INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Trust, Security And Governance In Cloud Computing

Nandini Mishra
Department of computer Science,Bhagwant University,India
Saurabh Sharma
Department of computer Science,Bhagwant University,India
Ritu Chasta
Department of computer Science,Bhagwant University,India

Abstract:
One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, in this article we identify and classify the main security concerns and solutions in cloud computing, and propose a taxonomy of security in cloud computing, giving an overview of the current status of security in this emerging technology. In this highly competitive and distributed service environment, the assurances are insufficient for the consumers to identify the dependable and trustworthy Cloud providers. Governance with cloud computing offers integration management with automated problem resolution, manages security end to end, and helps budget based on actual usage of data. governance is not yet mature enough to consistently and reliably protect their data. As the trend toward cloud-based services continues to grow, it has become clear that one of the key barriers to rapid adoption of enterprise cloud services is customer concern over data security (confidentiality, integrity, and availability). This paper introduces the concept of transparent security and makes the case that the intelligent disclosure of security design, practices, and procedures can help improve customer confidence while protecting critical security features and data, thereby improving overall governance. Cloud Computing is better for medium and small sized enterprises as compared to large enterprises in terms of both cost and data security.

Keywords: *Cloud computing, security, Trust, Governance.*

1.Introduction

Cloud computing offers dynamic, scalable, shared, and elastic resources (e.g., computing power, storage, software, etc.) over the internet from remote data centres to the users (e.g., business organizations, government authorities, individuals, etc.). The opportunities afforded by cloud computing are too attractive for the consumers (which we also refer to as "customers") to ignore in today's highly competitive service environments (which we also refer to as "marketplaces"). The way to realizing these opportunities, however, is not free of obstacles. The highly distributed and non-transparent nature of cloud computing represents a considerable obstacle to the acceptance and market success of cloud services. Potential users of these services often feel that they lose control over their data and they are not sure whether cloud providers can be trusted. It is not that users don't trust the Cloud providers to be willing to provide a service well, rather they are concerned and confused about the capabilities of Cloud providers . Many contend that cloud computing holds promise to provide considerable benefits for colleges and universities. By moving storage, processing, applications, or other IT infrastructure and services to the cloud, institutions might realize increased reliability and flexibility, with lower or more transparent costs. Even the most optimistic scenarios, however, must account for a raft of security questions that are complicated or exacerbated due to the loss of control. Information security depends on the three principles of confidentiality (who has access), integrity (correctness of information), and availability (ability to access information and services at appropriate times). These elements constitute computer security in any context, and they take on new significance in cloud computing because it depends on third-party providers. Higher education is subject to regulations concerning the protection of student records and other data, and individual campuses tend to be idiosyncratic with respect to state or local requirements and cultural attitudes towards risk. In this context, any institution that turns to cloud computing faces important questions about how information assets will be safeguarded and what measures are in place to secure those assets over time kj. This article is the first survey focusing on the hindrances for adopting Cloud computing and how the trust concepts can support the consumers in overcoming these hindrances.

Cloud computing is a recent technology and a lot of research are made in that domain to improve it. Also due to the relation between cloud and virtualization there are as well many researches on virtualization to enhance virtualization performances. Cloud computing is more and more popular and most of the enterprise begin to adopt it.

However there are still some obstacles which can restrained the adoption of cloud services by enterprise such as the lack of standardisation, reliability associate to the cloud, the security and so on. The reason of the adoption of cloud computing by enterprise is principally for economical reasons because cloud computing allow customers to reduce their hardware cost as well as energy consumption and so on.
Governance and the service in the cloud Encourage collaboration between governments, the private sector, civil society andthe Internet technical community in building an understanding of the impact of the Internet on minors in order to enhance their protection and support when using the Internet.

1.1.Definition Of Cloud Computing

"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."

1.2.Types of Cloud Computing

1.2.1. Public Cloud

Public cloud (also referred to as 'external' cloud) describes the conventional meaning of cloud computing: scalable, dynamically provisioned, often virtualized resources available over the Internet from an off-site third-party provider, which divides up resources and bills its customers on a 'utility' basis. An example is Think Grid, a company that provides a multi-tenant architecture for supplying services such as Hosted Desktops, Software as a Service and Platform as a Service. Other popular cloud vendors include Salesforce.com, Amazon EC2 and Flexi scale.

1.2.2.Private Cloud

Private cloud (also referred to as 'corporate' or 'internal' cloud) is a term used to denote a proprietary computing architecture providing hosted services on private networks. This type of cloud computing is generally used by large companies, and allows their corporate network and data centre administrators to effectively become in-house 'service providers' catering to 'customers' within the corporation. However, it negates many of

the benefits of cloud computing, as organizations still need to purchase, set up and manage their own clouds.

1.2.3.Hybrid Cloud

It has been suggested that a hybrid cloud environment combining resources from both internal and external providers will become the most popular choice for enterprises. For example, a company could choose to use a public cloud service for general computing, but store its business-critical data within its own data centr.

2.Security

Aiming to concentrate and organize information related to cloud security and to facilitate future studies, in this section we identify the main problems in the area and group them into a model composed of seven categories, based on the aforementioned references. Namely, the categories are: network security, interfaces, data security, virtualization, governance, compliance and legal issues. Each category includes several potential security problems, resulting in a classification with subdivisions that highlights the main issues identified in the base references

2.1.Network security

Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is to have cloud services as an extension of customers' existing internal networks, adopting the same protection measures and security precautions that are locally implemented and allowing them to extend local strategies to any remote resource or process .

2.2.Transfer Security

Distributed architectures, massive resource sharing and virtual machine (VM) instances synchronization imply more data in transit in the cloud, thus requiring VPN mechanisms for protecting the system against sniffing, spoofing, man-in-the-middle and side-channel attacks.

2.3.Firewalling

Firewalls protect the provider's internal cloud infrastructure against insiders and outsiders. They also 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 similar security measures specific for cloud environments reveal the urge for adapting existing solutions for this new computing paradigm.

Security configuration: Configuration of protocols, systems and technologies to provide the required levels of security and privacy without compromising performance or efficiency.

2.4.Interfaces

Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds.

2.4.1.API

Programming interfaces (essential to IaaS and PaaS) for accessing virtualized resources and systems must be protected in order to prevent malicious use .

2.4.2. Administrative interface

Enables remote control of resources in an IaaS (VM management), development for PaaS (coding, deploying, and testing) and application tools for SaaS (user access control, configurations).

2.4.3.User interface

End-user interface for exploring provided resources and tools (the ser(d) Authentication: Mechanisms required to enable access to the cloud . Most services rely on regular accounts consequently being susceptible to a plethora of attacks whose consequences are boosted by multi-tenancy and resource sharing.

2.4.4.Data security

Protection of data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution requiring basic security levels).

- Cryptography: Most employed practice to secure sensitive data, thoroughly required by industry, state and federal regulations.

- Redundancy: Essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes and, thus, mission-critical data integrity and availability must be ensured.
- Disposal**:** Elementary data disposal techniques are insufficient and commonly referred as deletion .In the cloud, the complete destruction of data, including log references and hidden backup registries, are an important requirement.

1.4.5.Virtualization**:**

Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies.

- Isolation: Although logically isolated, all VMs share the same hardware and consequently the same resources, allowing malicious entities to exploit 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.
- 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.
- Data leakage: Exploit hypervisor vulnerabilities and lack of isolation controls in order to leak data from virtualized vice itself), infrastructures, obtaining sensitive customer data and affecting confidentiality and integrity.
- VM identification: Lack of controls for identifying virtual machines that are being used for executing a specific process or for storing files.
- Cross-VM attacks: Includes attempts to estimate provider traffic rates in order to steal cryptographic keys and increase chances of VM placement attacks. One example consists in overlapping memory and storage regions initially dedicated to a single virtual machine, which also enables other isolation-related attacks.

1.4.6.Governance

Issues related to (losing) administrative and security controls in cloud computing solutions.

- Data control: Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations.
- 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.
- 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.

1.4.7.Compliance

Includes requirements related to service availability and audit capabilities.

- Service Level Agreements (SLA): Mechanisms to ensure the required service availability and the basic security procedures to be adopted.
- Loss of service: Service outages are not exclusive to cloud environments but are more serious in this context due to the interconnections between services (e.g., a SaaS using virtualized infrastructures provided by an IaaS), as shown in many examples[25]. This leads to the need of strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.
- Audit: Allows 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 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 .
- Service conformity: Related to how contractual obligations and overall service requirements are respected and offered based on the SLAs predefined and basic service and customer needs.

1.4.8.Legal Issues

Aspects related to judicial requirements and law, such as multiple data locations and privilege management.

- Data location: Customer data held in multiple jurisdictions depending on geographic location are affected, directly or indirectly, by subpoena law-enforcement measures.

- E-discovery: As a result of a law-enforcement measures, hardware might be confiscated for investigations related to a particular customer, affecting all customers whose data were stored in the same hardware. Data disclosure is critical in this case.
- Provider privilege: Malicious activities of provider insiders are potential threats to confidentiality, availability and integrity of customers' data and processes' information.
- legislation: Juridical concerns related to new concepts introduced by cloud Computing.

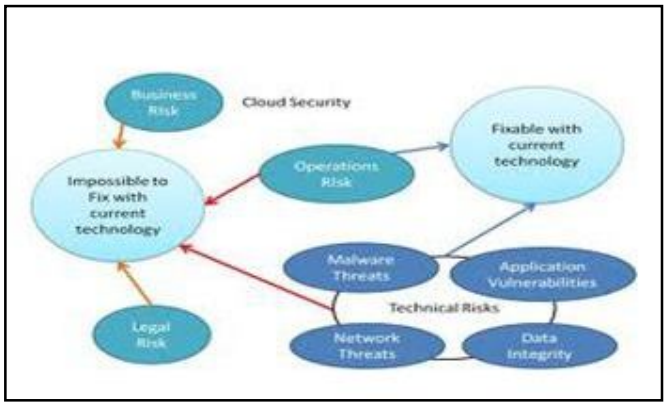

Figure 1: Security Cloud

3.Trust

3.1.Trust Cloud Application

"Identity Providers have a responsibility to issue IDs that can be used holistically by the individual and not just for the relationship with that provider. This includes governments."

- "Identity and access management must absolutely be applied to devices, data and applications as well as users."
- "Cloud service providers should by default NOT seek to be identity providers unless there is a compelling public interest being served and IDP is a core business."

- "Consumers should reward cloud service providers who offer their services as relying parties to well known and trusted identity providers and minimize their own collection of identity information"
- "Strong authentication should be ubiquitous, flexible and natively supported by the identity provider."
- "Individuals should have the tools to manage their own digital identity and be able to leverage claims-based identity principles to access cloud services."
- "Major cloud identity providers need to publicly commit to 'network neutrality' principles to provide no competitive advantage to their own SaaS commercial applications over third party SaaS commercial applications."

3.2.Trust In Cloud Computing

Trust issues become particularly important when data processing is decentralized across geographically dispersed data centers and resources are distributed beyond a definable and controllable perimeter, which is especially true in the Cloud computing scenario. in particular establishing trust on Cloud providers.

Current

3.3.Trust Evaluation

For complex, distributed environments (e.g., Cloud computing) we introduce a categorization of mechanisms that are relevant for trust evaluation that – to the best of our knowledge – have not been discussed in this context before:

- Black box approach: Following this approach, the trustworthiness of an entity or a service is evaluated taking into account only the observed output, for example by only considering user feedback. Models in this class treat the service as a black box, and do not require (or consider) any knowledge about the internal processes and components of the service.
- Inside-out approach: Following this approach, the trustworthiness of an entity or a service is derived based on the knowledge about the architecture of the service and the trustworthiness of its components (or subsystems). For recent approaches
- Outside-in approach: A model that is following this approach requires knowledge about the internal architecture of a service and its components as input as well as information stating the observed behavior of the overall service. The goal of this

kind of model is to derive the trustworthiness of internal components of a service composition based on its external behavior[30].

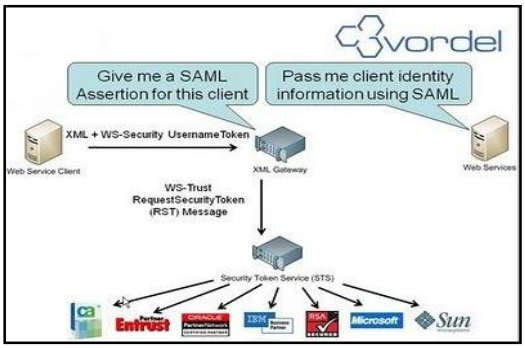

Figure 2: Trust cloud

4.Governance

4.1.E-Governance Requirements

E-Governance is a process of reform in the way and deliver services to external and internal clients for the benefit of both government and the clients that they serve. Governments have innumerable applications that can be automated. Government spending increase the productivity of the government etc. Applications in the government all the applications fall under these categories:

- Government to Government (work. Majority of these applications are both a specific application of the degree of message passing across departments.
- Government to Enterprise (governments and should react quickly to government policies auditing (for accountability) are the biggest challenges.
- Government to Business (G2B enforcement, collection of taxes, contract management etc. The biggest area that falls under government is Contract Man.
- Government to Consumer Different departments offer various a starting workflow related governments work, share information, engage citizens and would help in decision making and policy enforcement.

4.2.Components Of A Typical E-Governance Application

Elements of three tier architecture with an over view of E-Government services is presented below. For E-Governance services three tier architecture is used because it provides following advantages:

- Heterogeneous Systems: Applications can utilize strengths of different platforms and different software components at the different tiers.
- Modifiability: As responsibilities are separated, it becomes easy to replace the code at any tier without affecting other tiers as modifiability is imp architectural driver of the case.
- Scalability to handle many clients: Each client is light weight and all access to the system is through the middle tier. The middle tier can share the database connection across the clients, and if middle tier becomes bottleneck, we can deploy several servers executing the middle tier code; clients can connect to any of these servers.
- Integrated Data Access: In many applications, the data must be accessed from several sources. This can be handled transparently at the middle tier, where we can centrally manage connections to all database system involved.

4.3.E-Governance Challenges And Cloud Benefits

4.3.1.Data Scaling

Cloud databases available for deployment offer unprecedented level of scaling without compromising on the performance. Cloud databases must be considered if the foremost concern is on-demand, high-end scalability – that is, large scale, distributed scalability, the kind that can't be achieved simply by scaling up.

4.3.2.Auditing And Logging

Traceability to any changes to information content in E-Governance services is required. Corruption in government organizations can be controlled by using Information Technology services, by keeping the providers of the services accountable. Process audits, security audits must be done periodically to ensure the security of the system.It can help in building and placing defense mechanisms to enhance the security, thereby making the applications reliable and available.

4.3.3.Rolling Out New Instances, Replication And Migration

Applications in E-Governance work for department states and municipalities and hence take more time, effort, resources and budget. This happens for all the instances of these

applications. Capabilities must exist to replicate these to include another municipality or e-court as part of Governance.

4.3.4.Disaster Recovery

Natural disasters like floods, earthquakes, wars and internal disturbances could cause the E-Governance applications not only loose data, but also make services unavailable. Multiple installations in geographically separated locations with complete backup and recovery solutions must exist. Cloud virtualization technologies allow backups and restoring. It offers application migration seamlessly compared to traditional data center. Cloud helps to increase the number of resources dynamically to maintain quality of service intact even at the times of high load, which generally happens in E-Governance.

4.3.5.Performance And Scalability

The architecture and technology adopted for the E-Governance initiatives should be scalable and common across delivery channels .It is required to meet growing numbers and demands of citizens. If implemented, the E-Governance portals could become the biggest users and beneficiaries of Information Technology. A simpler solution is to cluster the applications and scale horizontally by adding resources.

4.3.6.Reporting And Intelligence (Better Governance)

Data center usage (CPU, storage, network etc), peak loads, consumption levels, power usage along with time are some of the factors that needs to be monitored and reported for better utilization of resources. It minimizes costs and plan well. Profiling data enables better visibility into various services provided by the government. Cloud offers better Business Intelligence infrastructure compared to traditional ones because of its sheer size and capabilities. Cloud computing offers seamless integration with frameworks like Map Reduce (Apache Hadoop) that fit well in cloud architectures. Applications can mine huge volumes of real time and historic data to make better decisions to offer better services.

4.3.7.Policy Management

E-Governance applications have to adhere and implement policies of the governments in terms of dealing with citizens.

4.3.8.Systems Integration And Legacy Software

The power of Information Technology comes in co-relating the data across applications and pass messages across different systems to provide faster services to the end users. Cloud is built on SOA principles and can offer excellent solutions for integration of various applications. Also, applications can be seamlessly easily moved into cloud.

4.3.9.Obsolete Technologies And Migration To New Technologies

Technology migration is the biggest challenge. Moving to different versions of software, applying application and security patches is the key to maintaining a secure data center for E-Governance. With cloud, E-Governance applications can manage the policies well by providing security and adoptability. Various E-Governance applications can be integrated easily.

4.3.10.Going Green

More emphasis is laid out today in terms of data centers can create. The power usage, air electronic waste could create bio-hazard. This could be one of the reasons for moving to governance. Instead of duplicating these facilities, with cloud, one can offer centralized infrastructure that can be efficiently used to minimize pollution.

Figure : Governance cloud

5.Summary And Conclusions

Cloud provides a solid foundation for the introduction of widespread provision of services to various stakeholders. Applications designed using the principles of Service Oriented Architecture and deployed in cloud architectures will benefit the government in reducing operating costs and increasing the governance. SOA and cloud architectures when properly applied to developing E-Governance applications have the capability to transform the nation into an Information Society. Service Level Agreements are keys for

the government to measure how well the services are being performed and provided by the government. Cloud helps enabling E-Governing services faster and cheaper thereby accelerating the adoption and use of Information Technology for e-services. Cloud architectures allow rapid deployment of turnkey test environments with little or no customization. Cloud computing has low levels of awareness, trust and adoption among IT decision makers in the U.S. defense/military and federal government. Despite all the attention cloud computing receives as one of the leading IT trends, a third of government IT decision makers surveyed were not familiar with cloud computing, and a similar percentage do not trust it. Trust are lacking even among professionals who are familiar with it and may be responsible for securing enterprise systems and information. While cloud adoption is expected to grow, respondents' inexperience with cloud computing, security concerns (and in some cases, lack of concern) and uncertainty about governance could make it difficult for organizations to effectively implement cloud computing or realize full value from it. These challenges range from governance, through to securing application and infrastructure. Fundamentally it is important to be able to assure the security of these new models in order to build trust and confidence. The key to establishing trust in these new models is choosing the right cloud computing model for your organization. Place the right workloads in the right model with the right security mechanisms. For those planning to consume cloud services • looking for trust and assurance from the cloud provider; understanding the service level agreements and the approaches to security is key. Assessing that this can be delivered, including what assurances can be provided will be important. • For those providing or building a cloud infrastructure, using a proven methodology and technologies that can deliver appropriate security is key.

Our main finding is that the performance and the reliability of the tested cloud are low. Thus, the tested cloud is insufficient for scientific computing at large, though it still appeals to the scientists that need resources immediately and temporarily. Motivated by this finding, we have analyzed how to improve the current clouds for scientific computing, and identified two research directions which hold each good potential.

6.Reference

1. Cloud Security the Federated Identity Factor, by Patrick Harding and Gunnar Peterson http://www.hpcinthecloud.com/hpccloud/2010-11-09/cloud_security_the_federated_identity_factor.html
2. Monitoring Up the Stack: Adding Value to SIEM, Securosis Report http://securosis.com/reports/Securosis- Monitoring_up_the_Stack_FINAL.pdf
3. Salesforce.com oath client http://wiki.developerforce.com/index.php/Building_Android_Applications_with_the_Force.com_REST_API
4. NIST/NSA Survey of Access Controls http://csrc.nist.gov/news_events/privilege-management-workshop/PvM-Model-Survey-Aug26-2009.pdf
5. Hinden R, Deering S: IP Version 6 Addressing Architecture, IETF RFC 4291, 2005, retrieved in August 2011, [http://www.rfc.net/rfc4291.html]
6. Kawamura S, Kawashima MA: Recommendation for IPv6 Address Text Representation, IETF RFC, retrieved in August 2011, [http://tools.ietf.org/html/rfc5952]
7. Security Gateway Buyer's Guide http://www.dynamicperimeter.com/download/SecurityGateway_BuyersGuide
8. How to do Application Logging Right, by Anton Chuvakin & Gunnar Peterson, IEEE Security & Privacy
9. Don't Trust. And Verify. A security architecture stack for the Cloud, by Gunnar Peterson, IEEE Security & Privacy http://arctecgroup.net/pdf/donttrustandverify.pdf
10. Security > 140 Conversations with Gerry Gebel (XACML, Axiomatics), Chuck Mort more (Sales force, Identity), and Brian Chess (Fortify, Static Analysis) http://1raindrop.typepad.com/1_raindrop/security-140/
11. Software as a service, Wikipedia, <http://en.wikipedia.org/wiki/Software_as_a_service>
12. Welcome to the Data Cloud, Semantic Web blog, ZDnet, 6 Oct 2008, <http://blogs.zdnet.com/semanticweb/? p=205>
13. Any any any old data, Paul Walk's blog, 7 Oct 2008, <http://blog.paulwalk.net/2008/10/07/an y-any-any-old-data/>
14. 4 Hand, Eric. "Head in the Clouds." Nature. 25;449 (2007 Oct).
15. 5 Pollette, Chris. "How the Goog

16. Liu Z, Lallie HS, Liu L (2011) ―A Hash-based Secure Interface on Plain Connection‖, Proceedings of CHINACOM'11. ICST.OTG & IEEE Press, Harbin, China
17. Kozierok CM: The TCP/IP guide: a comprehensive, illustrated Internet protocols reference, No Starch Press, Rotterdam Area. ISBN 159327047X, 9781593270476, pp7, 379
18. Hinden R, Deering S: IP Version 6 Addressing Architecture, IETF RFC 1884, 1995, retrieved in August 2011, [http://tools.ietf.org/html/rfc1884]
19. Elz R: ―A Compact Representation of IPv6 Addresses‖, IETF RFC 1924, 1996, retrieved in August 2011, [http://tools.ietf.org/html/rfc1924]
20. Parwez R, Haq E et al (2010) Translucent implementation of ipv6 addressing scheme in communication networks. Int J Infonomics (IJI) 3(3):338–344
21. Davies J: Understanding IPv6, Second Edition, Microsoft Press, Redmond, Washington. ISBN-10: 0735624461, 978–0735624467, 2008, pp43-45, 50, 92
22. Fujitsu Research Institute (2010) Personal data in the cloud: A global survey of consumer attitudes. Technical Report, Fujitsu Research Institute
23. Uusitalo I, Karppinen K, Juhola A, Savola R (2010) Trust and cloud services – an interview study. In: Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on. p. 712–720