ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Security and Privacy-Enhancing Multi Cloud Architectures

A.Tulasi Ram
M.Tech Student
Department of Computer Science & Engineering
Raghu Engineering College
Visakhapatnam

Anil Kumar Mahapatro, M.Tech
Associate Professor
Department of Computer Science &Engineering
Raghu Engineering College
Visakhapatnam

Abstract:
Security challenges are still among the biggest obstacles when considering the adoption of cloud services. This triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues, the cloud paradigm comes with a new set of unique features, which open the path toward novel security approaches, techniques, and architectures. This paper provides a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects.
Keywords: Cloud, security, privacy, multi cloud, application partitioning, tier partitioning, data partitioning, multiparty computation.

Introduction

1.1 Defining Cloud Computing

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. These services have long been referred to as Software as a Service (SaaS). Some terms such as PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) are used by vendors to describe their products, but we avoid these because accepted definitions for them still vary widely. There is no crisp line between "low-level "infrastructure and a higher-level "platform ". We believe both of these are more alike than different, and we do consider them together. Similarly, some related term such as "grid computing," from the high-performance computing community, suggests protocols to offer storage over long distances and shared computation, however those protocols did not lead to a software environment that grew beyond its own community. The data center hardware and software is what we will call a *cloud*. When a cloud is made available in a pay-as you- go manner to the general public, we call it a *public cloud*; the service being sold is *utility computing*. We use the term *private cloud* to refer to internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing that we discuss here. The cloud computing is the sum of SaaS and utility computing, but does not include medium sized data centers, even if these depend on virtualization for management. People can be users or providers of SaaS, or users or providers of utility computing. We focus on SaaS providers (cloud users) and cloud providers, which have received less attention than SaaS users. Figure 1 makes provider-user relationships clear. There are some case in which the same actor plays multiple roles. For instance, a cloud provider might also host its own customer-facing services on cloud infrastructure.

1.2 All kinds of clouds

Major IT companies have spent billions of dollars since the 1990s to shape cloud computing. Like, Sun's well-known slogan "the network is the computer" was made in 1980s. Salesforce.com is the website which

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

has been providing on-demand Software as a Service (SaaS) for customers since 1999 to present era. IBM and Microsoft are the first two companies that started to deliver Web services in the early 2000s. Microsoft's Azure service provides an operating system and a set of developer tools and services. Google's popular Google Docs software provides Web-based word-processing, spreadsheets and all the Microsoft office applications. Google App Engine allows system developers to run their Python/Java applications on Google's infrastructure. Sun provides $1 per CPU hour. Amazon is well-known for providing Web services such as EC2 and S3. Yahoo! announced that it would use the Apache Hadoop framework to allow users to work with thousands of nodes and petabytes (1 million gigabytes) of data.

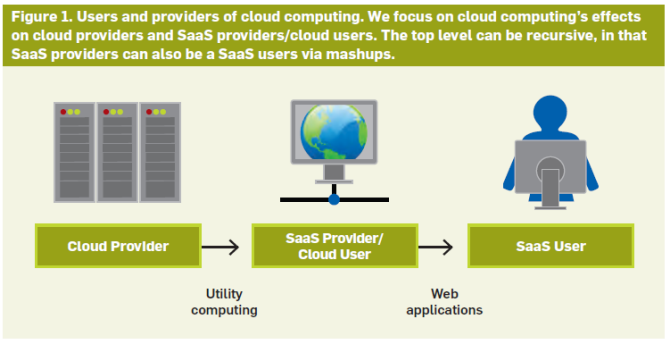
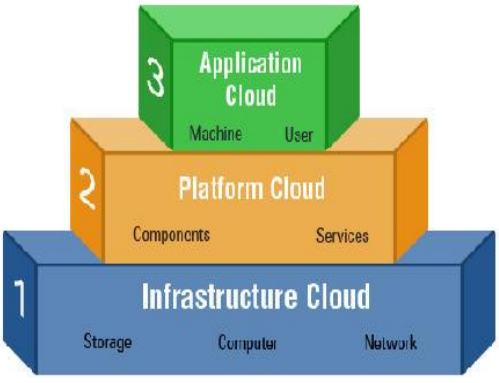


Figure 1. Users and providers of cloud computing. We focus on cloud computing's effects on cloud providers and SaaS providers/cloud users. The top level can be recursive, in that SaaS providers can also be a SaaS users via mashups.

These examples demonstrate that cloud computing providers are offering services on every level, from different hardware (e.g., Amazon and Sun), to the different operating systems (e.g., Google and Microsoft), to software and different services (e.g., Google, Microsoft, and Yahoo!). At present era Cloud-computing providers target a variety of end users, from developers of the software to the general public. For additional information regarding cloud computing models, the University of California (UC) Berkeley's report provides a good comparison of these models by Amazon, Microsoft, and Google. As cloud computing providers prices are low and IT advancements remove technology barriers—such as virtualization, simulation, network bandwidth — cloud computing has moved into the mainstream of technology . Gartner stated, "Organizations are switching from company owner hardware and software to per-use service-based models." For example, the U.S. government website (http://www.usa .gov/) will soon begin using cloud computing. The *New York Times* used Amazon's EC2 and S3 services and used Hadoop application to provide open access for the public domain articles from 1851 to 1922. The *Times* loaded 4 TB of raw TIFF images on web and their derivative 11 million PDFs into Amazon's S3 in twenty-four hours at very less cost. This project is very similar to digital library projects run by academic libraries. Few years ago OCLC announced its movement of library management services to the Web It is clear that OCLC is going to deliver a Web-based integrated library system (ILS) on web for enhancing the technology to provide a new way of running an ILS. Dura Space, a joint organization by Fedora Commons and D Space Foundation, announced that they would be taking advantage of cloud storage and cloud computing.

2. Delivery Models of Cloud Computing

The NIST definition of cloud computing defines three delivery models:



2.1. Software as a Service (SaaS)

The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it's running. The SaaS model shown in the diagram admits that
the provider manages the entire suite of applications delivered to end-users. SaaS providers are responsible for securing these applications. Customers can be normally responsible for operational security

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

processes. However the following questions, along with other sections within this document, should assist in assessing their offerings:

• Administration controls are provided by them and can these be controls used to assign read and write privileges to other users?

• SaaS access control is quite fine grained and can be customized to ones organizations policy?

2.2. Platform as a Service (PaaS)

The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework. Generally speaking, PaaS service providers are responsible for the security of the platform software stack, and the recommendations throughout this document is a good foundation for ensuring a PaaS provider has considered security principles before designing and managing their PaaS platform. It is very difficult to get or obtain the detailed information from PaaS providers on exactly how they secure their platforms however there are some of the following questions that should be along with other sections within these document.

• A high level description of containment and isolation measures is required for request information on how multi-tenanted applications are isolated from each other.

• What assurance can the PaaS provider give by which the data can be accessed?

• Does the provider ensure that the PaaS platform sandbox is monitored for new bugs, new attacks and vulnerabilities?

2.3. Infrastructure as a Service (IaaS)

The consumer uses "fundamental computing resources" such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them., Many of the potential issues with personnel security arise because the IT infrastructure is under the control of a third party like traditional outsourcing, multiple customers get effect because of a physical security breach.

• What assurance can be provided to the customer regarding the physical security of the location?

• Who has unescorted access to IT infrastructure? For example, vendors', managers, physical security staff, contractors, consultants, cleaners, etc.

• How often are access rights reviewed?

• How quickly can access rights be revoked?

• Does the security risks are assessed and parameters evaluated on a regular basis?

• How frequently?

• Are regular risk assessments being done which may include things such as neighboring buildings?

• Is access secure areas controled or monitored personnel (including third parties)?

• What are the policies/procedures that are used for loading, unloading and installing equipment?

• When are processes or procedures required to destroy old media or systems?

• Data overwritten?

• Physical destruction?

• How often are checks made to ensure compliance with the environment with the appropriate legal and regulatory requirements of a organization.

• **Public Cloud:** A public cloud is a standard cloud computing model wherein a service provider manages storage and computing resources on behalf of consumer over the Internet.

The term "public cloud" arose to differentiate between the standard model and the private cloud, which runs on proprietary network or data center of the user.

Public clouds are run by third parties, and applications from different users are shared on the provider's cloud servers, storage systems, and networks. Public clouds are most often hosted away from customer premises, and they try to reduce customer risk and cost by substituting their enterprise infrastructure.

Applications which are required for temporary purpose or for short duration are the best suitable for

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

deployment in a public cloud because it avoids the need to purchase additional equipment to solve a temporary need.

• **Private Cloud:** Private cloud (also called internal cloud or corporate cloud) is typically hosted on customer premises. With proprietary computing architecture, it provides hosted services to authorized users behind a company firewall. Thus company has control over resources, data, security and QoS.
The company owns the infrastructure and controls how applications are deployed on it.

Private clouds can be deployed in an organization datacenter or also at a collocation facility. Company's own IT department or cloud service provider can built and manage private clouds. In this type of cloud computing, a company can install, configure, and operate the infrastructure as per its requirement and demand. A permanent application, or one that has specific requirements on quality of service or location of data, is most suitable to deploy in a private or hybrid cloud. Company's own IT department uses their own private clouds for critical and other secured systems deployments

• **Hybrid cloud** is a cloud computing infrastructure composed of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability
In hybrid cloud architecture, companies and individuals can obtain degrees of fault tolerance combined with locally immediate usability without internet connectivity. Y Hybrid Cloud architecture is the ideal combination that requires on premises resources and off site (remote) server based cloud infrastructure. Hybrid clouds do not have the flexibility, security and certainty of in-house applications.

4. Security Issues in Private Cloud Computing

Due primarily to the security concerns associated with the public cloud, many firms have elected to favor private cloud deployments over public clouds. While security pros are on their guard when it comes on private cloud. Private cloud gives more control to in house staff, but increased control cannot ignore the security. On the other hand, there are some security risks associated with all cloud models, private included. Because of security pros are less sensitive to risks and the control is high in the private model.

4.1 Comingled regulatory environments

Security cannot be fitted in every situation of IT environment. For example, that an entity regulated under PCI would find a non PCI certified environment is unacceptable for systems which are in cardholder data environment. This is true for both the public and private cloud.

An infrastructure is dedicated to be used alone does not mean everything can go with equal ease. Because private cloud grants greater control over regulatory compliance and security, the security should always be given the forefront of planning, particularly when multiple types of regulated data are in play, such as a customer data, comingled mix of payment card data and sensitive business intelligence.

4.2 Viability of security tools

When an organization virtualizes a physical host it always needs to evaluate how network aware tools will be impacted. If visibility into traffic can be impacted: network IDS and sniffers. For example, consider an n-tier Web application with separate Web, application and DB servers that attach to one switch that is monitored by IDS. If these three devices are moved to virtual slices on a hypervisor, traffic will no longer visible on the wire, which will cause the IDS to lose visibility. At one time particularly true when large numbers of hosts are virtualized; more number of hosts' means less time spent planning per host.

4.3 Data expansion

Cloud is a fantastic enabler of resource centralization. For example, a virtualized environment can allow far-flung resources to come together under an

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

environment. However, if resources are centralized, data becomes denser. While this its a boon for management, it is challenging from security standpoint, particularly when considering tools are being used that operate across the data in aggregate. Antimalware scanning, bulk encryption and data discovery tools required that when we have a harder time dealing very large amounts of data. Existing tools should be examined to determine what impact they have on data volumes increase and new tools are considered when operation would be impacted severely and old tools are ineffective.

4.4 Future proofing

Private cloud does not means "on-premise," but some may think that way. The defining aspect of private cloud is about which are users that use the infrastructure, not who maintains the infrastructure. So it is not necessarily many private cloud deployments will use on-premise infrastructure. And even if a deployment uses on-premise or dedicated resources today, that cannot prevent it from migrating off-premises to use a service provider or onto shared infrastructure. Organizations that put into a private environment today can easily migrate tomorrow. So private cloud deployments have many security advantages A private cloud deployment is every bit as serious as a move to public cloud and needs to be planned for accordingly.

4.5 Fear of change.

IT team may not be familiar with the term private clouds, so because of that there will be a big learning curve. There can also be new operational processes and some of old processes that need much of the rework. To turn this into a growth opportunity for people, the stress of doing and learning all this can be mitigated by helping your collogues keep in mind that these are important new skills in today's business environment.

Existing System:

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more, if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. How does a cloud customer know whether his data were processed correctly within the cloud? There is no technical way to guarantee that an operation performed in a cloud system was not tampered with or that the cloud system was not compromised by an attacker. The only kind of guarantee is based on the level of trust between the cloud customer and the cloud provider and on the contractual regulations made between them such as SLAs, applicable laws, and regulations of the involved jurisdictional domains. But even if the relation and agreements are perfectly respected by all participants, there still remains a residual risk of getting compromised by third parties.

Disadvantages:

1. Cost is high related to operational expenditures (hardware, software)
2. Third party auditors are not control the all security risks.
3. Misuse the cloud services
4. Attackers are going to alter and manipulations of data.

Proposed System:

One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple clouds. Several approaches employing this paradigm have been proposed recently. They differ in

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

partitioning and distribution patterns, technologies, cryptographic methods, and targeted scenarios as well as security levels. This paper is an extension of and contains a survey on these different securities by multi cloud adoption approaches. It provides four distinct models in form of abstracted multi cloud architectures. These developed multi cloud architectures allow to categorize the available schemes and to analyze them according to their security benefits. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular. The rest of this paper is organized as follows: motivates the need for effective cloud security countermeasures by briefly reviewing the current state of play. The observations further lead to the fact that most of the research and development work is currently devoted to dedicated security schemes, which do not consider the specific properties of the cloud itself. Only recently some proposals on making use of multiple distinct clouds at the same time to realize security goals started to appear.

Advantages:

1. Reduce the capital and expenditure.
2. Reduce the attacker risks
3. Its gives the confidentiality and mitigate the attacks

Modules Description:

1. Replication of applications
2. Partition of application system into tiers
3. Partition of application logic into fragments
4. Partition of application data into fragments

Replication of applications:

Multiple distinct clouds executing multiple copies of the same application can be deployed. Instead of executing a particular application on one specific cloud, the same operation is executed by distinct clouds. By comparing the obtained results, the cloud user gets evidence on the integrity of the result. In such a setting, the required trust toward the cloud service provider can be lowered dramatically. Instead of trusting one cloud service provider totally, the cloud user only needs to rely on the assumption that the cloud providers do not collaborate maliciously against herself.

Partition of application system into tiers:

It needs to be noted, that the security services provided by this architecture can only be fully exploited if the execution of the application logic on the data is performed on the cloud user's system. Only in this case, the application provider does not learn anything on the users' data. Thus, the SaaS-based delivery of an application to the user side in conjunction with the controlled access to the user's data performed from the same user's system is the most far reaching instantiation. Besides the introduced overhead due to the additionally involved cloud, this architecture requires, moreover, standardized interfaces to couple applications with data services provided by distinct parties. Also generic data services might serve for a wide range of applications there will be the need for application specific services as well.

Partition of application logic into fragments:

The idea of this architecture is that the application logic needs to be partitioned into fine-grained parts and these parts are distributed to distinct clouds. This approach can be instantiated in different ways depending on how the partitioning is performed. The clouds participating in the fragmented applications can be symmetric or asymmetric in terms of computing power and trust. Two concepts are common. The first involves a trusted private cloud that takes a small critical share of the computation, and a un-trusted public cloud that takes most of the computational load. The second distributes the computation among several un-trusted public clouds, with the assumption that these clouds will not collude to break the security.

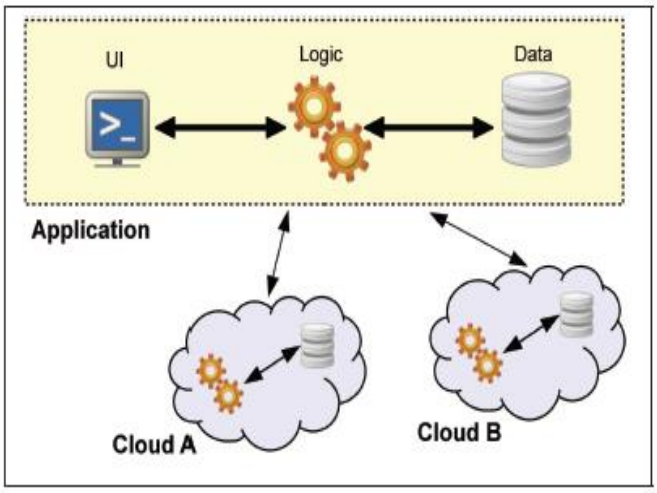
Partition of application data into fragments:

The most common forms of data storage are files and databases. Files typically contain unstructured data and do not allow for easily splitting or exchanging parts of the data. This kind of data can only be partitioned using cryptographic methods. Databases contain data

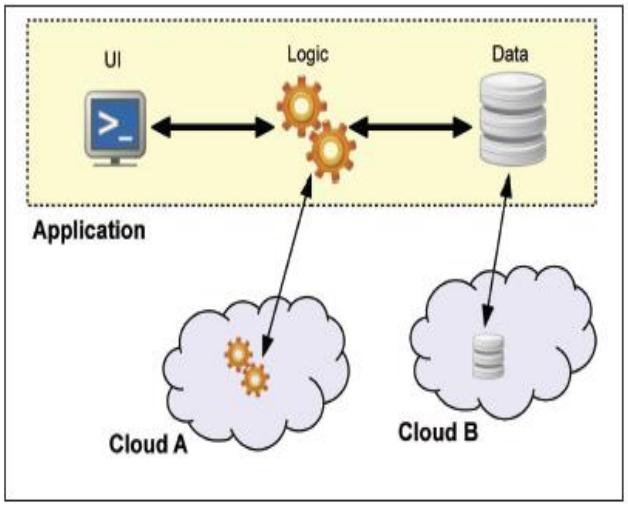
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

in structured form organized in columns and rows. Here, data partitioning can be performed by distributing different parts of the database to different cloud providers. Finally, files can also contain structured data. Here, the data can be splitted using similar approaches like for databases.

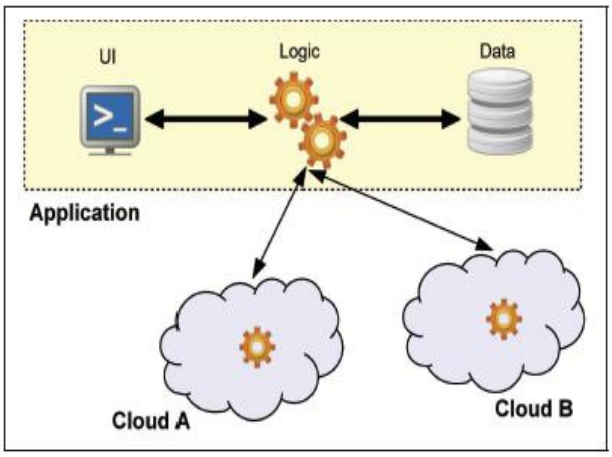
Architecture:



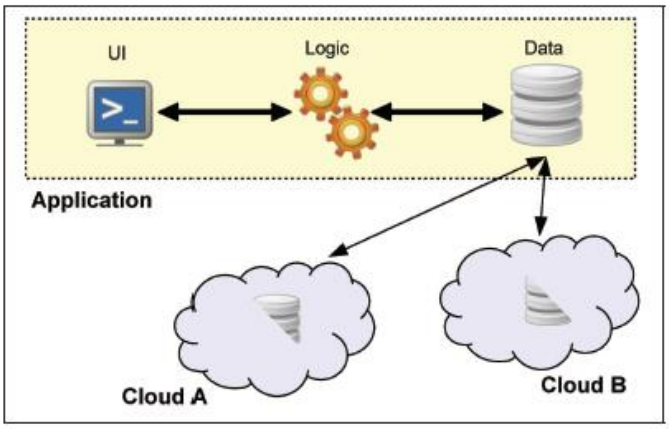
Replication of Application Systems



Partitioning of application system into tiers



Partitioning of application logic into fragments



Partition of application data into fragments

Conclusion

We explicitly do not investigate this field here—due to space restrictions; however we encourage the research community to explore these combinations, and assess their capabilities in terms of the given evaluation dimensions.Second, we identified the fields of homomorphic encryption and secure multiparty computation protocols to be highly promising in terms of both technical security and regulatory compliance. As of now, the limitations of these approaches only stem from their narrow applicability and high complexity in use. However, given their excellent properties in terms of security and compliance in multicloud architectures, we envision these fields to become the major building blocks for future generations of the multicloud computing paradigm.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

References

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE, Luigi Lo Iacono, and Ninja Marnau"Security and Privacy-Enhancing Multicloud Architectures" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, Version 15," Nat'l Inst. of Standards and Technology, Information Technology Laboratory, vol. 53, p. 50, http://csrc.nist.gov/groups/SNS/cloud-computing/, 2010.

[3] F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits & Challenges," blog, http://blogs.idc.com/ie/?p=210, 2008.

[4] Gartner, "Gartner Says Cloud Adoption in Europe Will Trail U.S. by at Least Two Years," http://www.gartner.com/it/page. jsp?id=2032215, May 2012.

[5] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD), 2011.

[6] D. Hubbard and M. Sutton, "Top Threats to Cloud Computing V1.0," Cloud Security Alliance, http://www. cloudsecurityalliance.org/topthreats, 2010.

[7] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing," Proc. IEEE Int'l Conf. Cloud Computing (CLOUD-II), 2009.

[8] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third- Party Compute Clouds," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 199-212, 2009.

[9] Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 305-316, 2012.

[10] N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," Proc. IEEE Int'l Conf. Web Services (ICWS '09), 2009.

[11] M. McIntosh and P. Austel, "XML Signature Element Wrapping Attacks and Countermeasures," Proc. Workshop Secure Web Services, pp. 20-27, 2005.

[12] J. Kincaid, "Google Privacy Blunder Shares Your Docs without Permission," TechCrunch, http://techcrunch.com/2009/03/07/ huge-google-privacy-blunder-shares-your-docs-withoutpermission/, 2009.

[13] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces," Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW '11), pp. 3-14, 2011.

[14] S. Bugiel, S. Nu¨ rnberger, T. Po¨ppelmann, A.-R. Sadeghi, and T. Schneider, "AmazonIA: When Elasticity Snaps Back," Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11), pp. 389-400, 2011.

[15] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the Intercloud—Protocols and Formats for Cloud Computing Interoperability," Proc. Int'l Conf. Internet and Web Applications and Services, pp. 328-336, 2009.