Int. J. Communications, Network and System Sciences, 2014, 7, 529-535
Published Online December 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.712053

Scientific Research

Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services

Patrick Mosca[1], Yanping Zhang[1], Zhifeng Xiao[2], Yun Wang[3]

[1]Department of Computer Science, Gonzaga University, Spokane, USA
[2]Department of Computer Science & Software Engineering, Penn State Erie, Erie, USA
[3]Department of Computer Science and Information Systems, Bradley University, Peoria, USA
Email: zhangy@gonzaga.edu

Received 15 October 2014; revised 26 November 2014; accepted 10 December 2014

Abstract

Recent advances have witnessed the success and popularity of cloud computing, which represents a new business model and computing paradigm. The feature of on-demand provisioning of computational, storage, and bandwidth resources has driven modern businesses into cloud services. The cloud is considered cutting edge technology and it is solely relied on by many large technology, business, and media companies such as Netflix or Salesforce.com. However, in addition to the benefit at hand, security issues have been a long-term concern for cloud computing and are the main barriers of the widespread use of cloud computing. In this paper, we briefly describe some basic security concerns that are of particular interest to cloud technology. We investigate some of the basic cloud concepts and discuss cloud security issues. Amazon Web Services is used as a case study for discussing common cloud terminology. Data security, as well as some cloud specific attacks is introduced. The current state and the future progression of cloud computing is discussed.

Keywords

Could Computing, Security, Amazon, Cloud Storage

1. Introduction

Recent advances have witnessed the success and popularity of cloud computing, which represents a new business model and computing paradigm [1]. The feature of on-demand provisioning of computational, storage, and bandwidth resources has driven modern businesses into cloud services [2]. The cloud is considered cutting edge technology and it is solely relied on by many large technology, business, and media companies such as Netflix or Salesforce.com. However, in addition to the benefit at hand, security issues have been a long-term concern and are the main barriers of the widespread use of cloud computing [1]. There are three main challenges [1] for

How to cite this paper: Mosca, P., Zhang, Y.P., Xiao, Z.F. and Wang, Y. (2014) Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services. *Int. J. Communications, Network and System Sciences*, **7**, 529-535.
http://dx.doi.org/10.4236/ijcns.2014.712053

building a secure and trustworthy cloud:

- *Outsourcing* reduces both capital expenditure and operational expenditure for cloud customers [1]. However, outsourcing also indicates that cloud customers no longer retain the physical control on hardware, software, and data. To address this challenge, a trustworthy cloud is expected, meaning that cloud customers are enabled to verify the data and computation in terms of confidentiality, integrity, and other security services [1].
- *Multi-tenancy* means that a cloud is shared by multiple customers [1]. Virtualization is heavily used by cloud vendors to optimize resource allocation and management [1]. A common but risky situation is that data belonging to different customers may be stored in the same physical machine. Adversaries can exploit this vulnerability to launch various attacks such as data/computation breach, flooding attack, etc. [1].
- *Massive data and intensive computation* are two other features of cloud computing. Therefore, traditional security mechanisms may not suffice the new security requirements due to unbearable computation or communication overhead [1].

This paper investigates various aspects on cloud security [2]-[4], including data security [5], cloud risks [8] and API concerns [9] [10], cloud services and account hijacking [2]-[14]. The goal of this paper is twofold: first, we focus on the valuable and unique security aspects of the cloud that are different from security issues that widely exist in other computing platforms, since there are certain risks and vulnerabilities only presenting themselves on the cloud environment; second, our intention is to provide an overview of cloud security from the practitioners' point of view. Therefore, we start from Amazon's cloud service [12], and then proceed to discuss the security concerns and the applicable criteria that follow (**Figure 1**).

The rest of this paper is organized as follows: Section 2 presents the background knowledge of Amazon's cloud storage; Section 3 discusses the aspect of data security in cloud; Section 4 investigates other cloud risks and API concerns; Section 5 reviews cloud services and the risk of account hijacking; Section 6 sheds some light on the future of cloud security; Section 7 concludes the paper.

2. Amazon's Cloud Storage

In this section, we will discuss basic technical terms and concepts associated with Amazon's cloud platform. There are different types of storage on Amazon's cloud: AMI (Amazon Machine Image) [15], EBS (Elastic Block Store) [16], snapshots [17], and volumes [16]-[19].

- A volume consists of stored data and possibly empty space. Also, a volume can exist virtually or can consume a full physical hard drive [18].

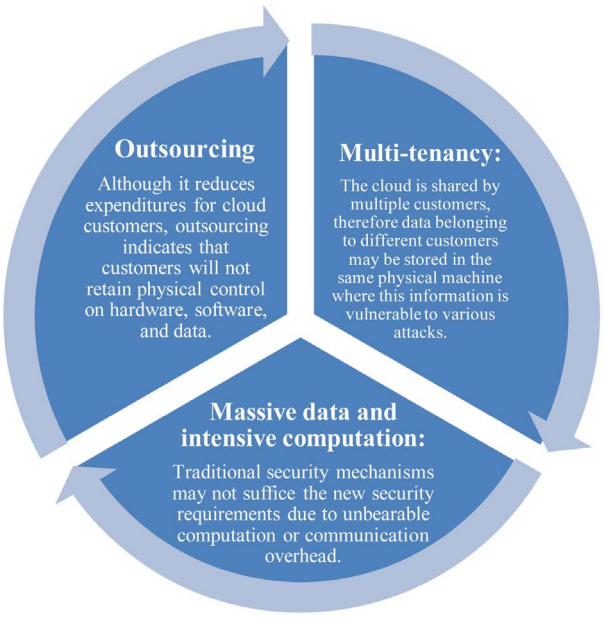

Figure 1. Three main challenges in cloud secruity [1].

- A snapshot is simply a backup or copy of an instance's volume data. A snapshot can be used to restore the data on an instance, similar to restoring from a backup. A snapshot is typically not a bootable form of storage [17].
- EBS is a new form of data storage. An EBS is virtual data storage that acts identically to a volume, but the data can be spread across many physical hard drives and can be moved quickly and easily [16]. The motivation behind EBS is to increase storage efficiency in the cloud. Cloud providers can then sell leftover storage to more customers. Additionally, an EBS can consist of multiple volumes, similar to partitions on a drive [16].
- An AMI is an advanced image of a virtual machine that can be used to create one or more instances of that AMI [15]. These images are similar to bootable snapshots that carry additional information about the virtual machine. An AMI is loaded onto an EBS when an instance is created [15]. For example, when a user obtains an instance and sets it up to host his or her website, all he or she needs to do is save the instance as an AMI, copy it to clouds across the world, and then produce duplicate instances of that AMI. All of his or her instances are live, working clones of the original image that are spread throughout regions.

3. Data Security

Cloud customers may store sensitive information in cloud instances. From a security perspective, cloud companies need to ensure the confidentiality of the service [2]. For example, this data could be the backend database for a financial service. A client of any cloud service is supposed to know the risks associated with data security, e.g., data loss and data theft [8]. When storing sensitive information, encryption is always a powerful scheme. Naturally, it would make sense to encrypt sensitive information such as credit card numbers that are stored in the cloud. A potential weakness to encryption in the cloud is the security of the keys. In the hacker world, it is commonly known that physical access to a machine always results in game over. This is because an attacker has control over the machine [2] [5]. Simple passwords on the operating system will not prevent an attacker from stealing data. A break-in is unavoidable unless the full disk is encrypted [8]. Full disk encryption means that the entire volume is encrypted, including the operating system [20]. While full disk encryption is possible in the cloud-computing world, many clients do not encrypt their data for performance and financial reasons. Disk encryption adds additional overhead to the total data stored. Even though data rates vary from region to region, when clients pay by the terabyte, less data is best (see **Table 1**) [3]. Additionally, many large data stores require quick access. For example, a video streaming service needs to read data quickly [3]. Disk encryption will slow this process down significantly and increase business costs. To this end, many cloud customers do not encrypt their volumes.

When cloud customers do not encrypt their volumes, a security risk is presented. A rogue employee of the provider has the power to snoop around without the customer's knowledge. Since the employee has physical access to the costumer's cloud instance, there is nothing to stop the employee from grabbing vital information and any other private keys [2] [8]. This employee can do this simply by cloning the victim's virtual machine, and then running the clone on a second offline hypervisor [5]. The employee can monitor the behavior of the virtual machine and take their time looking for valuable data. The rogue employee can then proceed to steal the data or use the keys to break into more cloud instances. When storing data in the cloud, trust is a very important part of data privacy. "The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure" [2]. Therefore, a trustworthy cloud is an essential step toward the success of cloud computing.

A key concern when encrypting data is determining whether or not the encryption software is open source.

Table 1. Amazon storage pricing [3].

	Standard storage	Glacier storage
First 1 TB/month	$0.105 per GB	$0.011 per GB
Next 49 TB/month	$0.090 per GB	$0.011 per GB
Next 450 TB/month	$0.075 per GB	$0.011 per GB
Next 500 TB/month	$0.070 per GB	$0.011 per GB
Next 4000 TB/month	$0.065 per GB	$0.011 per GB
Next 5000 TB/month	$0.060 per GB	$0.011 per GB

Opening encryption software is key to ensuring that no back doors or additional keys are created [1]. This has become a major problem for many services such as text messaging, videoconferencing, and email. For example, Apple has a service called, "iMessage" that handles text messages in the cloud. All messages are encrypted end-to-end, ensuring that no middleman can read your conversations [4]. What Apple does not tell you is that they are legally required to keep a copy of the key. Again customers are putting trust in the provider, Apple.

4. Cloud Risks and API Concerns

4.1. General Server Risks

Of all the risks being reported by the news and blogs on the Internet, many of them are not risks inherent to cloud services, meaning they would apply to all servers. Although, the cloud does increase the risk of some of them (**Figure 2**):

- Denial of Service (DoS) [5] being of the latter is obviously always an issue for servers. The added risk to using the cloud is that attacks on other users of the cloud would affect your portion. If an attack on the cloud unrelated to you brought it down it would also bring your server down or at least slow it down [5]. So while your server may not be the target of attacks, consideration needs to be added which include the notion that you may be working on the same hardware with anyone.
- Data breaches have greater potential of disaster on the cloud. A single flaw in a cloud service could cause one data breach to extend to a breach of the entire system [2]. Methods more simple than side channeling could extract keys or gather unencrypted data. While some individuals think that it is a considerable risk of cloud computing, it is in fact more realistically less of a risk than it would be to create one's own server and service it [8]. In the latter case there are many precautions to be taken, which have already been implemented by cloud services.
- Data loss is an issue not unique to the cloud. Power loss is a potential scenario everywhere on Earth and sometimes unavoidable [8]. Articles have defamed cloud services for losing data when in reality those servers probably have better surge and outage protection than you could afford [14].
- The risk of giving other access to your server's internals and secrets is once again almost unavoidable [2] [5]. Unless you were to buy, setup, and implement your own server in your home you will probably have to trust someone else to help you, thereby risking the data's integrity. It would be unwise to attempt to secure grand amounts of money on the cloud for this reason; even on your own server the temptation would exist for the valuables to be stolen [2]. Perhaps an employee would risk their job and reputation for a chance at this money or perhaps the cloud service has taken precautions against employees gaining too much valuable information. This much is unclear and unreported by cloud service businesses. Nonetheless if looking toward using a cloud one should remember that risks surround every server and the most important question is: would you do the extra work for the extra security?

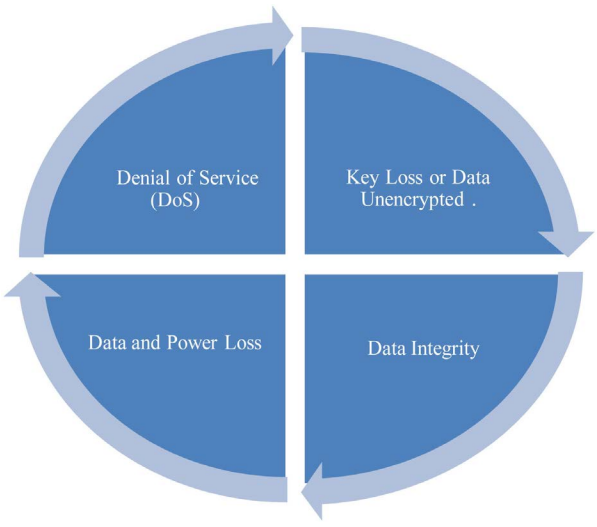

Figure 2. Four general server risks in the cloud [5] [8].

4.2. API Keys

Application Programming Interface (API) Keys [19] on the cloud were first used solely as the identifier for client programs running on a cloud. This allowed for the management of client programs and users to be monitored so as to backtrack events and log usage. While initially this had no security issues involved, later progress on cloud infrastructure has expanded the use of these keys [2]. In some cases it has been reported that these keys are used for authorization. Thus having this key gives one the power to alter delete or transfer an account's data or to use the servers for any other purpose, which would then be traced back and billed to the account holder [2]. After these keys became security risks the major problem was that they were not treated like them. Developers would email them around and store them in their hard drives, where snooping and sniffing could find them.

Years ago Google and Yahoo were making this mistake, but it was not long until the risks were found. They have since bulked their authorization security using Security Assertion Markup Language [21], and hashed-based authentication codes [22]. Yet the issue remains a threat as developers fail to follow best practices and continue to use API Keys for security purposes [2]. The older, more experienced businesses like Yahoo, Google, and Amazon have all either fallen into this trap before or are aware of the faults present. These companies can be trusted to build better software and control data flow than startups. If API Keys are going to secure information, they need to be handled with greater care.

4.3. APIs

Application Programming Interfaces or APIs, give what is almost a roadmap into how an application works [9] [10]. They are usually treated securely but not often enough. The University of Texas at Austin and Stanford University examined several commonly used web services [10]. Payment services at several of them were found to have vulnerabilities in the Secure Sockets Layer (SSL) protocol when accessed through APIs not meant for a browser [3]. Taking advantage of this flaw led to getting access to a user's files. Applications like Chase Mobile Banking and Instagram failed to implement SSL with complete security [10].

5. Service and Account Hijacking

At this point in its development, the cloud is seriously at risk for service and account hijacking [2]. This entails the unauthorized access to and use of the accounts and services of clients who utilize the cloud. This hijacking can happen any number of ways—since the cloud is simply a network run on many different servers, it is vulnerable to all the same attacks as both networks and servers [2].

Once an attacker has hijacked a service or account, he or she may be able to eavesdrop on the activities of the authorized users, impersonate authorized users, tamper with the network data, or utilize the service or account to propagate malware, e.g. by redirecting clients to malicious websites—all the threats typical for non-cloud networks and servers [2]. Unique to the cloud, however, the attacker may use the hijacked service or account as a base of operations to perform further attacks on other machines in the cloud [2] [5].

5.1. Recent Examples

In recent years, one of the companies on the vanguard of cloud technology—Amazon.com, Inc.—fell prey to such an attack. In 2010 hijackers performed a cross-site scripting (XSS) attack on some site to gain its credentials, and were successful [23]. The attackers then infiltrated the Amazon Relational Database Service (RDS) [7] such that, even if they lost their original access, they would still have a backend into the Amazon system. From that point on, they could capture the login information of anyone who clicked the login button on the Amazon homepage.

The attackers used their servers to infect new machines with the Zeus Trojan horse [23] and control machines already infected with it (Zeus is a piece of malware designed for Windows most often used for stealing bank information through form-grabbing and password-logging via a man-in-the-browser attack [24] [25]). Computers infected with the malware began to report to Amazon's EC2 for updates and instructions [23].

One of the most interesting facts about this case was that it was not, strictly speaking, Amazon's fault. The attackers gained access through some other, more vulnerable domain [23]. This reveals one truth about the cloud: on it, even one vulnerable system may lead to the compromising of the whole network. Furthermore, Amazon was only one of several sites to suffer this type of attack in the period of just a few months, and it was not in bad

company: Twitter, Google's app engine, and Facebook all experienced similar threats [23].

5.2. Possible Defenses

To prevent this type of breach, the Cloud Security Alliance (CSA) admonishes organizations to disallow users and services from sharing account credentials between themselves, and in addition to employ multi-factor authentication requirements when feasible [2]. However, both these changes may make systems more difficult to use, more expensive, and slower. Multi-factor authentication [26] is authentication demanding at least two of the following: knowledge, or something one knows; possession, or something one has; and inference, or something one is. Thus, multi-factor authentication places much more of a burden on users and services than single-factor authentication. And if users and services are disallowed from directly sharing credentials, cloud service providers may have to construct secure channels (an expensive undertaking) or hire a third party for communication between users and services (likewise expensive) [26].

6. The Future of Cloud Security

6.1. PRISM Scandal

In June 2013 Edward Snowden revealed that the National Security Agency (NSA) has been collecting enormous amounts of communication and search data from internet companies such as Microsoft, Yahoo, Google, and many more, including data about the activities of American citizens [27]. Snowden also explained that even low-level NSA employees have the ability to access this data without warrants. Such surveillance has taken place since January 2007. It may not be immediately clear why this information is particularly relevant to the cloud. The government can force cloud service providers to install backdoors in their hypervisors, but it can do the same for operating systems and even individual machines [11]. However, targeting the machine of one individual is much less likely, since at that point the government has singled out that user specifically. Instead, the cloud provides the NSA with a brimming ocean of network activity, in which it can cast its net and hope to catch something of use—much more efficient than targeting individual machines. As one writer for Porticor said: "Scanning all the data from a cloud provider is relatively easy, because massive amounts of data from multiple owners is all available" [11]. Porticor recommends that users encrypt their own data to combat such invasions of privacy, but it is doubtful that such a solution will ever prove widely acceptable, seeing as it places undue responsibility on users and requires a degree of expertise. The example of PRISM [27] touches on many issues within the future of cloud security: maintenance of privacy, government policy, and data theft (since attackers may capture user data using NSA techniques, or even the NSA channels themselves). These issues are not often considered by users of cloud services, and are not being discussed on a large scale.

6.2. A Better Cloud

There are organizations working towards a more secure cloud, such as the CSA [2]. Another is Silver Sky, an expert provider of cloud security and provider of "the industry's only advanced Security-as-a-Service platform from the cloud" [13] [28]. The CTO of Silver Sky, Andrew Jaquith, explains that many CIOs are moving their services to the cloud in order to save money, but that security remains a key concern and these moves may be insecure or at least hasty. But on the other hand, he also explains that many cloud service providers are becoming clearer, more transparent, and more assured than ever before that they could protect customer data [13].

Thus, the move to the cloud, while it may in some ways be insecure, does not herald anyone's doom. And, with its ever-increasing popularity, even hesitant companies may not soon have a choice.

7. Conclusion

In this paper, we provide an overview of cloud security in various aspects. We first review the data storage scheme for Amazon's cloud. The unique forms of products and services offered through cloud services show the incentive for modern business use. Using Amazon Web Services [12] as a case study, we are able to implore some of the basic terms and concepts of cloud computing. We then proceed to discuss data security, API concerns, account hijacking, and other security concerns. These general concerns are shown to be of particular interest to cloud security. The main differences between traditional services and cloud services are compared from a security perspective. Service and account hijacking is covered, as well as possible defenses. We investigate

differences between security issues in cloud services and in traditional services. From the practitioners' view, we briefly overview the security in cloud. The study in this paper provides a guideline of research on cloud services and security issues. Finally, we give some ideas on how to build a more secure cloud. Our future work will focus on the security concerns in cloud services. It will include the privacy protection of data information stored in cloud, data integrity with multiple backups for services purpose, etc.

References

[1] Xiao, Z. and Xiao, Y. (2013) Security and Privacy in Cloud Computing. *IEEE Communications Surveys & Tutorials*, **15**, 843-859.

[2] Cloud Security Alliance (2010) Top Threat to Cloud Computing. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[3] Amazon: Amazon Glacier. http://aws.amazon.com/glacier/

[4] Quarks Lab (2013) iMessage Privacy. http://blog.quarkslab.com/imessage-privacy.html

[5] Mutch, J. (2010) How to Steal Data from the Cloud. http://www.cloudbook.net/resources/stories/how-to-steal-data-from-the-cloud

[6] Yorozu, Y., Hirano, M., Oka, K. and Tagawa, Y. (1982) Electron Spectroscopy Studies on Magneto-Optical Media and Plastic Substrate Interface. *IEEE Translation Journal on Magnetics in Japan*, **2**, 740-741.

[7] Amazon: Service Level Agreement. http://aws.amazon.com/ec2-sla/

[8] Kirchgaessner, S. (2013) Cloud Storage Carries Potent Security Risk. http://www.ft.com/cms/s/0/4729ed7c-3722-11e3-9603-00144feab7de.html

[9] Lemos, R. (2012) Insecure API Implementations Threaten Cloud. http://www.darkreading.com/cloud/insecure-api-implementations-threaten-cl/232900809

[10] Lemos, R. (2013) Vulnerable APIs Continue to Pose Threat to Cloud. http://www.darkreading.com/services/vulnerable-apis-continue-to-pose-threat/240146453

[11] Porticor Cloud Security (2013) Did Snowden Compromise the Future of Cloud Security? http://www.porticor.com/2013/07/cloud-security-snowden/

[12] Amazon: Amazon Web Services. http://aws.amazon.com

[13] SilverSky (2013) The Future of Cloud Computing and the Latest Security Threats. https://www.silversky.com/blog/the-future-of-cloud-computing-and-the-latest-security-threats

[14] Columbia University (2012) Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. http://www.cs.columbia.edu/~angelos/Papers/2012/Fog_Computing_Position_Paper_WRIT_2012.pdf

[15] Amazon: Amazon Machine Image (AMI). http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

[16] Amazon: Amazon EBS. http://aws.amazon.com/ebs/

[17] Amazon: Amazon EBS Product Details. http://aws.amazon.com/ebs/details/#snapshots

[18] Amazon: Amazon EC2 Instance Store. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

[19] MailChimp (2014) About API Keys. http://kb.mailchimp.com/accounts/management/about-api-keys

[20] Janssen, C. Full-Disk Encryption (FDE). http://www.techopedia.com/definition/13623/full-disk-encryption-fde

[21] Cover, R. (2010) Security Assertion Markup Language (SAML). http://xml.coverpages.org/saml.html

[22] United Sates Department of Veterans Affairs (2014) Keyed-Hash Message Authentication Code (HMAC). http://www.va.gov/trm/StandardPage.asp?tid=5296

[23] Goodin, D. (2009) Zeus Bot Found Using Amazon's EC2 as C&C Server. http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/

[24] Nahorney, B. and Nicolas, F. (2010) Trojan.Zbot. http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

[25] Acunetix: Cross Site Scripting Attack. https://www.acunetix.com/websitesecurity/cross-site-scripting/

[26] Amazon: Multi-Factor Authentication. http://aws.amazon.com/iam/details/mfa/

[27] The Guardian: The NSA Files. http://www.theguardian.com/world/the-nsa-files

[28] SilverSky (2013) About Us. https://www.silversky.com/about-us

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.