International Journal of Research in Advent Technology (IJRAT)
Vol. 1, No. 3, October 2013, ISSN: 2321–9637

CLOUD COMPUTING PRIVACY ISSUES: A REVIEW

Rahul Bhoyar[1], Prof. Nitin Chopde[2]
Department of Computer Engineering)
[1]*M.E Scholar*
2Assistant Professor
[1]rahulbhoyar46@yahoo.com
[2]nitin.chopde@raisoni.net

ABSTRACT:
The evolution of cloud computing over the past few years is potentially one of the major advances in the history of computing. From a user's perspective, cloud computing involves performing a task using someone else's computers and possibly software. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. While the economic case for cloud computing is compelling, the security challenges it poses are equally striking. Cloud provides many advantages for IT organizations, cloud has some issues that must be consider during its deployment. The main concern is security privacy and trust. In this paper we reviewed security privacy & trust issues of cloud computing.

Keywords: *cloud computing, software, resources, security, challenges.*

1. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing is a technology that keep up data and its application by using internet and central remote servers [1]. The emergence of the phenomenon commonly known as cloud computing represents a fundamental change in the way informationtechnology (IT) services are invented, developed, deployed, scaled, updated, maintained and paid for. Computing as we know todayreflects a paradox — on one hand, computers continue to becomeexponentially more powerful and the per-unit cost of computingcontinues to fall rapidly, so much so that computing power per se isnowaday's considered to be largely a commodity [2,3]. On theother hand, as computing becomes more pervasive within theorganization, the increasing complexity of managing the wholeinfrastructure of disparate information architectures and distributeddata and software has made computing more expensive than everbefore to an organization [4]. The promise of cloud computing isto deliver all the functionality of existing information technologyservices (and in fact enable new functionalities that are hithertoinfeasible) even as it dramatically reduces the upfront costs ofcomputing that deter many organizations from deploying manycutting-edge IT services [5].Cloud computing enables hardware and software to be delivered as services, where the term service is used to reflect the fact that they are provided on demand and are paid on a usage basis – the more you use the more you pay. Draw an analogy with a restaurant. This provides a food and drinks service. If we would like to eat at a restaurant, we do not buy it, just use it as we require. The more we eat the more we pay. Cloud Computing provides computing facilities in the same way as restaurants provide food, when we need computing facilities; we use them from the cloud. The more we use the more we pay,when we stop using them we stop paying.

Figure 1 - Introduction to cloud computing [53]

2. CLOUD SERVICE MODELS

Cloud computing providers offer their services according to three fundamental models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models. In 2012 network as a service (Naas) and communication as a service (CaaS) were officially included by ITU (International Telecommunication Union) as part of the basic cloud computing models, recognized service categories of a telecommunication-centric cloud ecosystem.[7]

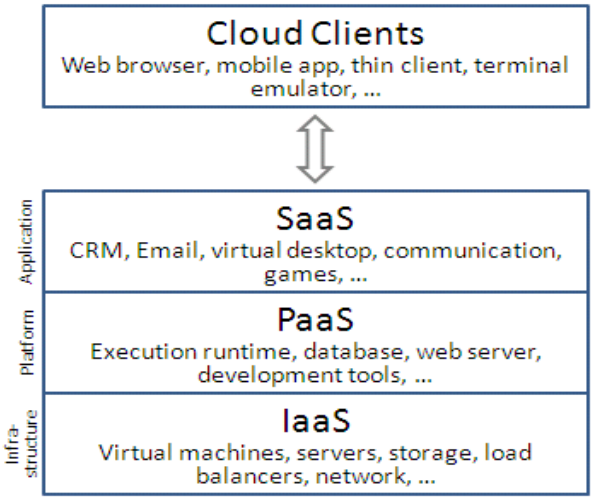

Figure 2 - Service models [6]

- **Infrastructure as a service (IaaS)**

This covers a wide range of features, from individual servers, to private networks, disk drives, various long term storage devices as well as email servers, domain name servers as well as messaging systems. In the most basic cloud-service model, providers of IaaS offer computers - physical or (more often) virtual machines - and other resources. IaaS clouds often offer additional resources such as images in a virtual-machine image-library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centres. For wide area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks).To deploys their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the amount of resources allocated and consumed. [7]

Examples of IaaS providers include Amazon CloudFormation, Amazon EC2.

- **Platform as a service (PaaS)**

"PaaS is intended to enable developers to build their own applications on top of the platform. As a result, it tends to be more extensible than SaaS, at the expense of customer-ready features. This trade-off extends to security features and capabilities, where the build-in capabilities are less complete, but there is more flexibility to layer on additional security."[7]
In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Used by software development companies to run their software products. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. [7]
Examples of PaaS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, OrangeScape. [7]

- **Software as a service (SaaS)**

In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. [7]
This is typically end user applications delivered on demand over a network on a pay per use basis. The software requires no client installation, just a browser and network connectivity. An example of SaaS is MicrosoftOffice365. Until its launch, if a user required say Word, they would have to purchase it, install it, backup files etc. With Office365 Word can be acquired for a small monthly fee, with no client installation, the files are automatically backed up, software upgrades are automatically received and the software can be accessed from anywhere. Decide you do not require Word anymore – stop paying the monthly fee. It is that simple.[7]
Examples of SaaS include: google apps, MicrosoftOffice365, Onlive,GTNexus,Marketo, and TradeCard.

- **Network as a service (NaaS)**

A category of cloud services where the capability provided to the cloud service user is to use network/transport connectivity services and/or inter-cloud network connectivity services. NaaS involves the optimization of resource allocations by considering network and computing resources as a unified whole. Traditional NaaS services include flexible and extended VPN, and bandwidth on demand. NaaS concept materialization also includes the provision of a virtual network service by the owners of the network infrastructure to a third party (VNP – VNO). [7]

3. CLOUDDEPLOYMENT MODELS

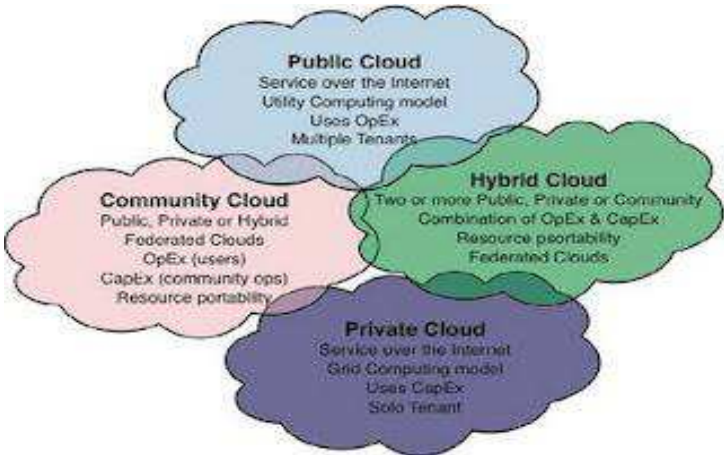

Figure 3 -Deployment models operated by Cloud Computing [9]

Private cloud -- The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.[8]

Community cloud -- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.[9]

Public Cloud --Enterprises may use cloud functionality from others, respectively offer their own services to users outside of the company. Providing the user with the actual capability to exploit the cloud features for his her own purposes also allows other enterprises to outsource their services to such cloud providers, thus reducing costs and effort to build up their own infrastructure. As noted in the context of cloud types, the scope of functionalities thereby may differ. Example: Amazon, Google Apps, Windows Azure.[8]
Hybrid cloud -- The cloud infrastructure is a composition 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 (e.g., cloud bursting for load-balancing between clouds).[9]

4. CLOUD SECURITY ISSUES AND CHALLENGES

4.1 CLOUD COMPUTING SECURITY

1) Network security: Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is having cloud services as an extension of customer's existing internal networks [13], adopting the same protection measures and security precautions that are locally implemented and allowing to extend local strategies to any remote resources or processes.
a) Transfer security: Distributed architectures, massive resource sharing and virtual machine (VM) instances synchronization imply more data in transiting the cloud, thus requiring VPN mechanisms for protecting the system against sniffing, spoofing, man-in-the-middle and side-channel attacks.
b) Firewalling: Firewalls protect the provider's internal cloud infrastructure against insiders and outsiders [14] and enable VM isolation, fine-grained filtering for addresses and ports, prevention of Denial-of-Service (DoS) and detection of external security assessment procedures. Efforts for developing consistent firewall and other security measures specific for cloud environments [15], [16]reveals the urge for adapting existing solutions for this new computing paradigm.
c) Security configuration: Configuration of protocols, systems and technologies to provide required levels of security and privacy without compromising performance or efficiency.
2) Interfaces: Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds.
a) API: Programming interfaces (essential to IaaS andPaaS) to access virtualized resources and systems must be protected in order to prevent malicious use[17], [18], [19], [20], [21].
b) Administrative interface: Enables remote control of resources in an IaaS (VM management), development for PaaS (coding, deploying, testing)and application tools for SaaS (user access control, configurations).
c) User interface: End-user interface for exploring provided resources and tools (the service itself), implying the need of adopting measures for securing the environment [22], [23], [24], [25].
d) Authentication: Mechanisms required to enable access to the cloud. Most services rely on regular accounts [18], [26], [27] consequently being susceptible to a plethora of attacks [28], [29], [30],[31], [32]. The consequences are boosted by multitenancy and resource sharing.
3) Data security: Protection of data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution which requires basic security levels).
a) Cryptography: Most employed practice to secure sensitive data [33], thoroughly required by industry, state and federal regulations.
b) Redundancy: Essential to avoid data loss. Mostbusiness models rely on information technology forits core functionalities and processes [34], [35] and, thus, mission-critical data integrity and availabilitymust be ensured.
c) Disposal: Elementary data disposal techniques are insufficient and commonly referred as deletion [36].In the cloud, the complete destruction of data, including log references and hidden backup registries, are an important requirement [37].

4) Virtualization: Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies [38].
a) Isolation: Even though logically isolated, all VMs share the same hardware and consequently the same resources, allowing the exploit of data leaks and cross-VM attacks. The concept of isolation can also be applied to more fine-grained assets, such as computational resources, storage and memory.
b) Hypervisor vulnerabilities: The hypervisor is the main software component of virtualization. Even though there are known security vulnerabilities for hypervisors, solutions are still scarce and often proprietary, demanding further studies to harden these security aspects.
5) Governance: Issues related to (losing) administrative and security controls in cloud computing solutions.
a) Data control: Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations [39].
b) Security control: Loss of governance over security mechanisms and policies, as terms of use prohibit customer-side vulnerability assessment and penetration tests while insufficient Service Level Agreements (SLA) lead to security gaps.
c) Lock-in: User potential dependency on a particular service provider due to lack of well-established standards (protocols and data formats), consequently becoming particularly vulnerable to migrations and service termination.
6) Compliance: Category which includes requirements related to service availability and audit capabilities [40].
a) Service Level Agreements (SLA): Mechanisms to ensure the required service availability and thebasic security procedures to be adopted.
b) Loss of service: Service outages are not exclusive to cloud environments but are more serious in this context due to interconnections between services (aSaaS using virtualized infrastructures provided byan IaaS), [41], [42],[43]. Thus it is required strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.
c) Audit: Enables security and availability assessments to be performed by customers, providers
and third-party participants. Transparent and efficient methodologies are necessary for continuously analyzing service conditions [44] and are usually required by contracts or legal regulations. There are solutions being developed to address this problem by offering a transparent API for automated auditing and other useful functionalities [45].
7) Legal issues: Juridical concerns related to new concepts introduced by cloud computing [46], such as multiple data locations and privilege management.
a) Data location: Customer data held in multiple jurisdictions depending on geographic location [47], therefore being affected, directly or indirectly, bysubpoena law-enforcement measures.
b) E-discovery: As a result of a law-enforcement measure, hardware might be confiscated for investigations related to a particular customer, affectingall customers whose data were stored in the samehardware [48], [49], [50]. Data disclosure is critical in this case.
c) Provider privilege: Malicious activities of provider insiders are potential threats to confidentiality, availability and integrity of customers' data and processes' information [51], [52].

4.2 CLOUD COMPUTING CHALLENGES

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows: A. Security: It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model andthe pooled computing resources in cloud computing has introduced new security challenges thatrequire novel techniques to tackle with. For example, hackers can use Cloud to organize botnetas Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack. [10]
B. Costing Model: Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed

amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, ondemandcomputing makes sense only for CPU intensive jobs. [10]

C. Charging Model: The elastic resource pool has made the cost analysis a lot more complicated than regular data canters, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multitenancy within their offering can be very substantial. These include: re-design and redevelopment of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provision of multitenancyand the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viablecharging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloudproviders. [10]

D. Service Level Agreement (SLA): Although cloud consumers do not have control over theunderlying computing resources, they do need to ensure the quality, availability, reliability, andperformance of these resources when consumers have migrated their core business functionsonto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees fromproviders on service delivery. Typically, these are provided through Service Level Agreements(SLAs) negotiated between the providers and consumers. The very first issue is the definition ofSLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by theresource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS,andSaaS) will need to define different SLA met specifications. This also raises a number ofimplementation problems for the cloud providers. Furthermore, advanced SLA mechanisms needto constantly incorporate user feedback and customization features into the SLA evaluationframework. [11]

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, the sevenIT systems/applications being migrated to the cloud are: IT Management Applications (26.2%),Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%),Applications Development and Deployment (16.8%), Server Capacity (15.6%), and StorageCapacity (15.5%). This result reveals that organizations still have security/privacy concerns inmoving their data on to the Cloud. Currently, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are conservative inemploying IaaS compared to SaaS. This is partly because marginal functions are oftenoutsourced to the Cloud, and core activities are kept in-house. The survey also shows that inthree years time, 31.5% of the organization will move their Storage Capacity to the cloud.However this number is still relatively low compared to Collaborative Applications (46.3%) at thattime. [12]

F. Cloud Interoperability Issue: Currently, each cloud offering has its own way on how cloudclients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. Thisseverely hinders the development of cloud ecosystems by forcing vendor locking, which prohibitsthe ability of users to choose from alternative vendors/offering simultaneously in order to optimizeresources at different levels within an organization. More importantly, proprietary cloud APIsmakes it very difficult to integrate cloud services with an organization's own existing legacysystems (e.g. an on-premise data centre for highly interactive modeling applications in apharmaceutical company).The primary goal of interoperability is to realize the seamless fluid dataacross clouds and between cloud and local applications. There are a number of levels thatinteroperability is essential for cloud computing. First, to optimize the IT asset and computingresources, an organization often needs to keep in-house IT assets and capabilities associatedwith their core competencies while outsourcing marginal functions and activities (e.g. the humanresource system) on to the cloud. Second, more often than not, for the purpose of optimization,an organization may need to outsource a number of marginal functions to cloud services offeredby different vendors. Standardization appears to be a good solution to address the interoperabilityissue. However, as cloud computing just starts to take off, the interoperability problem has notappeared on the pressing agenda of major industry cloud vendors. [10]

5. CONCLUSION

Cloud computing is the most modern technology so lots of issues are remained to consider.This paper has provided a summary and analysis of some of the current literature in the area of cloud security. It has many open

issues some are technical that includes scalability, elasticity ,data handling mechanism, reliability, license software, ownership, performance, system development and management and non-technical issues like legalistic and economic aspect.The paper addresses the issues and challanges that can arise during the deployment of cloud services.

REFERENCES

[1] PriyankaArora, Arun Singh, HimanshuTyagi ―Analysis of performance by using security algorithm on cloud network‖ in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 june, 2012.
[2] S. Hackett, Managed Services: An Industry Built on Trust, IDC, 2008.
[3] J.D. Lasica, Identity in the Age of cloud computing: The Next-generation Internet'sImpact on Business, Governance and Social Interaction, The Aspen Institute, 2009.
[4] P. Roehrig, New Market Pressures Will Drive Next-Generation IT ServicesOutsourcing, Forrester Research, Inc., 2009
[5] J. Staten, Hollow Out The MOOSE: Reducing Cost With Strategic Rightsourcing,Forrester Research, Inc., 2009
[6] http://en.wikipedia.org/wiki/File:Cloud_computing_layers.png
[7] Rahul Bhoyar,Nitinchopde,CloudComputing:Servicemodels,Types,Database and Issues,2013
[8] Harjit Singh, Current Trends in Cloud Computing A Survey of Cloud Computing Systems.
[9] K.S.Suresh,K.V.Prasad,Security Issues and Security Algorithms in Cloud Computing,2012
[10] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" InPROC 2010 IEEE International Conference on Cloud Computing 2010.
[11] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser."Business Models in the ServiceWorld."IT Professional, vol. 11, pp. 28-33, 2009.
[12] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges",IDC eXchange,Available:<http://blogs.idc.com/ie/?p=730>[Feb.18,2010].http://www.csoonline.com/article/658121/cloudpassage-aimsto-ease-cloud-server-security-management, January 2011.
[13]D.Tompkins,"Securityfor cloud-based enterprise applications,"http://blog.dt.org/index.php/2009/02/security-for-cloud-basedenterprise-applications/, February 2009.
[14] TrendMicro, "Cloud Computing Security - Making Virtual MachinesCloud-Ready," Trend Micro White Paper, May 2010.
[15] S. Genovese, "Akamai introduces cloud-based firewall,"http://cloudcomputing.sys-con.com/node/1219023, December 2009.
[16] G. V. Hulme, "Cloudpassage aims to ease cloud server security management,"http://www.csoonline.com/article/658121/cloudpassage-aimsto-ease-cloud-server-security-management, January 2011.
[17] Google, "Google App Engine," code.google.com/appengine/, 2011.
[18]"Googlequerylanguage(gql),"code.google.com/intl/en/appengine/docs/python/overview.html, 2011.
[19] StackOverflow, "Does using non-sql databases obviatethe need for guarding against sql injection?"stackoverflow.com/questions/1823536/does-using-non-sql-databasesobviate-the-need-for-guarding-against-sql-injection, 2011.
[20]J.Rose,"Cloudy with a chance of zero day,"www.owasp.org/images/1/12/Cloudy_with_a_chance_of_0_day_-_Jon_Rose-Tom_Leavey.pdf, 2011.
[21] A. Balkan, "Why Google App Engine is broken and what Google mustdo to fix it," aralbalkan.com/1504, 2011.
[22] Salesforce, "Salesforce security statement," salesforce.com/company/privacy/security.jsp, 2011.
[23] T. Espiner, "Salesforce tight-lipped after phishing attack,"zdnet.co.uk/news/security-threats/2007/11/07/salesforce-tight-lippedafter-phishing-attack-39290616/, November 2007.
[24]A.Yee,"Implications of salesforce phishing incident,"ebizq.net/blogs/security_insider/2007/11/-implications_of_salesforce_phi.php, November 2007.

[25] Salesforce, “Security Implementation Guide,” login.salesforce.com/help/doc/en/salesforce_security_impl_guide.pdf,April 2011.
[26] Amazon, “Elastic compute cloud (ec2),” aws.amazon.com/ec2/, 2011.
[27] C. Kaufman and R. Venkatapathy, “Windows azure security overview,”go.microsoft.com/?linkid=9740388, 2010, august.
[28] R. McMillan, “Google attack part of widespread spying effort,” PCWorld,January 2010.
[29] E. Mills, “Behind the china attacks on google,” CNET News, January,2010.
[30] M. Arrington, “Google defends against large scale chinesecyber attack:May cease chinese operations,” TechCrunch, January 2010.
[31] J. Bosch, “Google accounts attacked by phishing scam,” BrickHouseSecurity Blog, October 2009.
[32] T. Telegraph, “Facebook users targeted by phishing attack,” The Telegraph,May 2009.
[33] L. Musthaler, “Cost-effective data encryption in the cloud,” NetworkWorld, December 2009.
[34] C. Tech, “Examining redundancy in the data center powered by the cloudand disaster recovery,” Consonus Tech, 2010.
[35] M. Lyle, “Redundancy in data storage,” Define the Cloud, February2011.
[36] P. Dorion, “Data destruction services: When data deletion is not enough,”SearchDataBackup.com, 2010.
[37] R. Mogull, “Cloud data security: Archive and delete (roughcut),” securosis.com/blog/cloud-data-security-archive-and-delete-roughcut/,September 2009.
[38] E. Messmer, “Gartner: New security demands arising for virtualization,cloud computing,” http://www.networkworld.com/news/2011/062311-security-summit.html, June 2011.