evolution if we are to realize this grand vision of interoperable clouds. She also emphasizes that the promise of the "interoperable cloud ecosystem is broad and pervades industries of all types, from the smart grid to the life sciences and beyond." As Grise points out, with the realization of this vision, a new era of cloud innovation and competition will emerge.

PARTING THOUGHTS

While hailing the features of current and potential new cloud services that help users adopt and tailor the services they use according to their needs, it is important to recognize that the new interlinked cloud ecosystem presents several challenges and concerns — particularly those relating to interoperability, the quality of service of the entire cloud chain, compliance, security and privacy of data, access control and management, the impact of service failures, and more. All these issues need to be addressed innovatively, and this calls for collaboration among various players in the cloud ecosystem, as Grise suggests. The good news is that investors, established corporations, and startups are eagerly investing in promising cloud computing technologies and services and are willing to collaborate (to an extent) to raise clouds to new heights. We hope to soon see a brighter, bigger, more collaborative cloud ecosystem that benefits all of its stakeholders and society at large.

This issue of *Cutter IT Journal* presents just a glimpse of this future cloud ecosystem. Innovations in technology, service delivery, and business models are needed to make further inroads and embrace the cloud ecosystem's untapped potential. Cloud service providers, the IT industry, professional and industry associations, governments, and IT professionals all have a role to play in shaping, fostering, and harnessing the full potential of the emerging cloud ecosystem. I hope this issue kindles all of our thinking and helps to make the grand vision of an all-encompassing, interoperable, collaborative cloud ecosystem a reality in the near future. I invite you to share your insights, ideas, and concerns about clouds with me at smurugesan@cutter.com.

ENDNOTES

[1]Murugesan, San. "Cloud Computing Gives Emerging Markets a Lift." *IT Professional*, Vol. 13, No. 6, November-December 2011, pp. 60-62.

[2]Murugesan, San. "Cloud Computing: The New Normal?" *Computer*, Vol. 46, No. 1, January 2013, pp. 77-79.

San Murugesan is a Senior Consultant with Cutter Consortium's Business Technology Strategies *practice, Director of BRITE Professional Services, and an Adjunct Professor in the School of Computing and Mathematics at the University of Western Sydney, Australia. Dr. Murugesan's expertise and interests include cloud computing, green computing, Web 2.0 and 3.0, and IT in emerging markets. He offers training programs on cloud computing and green IT. His recent book,* Harnessing Green IT: Principles and Practices*, is well recognized in professional and academic circles. He edits the new "Cloud Cover" column in the IEEE Computer Society's flagship magazine* Computer *and leads the publication group of the IEEE CS Cloud Computing Strategic Technology Committee. He is Associate Editor in Chief of the IEEE's* IT Professional *magazine and Editor of* Computer*. He is a fellow of the Australian Computer Society and a distinguished visitor of the IEEE Computer Society. Dr. Murugesan held various senior positions at Southern Cross University and the University of Western Sydney, both in Australia, and at the Indian Space Research Organization, Bangalore, India. Dr. Murugesan also served as Senior Research Fellow of the US National Research Council at the NASA Ames Research Center. He can be reached at smurugesan@cutter.com.*

Merging IaaS with PaaS to Deliver Robust Development Tools

by Beth Cohen

Building applications in the cloud is supposed to be easy. Point and click at a few buttons, and you're done, right? As many companies have found, however, there is an enormous gap between the true availability and maturity of cloud development tools and market hype. This is not entirely surprising given that the platform as a service (PaaS) concept is in its infancy. Bundling a suite of software development tools and layering them on top of a cloud-based virtual operating system image was something Microsoft only pioneered with its introduction of Azure in 2010.

Since then, vendors have been scrambling to address the lack of cloud-optimized tools with a plethora of emerging PaaS and cloud management products. The market and the technology are very immature, so these tools are still fragmented, costly, sophisticated, and complex. Even so, they are still worth pursuing if they are integrated into the underlying public or private cloud infrastructure, as that simplifies deployments and improves their effectiveness in the application development lifecycle.

In this article, we will discuss how PaaS is the key to maximizing the benefits of cloud architectures, allowing companies to create new business models for delivering services better, faster, and cheaper. Some of the issues and solutions we will explore include:

- PaaS tools maturity and the market landscape
- How PaaS can be used to facilitate the cloud software development lifecycle (SDLC)
- Why PaaS should be integrated into underlying infrastructure as a service (IaaS) cloud infrastructures, both public and private
- How PaaS can be used to create new business paradigms that benefit both business and consumers

PaaS tools will continue to mature over the next 12-18 months, and companies will soon realize their great value for speeding application development. Market pressure will grow to merge PaaS tools into the underlying IaaS, as users see the simplicity of taking this approach for building cloud-based applications. As the tools become easier to deploy and use, expect a bright future for PaaS, with widespread adoption in both established enterprises and emerging companies.

THE STATE OF THE PAAS MARKET

By now everyone from executive management on down has heard of or is using cloud computing services in one form or another. There are plenty of good reasons for the proliferation of cloud services in the enterprise setting. Unlike consumers and small businesses, which are often willing to sacrifice features and functionality in exchange for reduced costs, enterprises expect a full set of services and tools and are willing to pay for them — *if* they can prove their value.

Enterprises are purchasing infrastructure cloud services to replace their physical data centers not only to reduce costs (which it certainly does), but also to increase business agility and simplify operations. There has been a rapid adoption of business-focused software as a service (SaaS) products such as Salesforce.com for CRM and Netsuite for ERP in order to improve IT service delivery and allow for usage elasticity to match fluctuating business cycles. With an estimated US $14.5 billion in SaaS sales during 2012 alone (an increase of 17% from 2011), enterprise cloud service expenditures have been growing at an exponential clip with no slowdown in sight.[1] The added cloud features such as self-service, tighter role-based access control security, and governance capabilities are not lost on corporate management, which is always looking for ways to improve IT operational efficiencies and the bottom line.

What is missing from this rosy growth picture are the PaaS and cloud management tool suites, sometimes referred to as cloud orchestration. Adoption of cloud computing, particularly the ability to develop applications directly in the cloud by enterprise development teams, has been held back due to the lack of good development tools and the kind of comprehensive, feature-rich suites needed to support an enterprise

cloud portfolio. The emerging PaaS toolsets have seen less growth, principally due to their immaturity and unfamiliarity to consumers of cloud application development services, such as application developers and architects. While the PaaS segment is lagging the rapid expansion of the overall cloud market, it is poised for huge growth in the coming year or two.[2] As the tools become more standardized, more companies will adopt them as a viable approach to managing their cloud application portfolios.

To put things in context, a quick overview of the constantly shifting current PaaS market is in order (see Table 1). The earliest versions of integrated cloud application tools were generally associated with specific service providers, specifically Google (App Engine) and Salesfore.com (Force.com, Heroku). Amazon's Electric Beanstalk, another early entrant, is not really considered a true PaaS; think of it more as a deployment tool for EC2.[3] These initial tools were not designed to allow applications to migrate across clouds, nor were they ever seen as anything other than tools to attract developers to a given service provider. One could even argue that they promoted vendor lock-in rather than easing application migrations across cloud platforms.

Another consideration is that until very recently, many of the PaaS options offered limited support for multiple development languages or environments. For example, Heroku and Engine Yard are primarily Ruby-based systems, while CumuLogic offers only a Java environment. This scenario is rapidly changing, however, as more PaaS vendors realize that they will need to support the majority of standard programming environments if they are to remain viable in the long term. Consequently, such support is rapidly becoming the norm, at least among the more established companies.

Microsoft Azure

Microsoft Azure is probably the best example of a fully integrated PaaS development environment available on the market today. Since Microsoft pretty much invented the concept, in many ways it has had the chance to set the standard for others to aspire to. Azure delivers on that promise with a rich suite of tools for developing, testing, building, staging, and deploying cloud applications. The idea is to allow application developers to build and deploy applications in the same seamless environment.

As a technology, Azure has much merit, but as a rival to Amazon, customers have been less enamored of it. After vigorous lobbying by its core enterprise customers,

Table 1 — Key Feature Comparison of PaaS Platforms

Product	Supported Technologies	Development Status	Open Source	API	Console
AppFog	Java, .NET, Node.js, Ruby, PHP, Python	Production	Yes		Yes
AppHarbor	.NET	Production	No	REST API	No
AWS Elastic Beanstalk	Java, .NET, PHP	Production	No		No
CloudBees	Java	Production	No	CLI, REST API	Yes
Cloud Foundry	Groovy/Grails, Java/Spring, .NET, Node.js, Ruby Rails, Sinatra	Beta	Yes	CLI	No
Cloudify	C++, Chef, Groovy, Java, .NET, Node.js, Ruby, Spring	Production	Yes	CLI, REST API, Web	Yes
CumuLogic	Java, Spring	Beta	Yes	REST API	Yes
dotCloud	Java, Node.js, Perl, PHP, Python, Ruby	Production	No	REST API	Yes
Engine Yard	Node.js, PHP, Ruby	Production	No		Yes
Google App Engine	Java, Python	Production	No		Yes
Heroku	Ruby	Production	No	Yes	Yes
Jelastic	Java, PHP	Production	No	Yes	Yes
Microsoft Windows Azure	C#, Java, .NET, PHP, Ruby	Production	No	REST API, Storage	No
Red Hat OpenShift	Java, Java EE, Node.js, Perl, PHP, Python, Ruby	Beta	Yes	REST API	Yes
Relbit	MySQL, PHP	Beta	No	REST API	Yes
SalesForce Force.com	Apex, Visualforce	Production	No		No

Microsoft tweaked the pricing models and service offering throughout 2012. In another bow to market pressures, Azure now also supports Red Hat Enterprise Linux.[4] If even Microsoft supports the rival operating system, clearly the market has spoken, and Linux needs to be part of any serious PaaS toolkit. For now, Azure seems to be a niche player for serious Windows and .NET shops. Whether it can get back on track and appeal to a broader audience remains to be seen.

PaaS has taken great leaps forward since Microsoft's launch of Azure in 2010, both in terms of features and market uptake, but it still has a long way to go.

Linux-Based Offerings

On the Linux side of the house, there are many emerging options. Cloud Foundry, with the backing of VMware (which purchased the company in April 2011), is probably the most widely implemented of the open source PaaS products. Several vendors have taken the basic Cloud Foundry platform and added much-needed enterprise-ready features such as better security models and extensive support for the software development and deployment process — see, for example, ActiveState's Stackato product. Other products based on the Cloud Foundry platform and set of APIs include AppFog, which is using them to build an orchestration layer across public cloud providers. ActiveState, Tier 3, and Uhuru Software are all incorporating .NET into their products to appeal to the Microsoft shops that want to get out of the Azure ghetto. Janakiram MSV, chief editor of CloudStory.in, stirred up much controversy when he announced in August 2012 that Cloud Foundry was on its way to becoming the de facto PaaS standard.[5] That seems a bit premature given that the entire PaaS market is only about two years old, but Cloud Foundry plainly has a growing fan base.

I should also mention Red Hat's OpenShift, designed to appeal to those in the company's core enterprise customer base that want to use open source but like the traditional vendor support model. Just moving out of beta, the environment looks promising. OpenShift has a nice mix of rich development tools and some cloud and image management utilities wrapped around them, but it will be a while before the rough edges have been knocked off. Time will tell whether Red Hat can make up for its late market entry with a more advanced platform.

And the Rest

Moving on to the second-tier vendors with less enterprise name recognition, CloudBees has gotten lots of buzz with its Java-based offering. They and others such as CumuLogic, FeedHenry, and AppsFirst offer more affordable PaaS platforms in various flavors designed to appeal to emerging companies that are primarily building their applications directly in the public cloud. These tools are sold using the SaaS model, without the orchestration layers and other management features that are included in more integrated packages. AppsFirst does have some nice built-in SDLC tools similar to enterprise system workflow engines, in addition to some monitoring tools, but they are rudimentary when compared to the more comprehensive features of a fully integrated package such as ServiceMesh's Agility Platform. On the periphery are a laundry list of startups whose products may or may not ever see the light of day, such as PHP Fog, dotCloud, and BitNami, to name just a few that still have active websites in March 2013.[6] The race to grab market share is on, with the number of new entrants seeming to multiply monthly. The venture capital (VC) community is actively investing in many of these nascent companies in hopes of striking it rich with another Cloud Foundry.

PaaS has taken great leaps forward since Microsoft's launch of Azure in 2010, both in terms of features and market uptake, but it still has a long way to go. As the market continues to mature over the next year or so, expect to see the cycle of consolidation and emerging new vendors continue to play out. VC companies are investing in promising opportunities while larger established vendors, such as IBM and VMware, are on the lookout to purchase what they consider the most likely emerging technologies to incorporate into their cloud tool portfolios. There are already a few leaders in the pack that are creating truly integrated PaaS/IaaS environments, but they might be better categorized as technology visionaries at this point in the hype cycle.

A PAAS AND IAAS MASHUP

As we can see, the existing available PaaS tools have plenty of features that will appeal to any developer working in a cloud environment, but future PaaS tools need better coordination across internal and public cloud environments, fully integrated SDLC orchestration, and cloud brokering tools rolled into one seamless package so that companies can take full advantage of their benefits. Some emerging PaaS vendors are addressing their customers' needs more holistically by

creating products that incorporate a full suite of tools to provide end-to-end application management, from idea to staging and on to support of the production environments. Full integration will help foster better SDLC and business delivery models by maximizing architecture abstraction, encouraging standards adoption, and reducing infrastructure complexity and costs. As cloud tech specialist Dustin Amrhein observes, "Adopting a converged/integrated approach to IaaS and PaaS will not be easy,"[7] but it should be the ultimate goal.

Azure would seem to be the poster child for a fully integrated system. As an end-to-end, integrated, Microsoft-based cloud development platform, Azure can be a very appealing solution. However, since it has few cloud infrastructure management tools, little or no access to the underlying IaaS, and cannot be deployed in a private cloud, it falls short of what is needed to take full advantage of cloud computing.

In contrast, the ServiceMesh Agility Platform offering was originally created as a suite of data center management tools similar to IBM Tivoli. It has since been transformed into a full complement of software development, orchestration, and operational management tools. The product is designed to be modular so it can be implemented as a company gains confidence in its ability to deliver value to the development cycle, but the steep price of entry and complex deployment process make it a viable option for only the largest enterprise development shops.

For companies that are looking for other PaaS/IaaS integrated solutions, the options are more limited. VMware has vFabric Cloud Application Platform, which incorporates SpringSource development tools integrated into the VMware virtualization platform. It is a great virtualization platform, but the self-service and automation tools that mark it as a true cloud are still works in progress. It remains to be seen if VMware will be able to seamlessly incorporate Cloud Foundry into its existing infrastructure management toolkits to round out the suite.

On the open source side of things, initial efforts were strictly aimed at getting the infrastructure components right, including the install frameworks. This left a number of needs unaddressed, including the integration of PaaS tools and management tools. The good news is that the community has now realized the existence of those gaps and is working to fill them. Moreover, vendors (some of which participate in the open source community in addition to delivering proprietary products) have their own initiatives to address these needs. Here are a few key examples of this evolution:

- The OpenStack community is actively discussing how to integrate PaaS tools into the OpenStack IaaS platform, and a project is underway to support Red Hat's Open Source PaaS, OpenShift.
- OpenStack continues to lack management tools, but as the project matures, more tools will emerge to make deployment easier.
- PaaS vendors, such as ActiveState, are actively working on integrating their products with OpenStack.
- Cloudscaling has decided to partner with ActiveState in the Stackato program.
- There is growing support for Cloud Foundry by a number of vendors. For example, Piston Cloud will be including Cloud Foundry to take advantage of the latter's BOSH API project.[8]

Companies want applications that work, not just infrastructure that gathers dust in the data center.

The reason so few integrated products have yet emerged is the great difficulty in integrating all the various components into a viable solution. Other vendors actively working to offer integrated solutions include IBM with its SmartCloud tool suite and Red Hat with its Cloudforms, which hopefully will be able to combine its cloud orchestration management utilities with OpenShift for the development tools component. There are a tiny handful of VC-backed companies working on products that take a more holistic approach to building tools for cloud infrastructures, but most of them are still in stealth mode. Given the effort of integrating all the moving parts, it should be interesting to see what comes out. Table 2 lists the capabilities of the integrated PaaS/IaaS tools available today.

At the end of the day, the contents of the virtual machine images, service catalogs, and application-facing tools really do matter. Companies want applications that work, not just infrastructure that gathers dust in the data center. Businesses need complementary IaaS and PaaS, and the only way to achieve this goal is to break down the artificial wall between the two development communities.

Table 2 — Integrated PaaS/IaaS Tools

Product	PaaS	Orchestration	Cloud Broker	SDLC
IBM SmartCloud	X	X		X
vFabric	X	X		X
ServiceMesh	X	X	X	X
Microsoft Windows Azure	X		X	
Red Hat CloudForms		X	X	

At the infrastructure level, expect to see more comprehensive suites that roll brokering, orchestration, and image lifecycle management into one framework. This simplifies the development-to-production process by providing more automation and self-service tools than ever. These new tools benefit the enterprise the most because they address larger companies' interest in building private clouds rather than relying solely on the public offerings. Private clouds allow companies the luxury of full control over their environments and applications. This is a particularly attractive proposition to companies that have strict security or regulatory requirements.

On the application side, PaaS offers more SDLC workflow, tighter governance and controls of the development tools, and more agile tooling for development and automated testing frameworks. Everyone wins: developers get the resources they need instantly, business can respond faster to demand for new applications, and IT doesn't get blamed for holding up the queue.

LEVERAGING PAAS: NEW BUSINESS MODELS

PaaS as a concept for delivering development tool suites is compelling. It makes logical sense to focus on the application development piece by making the infrastructure component transparent by layering a PaaS on top of a robust IaaS. For most businesses, what really counts are the applications and how fast they can be launched to catch the next business opportunity. To achieve this goal, there is increasing interest in using cloud-integrated toolsets and platforms that help developers remain focused on building the applications that, at the end of the day, are what deliver the goods and pay the bills.

PaaS development environments allow savvy companies to deliver applications more effectively by enforcing development tools standards, making component reuse simpler by creating a true SOA framework, and improving the management of the development lifecycle. These tools can be used to enforce QA processes, code reviews, operational handoffs from development to production, and a host of other methods to improve the messy process of building working software.

Corporate governance and security are also concerns that can be addressed by an enterprise-grade PaaS such as ActiveState's Stackato, which has incorporated a full role-based account system that allows fine-grained control over developer and administrative access to the systems and applications. These types of features are increasingly becoming a standard part of the PaaS toolset.

INTEGRATED PAAS: A GAME CHANGER?

A typical enterprise has 3,000-5,000 applications to manage across its IT portfolio, on top of a tangle of systems and infrastructure. It is obvious why IT application portfolio management is often seen as a costly nightmare. The PaaS environment and tools can be used to rationalize a company's IT portfolios by quickly identifying the applications that are making the most impact, thereby reducing the cost of maintaining legacy systems that are no longer returning value. Many PaaS tools have capabilities for managing the production environment as well, with sophisticated rule sets that can automatically take advantage of the elasticity of the cloud for applications with spiky usage patterns, such as a time-reporting application that could expand to meet "payroll Monday" usage demands. For companies

that are only leveraging a public cloud provider, a tool that manages just software development might make more sense, but often PaaS tools are used not only to manage development, but also to orchestrate the end-to-end lifecycle.

Even taking a comprehensive approach to PaaS is not a panacea; there are barriers that need to be taken into consideration when contemplating a move to a PaaS development environment. The available integrated PaaS tools can be difficult to set up in a corporate environment. Often there is an incumbent set of tools that the development team is already comfortable with. Depending on the sophistication of the tools being replaced and the skills of the development team, this can be an expensive investment for a larger company, with a payback time measured in years. Another issue is confusion as to how the integrated products work at more than one level of the cloud architecture stack, including infrastructure, platform, and, of course, applications. In a traditional enterprise IT shop with a high degree of separation of duties, taking an integrated approach to application deployment can be a hard sell.

That said, PaaS software development tools are changing to meet the new demands for automated elasticity, sophisticated rules engines, orchestration across heterogeneous clouds, and support for a different SDLC model. By adopting a PaaS environment that addresses the need for cloud-ready tools, a company can respond to market needs and business objectives far more easily than ever before.

CONCLUSION

PaaS has come a long way in the past two years, but it still has a ways to go before it becomes a standard platform for the application development and production management processes in most companies. Even so, integrated PaaS is a game changer for many businesses that need to maximize the benefits of cloud architectures. These tools allow companies to create new business models for delivering services better, faster, and cheaper. To achieve this goal, there needs to be full integration of the SDLC, orchestration, and cloud brokering tools.

ENDNOTES

[1]Swann, Allan. "Software as a Service to Reach $14.5B in Revenue in 2012." *Computer Business Review*, 27 March 2012 (www.cbronline.com/news/software-as-a-service-to-reach-27-03-12).

[2]Blaisdell, Rick. "Cloud Computing Market Size — Facts and Trends." *Rickscloud*, 27 February 2012 (www.rickscloud.com/cloud-computing-market-size-facts-and-trends).

[3]Oliver, Andrew C., and Lifford Pinto. "Which Freaking PaaS Should I Use?" *InfoWorld*, 8 October 2012 (www.infoworld.com/d/cloud-computing/which-freaking-paas-should-i-use-204189?page=0,0).

[4]Clarke, Gavin. "Microsoft's Magic Bullet for Azure: Red Hat Linux." *The Register*, 26 January 2012 (www.theregister.co.uk/2012/01/26/windows_azure_money_maker_not).

[5]MSV, Janakiram. "Is Cloud Foundry on Its Way to Become the De Facto PaaS Standard of the Industry?" CloudStory, 2 August 2012 (http://cloudstory.in/2012/08/is-cloud-foundry-on-its-way-to-become-the-de-facto-paas-standard-of-the-industry).

[6]Hu, Andy. "List of Current and Upcoming Cloud Platforms." *Andyland*, 11 October 2011 (http://blog.huchunhao.com/current-and-upcoming-cloud-platforms).

[7]Amrhein, Dustin. "The Convergence of IaaS and PaaS." Ulitzer, 7 July 2011 (http://dustinamrhein.ulitzer.com/node/1899117).

[8]Mueller, Diane. "Cloud Distros & PaaS: Another Lightbulb Moment." devopsANGLE, 28 February 2013 (http://devopsangle.com/2013/02/28/cloud-distros-paas-another-lightbulb-moment).

Beth Cohen is a Senior Cloud Architect for Cloud Technology Partners, Inc., a firm focused on delivering solutions to help enterprises leverage the efficiencies of cloud architectures and technologies. Some of Ms. Cohen's recent projects include: architecting a new infrastructure platform to support a SaaS software implementation; building the cloud infrastructure for a major international electronics company in support of consumer-facing applications that will scale to millions of users; creating migration architectures and processes to move over 11,000 applications into the cloud for a major international telecom; building the operational systems to support a cloud-based portable medical records service designed to securely and transparently store millions of records; and creating a unique cloud-based data protection service that delivered cost-effective data protection, disaster recovery, and business continuity solutions for the SMB market. Previously, Ms. Cohen was the Director of Engineering IT for BBN Corporation, where she was involved with the initial development of the Internet, working on some of the hottest networking and Web technology protocols in their infancy. She can be reached at beth.cohen@cloudtp.com.

.

Intrusion Detection as a Service (IDaaS) in an Open Source Cloud Infrastructure

by John Prakash Veigas and K Chandra Sekaran

Cloud computing processes and stores an organization's sensitive data in a third-party infrastructure. Monitoring these activities within the cloud environment is a major task for security analysts and the cloud consumer. Cloud service providers may suppress the security threats detected in their infrastructure, hiding them from consumers. Our goal should be to decouple intrusion detection system (IDS)–related logic from individual application business logic and adhere to service-oriented architecture standards.

In this article, we offer an overview of IDSs and the work that is being done to adapt them to the cloud. We then introduce a framework for an intrusion detection and reporting service for cloud consumers based on the type of application and the consumer's security needs. Cloud consumers can choose the desired signatures from this framework to provide adequate protection for their applications running in the cloud.

A BRIEF OVERVIEW OF IDSs

Advances in recent decades in the areas of distributed computing, grid computing, and virtualization techniques have led to the cloud computing industry model, which delivers everything as a service. Today clients are capable of running their applications remotely in the cloud. For cloud users, it is extremely important to feel comfortable that their data, processes, software, and applications are running safely in the cloud environment. As organizations and individuals move their applications to the cloud, monitoring these applications for intrusions is a major concern.

An IDS is a software or hardware tool that detects intrusions into the system being protected. The intrusion can occur from inside or outside the network to which the protected system is connected, and it can be intentional or accidental. An intrusion is an unauthorized or unwanted activity that puts at risk various security services such as confidentiality, integrity, and/or availability of the information or computer resource.

As shown in Figure 1, the basic architecture of an IDS consists of three main modules: (1) information collector module, (2) analysis and detection module, and (3) response module.[1] The information collector module contains information extractor and event generator submodules. As its name implies, the information extractor extracts information from the raw data, which it then passes to the event generator. The raw data can come from the operating system, network traffic, or an application-generated log. The event generator creates the events for the analysis and detection module, which contains analyzer, system information, detection, and policy submodules. The analyzer analyzes the events with system information and passes them to the detection module, which matches the traffic with the rule sets in the policy repository. Suspicious traffic will be moved from the detection module to the response module for appropriate action. A log will be generated, and the response module will generate the alert.

Enterprises can use IDSs to detect and identify unauthorized use of computing resources and computer networks with a large number of nodes. In a traditional IDS, due to the static nature of the monitored systems, the policies tend to be static since the node groups have stable requirements that have been identified over time. Traditional IDSs do not have a facility to perform selective and dynamic update of intrusion signatures in the cloud, where consumer applications reside.

According to NIST, IDS technologies are primarily categorized by the types of monitored events and the ways in which they are deployed:[2]

1. **Network-based** — monitors particular network segment traffic or devices and performs network analysis to identify suspicious activities
2. **Wireless** — monitors wireless network traffic and performs network analysis to identify suspicious activities
3. **Network behavior analysis** — identifies unusual traffic flows and network policy violations

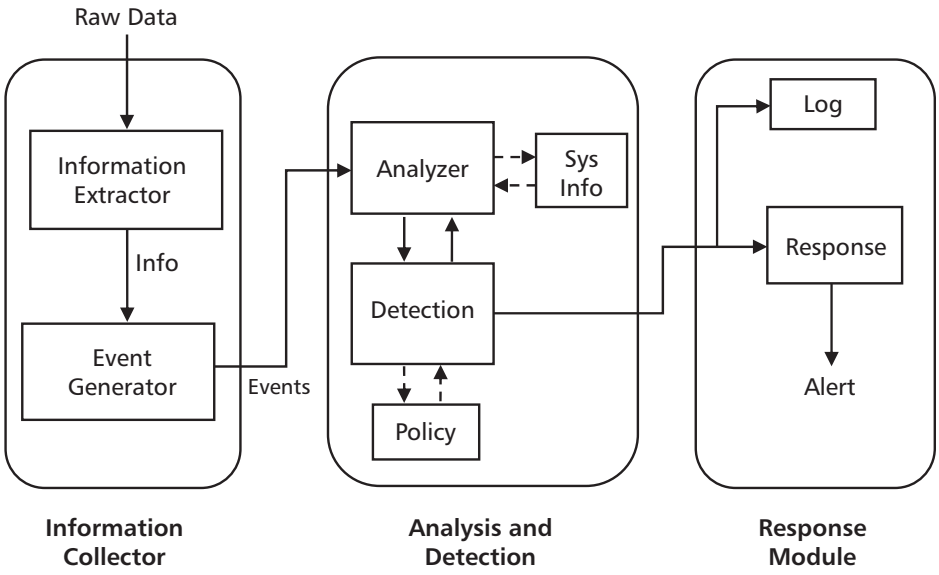


Figure 1 — Basic architecture of an IDS.

4. **Host-based** — monitors and analyzes features of a single host and the events occurring within that host for suspicious activity

In the last two decades, researchers have conducted many studies on technologies, architectures, and methodologies that can increase IDS effectiveness.[3, 4] We will discuss some of these now.

IDSs IN THE CLOUD

To address the issue of intrusion detection within cloud computing environments, multiple research efforts are being carried out. These efforts can be divided between those that detect intrusions against the cloud itself and those that detect attacks targeting individual machines inside the cloud.

Amongst the different published works in this field, Kleber Vieira and his colleagues at the Federal University of Santa Catarina, Brazil, have proposed the Grid and Cloud Computing Intrusion Detection System (GCCIDS),[5] which is designed as an audit system for attacks that the networks and hosts cannot detect. Each node of the GCCIDS identifies local events that could represent security violations and alerts the other nodes. Each individual IDS cooperatively participates in intrusion detection. The system is designed for the purpose of detecting intrusions against the cloud and is not intended for use by clients, nor can the protection be customized by the cloud's clients. Therefore, the GCCIDS doesn't support the requirements of a subscription-based intrusion detection service.

Amir Vahid Dastjerdi from the University of Melbourne and Kamalrulnizam Abu Bakar and Sayed Gholam Hassan Tabatabaei from the Universiti Teknologi Malaysia have applied an agent-based IDS as a security solution for the cloud.[6] The model they propose is an enhancement of the Distributed Intrusion Detection System Using Mobile Agents.[7] The model basically works by sending an investigative task-specific mobile agent to every virtual host that has generated the same type of alert. The mobile agents can then help to verify attacks and later assist in banning the compromised virtual machines (VMs) and separating them from the network. The system is mainly designed to protect the network's resources and cannot be customized as a service.

Aman Bakshi and Yogesh B. Dujodwala from SRM University, India, have proposed another cloud intrusion detection solution;[8] its main concern is to protect the cloud from distributed denial-of-service (DDoS) attacks. The model uses an installed IDS on the virtual switch, and when a DDoS attack is detected, the attacking network gets blocked and the victim server is transferred to another virtual server. This solution blocks future connections from the attackers and redirects legitimate users to the new virtual server. As stated above, the model helps to protect the cloud itself, not the cloud clients, who in turn don't have any kind of authority over the IDS being used.

Researchers from Multimedia University Malaysia, Chan Gaik Yee and his colleagues,[9] have proposed an IDS designed specifically to detect SOAP/XML/SQL-related intrusions against Web services. The Web service they suggest cannot be controlled by consumers

and aims at protecting the Web service itself. Thus we can consider this another IDS designed to protect the cloud, which is usually the location where Web services are hosted.

Perhaps the most relevant research is the work of Sebastian Roschke, Feng Cheng, and Christoph Meinel of the Hasso-Plattner-Institute (HPI) and University of Potsdam,[10] who have proposed an intrusion detection Web service based on the VM-based IDS.[11] These researchers have developed a general Web service for intrusion detection, which consists of separate IDS sensors (which can be from different vendors) for each virtual host. To enable the collection and correlations of alerts from the different IDS implementations, an "event gatherer" works as a medium for standardizing the output from the various sensors as well as realizing the logical communication. Cloud users can have access to both the applications and the IDS sensors. They can access the sensors, configure or modify IDS rule sets, modify detection thresholds, and review the alerts. As promising as this sounds, though, a Web service based on the VM-IDS approach is not preferred for two reasons. The first is the large consumption of computing resources, since every virtual application, platform, or host needs a separate VM-based IDS. The second is that it can be dangerous to allow users to fully control and manage the IDS hosts, as a user may turn out to be malicious.

Another recent and significant contribution to this field is the work of Claudio Mazzariello, Roberto Bifulco, and Roberto Canonico of the University of Napoli Federico II, Italy,[12] who have proposed a model for detecting DoS attacks against the Session Initiation Protocol (SIP). The model is limited to detecting SIP flooding attacks and falls primarily into the category of IDSs designed to protect the cloud itself.

Hisham A. Kholidy and Fabrizio Baiardi, of the Università di Pisa, Italy,[13] have proposed a Cloud Intrusion Detection System (CIDS) framework to define a proper defense strategy for cloud systems. CIDS is a scalable and elastic solution with a peer-to-peer (P2P) architecture with no central coordinator, thus avoiding a single point of failure. CIDS has two P2P deployment models: hybrid P2P and pure P2P. To increase flexibility and portability, the middleware — where the framework resides — can be installed in distinct cloud and grid systems. To increase attack coverage, CIDS integrates knowledge-based and behavior-based approaches and monitors each node to identify local events that could represent security violations. When an attack occurs, CIDS alerts other nodes. CIDS exploits the distinct execution spaces of a VM manager to separate the IDS from the system under monitoring so that the intrusion detector components become invisible and inaccessible to intruders. CIDS includes an audit system to discover those attacks that network-based and host-based systems cannot detect. It also parses and summarizes a high-intensity number of alerts fired by the network IDS component to prepare a readable report for the cloud administrator.

DRAWBACKS TO THE EXISTING SYSTEMS

Current research into intrusion detection for grid and cloud environments is limited to addressing the requirements for intrusion detection as part of the security infrastructure. Following are some of the disadvantages of the existing cloud scenarios:

- **Cloud provider–centric IDS.** Most existing systems carry out monitoring for possible intrusions on the cloud provider's infrastructure. Even if a serious vulnerability or security loophole exists, the cloud provider may still hide it from the cloud consumer.
- **No customization for cloud consumers.** In most of the proposed systems, there aren't any customizable security settings for possible intrusion in cloud consumers' applications. Either cloud consumers have to rely on the security provided by the cloud provider, or they need to create their own security strategy for their deployed applications.
- **Redundant deployments.** In some proposed systems, the intrusion detection sensors are deployed at too many places in the cloud infrastructure. This will reduce the performance of the overall system.
- **Unknown service-level agreement (SLA) violations.** There is no adequate monitoring system to detect and report security-related SLA violations in the cloud infrastructure.

A PROPOSED FRAMEWORK FOR SERVICE-ORIENTED INTRUSION DETECTION IN THE CLOUD

Given the aforementioned drawbacks to current IDS solutions in the cloud computing environment, we propose an Intrusion Detection as a Service (IDaaS) framework, which is a network-based IDS for the cloud that uses a signature- and subscription-based service. The subscription charges can be based on the number of rules the consumer subscribes to for the intrusion detection service. The user can select different levels of service: basic, intermediate, and advanced.

The high-level framework is shown in Figure 2. The software sensors are deployed in a cloud cluster, which collects the traffic and passes it to the intrusion detection engine (IDE). The cloud cluster contains multiple nodes in which VMs are running. All the traffic is allowed only through the cluster controller. All the signature details and subscription details are stored in the global master, which is a global repository of all the details of the subscriber. The cluster rule repository contains recently used rules; as a local repository, it reduces the burden of moving the rules dynamically. Depending on the cloud user's application, the rules subscribed by the cloud user will be dynamically loaded to the IDS rules engine. The following components make up the proposed framework:

Global Master

This component is made up of three submodules:

1. **Signature** — consists of details of all the available signatures, which are grouped into different categories
2. **Subscription** — consists of details of the consumers and their subscriptions
3. **Alert** — consists of details about the malicious activity detected by the IDS

The global master is useful in case the cloud provider provides infrastructure in a geographically separated area.

Local Repository

The local repository consists of details of signatures available at the cluster node at a given point in time. It also stores the event and alert details. When a cloud controller decides that a particular consumer application needs to be deployed on the nodes in the cluster, it will search the local repository for the signature subscribed by the consumer. If it is found, the IDE will use the signature; if not, it will load a fresh copy of the signature from the global master. If a consumer is no longer using the VM up to a specified time limit, then those signatures are deleted from the local repository. The time limit can be decided based on how frequently the consumer uses the VM.

Intrusion Detection Engine

The IDE dynamically loads the signatures based on the consumer's application running VMs in the cluster. The IDE is deployed on the edge of the cluster, where it connects to the external world. The traffic is monitored against the rules/signature. If any part of the traffic matches any of the rule set, the IDE will generate an

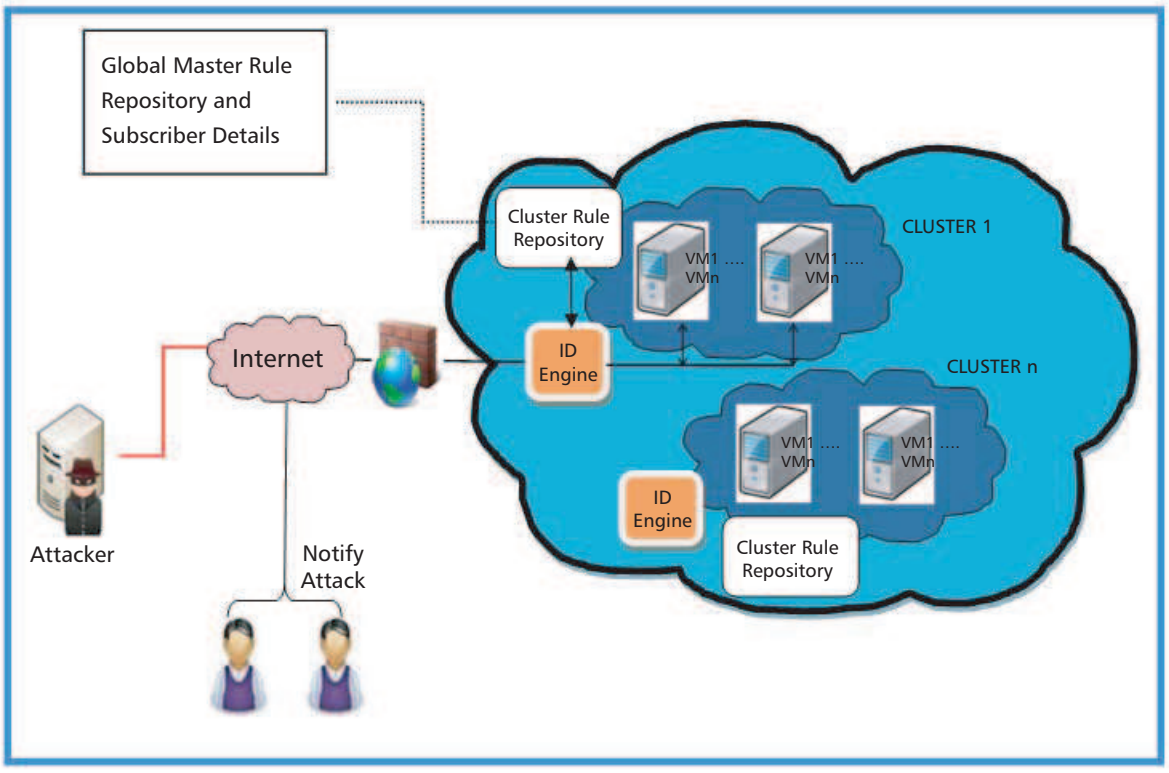


Figure 2 — High-level proposed framework for IDaaS.

alert and log the details in the local repository. It sends a notification to the consumer and then updates the details in the global master.

Hosts

Hosts are the individual nodes inside the cluster in which VMs are deployed. VMs are allocated to the cloud consumer based on demand.

Cluster Controller

The cluster controller is the node that manages the number of other nodes in the cloud infrastructure. In this framework, the IDS is deployed on the cluster controller.

Web Interface

Through the Web interface, the IDaaS administrator can add new rules and signatures. IDaaS consumers are provided with a Web interface, through which they can subscribe to the desired category of signatures and view attack details, if any. Figure 3 shows the details of the IDE and its interactions with other subcomponents.

PROVING OUR CONCEPT

We implemented our framework's proof-of-concept using the Eucalyptus Cloud IaaS environment. Eucalyptus IaaS will work similar to Amazon Web Services.[14] We have configured Eucalyptus in "managed mode,"[15] which mimics Amazon Elastic Compute Cloud (EC2). We have created multiple clusters, each of which has several nodes, and placed a local repository of signatures at the cluster controller. We have used Xenon Servers as node controllers. In our implementation, Snort IDS[16] serves as the intrusion detection system.

We have also provided a user interface through which the cloud consumer can subscribe to the different categories of signatures available. Consumers' applications are deployed on the VMs in the node controller of Eucalyptus. We have created different categories of signatures, each of which consists of a list of rules that filter the traffic and, if a certain pattern is found, alert the subscriber, storing the alert in the database. MySQL database has been used to store consumer subscription details. The administrator has a provision for adding new categories of rules, which contain lists of signatures that belong to various categories of vulnerabilities that specific organizations may face. Of the possible categories of vulnerabilities, we used the following ones for experimental purposes:

- Internet Control Message Protocol (ICMP) flooding
- Backdoor attack
- SQL injection
- DDoS attack

Figure 4 shows a snapshot of a consumer, John, subscribing to various categories of intrusion detection services. Based on John's choices, monitoring for ICMP flooding and backdoor attack is performed. Two attacks were detected by the IDS deployed on the cluster node of Eucalyptus. Figure 5 shows the alerts that

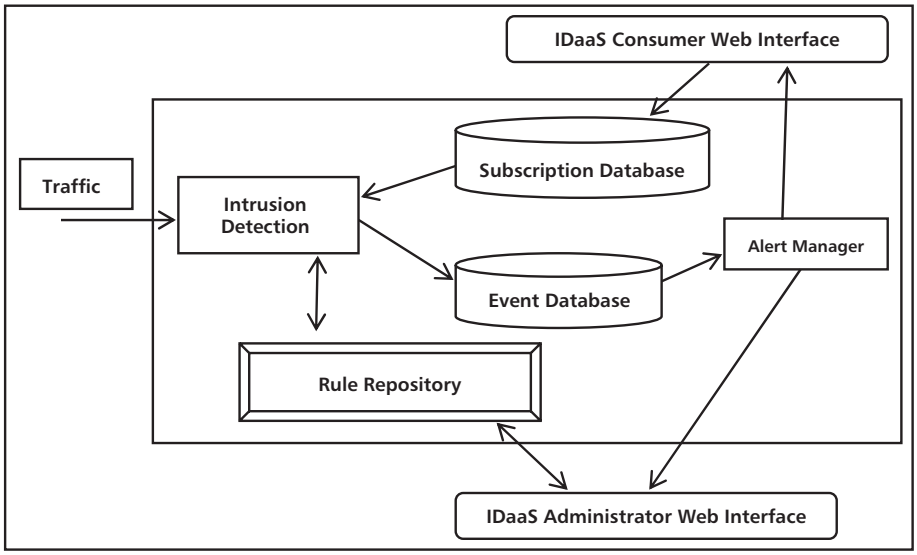


Figure 3 — The IDE and its database interfaces.

are displayed to John, who may access the alerts from anywhere by just logging into his account.

Analysis and Advantages

Our approach requires the minimum amount of installation and configuration without sticking to a single-vendor IaaS such as Amazon EC2 or Google. It is flexible enough to adapt to any other IaaS provider. This approach provides cloud consumers with more transparency into their applications running on the cloud infrastructure, which increases their level of trust. Even cloud providers may not be able to suppress security vulnerabilities in their infrastructure. We effectively used available open source software and cloud infrastructure, so no cost was involved for licensing.

FUTURE ENHANCEMENTS

An IDS is a crucial part of defensive operations that complements static defenses such as firewalls. Essentially, IDSs search for signs of an attack and flag intrusions when they are detected. In this article, we have proposed a new framework for intrusion detection as a service. We have also implemented this framework

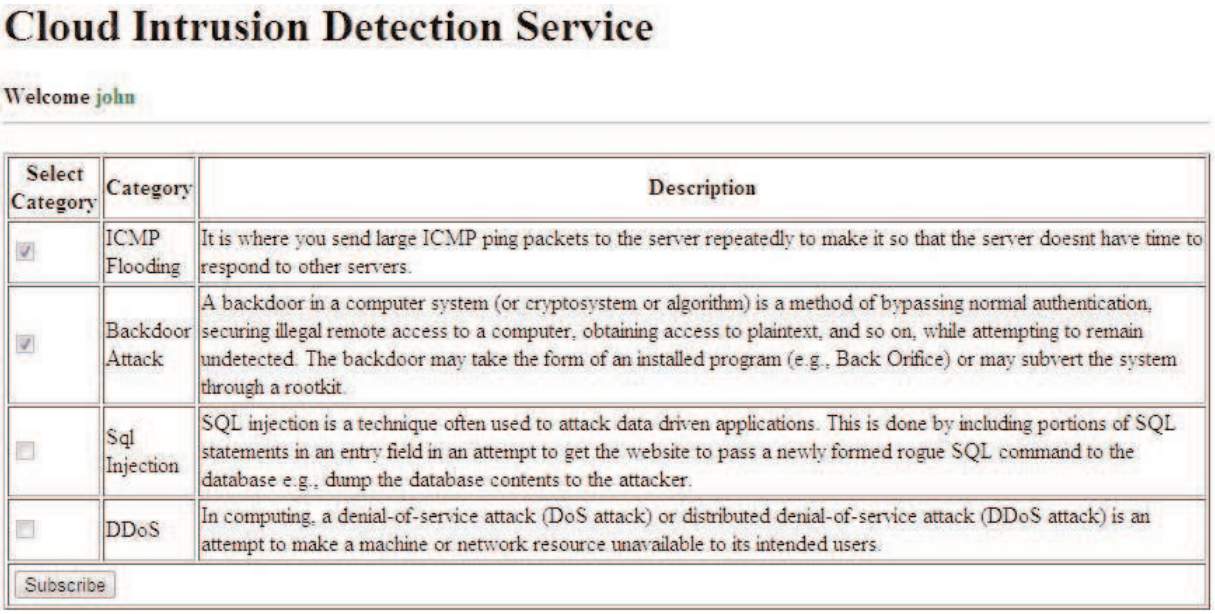


Figure 4 — A consumer subscribes to the intrusion detection service.

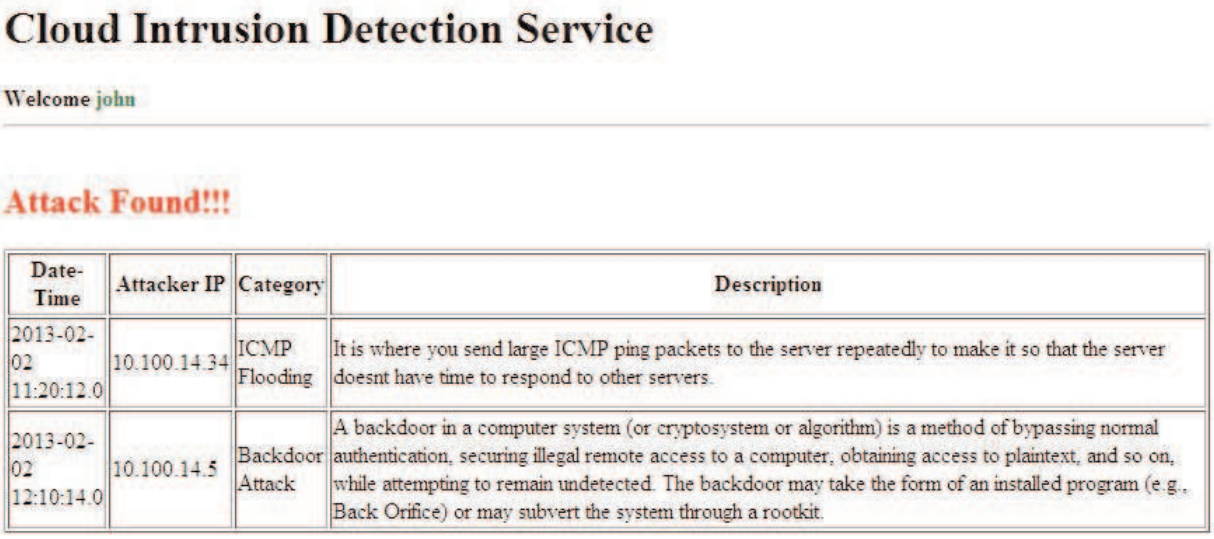


Figure 5 — The security alerts displayed to the consumer.

in a service-oriented manner, so that consumers can customize their security requirements in order to protect their applications running on the cloud.

As of now, the rules/signatures in our framework are not loading from the global master, so the required rules can be synchronized with the local cluster repository only. In addition, the performance of the system needs to be tested with a large number of nodes and in a real cloud computing environment. The IDS has emerged as a savior in many attacks, but there is still scope for improvement.

ENDNOTES

[1]Páez, Rafael. "An Agent Based Intrusion Detection System with Internal Security." In *Intrusion Detection Systems*, edited by Pawel Skrobanek. Intech, 2001.

[2]Nitin, Tiwari, Solanki Rajdeep Singh, and Pandya Gajaraj Singh. "Intrusion Detection and Prevention System (IDPS) Technology — Network Behavior Analysis System (NBAS)." *ISCA Journal of Engineering Sciences*, Vol. 1, No. 1, July 2012, pp. 51-56.

[3]Debar, Hervé, Marc Dacier, and Andreas Wespi. "Towards a Taxonomy of Intrusion-Detection Systems." *Computer Networks*, Vol. 31, 1999, pp. 805-822.

[4]Nazer, G. Mohammed, A. Arul, and Lawrence Selvakumar. "Current Intrusion Detection Techniques in Information Technology — A Detailed Analysis." *European Journal of Scientific Research*, Vol. 65, No. 4, 2011, pp. 611-624.

[5]Vieira, Kleber, Alexandre Schulter, Carlos Becker Westphall, and Carla Merkle Westphall. "Intrusion Detection for Grid and Cloud Computing." *IT Professional*, Vol. 12, No. 4, July/August 2010, pp. 38-43.

[6]Dastjerdi, Amir Vahid, Kamalrulnizam Abu Bakar, and Sayed Gholam Hassan Tabatabaei. "Distributed Intrusion Detection in Clouds Using Mobile Agents." *Proceedings of the Third International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP '09)*. IEEE, 2009, pp. 175-180.

[7]Kannadiga, Pradeep, and Mohammad Zulkernine. "DIDMA: A Distributed Intrusion Detection System Using Mobile Agents." *Proceedings of the 6th International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/ Distributed Computing* and *First ACIS International Workshop on Self-Assembling Wireless Networks*. IEEE, 2005, pp. 238-245.

[8]Bakshi, Aman, and Yogesh B. Dujodwala. "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine." *Proceedings of the 2010 Second International Conference on Communication Software and Networks (ICCSN '10)*. IEEE, 2010, pp. 260-264.

[9]Yee, Chan Gaik, Wong Hui Shin, and G. Rao. "An Adaptive Intrusion Detection and Prevention (ID/IP) Framework for Web Services." *Proceedings of the International Conference on Convergence Information Technology*. IEEE, 2007, pp. 528-534.

[10]Roschke, Sebastian, Feng Cheng, and Christoph Meinel. "Intrusion Detection in the Cloud." *Proceedings of the Eighth IEEE International Conference on Dependable, Autonomic, and Secure Computing (DASC '09)*. IEEE, 2009, pp. 729-734.

[11]Laureano, Marcos, Carlos Maziero, and Edgard Jamhour. "Protecting Host-Based Intrusion Detectors Through Virtual Machines." *Computer Networks*, Vol. 51, No. 5, April 2007, pp. 1275-1283.

[12]Mazzariello, Claudio, Roberto Bifulco, and Roberto Canonico. "Integrating a Network IDS into an Open Source Cloud Computing Environment." *Proceedings of the Sixth International Conference on Information Assurance and Security*. IEEE, 2010, pp. 265-270.

[13]Kholidy, Hisham Abd Elazeem Ismail, and Fabrizio Baiardi. "CIDS: A Framework for Intrusion Detection in Cloud Systems." *Proceedings of the IEEE Ninth International Conference on Information Technology — New Generations (ITNG)*. IEEE, 2012, pp. 379-385.

[14]"Amazon Web Services (AWS) and Eucalyptus Partner to Bring Additional Compatibility Between AWS and On-Premises IT Environments." Press release, Eucalyptus Systems, Inc., 22 March 2012 (www.eucalyptus.com/news/amazon-web-services-and-eucalyptus-partner).

[15]"Managed Mode." Eucalyptus (www.eucalyptus.com/docs/3.1/ig/planning_managed.html).

[16]Rehman, Rafeeq Ur. *Intrusion Detection Systems with Snort*. Prentice Hall PTR, 2003.

John Prakash Veigas is currently a postgraduate student in the Department of Computer Science and Engineering at the National Institute of Technology Karnataka, Surathkal, India, with four years of experience in teaching and two years of industrial experience. His research interests include distributed computing systems, cloud computing, and security. He can be reached at john.veigas@gmail.com.

K Chandra Sekaran is a Professor in the Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, India, with 26 years of experience in teaching. Dr. Sekaran's research interests include distributed computing systems, computer networks, cloud computing, and enterprise information systems. He has more than 120 research publications in peer-reviewed journals and international conferences. Dr. Sekaran was Visiting Fellow/Professor at various institutions of higher learning in India and abroad, including London Metropolitan University UK, AIT Bangkok, University of Florida, CLOUDS Lab at the University of Melbourne, and Department of Management Studies, IIT Madras. He can be reached at kch@nitk.ac.in.

Cloud Ecology: Surviving in the Jungle

by Claude R. Baudoin

The technology of the cloud has been evolving fairly quickly, in fact faster than many people expected, this author included. The number of serious market players and their sheer size (including companies such as Amazon, Google, IBM, and Microsoft) attests that we have passed the point of no return: this new model is here to stay. Indeed, no selection process for an IT capability is complete today unless it includes cloud-based solutions. Even government entities have embraced the trend, in part because of the usual promise of cost savings, flexibility, and scalability, but also with a view toward creating more employment in the private sector rather than in already large government agency staffs. The US federal government, as well as the governments of some other countries, actually now mandates that cloud solutions be the preferred choice, not the exception, for new systems.

When organizations consider a cloud option, they always look first at functionality and cost. They realize that a cloud offering must also meet other capabilities without which an IT service is not viable: performance assurance, resilience, disaster recovery, notification schemes, security, privacy, and so on. Much needs to improve in terms of how to negotiate, ensure, and/or verify those capabilities. This part of the discussion between suppliers and clients is not very rational or balanced: we are still at a stage where cloud providers tell you, "These are our standard terms and conditions and the (very) few promises we make to you. Take it or leave it." In this ecosystem, it seems that the big fish are the large providers named earlier; the small fish are niche-oriented or regional cloud providers, the brokers, and the contractors; and the plankton are the customers. Should it not be the other way around or at least better balanced?

AN EMERGING BUT INCOMPLETE ECOSYSTEM

First, let's address the question of scope. *Private* clouds do not create a significant "ecosystem" in the sense implied by the questions in this issue's call for papers. In fact, I personally believe that the phrase "private cloud" is often used to make a fairly modest architecture change — consisting of data center consolidation accompanied by virtualization — sound like a bold step into the future. Whether one agrees with this criticism or not, a private cloud does not create a complex interaction between multiple partners. The partners (an organization's users, its IT department, and its equipment and software suppliers) are continuing to function in essentially the same way they were before such a program was put in place. If the consolidated data center is outsourced to a hosting provider, the relationship is a little more elaborate and is based on a service-level agreement, but this is still not as complex as a public cloud service; the client has just subcontracted the management of a dedicated infrastructure. Therefore, as is often the case in discussions about the cloud, I will only write here about *public* clouds (or, in the case of hybrid clouds, about the public part of those clouds).

The "conceptual reference model" from the NIST Cloud Computing Reference Architecture[1] defines five actors in cloud computing (see Table 1):

1. Cloud consumer
2. Cloud provider
3. Cloud auditor
4. Cloud broker
5. Cloud carrier

In reality, the roles of cloud broker and cloud auditor are rarely filled today — although NIST includes cloud aggregation, a separate emerging value-added service, in the offerings of a cloud broker instead of identifying aggregators as distinct actors. And while there are always telecommunications carriers involved, they are not explicitly part of the deal, since public cloud services are usually accessed over the Internet using whatever ISPs the provider and the consumer already contract with. As a result, most deals explicitly mention only the consumer and the provider.

The consumer's own users, who may be its employees but may also be external customers or partners, are also missing from this list. They typically don't participate in any of the discussions between the five actors listed

Table 1 — Actors in Cloud Computing (Source: NIST)

Cloud consumer	A person or organization that maintains a business relationship with, and uses services from, *cloud providers*.
Cloud provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud auditor	A party that can conduct independent assessments of cloud services, information system operations, performance, and security of the cloud implementation.
Cloud broker	An entity that manages the use, performance, and delivery of cloud services and negotiates relationships between *cloud providers* and *cloud consumers*.
Cloud carrier	An intermediary that provides connectivity and transport of cloud services from *cloud providers* to *cloud consumers*.

in Table 1, but they are clearly impacted by the cloud service, and their own behavior may on occasion impact the service. They should also be consulted about their requirements when a provider is chosen and about their satisfaction once the service is delivered.

Finally, the NIST model omits the regulatory bodies and agencies that strongly influence the use of cloud services in both the public and private sectors. For example, HIPAA regulations impact the potential uses of the cloud for patient data storage, and financial regulations impact the use of cloud solutions by banks.

Seeing cloud adoption as an activity involving just two of these multiple players (providers and consumers) significantly limits the "ecosystem" view of the cloud world. This is something that should evolve as the industry matures — with new classes of service providers emerging to play the roles of brokers, aggregators, auditors, and regulators — and as the NIST model is, one hopes, further revised to acknowledge the role of end users. As for the carriers, they will become more important when consumers of large, mission-critical amounts of computing or storage start requiring dedicated high-speed links with quality-of-service guarantees that the public Internet may never offer.

Once a more complete model is in place, with its full range of actors, we will need to define better than we have done so far the relationships between these participants. You may think of these relationships as food chains, to pursue the ecosystem metaphor, or as value exchanges, to follow a value stream analysis approach. One way to formalize this is to draw a RACI (Responsible–Accountable–Consulted–Informed) matrix.[2] Table 2 shows the classical definition of the RACI roles.

We can now associate each role of the NIST model to certain RACI levels with respect to each aspect of a cloud service. To take a few examples:

- Cloud consumers are *accountable* for timely bill payment and for complying with terms of service (e.g., for not using a service to spam others or to distribute illegal content).
- Cloud auditors are *accountable* for providing a fair assessment based on the information they were able to collect.
- The service quality manager of a cloud provider is *accountable* for the contracted uptime of the service.
- The IT operations staff of the cloud provider is *responsible* for that uptime.
- Cloud consumers are *consulted* by a cloud provider who needs to schedule some downtime for maintenance reasons.
- Cloud consumers are *informed* about the anticipated recovery time from an unexpected service interruption.
- A cloud carrier is *accountable* for the throughput and latency of a circuit.

AN UNEQUAL RELATIONSHIP

So far, we've established that there are currently only two actors on the stage, the provider and the consumer; therefore we will focus on those. Following the RACI model, their respective roles should be defined in terms of accountability, responsibility, consultation, and information. How does this work in practice today?

The relationship between the two parties is formalized in multiple contractual documents, which go by

Table 2 — RACI Definitions (Source: Wikipedia)

R	Responsible	Those who do the work to achieve the task. There is typically one role with a participation type of *responsible*, although others can be delegated to assist in the work required.
A	Accountable	The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one from whom *responsible* is delegated the work. In other words, an *accountable* must sign off on (approve) work that *responsible* provides. There must be only one *accountable* specified for each task or deliverable.
C	Consulted	Those whose opinions are sought, typically subject matter experts, and with whom there is two-way communication.
I	Informed	Those who are kept up to date on progress, often only on completion of the task or deliverable, and with whom there is just one-way communication.

different names (see sidebar "Examples of Contractual Documents from Cloud Providers"). It is not uncommon for a public cloud provider to make the consumer sign the following:

- A **master services agreement**, sometimes called a customer agreement, which may or may not be separate from the next document, or may include it
- A generic **service-level agreement** (SLA), which will usually exist if the company provides other services besides a public cloud offering
- A specific **cloud service-level agreement** (CSLA)
- An **acceptable use policy** (AUP), sometimes called terms of service
- A **support agreement**

Clearly, the fact that there are multiple documents is an issue in itself, for three reasons. First, the consumer may not be fully aware of an obligation that is mentioned in the support agreement, expecting it to be, say, in the CSLA instead. Second, there may be overlaps, gaps, or contradictions between two or more of these documents. Third, this multiplicity, and the inconsistency of these documents across vendors, makes it really difficult to compare offerings during a selection process — something that may be intentional on the part of some vendors.

But a more serious problem awaits the cloud consumer who actually opens and reads the documents in question. Most of these documents:

- *Strictly* specify what the customer can or cannot do
- *Vaguely* mention what the provider is obligated to supply, often using inconsistent definitions of service levels that should be defined precisely, such as "availability"
- Are "one size fits all," with no real ability to *negotiate* a level of service corresponding to a price tier
- Do not establish *consultation and notification* channels

If we analyze this state of affairs in terms of the RACI matrix, we can summarize this by saying that most existing contractual documents, in particular the CSLA and the AUP:

- Make the consumer *accountable* for protecting the provider and its other clients from incidents for which the provider may unilaterally blame the consumer
- Make the provider *responsible*, but not *accountable,* for providing certain service levels
- Demand that the customer *inform* or *consult* with the provider before doing certain things, but impose almost no reciprocal obligation on the provider to inform or consult with the consumer

EXAMPLES OF CONTRACTUAL DOCUMENTS FROM CLOUD PROVIDERS

- **Master services agreement from AppFog** — www.appfog.com/products/appfog/service_agreement
- **Service-level agreement from GoGrid (a de facto CSLA)** — www.gogrid.com/legal/service-level-agreement-sla
- **Acceptable use policy (in the US) from Rackspace** — www.rackspace.com/information/legal/aup
- **Service plan from Salesforce.com (for one of several available support tiers)** — www2.sfdcstatic.com/assets/pdf/datasheets/DS_SuccessPlans.pdf

- Never mention the role of a carrier, such as to explain what the provider will do if its access to the Internet is disrupted by a circuit failure or a denial-of-service attack performed through that carrier

In some cases, the extreme lack of accountability expressed in provider documents borders on the ludicrous. My Cutter colleague Lou Mazzucchelli demonstrated this during the 2010 Cutter *Summit* by showing verbatim excerpts of SLAs that give the provider the contractual room to do just about anything it deems necessary, based solely on its judgment, without any negotiation or mediation protocol with the consumer, and regardless of the extraordinary efforts or harm it may impose on the consumer (see sidebar "Examples of One-Sided SLA Content").

Given such a situation, which unfortunately is common across providers, the cloud ecosystem is reduced to a sadly simple relationship: the provider collects the consumer's money and delivers services without sharing much of the risk. In fact, what mostly inconveniences the providers, and keeps them from invoking too often the excuses they have built into their agreements, is not the efforts they have to undertake to fix problems (they promise little), nor is it the financial penalties they will incur (these are limited and absolutely not commensurate with the impact of a service failure on the customer's earnings or its operations), but rather the impact on their reputation when a big outage makes the headlines of major print, TV, or Internet media. As for the other potential members of the food chain who could play a role in making the overall system better managed and more dynamic (brokers, carriers, auditors), they are simply ignored. So are, importantly, the *cloud customer's own customers*, who complete the food chain in many cases. They may be impacted by a cloud failure, or, conversely, they may be the cause of a problem (e.g., storage of illicit content) that could jeopardize the relationship between the provider and its primary client.

In summary, this looks a little too much like a jungle with a few powerful predators roaming among their rather defenseless prey.

EXAMPLES OF ONE-SIDED SLA CONTENT (ITALICS ADDED)

"… we may terminate this Agreement *for any reason* by providing you 30 days advance notice."

→ If this is for a totally unexpected reason, and without cause, 30 days is much too short to secure another provider and to migrate data or applications. This is not a hypothetical situation: in 2011, Novell shut down its Vibe cloud service, although it provided two months' advance notice.

"… if *we believe* providing the Services could create a substantial economic or technical burden or material security risk for us…"

→ Providing the service always entails a "substantial technical burden" — that's why the consumer is paying the provider. This is much too vague, one-sided, and definitive.

"We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, *given the nature of the Internet*."

→ This is a business inherently based on providing a service through the Internet, so the provider should deal with these risks, or involve the carriers in their SLAs, not invoke such a broad cop-out.

"… we will implement reasonable and appropriate measures designed to *help you secure* Your Content…"

→ This leaves the consumer, who may not have the skills to do so, in charge of fixing a problem that the provider may have allowed to happen through negligence, and which may have a severe impact on the customer's business.

Note: The quoted sentences are extracted from actual documents. Their source is not cited because I didn't want to single out a "bad guy" — many providers include similar clauses today.

WHAT CUSTOMERS NEED

Beginning in fall 2012, a working group of the Cloud Standards Customer Council (CSCC) set out to analyze in more detail the situation just depicted. The team reviewed dozens of public cloud contractual documents, including SLAs, AUPs, and the other types of documents mentioned earlier, with the following objectives:

- Understand how these documents are structured
- Determine what clauses are generally present or absent with respect to performance, security, privacy, service management, service failures, disaster recovery, and the exit process
- Analyze the gaps between what is generally included by providers and the legitimate expectations of consumers

- Present these results in the form of concrete guidance to the consumers and to the industry, enabling all parties to negotiate better agreements and restoring the balance that is missing today due to the one-sided agreements that currently prevail

Table 3 lists some of the key needs of cloud consumers. (Please note that this analysis is my interpretation of the findings, not an official position of the CSCC.) These are needs that the providers may not particularly *like* to fulfill, but they are *able* to fulfill. In other words, we are not letting the pendulum swing all the way to the opposite extreme, where SLAs would contain everything that's ideal for consumers but no sane provider would accept.

DON'T GET EATEN ALIVE, OR AT LEAST PUT UP A GOOD FIGHT

The CSCC working group subtitled its forthcoming report "What to Expect and What to Negotiate" because its advice to cloud customers is to review the agreements proposed by providers in detail and to choose their battles intelligently. Some desirable clauses may not be offered by anyone, and the providers know that; therefore the customer cannot leverage the prospect of choosing a competitive supplier. In other cases, it is possible, based on knowledge of what other providers offer, to ask for higher commitments or for greater penalties if a service level is not met. Today, too many customers sign on a cloud contract's dotted line with a shrug, as though pressing the "click here to accept" button at the bottom of an end-user license agreement (which most of us do without reading what we are accepting). The kind of review I'm proposing here should allow customers to sign a final deal with their eyes open, after negotiating what needs to be negotiated.

Of course, a well-conducted sourcing process for a major cloud service should include a request for proposals, in which the customer may specify in advance that it wants the bidders to address each of the issues in Table 3. Some providers may respond by stating that their documents are not negotiable, but some may decide, when faced with an educated and prepared customer, to show some flexibility and discuss how to meet some of these requirements, potentially at a price.

LOOKING FORWARD

The CSCC working group expects to complete the final draft of its new report in time for discussion at its meeting in April 2013, with formal adoption some time later in 2013. This means that cloud customers will have a series of three documents from the CSCC to guide their adoption of the cloud:

- The "Practical Guide to Cloud Computing"[3] presents nine steps in the process of determining whether a cloud-based solution is a valid approach to address a certain need and then discusses how to go about selecting and deploying such a solution.
- The "Practical Guide to Cloud Service Level Agreements"[4] provides a general approach to evaluating and comparing cloud SLAs.
- The new document, tentatively entitled "Cloud Service Agreements: What to Expect and What to Negotiate," will go more deeply into the implications of specific clauses, identifying which ones can be negotiated to achieve a better balance between provider and customer.

As more and more such negotiations occur, providers as well as customers will develop a greater understanding of the various clauses that matter to their healthy relationships, what terms need to be better defined to avoid harmful ambiguity, and what service levels can be measured using a numeric scale. But a few years down the road, we will have a much more complex situation than we do today because there will be thousands of cloud providers on the market and the food chains will be longer. For example, end-user A may subscribe to a service from company B, which uses software as a service supplied by C, which in turn uses infrastructure as a service from D.

By that time, to effectively compare different offerings, purely human processes will no longer be sufficient. This comparison may not only take place once, during the selection of a provider; it may in fact occur in real time, as a consumer turns virtual machines or application instances on and off all day long to handle variable loads, assessing each time which of its multiple contracted providers should get the next piece of the action based on price, performance, recent availability statistics, and so forth.

To answer this need, we can envision an "SOA for SLA" mechanism in which each provider exposes a service that can be queried to determine what is covered in the provider's SLAs, and what the service price is given certain parameters such as availability commitments, security and privacy commitments, and the like. The final deal will still certainly require some hours spent around a negotiating table, but the initial selection of a few finalists out of this much larger market will be

Table 3 — What Customers Should Request

Consistent document names	A preferred set of names needs to emerge to reduce the current confusion, perhaps along the lines of existing NIST work, although this is still overly complex.
Coherence of the whole set of agreements	It should be easy to find the privacy clauses, for example, rather than have to guess whether they are in a master services agreement, an SLA, an AUP, a security policy, etc.
Clear expression of commitments	Lawyers like to use verbs like "shall," "should," "may," etc., to convey different levels of commitment. That's fine, but an agreement must also specify unambiguously what it is that shall/should/may be done by whom to whom. The use of the RACI vocabulary (Responsible, Accountable, Consulted, Informed) would go a long way toward clarifying what happens in case of failures, performance degradation, planned outages, termination, security leaks, etc.
Recognition that the ecosystem may include the consumer's own external clients	These end users may be paying for a value-added service based on the cloud offering. This has several important implications. First, malfunctions impact not only the cloud consumer's operations, but also its revenue, and this may lead to offering a different tier of service. Second, the consumer may not be legally responsible for content that belongs to its users. If that content violates the AUP, there need to be reasonable processes to cut off the actual culprit without terminating the whole service to the consumer, which in turn would cut off its business with all its other users.
Effective security measures	It is not enough to promise to "help" the consumer secure its content, including in the case of a security breach. The cloud provider should have a professional services department, or certified subcontractors, who can do two things: (1) implement encryption mechanisms — both for data at rest and in transit — for clients who want to store confidential data in the cloud; and (2) react to cyber attacks to protect the clients' data from being stolen. The obligations of this cyber security department or partner should be defined with their own service levels, such as maximum notification delays, maximum reaction time for certain incidents, pricing terms for security design services, etc.
Privacy of end-user data	The provider's privacy obligations must extend not only to the information it may collect about its direct customer in the course of doing business, but to the information about end users that the customer may store in the cloud. For example, a company that uses Salesforce.com should receive certain guarantees about the privacy of the customer records it will create in the system. While Salesforce has a legitimate need to ask me for certain contact and payment information to do business with me, it has no right to access the phone number of a client of mine.
Availability commitments that are specified over short enough observation periods	This need is not new; it has been present for many years in data center outsourcing contracts and was rarely met adequately. The proliferation of cloud consumers just makes any vagueness about observation periods, or the specification of long periods, more potentially harmful. If a provider promises 99.75% availability, is it 99.75% each day, which amounts to less than 4 minutes of outage per day? Or is this measured over a year, in which case there could be a single outage of almost 22 hours on your busiest day of the year, and the provider could insist the SLA was met and that it does not owe you a refund?
Mechanisms for discussion, appeal, and mediation	Say the customer inadvertently violates a clause in the AUP, and is threatened with contract termination. It claims, however, that it did not do what the provider claims it did, or that it is not responsible for a violation by one of its own users. In such cases, there needs to be a way to avoid a damaging interruption in service if at all possible. Current SLAs lack provisions for customers to prove their *bona fides* and avoid severe business impact.
Agreement about auditing mechanisms	A competent customer may want to assess, through nondestructive methods, that the cloud service cannot easily be misused. In most AUPs, any such attempt is prohibited. As an acceptable alternative, a provider may contract an *independent* company, with properly certified experts, to perform periodic, documented assessments of all its safety and security measures, including physical safety and currency of all software updates. Eventually, a specific category of service providers (the "cloud auditors" in the NIST list) will fill this market niche.

subject to a certain level of automation. This is not a far-fetched idea. Similar specifications — WS-Agreement and WS-Agreement Negotiation[5] — have been defined by the Open Grid Forum to automate the negotiation of valid agreements between a Web service provider and a consumer. Extending these protocols to the issue of agreeing on a cloud SLA is not trivial, but it is certainly possible.

ENDNOTES

[1]Liu, Fang, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, and Dawn Leaf. "NIST Cloud Computing Reference Architecture." National Institute of Standards and Technology (NIST), September 2011 (www.nist.gov/customcf/get_pdf.cfm?pub_id=909505).

[2]Haughey, Duncan. "RACI Matrix." Project Smart (www.projectsmart.co.uk/raci-matrix.html).

[3]"Practical Guide to Cloud Computing." Cloud Standards Customer Council (CSCC), October 2011 (www.cloud-council.org/10052011.htm).

[4]"Practical Guide to Cloud Service Level Agreements." CSCC, March 2012 (www.cloud-council.org/04102012.htm).

[5]Waeldrich, Oliver (ed.). "WS-Agreement Negotiation." Open Grid Forum, 31 January 2011 (www.gridforum.org/Public_Comment_Docs/Documents/2011-03/WS-Agreement-Negotiation+v1.0.pdf).

Claude R. Baudoin is a Senior Consultant with Cutter's Data Insight & Social BI *and* Business & Enterprise Architecture *practices. Prior to becoming an independent consultant, Mr. Baudoin spent 35 years in the corporate world, occupying various positions in software engineering and IT management, in France and the US, mostly for the global oilfield services company Schlumberger. Over his career, he developed expertise in enterprise and information architecture, business process modeling, enterprise security strategy, building communities of practice, collaboration methods and environments, and the use of social media in business. Mr. Baudoin is the coauthor of two books,* Realizing the Object-Oriented Lifecycle *and* Méthodes de Programmation. *He has served as Guest Editor for* Cutter IT Journal*, presented at international IT events, published many papers, and holds two patents on networking and information security. Mr. Baudoin has an MS in computer science from Stanford University and an undergraduate degree in engineering from Ecole Polytechnique (Paris). He can be reached at cbaudoin@cutter.com.*

The Promise of a Diverse, Interoperable Cloud Ecosystem — And Recommendations for Realizing It

by Kathy L. Grise

The cloud is here to stay. It is a vital part of the information and communications technology (ICT) ecosystem, even though it is still a dynamic, fluid, and ever-changing addition to the ICT environment.

Five years from now, businesses and consumers will likely have access to a diverse cloud ecosystem that will be capable of interconnecting and moving data from one cloud to another in transparent fashion. Services carried over the infrastructure will extend the reach of these clouds to support emerging industries, such as the smart grid, and revolutionize others, such as medicine. Clouds will also become a part of everyday life as consumers from all demographic, socioeconomic, and geographic sectors come to rely more and more on cloud-based social media and mobile applications for essential communications; personal health device, home appliance, and home security management functions; as well as routine photo, video, and music services.

One may think we already have this type of ecosystem today, and it is true that a vibrant cloud ecosystem is forming and that businesses and consumers in many regions are enjoying the benefit of its early services. But cloud services are not yet ubiquitous and mainstream.

Transparent integration of services across clouds will be a fundamental attribute of this future ecosystem. One can expect to see a seamless use of cloud services and applications that, for example, can transfer data across public clouds, between public and private clouds, or from public or private clouds to hybrid clouds.

This vision of cloud computing will be driven by innovation, competition among third-party providers, and consumer demand for cloud services that are convenient, sophisticated, and affordable. However, this vision can't be achieved in an unstructured environment. Careful collaboration and coordination among ecosystem participants will be necessary to advance cloud technologies and services in a way that benefits everyone.

RECOMMENDED APPROACHES FOR REALIZING A DIVERSE, INTEROPERABLE CLOUD ECOSYSTEM

Industry participants should follow some essential approaches and steps to help facilitate the cloud ecosystem's evolution to this vision. In particular, service providers must:

- Employ flexible business strategies that allow adaptation to this new diverse and interoperable cloud ecosystem
- Ensure they have the capabilities needed to meet customer expectations and demands
- Adopt compatible and open technologies in lieu of proprietary or standalone options
- Collaborate with others in the industry to advance interoperability standards
- Embrace innovation to improve the technology's functional and performance characteristics and to effectively and securely incorporate mobile and social clouds

Have a Flexible and Adaptable Business Model

To be successful in this evolving competitive environment, third-party service providers must be flexible and ready to rapidly adapt their business plans and strategies to the cloud lest they fall behind. For example, software development in a cloud environment is much faster and more efficient than has been possible with traditional development techniques. The typical traditional software development lifecycle involved a lengthy time frame from start to completion, and the process was also often complex, requiring detailed analysis and design, actual code development, followed by testing, integration, more testing, and implementation.

With new software development techniques, however, cycles have been significantly shortened. Today

developers can access more readily and quickly the needed software tools and services in the cloud. Traditional processes might have included time spent researching and determining what tools and services to purchase, and then arranging their purchase, installation, and access. In addition, this may have required securing the hardware to host the tools and services. With the cloud, the time spent on these activities — if not eliminated entirely — is greatly reduced. This streamlined cloud environment allows companies to release more applications, but it also forces providers to stay more aware of customer needs and wants and respond to them more quickly.

Providers must keep abreast of changing trends and standards. They must weigh both the demands of running their businesses and the need to invest in the right resources when selecting technologies and services they will use and offer.

Stay on Top of Customer Expectations and Demands

Customers expect well-managed, integrated, interoperable, and affordable services from their providers, and this will be the case with cloud computing, too. Indeed, cloud computing is rapidly becoming a service that the consumer cannot do without.

Imagine you're Netflix. Your customers are sitting down with their families on a cozy winter night, ready to stream a newly released movie through your service. Suddenly they're told that, due to technical difficulties, they cannot access any videos. This scenario, in fact, occurred on Christmas Eve last year. What happened? Netflix relies on Amazon Web Services as its cloud computing provider to store and stream its movies. That night, Amazon's infrastructure could not handle the high demand for its cloud services, and the network became overloaded. Millions of Netflix customers were affected — and probably highly annoyed.[1]

Consumers' generally high expectations for always-available, interoperable, yet also affordable cloud services — and vendors' abilities to deliver on these expectations — could influence the success or failure of individual service providers and the evolution of the general ecosystem. There are so many service providers in today's environment that competition will favor some at the expense of others. The companies that survive will be those that demonstrate and practice interoperability and are astute enough to recognize and meet consumer demand for low-cost, high-quality, reliable services.

Don't Operate as a Standalone Technology; Embrace Compatibility

Cloud service providers, standards organizations, and industry associations need to work together to help shape the most effective and successful future for cloud computing.

It wasn't that long ago that the video industry was mired in a technology war between the Betamax video cassette tape recorder/player format offered by Sony and the VHS format offered by JVC. The outcome of this battle can be answered by a simple question: does anyone still own a Betamax device (or even know what a Betamax is)?

There is a well-known lesson from this precedent. Betamax was a higher-quality format compared to VHS, but Sony made a catastrophic business decision by not sharing its technology and collaborating with other providers. The VHS format offered by JVC won out in the market because JVC was willing to share its technology and collaborate with other vendors, which helped make VHS more affordable and accessible and more appealing to the mass market. Betamax fell victim to the open licensing model presented by VHS.

Service providers in the cloud computing industry will find that they have similar strategic choices to make as they build and introduce their services, and we can expect that the ecosystem more likely will weed out service providers that use standalone or incompatible clouds. Furthermore, the choices individual service providers make will influence not only their own businesses, but the advancement of the industry and ecosystem overall. Given the rapid explosion of cloud applications and services, businesses can't afford *not* to work together to help shape the most effective future possible for cloud computing.

Collaborate with Other Ecosystem Participants to Promote Interoperability Standards

While cloud computing has been around for several years, it is still considered an emerging technology. There are many opportunities for industry, government, and academia to help create an open source, interoperable cloud architecture.

One example is participation in the IEEE Intercloud Testbed.[2] An intercloud architecture is essential to cloud computing because a cloud operated by one service provider or enterprise will interoperate with a cloud operated by another organization. This is a powerful concept, and it is also a valuable concept because it

increases the value of cloud computing to industry, enterprises, and consumers. However, clouds today cannot yet federate and interoperate to employ this model. The Intercloud will provide that federation.

The IEEE Intercloud Testbed is being developed in collaboration with universities, cloud companies, and standards organizations across the US, Europe, and the Asia-Pacific region. The testbed also provides opportunities for participation from groups in emerging geographies, such as South America and Africa. By participating, these groups will help open up opportunities to expand and advance technology accessibility to their respective regions and will very likely help spur their local economies.

The testbed will also provide a collective pool of open source resources to the cloud computing industry, which will help drive the creation of technical standards for interoperability, including the IEEE P2302 Standard for Intercloud Interoperability and Federation (SIIF).[3]

Another example of collaboration is the recent announcement that Microsoft is joining the Open Data Center Alliance (ODCA) to promote cloud standards and interoperability. The move will enable Microsoft to contribute to ODCA's technical workgroups, which "contribute to creating standards and usage models designed to help design secure federation, cloud security features and interoperability across clouds."[4-6]

Embrace Innovation to Improve Cloud Functionality and Performance and to Secure Mobile and Social Clouds

Many innovations are still needed to advance cloud computing to its envisioned future. Innovation is required to ensure that all components in the infrastructure, including all hardware and software, meet the functional and performance needs of both enterprises and consumers. Innovations must consider, for example, the demand for data, data speeds, reliability, security, responsiveness, storage capabilities, compression, low cost, and sustainability.

Businesses will need to incorporate mobile and social cloud services effectively and broadly if they want to compete successfully for customers and customer loyalty. Yet there will be challenges associated with the convergence of mobile, social, and cloud trends. Cloud computing represents today's most exciting IT paradigm shift. However, security and privacy concerns are perceived as primary obstacles to its wide adoption. Critical security challenges must be addressed and security solutions developed if we are to achieve a trustworthy public cloud environment.[7] This represents an important area of innovation that demands attention.

TODAY'S CLOUD IMPLEMENTATIONS PAVE THE WAY FOR THE FUTURE

Cloud computing is not limited to IT service providers. The interoperable cloud ecosystem is broad and pervades industries of all types, from the smart grid to the life sciences and beyond.

Think of electric utility service companies and their introduction and use of smart grid technologies. Utility companies are adapting to cloud technologies because they must leverage and use cloud-based applications, services, infrastructure, and storage to make the smart grid possible. These companies, including San Diego Gas & Electric (SDG&E)[8] and Arizona Public Service (APS),[9] are successfully using the cloud to operate and manage smart meters installed in consumers' homes and to oversee and efficiently manage the flow of electricity. According to industry analysts, worldwide smart meter shipments surpassed 15.4 million units in the third quarter of 2012, representing year-over-year growth of 126.9% and a 58.6% increase over the previous quarter.[10] The smart meter industry worldwide is a clear beneficiary of cloud technology, and its rapid growth illustrates the substantial impact the cloud can have on a sector of business.

The life sciences are also using cloud computing in impressive and transformative ways. In medicine, for example, the use of the cloud has literally removed many of the physical barriers that previously limited access to medical care or services in remote regions. Think of the patient who needs expert specialty care or diagnostic services but cannot access those services locally. Thanks to the cloud, a local physician can collect the patient's vital statistics or other data and then leverage cloud services to virtually consult with a specialist even if the specialist is based in another region or country.

Electronic health records (EHRs) are another innovation that is emerging as the healthcare industry begins to adopt systems and methods that leverage cloud-based options. The plethora of EHRs generated globally is increasing at a rapid pace. But with this growth in cloud-based electronic records, the traditional separation of patient care data from IT to protect patient privacy is no longer assured. This is a huge issue due to the personal and confidential nature of healthcare data. Providers realize they must still implement a reliable

and secure IT infrastructure platform, services, and applications when they embrace the cloud, and many companies are beginning to introduce cloud solutions that address these concerns. Reference Fusion, to name just one vendor, has an experimental open, cloud-based platform for large-scale, low-cost delivery of healthcare applications to facilitate the seamless and secure sharing of EHRs. These types of approaches will enable broader use of patient-centric management of electronic health records.[11]

CONCLUSION

Cloud computing is advancing rapidly. Before we know it, the technology will be employed to support all types of industries and businesses and deliver services that enhance everyday life for consumers in all parts of the world. This vision is a realistic one, and with it will come a new era of innovation and competition.

Service providers that want to play a role in the development of this emerging ecosystem and rise above the competition to thrive in the market five years from now must position their firms appropriately for success. Companies must adopt business strategies that are flexible and adaptable to this new environment. They must make sure their infrastructure and services can meet the market's high expectations and demands. They must avoid reliance on standalone technologies and embrace options that are compatible with others in the market. They must collaborate with other participants in the ecosystem to help advance interoperability standards. And they must innovate to improve the technology's functional and performance characteristics and ensure that mobile and social cloud solutions are secure.

As the industry evolves and competition intensifies during the next five years, service providers that follow these recommendations will have a greater chance of winning new customers, satisfying their existing customer base, and outpacing the competition to become market leaders in cloud computing.

ENDNOTES

[1]"Netflix Blames Amazon for Christmas Eve Outage." Reuters, 25 December 2012 (www.reuters.com/article/2012/12/26/net-us-companies-netflix-idUSBRE8BO06H20121226).

[2]For more information on the IEEE Intercloud Testbed, see the IEEE Cloud Computing Portal (http://cloudcomputing.ieee.org/intercloud).

[3]"IEEE P2302 Working Group (Intercloud)" (http://cloudcomputing.ieee.org/standards/standards-guidance-p2302).

[4]Whittaker, Zack. "Microsoft Joins Open Data Center Alliance to Promote Cloud Standards, Interoperability." ZDNet, 27 February 2013 (www.zdnet.com/microsoft-joins-open-data-center-alliance-to-promote-cloud-standards-interoperability-7000011905).

[5]"Open Data Center Alliance Welcomes Microsoft as Contributing Member." Press release, PR Newswire, 27 February 2013 (www.prnewswire.com/news-releases/open-data-center-alliance-welcomes-microsoft-as-contributing-member-193530571.html).

[6]Open Data Center Alliance (www.opendatacenteralliance.org).

[7]Ren, Kui, Cong Wang, and Qian Wang. "Security Challenges for the Public Cloud." *IEEE Internet Computing*, Vol. 16, No.1 January/February 2012, pp. 69-73.

[8]"SDG&E Installing New Smart Grid Technologies to Create 'Self-Healing' Electric Grid for San Diego." Press release, San Diego Gas & Electric, 30 January 2013 (www.sdge.com/newsroom/press-releases/2013-01-30/sdge-installing-new-smart-grid-technologies-create-%E2%80%9Cself-healing%E2%80%9D).

[9]"Arizona Public Service Expands Viewing and Analysis." *ArcNews*, Fall 2011 (www.esri.com/news/arcnews/fall11articles/arizona-public-service-expands-viewing-and-analysis.html).

[10]"Worldwide Smart Meter Shipments Surpass 15.4 Million Units in 3Q 2012, According to IDC Energy Insights." Press release, IDC Energy Insights, 10 December 2012 (www.idc.com/getdoc.jsp?containerId=prUS23849912).

[11]Basu, Sujoy et al. "Fusion: Managing Healthcare Records at Cloud Scale." *Computer*, Vol. 45, No. 11, November 2012, pp. 42-49 (www.computer.org/csdl/mags/co/2012/11/mco2012110042.html#bibmco20121100421).

Kathy Grise is Future Directions Senior Program Director, IEEE Technical Activities, at IEEE. She works directly with IEEE volunteers, IEEE staff, and consultants in support of new initiatives and is the IEEE Staff Program Manager for the IEEE Cloud Computing Initiative and the IEEE Technology Navigator. Prior to joining the IEEE staff, Ms. Grise held numerous positions at IBM and most recently was a Senior Engineering Manager for Enablement in the IBM Semiconductor Research and Development Center. She can be reached at k.l.grise@ieee.org.

Cutter Consortium

Executive Education+

SUMMIT 2013

4–6 November 2013
Cambridge, MA, USA

Intense, Interactive Instruction. Effective Learning.

Register today and save!

Single Seat: $1995 for a limited time (save $500!)

Team Builder: Buy 1 seat for $2495 and bring a colleague at a deep discount. (Save 30%)

Executive education on IT leadership and emerging trends. A year's worth of professional development and personal enrichment in 3 invigorating days.

From an in-depth case study taught in the popular business school style, to interactive small group exercises and keynotes that help you identify business opportunities made possible by emerging technologies, you'll enjoy truly unbiased discussion and meaningful debate on today's IT opportunities and challenges at the Cutter *Summit*. Discover and learn about new strategies, technologies, and leadership skills — from Cutter's exceptional lineup of experts —that will help you embrace the ever-unfolding opportunities and challenges of the SMAC business environment.

In addition, you'll benefit from hands-on seminars and roundtables led by Cutter's Practice Directors and Senior Consultants on topics such as software engineering and agility, business and enterprise architecture, CIO/CTO issues, and data insight and social BI, to name a few.

You'll enjoy (and join in on!) raucous panel debates; networking at lunches, breaks, and entertaining evening events; and get one-on-one guidance and input from expert presenters and participants.

Monday, 4 November 2013

The Evolving Role of 21st-Century Technology Leaders

Keynote by Robert D. Scott

Cutter Fellow; Director of the Information Systems Executive Forum, Ross School of Business, University of Michigan

Lightning Talks

Short and to-the-point presentations around a single strategy, technique, or success story.

Big — and Fast — Data Analytics

Case Study with Vince Kellen

Cutter Fellow; Senior Vice Provost for Academic Planning, Analytics & Technologies, University of Kentucky

Evening Cocktail Party

Unwind and socialize with the speakers and your fellow attendees while enjoying some of Boston's tastiest regional specialties.

Learn more at www.cutter.com/summit.html

Tuesday, 5 November 2013

Sustainable Growth: Achieve It with Highly Motivated Teams

Roundtable with Lynne Ellyn

Cutter Fellow

Agile in the API Economy

Keynote by Israel Gat

Fellow and Director, Cutter Agile Product & Project Management Practice

Digging for Gold in the Emerging Technology Pile of Hype

Keynote by Lou Mazzucchelli

Cutter Fellow

Putting Your Leadership Skills to the Test

Active Learning Exercises with Michael Roberto

Cutter Fellow; Trustee Professor of Management at Bryant University

Wednesday, 6 November 2013

Choose a Track ▸

BUSINESS TECHNOLOGY STRATEGIES TRACK

CIO/CTO Roundtable

Forum with Ron Blitstein

Fellow and Director, Cutter Business Technology Strategies Practice

AGILE TRACK

Agile, Software Engineering, and Product Development

Workshop

TBA

DATA INSIGHT & SOCIAL BI TRACK

Data Insight and Social BI

Workshop

TBA

BUSINESS & ENTERPRISE ARCHITECTURE TRACK

Business and Enterprise Architecture

Workshop

TBA

A Theory of Practice: Soft Decision-Making in the Context of a High-Pressure IT Organization

Keynote by Tom DeMarco

Cutter Fellow

See the full program at www.cutter.com/summit.html

About Cutter Consortium

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, groundbreaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and agile project management, enterprise architecture, business technology trends and strategies, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you Access to the Experts. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts, experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including content via online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products and training/consulting services, you get the solutions you need, while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

The Cutter Business Technology Council

The Cutter Business Technology Council was established by Cutter Consortium to help spot emerging trends in IT, digital technology, and the marketplace. Its members are IT specialists whose ideas have become important building blocks of today's wide-band, digitally connected, global economy. This brain trust includes:

- Rob Austin
- Ron Blitstein
- Tom DeMarco
- Lynne Ellyn
- Israel Gat
- Vince Kellen
- Tim Lister
- Lou Mazzucchelli
- Ken Orr
- Robert D. Scott