The Security of Cloud Computing

ALEXANDER POWELL
ajpowell@email.wm.edu
College of William & Mary
Computer and Network Security
CSCI 454
Prof. Kun Sun
May 8, 2016

Abstract

Cloud computing provides an efficient and effective way to increase computing capabilities without the need to invest in new infrastructure. It can also be an extremely economical decision for businesses and their IT needs. In the past decade alone, cloud computing has become one of the fastest growing segments of the IT industry. However, there are still a lot of unanswered questions about how secure the system is and how big a threat these issues pose. The purpose of this paper is to survey the major security threats to cloud computing models and look into the future of the industry.

Keywords: cloud-computing, software, security, deployment, business

Summary of Field

Cloud computing, otherwise known as on-demand computing is a type of computing that is based on the internet and set up in such a way that it can share processors and data between computers and other devices on demand. One of the biggest benefits of cloud computing is that it allows companies to avoid infrastructure costs up front, and therefore give more attentions to other projects. Additionally, cloud computing offers the ability to get applications up and running faster, and makes it easier to manage projects and spend less time maintaining them. In recent years, cloud computing has been in high demand due to its power, performance, price points, scalability, and availability. The most significant developments in this field have come about in the past decade. In 2008, NASA released the first open-source software package for developing provate and hybrid clouds, called OpenNebula.

Currently, there are three major service models in the cloud infrastructure. Together, these models form a stack: infrastructure, platform, and software. The most basic cloud service model is called infrastructure as a service (IaaS). IaaS refers to online services that abstract the user from the details of infrastructure like physical computing resources, location, security, etc. To deploy their applications, cloud users install operating-system images oand their software on the cloud infrastructure. In this way, the user patches and maintains the operating system. In platform as a service (PaaS), vendors offer a development environment to application developers. The provider then develops toolkits and standards for development as well as channels for distribution. It is important to note that in this platform, the provider givers a platform, usually an operating system and development environment on which the developers can develop and run their software solutions on a cloud platform. Examples of PaaS include frameworks like Microsoft Azure, the Google App Engine, etc. There also exists specialized applications of PaaS. These include integration platform as a service (iPaaS) and data platform as a service (dPaaS). Furthermore, consumers of PaaS do not manage or control the cloud infrastructure of their network, only the deployed applications and configuration settings. The last service model is software as a service (SaaS). In this model, users gain access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS gives businesses the potential to reduce IT operational costs by outsourcing hardware as well as software maintenance directly to the cloud provider.

Justification

Cloud computing is currently one of the fastest growing developments in the computing world. The economic case for it is extremely compelling, however there are a lot of concerns about the security challenges that it poses. Many businesses have accepted the economic case for cloud computing and more and more are moving towards similar solutions every day. Cloud computing providers can easily build large data warehouses for a relatively low cost to their customers. Also, as more individuals and businesses buy into these solutions, the resulting economies of scale increase revenue for cloud providers at a lower cost for cloud users. However, while cloud computing provides a convenient option for businesses to utilize, the security of the system has become it's greatest barrier to success. Currently, there are too many risks to service availability, data confidentiality, etc. for cloud computing to be presented as a feasible solution for most people, but the demand is nonetheless increasing as the price goes down. For this reason, it's important to evaluate the problems in cloud security and their implications. There are a number of concerns about the current state of cloud computing security. The biggest of these are access, compliance, location, recovery, viability, and availability. Access deals with who has administrator access to sensitive data as well as who makes decisions about hiring and supervision of such indivisuals. Compliance deals with potential issues like audits and security certifications from the outside. Unsurprisingly, the principle of location pertains to whether the cloud vendor allows for any control of the location of data. Recovery addresses the issue of whether data can easily be restored or recovered in the event of a disaster, and how much time would that take. Viability pertains to issues like what would happen if the client outlives the cloud vendor. Do they get their data back, and how is it returned to them. Finally, data availability means if their are periods when the vendor needs to change/update system requirements, is the data temporarily unavailable to the client.

Fortunately, the Internation Standard Organization (ISO), has published a number of themes that all security systems should be checked against. These themes are explained below.

- Identification & Authentication - Depending on what cloud model is being used, users must begin by providing necessary credentials so that they can be granted the permissions they need.
- Authorization - Authorization is used to ensure that integrity is maintained. Authorization is maintained by the system administrator to handle different priveleges and permissions of developers.
- Confidentiality - Confidentiality is essential in the world of cloud computing due to the accessible nature of public clouds. Making user profiles and data confidential ensures that information security protocols can be properly enforced at various stages down the line.
- Integrity - Integrity comes into play when users are accessing data. When employees are dealing with customer data there should always be some expectation of privacy.
- Non-repudiation - Non-repudiation means that the “author" of something won’t be able to challenge the fact that they wrote something. This principle comes up a lot in public key cryptography, so that as long as everyone keeps their private key a secret, noone will be able to impersonate them. In this way, individuals are able to leave digital signatures, timestamps, and confirmation receipts on data they are using.
- Availability - Finally, availability is a key decision factor when choosing between private, public, or hybrid clouds. The service level agreement highlights the downside of availability in cloud resources.

Classification Scheme

Topic #	Topic	Description
1	Services of cloud computing	Infrastructure, platform, software as a service (IaaS, PaaS, SaaS)
2	Models of cloud computing	Public, private, hybrid. Also smaller deployment models like community, distributed, intercloud, multicloud
3	Architecture	Explanation of the systems architecture for the systems used in delivering cloud computing services
4	Service Level Agreements (SLAs)	How to standardize SLAs dealing with priveleged access, regulatory compliance, data location, etc.
5	Main security vulnerabilities	Divided by model, reliability, availability, complexity, etc
6	Possible solutions to big security threats	Identification, authorization, confidentiality, integrity, non-repudation, and availability
7	Legal issues	Trademark infringement, security concerns, sharing of proprietary data resources
8	Current limitations and the future of cloud computing	Tradeoff between price and customizeability, R&D spending, etc.

Sources mapped to classifications

Topic #	Reference #
1	5, 17
2	10, 14
3	2, 6, 19
4	7, 16, 20
5	3, 11, 12, 15, 18
6	13
7	1, 4, 9
8	8, 18

Summary of Trends

More work in the field of cloud computing has been done in the last decade than any previous amount of time. As we have already seen, cloud computing appears to be an attractive business solution to many. However, its greatest weakness is its security, which is a major concern depending on the customer. In providing a secure cloud computing solution, a big decision is to decide the type of cloud to be implemented. There are currently three main types of cloud deployment models: public, private, and hybrid clouds. These all offer different advantages and disadvantages in terms of performance and security.

- Public Clouds

  The model of the public cloud allows user access to the cloud through an interface like an internet browser. In general, it's either free of maintained on a pay-per-use system, meaning the client will pay more during periods of higher demand. In terms of what the user sees, there may appear to be no difference between public and private cloud deployment models. However, the implications for security can differ substantially depending on the service. Some of the more famous public cloud service providers like Amazon, Microsoft, and Google own and operate the entire infrastructure at their own private data warehouse. The data is access using an internet connection.

- Private Clouds

  The concept of a private cloud computing system is intended for a single organization, and is either managed internally or by some third party. The private cloud model raised security issues that must be addresses in order to prevent dangerous security loopholes. Furthermore, private cloud centers often require a lot of space and resources, in addition to a significant level of engagement by the business. Because of this, many individuals choose the public cloud route because they don't end up saving money or resources. In this way, private cloud models aren't as economical as it's public or hybrid cousins.

- Hybrid Clouds

  Unsurprisingly, a hybrid cloud is a mix between the public and private cloud models. Examples of scenarios when hybrid clouds may be beneficial include situations when private client data may be stored on a private cloud application, but then that application is connected to a business intelligence application deployed on a public cloud. Another example would be when a public cloud is used to meet temporary capacity needs that cannot be met by the private cloud. This technique is known as cloud-bursting, and it is employed when an application normally runs on a private cloud but automatically transfers (or bursts) to a public cloud when the demand for computing capacity reaches a certain level.

References

1. Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan, *Study on the security models and strategies of cloud computing*, Procedia Engineering, 2011

2. Wentao Liu, *Research on Cloud Computing Security Problem and Strategy* , Wuhan Polytechnic University, 2014

3. Uma Somani, Kanika Lakhani, Manish Mundra, *Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing*, International Conference on Parallel, Distributed and Grid Computing, 2010

4. Chunming Ronga, Son T. Nguyena, Martin Gilje Jaatun, *Beyond lightning: A survey on security challenges in cloud computing*, Computers & Electrical Engineering, 2013

5. Farhan Bashir Shaikh, Sajjad Haider, *Security Threats in Cloud Computing*, International Conference on Internet Technology, 2011

6. Farzad Sabahi, *Cloud Computing Security Threats and Responses*, Azad University, 2013

7. Kuyoro S O, Ibikunle F, Awodele O, *Cloud Computing Security Issues and Challenges*, ResearchGate, 2012

8. Ramgovind S, Eloff MM, Smith E, *The Management of Security in Cloud Computing*, School of Computing, University of South Africa, 2009

9. Yanpei Chen, Vern Paxson, Randy H. Katz, *What's New About Cloud Computing Security?*, UC Berkeley, 2010

10. Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, *Cloud Security Issues*, IEEE International Conference on Services Computing, 2009

11. Mohamed Al Morsy, John Grundy, Ingo Muller, *An Analysis of The Cloud Computing Security Problem*, APSEC Cloud Workshop, 2010

12. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, *On Technical Security Issues in Cloud Computing*, IEEE International Conference on Cloud Computing, 2009

13. Radut Carmen, Popa Ionela, Codreanu Diana, *Cloud Computing Security*, IEEE International Revista Economica, 2012

14. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, *Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing*, IEEE Communications Society, 2010

15. S Subashini, V Kavitha, *A survey on security issues in service delivery models of cloud computing*, Journal of Network and Computer Applications, 2011

16. Peter Mell, Timothy Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, 2011

17. Sean Carlin, Kevin Karlin, *Cloud Computing Security*, International Journal of Ambient Computing and Intelligence, 2011

18. Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, *Cloud Computing Security*, International Journal on Recent and Innovation Trends in Computing and Communication, 2013

19. Jon Brodkin, *Seven cloud-computing security risks*, Network World, 2008

20. Dimitrios Zissis, Dimitrios Lekkas, *Addressing cloud computing security issues*, Future Generation Computer Systems, 2012