Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 62 (2013) 17799-17802

ISSN: 2229-712X

A smarter and efficient way to implement cloud computing

Sai Krishna Manohar

Department of Information Technology, Tirumala Engineering College, Narasaraopet, India.

ARTICLE INFO

Article history:

Received: 9 July 2013;

Received in revised form:

25 August 2013;

Accepted: 10 September 2013;

Keywords

Cloud, platform,

Saas,

Paas,

Cloud architecture.

ABSTRACT

Cloud computing is clearly one of today's most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. In this paper, we characterize the problems and their impact on adoption. In addition, and equally importantly, we describe how the combination of existing research thrusts has the potential to alleviate many of the concerns impeding adoption. In particular, we argue that with continued research advances in trusted computing and computation-supporting encryption, life in the cloud can be advantageous from a business intelligence standpoint over the isolated alternative that is more common today

Introduction

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet).Cloud computing provides computation, software, data access, and storage resources without requiring cloud users to know the location and other details of the computing infrastructure. End users access cloud based applications through a web browser or a light weight desktop or mobile app while the business software and data are stored on servers at a remote location. Cloud application providers strive to give the same or better service and performance as if the software programs were installed locally on end-user computers. At the foundation of cloud computing is the broader concept of infrastructure convergence (or Converged Infrastructure) and shared services [2]. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability and less maintenance, and enables IT to more rapidly adjust IT resources (such as servers, storage, and networking) to meet fluctuating and unpredictable business demand.

Working

To understand how does cloud computing work, imagine that the cloud consists of layers — mostly the back-end layers and the front-end or user-end layers. The front-end layers are the ones you see and interact with. When you access your email on Gmail for example, you are using software running on the front-end of a cloud. The same is true when you access your Facebook account. The back-end consists of the hardware and the software architecture that fuels the interface you see on the front end [1].

Because the computers are set up to work together, the applications can take advantage of all that computing power as if they were running on one particular machine. Cloud computing also allows for a lot of flexibility.

Depending on the demand, you can increase how much of the cloud resources you use without the need for assigning specific hardware for the job, or just reduce the amount of resources assigned to you when they are not necessary.

Fig 1: Pictorial representation of working of cloud

Fear of cloud

What are the "security" concerns that are preventing companies from taking advantage of the cloud? Numerous studies, for example IDC's 2008 Cloud Services User Survey of IT executives, cite security as the number one challenge for cloud users. [3]

In this section we present taxonomy of the "security" concerns. The Cloud Security Alliance's initial report contains a different sort of taxonomy based on 15 different security domains and the processes that need to be followed in an overall cloud deployment [3]. We categorize the security concerns as:

- Traditional security
- Availability
- Third-party data control

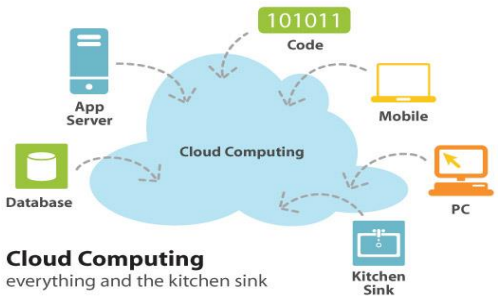

Fig-2: Graphical representation of Cloud Computation

Tele:

E-mail addresses: saikrishnamanohar@gmail.com

Traditional Security

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company. Another argument, made by the Jericho Forum, is: "It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats… In addition, it may be easier to enforce security via contracts with online services providers than via internal controls."[4]

Third-party data control

The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud.

All this is prompting some companies to build private clouds to avoid these issues and yet retain some of the advantages of cloud computing.

New problems

In this section we outline new problem areas in security that arise from cloud computing. These problems may only become apparent after the maturation and more widespread adoption of cloud computing as a technology.

Cheap data and data analysis. The rise of cloud computing has created enormous data sets that can be monetized by applications such as advertising. Google, for instance, leverages its cloud infrastructure to collect and analyze consumer data for its advertising network. Collection and analysis of data is now possible cheaply, even for companies lacking Google's resources [7]. What is the impact on privacy of abundant data and cheap data-mining? Because of the cloud, attackers potentially have massive, centralized databases available for analysis and also the raw computing power to mine these databases [4]. For example, Google is essentially doing cheap data mining when it returns search results. How much more privacy did one have before one could be Googled?

Because of privacy concerns, enterprises running clouds collecting data have felt increasing pressure to anonymize their data. EPIC has called for Gmail, Google Docs, Google Calendar, and the company's other Web applications to be shut down until appropriate privacy guards are in place . Google and Yahoo!, because of pressure from privacy advocates, now have an 18 month retention policy for their search data, after which it will be anonymized. This means that some identifying data will be removed such as IP addresses and cookie information. The anonymized data is retained though, to support the continual testing of their algorithms. Another reason to anonymize data is to share data with other parties. These may be to support research or to subcontract out data mining on the data.

We note that anonymizing data is a difficult problem. For example, in the Netflix data set was partially de-anonymized, and in the then-Governor of Massachusetts was identified as a patient of Massachusetts General Hospital from an anonymized list of discharged patients. Tools are needed for effective anonymization, which will increase in importance as clouds proliferate and more data is collected that needs to be analyzed safely or shared.

An example of indirect data-mining that might be performed by a cloud provi1der is to note transactional and relationship information [4]. For example, the sharing of information by two companies may signal a merger is under consideration.

Cost-effective defense of availability Availability also needs to be considered in the context of an adversary whose goals are simply to sabotage activities. Increasingly, such adversaries are becoming realistic as political conflict is taken onto the web, and as the recent cyber attacks on Lithuania confirm [6]. The damages are not only related to the losses of productivity, but extend to losses due to the degraded trust in the infrastructure, and potentially costly backup measures. The cloud computing model encourages single points of failure. It is therefore important to develop methods for sustained availability (in the context of attack), and for recovery from attack. The latter could operate on the basis of minimization of losses, required service levels, or similar measures.

Increased authentication demands. The development of cloud computing may, in the extreme, allow the use of thin clients on the client side. Rather than a license purchased and software installation on the client side, users will authenticate in order to be able to use a cloud application. There are some advantages in such a model, such as making software piracy more difficult and giving the ability to centralize monitoring [5]. It also may help prevent the spread of sensitive data on untrustworthy clients.

Thin clients result in a number of opportunities related to security, including the paradigm in which typical users do not have to worry about the risks of any actions – their security is managed by the cloud, which maintains the software they run. This architecture stimulates mobility of users, but increases the need to address authentication in a secure manner. In addition, the movement towards increased hosting of data and applications in the cloud and lesser reliance on specific user machines is likely to increase the threat of phishing and other abusive technologies aimed at stealing access credentials, or otherwise derive them, e.g., by brute force methods.

New directions

Information-centric security

In order for enterprises to extend control to data in the cloud, we propose shifting from protecting data from the outside (system and applications which use the data) to protecting data from within [8]. We call this approach of data and information protecting itself *information-centric*. This self-protection requires intelligence be put in the data itself. Data needs to be self-describing and defending, regardless of its environment. Data needs to be encrypted and packaged with a usage policy. When accessed, data should consult its policy and attempt to re-create a secure environment using virtualization and reveal itself only if the environment is verified as trustworthy (using Trusted Computing). Information-centric security is a natural extension of the trend toward finer, stronger, and more usable data protection [13].

High-Assurance Remote Server Attestation

We have noted that lack of transparency is discouraging businesses from moving their data to the cloud. Data owners wish to audit how their data is being handled at the cloud, and in particular, ensure that their data is not being abused or leaked, or at least have an unalterable audit trail when it does happen. Currently customers must be satisfied with cloud providers using manual auditing procedures like SAS-70[8].

Privacy-Enhanced Business Intelligence

A different approach to retaining control of data is to require the encryption of all cloud data. The problem is that

encryption limits data use. In particular searching and indexing the data becomes problematic [9]. For example, if data is stored in clear-text, one can efficiently search for a document by specifying a keyword. This is impossible to do with traditional, randomized encryption schemes. State-of-the-art cryptography may offer new tools to solve these problems. Cryptographers have recently invented versatile encryption schemes that allow operation and computation on the ciphertext. For example, searchable encryption (also referred to as predicate encryption; allows the data owner to compute a capability from his secret key [10]. A capability encodes a search query, and the cloud can use this capability to decide which documents match the search query, without learning any additional information. Other cryptographic primitives such as homomorphic encryption and Private Information Retrieval (PIR) perform computations on encrypted data without decrypting. As these cryptographic techniques mature, they may open up new possibilities for cloud computing security

While in many cases more research is needed to make these cryptographic tools sufficiently practical for the cloud, we believe they present the best opportunity for a clear differentiator for cloud computing since these protocols can enable cloud users to benefit from one another's data in a controlled manner [2]. In particular, even encrypted data can enable anomaly detection that is valuable from a business intelligen1ce standpoint. For example, a cloud payroll service might provide, with the agreement of participants, aggregate data about payroll execution time that allows users to identify inefficiencies in their own processes [1]. Taking the vision even further, if the cloud service provider is empowered with some ability to search the encrypted data, the proliferation of cloud data can potentially enable better insider threat detection (e.g. by detecting user activities outside of the norm) and better data loss prevention (DLP) (e.g. through detecting anomalous content).

Apart from ensuring privacy, applied cryptography may also offer tools to address other security problems related to cloud computing. For example, in proofs of irretrievability

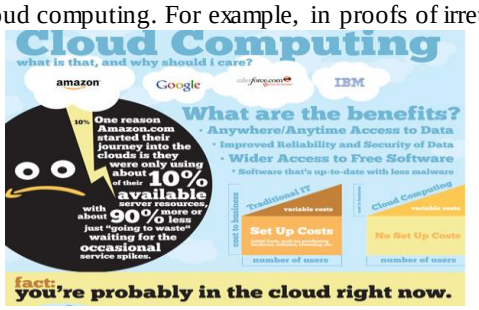

Fig 3: Benefits of Cloud

Uses

Scalable Website — Many websites experience fluctuations in demand — some can predict that demand, some cannot. Either way, the cloud's virtually infinite resources paired with RightScale auto-scaling make a perfect solution.

Grid Computing — Media transcoding, fraud detection, statistical research — all require batches of multiple "jobs" to process. The more servers, the faster the result. The cloud can be used to spread a workload over many more servers than you would be able to access in your own data center.

Development and Test — given the trend toward iterative, agile development, the ability to test and roll out fast can be a competitive differentiator [11]. With the cloud, developers can deploy and test complete production-scale systems — saving time and expense over traditional testing scenarios and enabling faster handoff from development to operations.

Social Gaming Applications — Building your own infrastructure to handle peak volume requires capital investments — and no matter how big you build it, it still may not be enough [11]. Cloud-based computer resources and sophisticated management platforms, on the other hand, can deliver increased flexibility and lower costs for large traffic events and ongoing life cycle management.

Windows in the Cloud — Running Microsoft stacks in the cloud is easier than ever with powerful Windows-based Server Templates™ [11]. High availability SQL Server, IIS, and Active Directory are some of the solutions RightScale has tailored for the cloud environment.

Conclusion

Cloud computing is the most popular notion in IT today; even an academic report from UC Berkeley says "Cloud Computing is likely to have the same impact on software that foundries have had on the hardware industry." They go on to recommend that "developers would be wise to design their next generation of systems to be deployed into Cloud Computing" [12]. While many of the predictions may be cloud hype, we believe the new IT procurement model offered by cloud computing is here to stay. Whether adoption becomes as prevalent and deep as some forecast will depend largely on overcoming fears of the cloud.

Cloud fears largely stem from the perceived loss of control of sensitive data. Current control measures do not adequately address cloud computing third-party data storage and processing needs. In our vision, we propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques [13]. These measures should alleviate much of today's fear of cloud computing, and, we believe, have the potential to provide demonstrable business intelligence advantages to cloud participation.

Our vision also relates to likely problems and abuses arising from a greater reliance on cloud computing, and how to maintain security in the face of such attacks. Namely, the new threats require new constructions to maintain and improve security. Among these are tools to control and understand privacy leaks, perform authentication, and guarantee availability in the face of cloud denial-of-service attacks.

References

"What's In A Name? Utility vs. Cloud vs Grid". Datacenterknowledge.com. Retrieved 2010-08-22.
www.wikipedia.com
"The Emerging Cloud Service Architecture". Aws.typepad.com
"Baburajan, Rajani, "The Rising Cloud Storage Market Opportunity Strengthens Vendors," infoTECH, August 24, 2011". It.tmcnet.com.
www.acm.org
"Performance Evaluation of a green Scheduling algorithm for energy savings in cloud computing" Troung Vinh Troung Duy, Yukinori Sato, Yashushi Inoguchi IEEE Xplore, March 2010
www.ibm.com/developerworks/websphere/zones/hipods
Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing, ver. 2.1," 2009.
M. Jensen, *et al.*, "On Technical Security Issues in Cloud Computing," presented at the 2009 IEEE International Conference on Cloud Computing, Bangalore, India 2009

C. Cachin, *et al*., "Trusting the cloud," *SIGACT News*, vol. 40, pp. 81-86,2009.
P. Parlier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. of EUROCRYPT'99,1999,pp.223-238.
P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on Jan. 23rd, 2010 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2010.
Cloud Security Alliance, "Security guidance for critical areas of focus incloud computing," 2009, online at http://www.cloudsecurityalliance.org.

Ch. Sai Krishna Manohar is pursuing the B.Tech degree in Information Technology at Tirumala Engineering College (JNTU-Kakinada) .He is a Certified Ethical Hacker (CEH) and also Certified Information Security Expert (CISE). He has already given so many presentations in various colleges and universities. Also he has been published number of technical papers at various Journals. His research interests include Network security, cloud computing, BIG DATA.