IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cloud Infrastructure Entitlement Management (CIEM) and a Case Study on Amazon Cloud Services (AWS)

Chinmay Mangesh Tawde
[1] Department of Information and Cyber Security, G.N. Khalsa College, Mumbai

Abstract

Recently the researcher has witnessed and observe that the popularity in the field of cloud-computing and specially in cloud services are rapidly increasing, which shows that there will be a new business model and computing-paradigm. This feature of cloud-computing and by seeing the popularity has driven the modern businesses totally into cloud services. Today cloud is the vastest technology and it is relied on many other large technology, business, and media companies such as Disney or Hot-star/Netflix etc. However, in addition to the benefit of cloud-computing at one hand, security issues have been a long-term concern for cloud and are main obstacles of this world-wide spread use of cloud computing. In this paper the researcher briefly describes some of the basic security concern that are of particular interest to cloud technology. Researcher investigate some of the cloud concepts and discuss the issues and obstacles that come between this technology. Amazon Web Services is used as a case study for delivering common cloud technology. In some point and some content researcher has also describe about Data Security in cloud. The current cloud technology state and the future of cloud is been discussed

Keywords

Cloud Computing, Security, Amazon Web Services, Cloud Storage

1. Introduction

Recently the researcher has witnessed the great success and the increasing popularity of cloud in various businesses, which shows new business model and computing paradigm. This type of feature which is on-demand provisioning of computational, storage, and bandwidth resources has brought various businesses into cloud services. Today cloud is the vastest technology and it is relied on many other large technology, business, and media companies such as Disney or Hot-star/Netflix etc. However, in addition to the benefit of cloud-computing at one hand, security issues have been a long-term concern for cloud and are main obstacles

of this world-wide spread use of cloud computing. There are three main challenges for building a secure and trustworthy cloud:

- Outsourcing reduces capital expenditure and operational expenditure for cloud customers. However, it also indicates that cloud customer will no longer retain in the physical control of hardware, software and data. To tackle down this challenge a trustworthy cloud is expected, this means that cloud customers are enabled to verify the data and computation in terms of confidentiality, integrity and other security services.
- Multi-tenancy means that a cloud is been shared by multiple customers. Virtualization of cloud is been done heavily by cloud vendors to optimize resource allocation and management. A common problem or risk is that data belonging to different customers on cloud may be store in a single physical machine. Hacker can exploit this vulnerability to launch various attack such as data-breach, flooding attack etc.
- Massive data and intensive computational are the features of cloud computing. Therefore traditional security mechanism may not suffice the new security requirement due to communication overhead.

  The researcher has investigate various aspects on cloud security, including data security, cloud risk and API concerns, cloud services and account hijacking. The ultimate goal of the paper is of twofold: first, researcher has focus on the unique security aspects of the cloud that are different from security issues that exist in other computational platforms, since there are some kind of risk presenting themselves on the cloud environment; second the researcher intention is to provide a detail overview of cloud security from the practitioner's point of view. Therefore the researcher started from Amazon cloud services, and then process for the discussion of the security concerns that follow **(figure 1)**.

  The rest of the paper is organized as follow: Section 2 represents the base knowledge of Amazon's cloud storage; Section 3 discuss about the aspects of data security in cloud; Section 4 the researcher has investigate the other cloud risk's and API concerns; Section 5 gives reviews about cloud services and the risk of account hijacking; Section 6 give some knowledge about future of cloud security ; Section 7 concludes the paper.

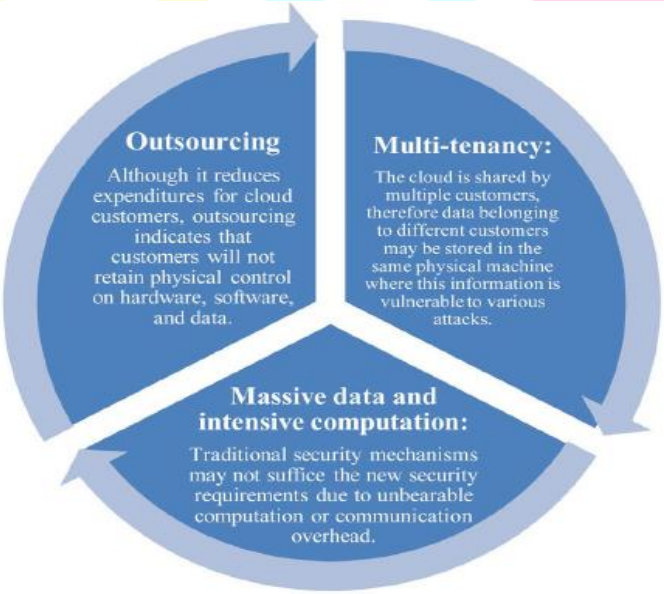

Figure 1. Three main challenges in cloud security.

2. Amazon's Cloud Storage

In this section the researcher has discuss the basic technical terms and concepts associated with Amazon's cloud platform. There are various different types of storage on Amazon's cloud: AMI (Amazon Machine Image), EBS(Elastic Block Store), snapshots and volumes.

- A volume contains of the stored data and empty spaces. Also, a volume can come virtually or can be consumed by a fully physical hard drive.
- A snapshot is nothing but a backup or copy of an instance's volume data. A snapshot can be used to restore the data from where it been kept off, similar to restoring from a backup. A snapshot is typically not a bootable form of storage.
- EBS is a new technique to store the data. An EBS is virtual platform to store data that behaves identically to a volume, but the data in that can be spread over many physical hard drives and can moved quick and easily. The motivation behind this EBS is to increase storage in the cloud. This makes the cloud providers to sell the remaining free space to more customers. In addition to that EBS can consist of multiple volumes, which is similar to partition on drives.
- An AMI is a advanced virtual image of virtual machine which is used to create one more instances of that AMI. These are similar to the bootable images/snapshots that carry additional information about that virtual machine. For example, when user obtains an instance and setup to host his or her website, all he or she has to do is to save the instance as an AML, copy it to cloud and then produce duplicates instance of that AMI. What will happen by this technique is that his or her website will be live, it will be working as clones rather than original image and spread through region.

3. Data Security

Data security in the cloud is a critical concern for individuals and organizations alike. As more and more data is being stored and processed in cloud environments, ensuring its protection has become a top priority. Cloud service providers employ various measures to safeguard data from unauthorized access, breaches, and loss. Encryption plays a crucial role in securing data in transit as well as at rest. By encrypting data before it is stored or transmitted, it becomes unreadable to anyone without the appropriate decryption key. Additionally, robust authentication mechanisms are implemented to ensure that only authorized individuals can access the data. This often involves multi-factor authentication, where users must provide multiple forms of identification such as passwords, biometrics, or security tokens. Regular backups and disaster recovery plans are also essential components of cloud data security. These measures help mitigate the risk of data loss due to hardware failures, natural disasters, or malicious activities. Furthermore, reputable cloud service providers adhere to industry-leading security standards and compliance regulations. They undergo regular audits and assessments to ensure their systems meet stringent security requirements. However, it's important for users to understand that while cloud providers take extensive measures to protect data, they cannot guarantee absolute security. Users must also play their part by implementing strong passwords, regularly updating software and applications, and practicing safe browsing habits. By adopting these best practices and working together with cloud service providers in maintaining data security protocols, individuals and organizations can confidently leverage the benefits of cloud computing while minimizing potential risks associated with storing

sensitive information online. Cloud customers can store most sensitive information in cloud instance. From a security point of view, cloud companies need to ensure the confidentiality of the services provided by them. For example, the data can be from a backend database for a financial service. A client of any cloud service should know the risk associated with data security, data loss and data theft. While storing information encryption is always a powerful scheme. By naturally it make sense to encrypt sensitive information such as credit-card number that are stored in cloud. The measure weakness in encrypting on the cloud is security of the keys. In the hacking world, it is commonly known that physical address of the system means always game over. This is because the hacker who has hack your system has the total control over your system. By keeping simple password on the operating system will not prevent you from an attacker to steal your data. A hacker will not break into your system until the full disk is encrypted. Full disk encryption means the entire volume is been encrypted including the operating system. This full disk encryption is possible in cloud-computing world, but at the same time many clients do not encrypt their data for performance and financial reasons. Even though data rates vary from region to region, when client pay for terabytes, less data is best (see **Table 1**). Additionally, large amount of data store require quick access. For example, a video streaming services need to read the data quickly. Disk encryption will slow the process down and increase business costs. All due to this the cloud customers do not encrypt their volumes.

When cloud customers do not encrypt their volumes a security risk is presented. A fake employee of the provider has the power to snoop around without the customer knowledge. Since the customer will have all the access to the cloud instance, there is nothing to stop the employee from grabbing vital information and any other private keys. This can be done by just making the cloning of the virtual machine and then running that clone on a second offline hypervisor. The employee can monitor all the behaviour of the virtual machine and can take some time to see the valuable information. The fake employee can easily steal the data or use the private keys to break down into the system. When storing the data into the cloud trust is a very important part of data privacy. Therefore, a trustworthy cloud is essential step for the success of cloud computing.

Table 1. Amazon storage Pricing

	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

A key concern during encryption data is determining whether the encryption software is open source. Opening encryption software is the key to ensure that no back backdoor or additional key is created. This has become a major problem for many services such as text messaging, video conferencing and email. For example, Apple has service called, “iMessage” that handle text message in the cloud. All message are encrypted end-to-end, ensuring that no middleman can read your conversations. What apple does not tell you that they are legally required to keep a copy of key. Again customer are putting trust in the provider, Apple.

4. Cloud Risk and API Concerns

4.1. General Server Risks

Of all among the risk being reported by the news and blogs on the internet, many of them are not risks inherent to cloud services, meaning that they would apply to all servers **(Figure 2):**

- Denial of Service (DoS) being of the latter is obviously always an issue for servers. The add-on risk of using the cloud is attack on other users of the cloud would affect your portion. If an attack has been done on cloud, then it can bring the server also down or at-least slow it down.
- Data breaches have greater potential of making huge disaster to cloud. A single flaw in cloud service can cause one data breach to extend to the entire system. Some people think that it is the considerable risk of the cloud computing. Later on there are many precaution taken and it has already been implemented by cloud services.
- Data loss is an issue and this is not unique to the cloud. Power loss is a potential scene everywhere on earth and sometime it is unavoidable. The articles have cause harm to the cloud services for losing data where in reality the server probably have better protection that you can afford.
- The another risk is of giving other access to your server's and secret is once again almost unavoidable. Unless if you buy, setup, and implement your own sever in your home you would probably have to trust someone to help you and there the risk include of data's integrity. Nonetheless if you are looking towards using a cloud one should remember that risk is surrounded on every server and the most important question is: will u be able to do extra work for the extra security?

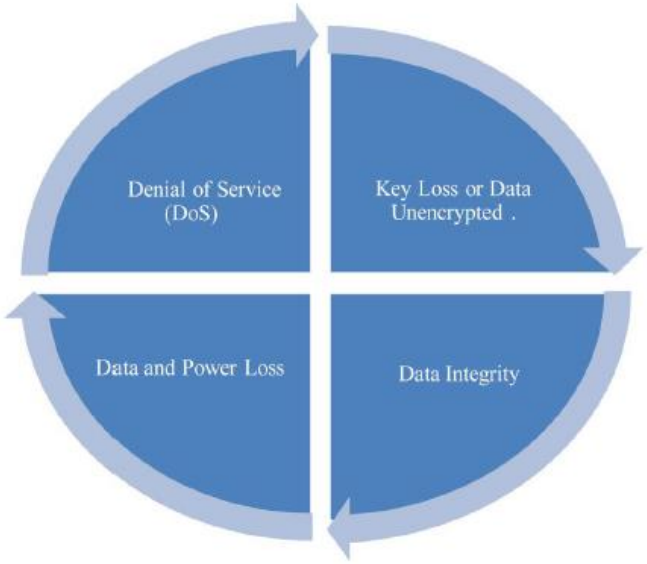

Figure 2. Four general risk of server in cloud

4.2. API Keys

Application Programming Interface (API) Keys on the cloud were first used as the identifier for client programs running on a cloud. This allowed for the management of client program and the user for monitoring so as to backtrack event and log usage. This has no security issues involved, in later it has been developed on cloud infrastructure has expanded the use of these keys. In some of the cases these keys are used for authorization process. Therefore these key give the power to alter delete or transfer an account's data or to use the sever for any other purpose which can be traced back to the account holder.

After some time and after some year these key has became the security risk and in this the major problem was that they were not treated with them. The developers will develop these keys and would email them around and store it them in their hard-disk where snooping and sniffing will be easy. Many years ago Google and Yahoo were making one mistake but it was not long enough until the risk were found. After getting this mistake to known they have bulk their authorization security using Security Assertion Markup Language, and hashed based authentication codes. Even after doing this the issue remains a threat as developers fail to follow best practices and continued to use the API's keys for security purpose. Most of the experienced business like Yahoo, Google, and Amazon have all either fallen into this trap before they get aware of this faults. If the API keys are going to secure information, they need to be handled with care.

4.3. APIs

Application Programming Interfaces or API's give a roadmap into how does an application works. They are usually treated securely but not often enough. The researcher has examined that the University of Texas at Austin and Standford University examined several used web services. Some of the payment services were found to have vulnerabilities in the Secure Socket Layer(SSL) protocol. Taking advantages of this flaw led to getting access to a user's file. Application like Chase Mobile Banking and Instagram failed to implement SSL with complete security.

5. Service and Account Hijacking

At this point, the cloud is seriously at risk for service and account hijacking. This entails the unauthorized and use of the account and services of the clients who utilize the cloud. The hijacking process can be happen in any number of ways--- since the cloud is simply a network run on many different server it is vulnerable to most of the attacks as both network and servers. Once when the attacker hijack a service or account, he or she can easily able to keep and eye on all the activities of the authorized users, tamper with the network data, or utilize the service or account to enter some malware, e.g. by redirecting the users to the malicious websites etc. Unique to the cloud attacker may used to hijacked service or a account as a base of operations to perform further attacks.

5.1. Recent Examples

In recent years, one of the companies of the cloud technology--- Amazon.com, Inc.---fell prey to such attack. In 2010 hijackers performed a cross-site scripting (XSS) attack on some site to gain its credentials, and were successful. The attacker then filtered the Amazon Relational Database Service (RDS) in such a way that, even if they lost their original access they would

still have a backend access to the Amazon system. From this point the attacker could capture the login information of the client who has click the login button on amazon homepage. The attacker then use their servers to infect the server with the help of trojans and control machines already infected with it. After the knowing of this incidents the computer which are infected with the malware began to report Amazon's EC2 for updates and instructions. One of the most interesting fact about this incidents that it was not strictly speaking the Amazon's fault. The Hackers gained access through some other different server which is more vulnerable. This reveal out the truth of the cloud. In future after that the Amazon was the only one of several sites to suffer this type of attack in the period of only some months.

5.2. Possible Defences

The researcher has found that to prevent this type of breach the Cloud Security Alliance (CSA) has given clear warning to the organizations to disallow user and services from sharing their account and credentials among themselves, and in addition to this the employ should set-up multi-factor authentication whenever it is feasible. However if we made this changes it will difficult to use the system and it will be more expensive and slower. In multi-factor authentication there demand is to use at-least two of the following: knowledge, or something one knows; possession, or something one has; and inference, or something one is. Due to this type of multi-factor it create much more burden on users and services than single factor authentication. Another contents is that suppose we disallowed all user and services to sharing their credentials cloud service provide may have to create one secure channel or hire a third party to set up communication between user and services

6. The Upcoming Future Of Cloud Security

6.1. PRISM Scandal

Researcher has seen that in the year 2013 Edward Snowden revealed that the National Security Agency (NSA) has been collecting enormous amount of communication and search data from internet companies like Microsoft, Google, Yahoo and much more. This agency are also collecting data about the activities of American citizens. Edward also explained that even the low-level NSA employee also has the rights to access the data without any warrants. This type of surveillance has taken place from the year 2007. The government can force cloud service provider to install a backdoor in their hypervisor, but it can also been done same for the operating system and even individual machines. However targeting the machine of one individual is much less likely. Instead of the Cloud Service Provider the NSA with a brimming ocean of network security it can cast its net and hope to catch something of use which is much more efficient than targeting one individual machines. Scanning all the data from the cloud provider is much easier because massive amount of data from different type of owners is all available. We can avoid this by encrypting the user data to combat such invasions of privacy, but at the same time it is doubtful that such a solution will be widely acceptable.

A Better Cloud

The researcher seen that there are various organizations working towards a more secure cloud, such as the CSA. Another is the Silver Sky which is an expert provider of cloud security and provider of "the industry's only advanced Security-as-a-Service platform from the cloud". The CTO(Chief Technology Officer) explain that many of the CIOs(Chief Information Officer) are moving their services to the cloud in order to save money, but at the same time the security concern remain the same and these moves may be insecure in some of the company. But at the same point of view the CTO also said that many of the cloud service provider are becoming more transparent, and more assured than even before and they can protect the customer data.

7. Conclusion

In this paper, researcher has provided an overview of cloud security in various aspects. We at the very first review the data Storage scheme of Amazon's cloud. The unique different forms of product and services offered through cloud services show the incentives of modern business use. Using Amazon's Web Services as a case study, researcher are able to explore some of the basic terms and concepts of cloud computing. After the first round of paper the second round comes about the discussion of data security, API concerns, account hijacking and other security concerns. This has been shown to be particularly interested in cloud security. Service and account hijacking is cover as well as possible defences. We later on investigate the difference between security issues in cloud services and in traditional services . From the practitioner's view, we briefly overview the security in cloud. The study in paper provide a guideline of research on cloud services and security concerns. In the final discussion researcher give some idea on how to build a more secure cloud. Our future work will focus on the security concerns in the cloud services. It will include the privacy protection of data information which is store in the cloud, etc.

References

[1] *IEEE Communications Surveys & Tutorial*

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

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

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

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

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

[7] An Investigation of Amazon Web Services from User's Perspectives. https://online-journals.org/index.php/i-jet/article/view/9902

[8] Analysis of Cloud Security Controls in AWS and Cloud. https://repository.stcloudstate.edu/msia_etds/112/

[9] Cloud Computing Security Issues and Challenges: A Survey. https://www.researchgate.net/publication/220790184_Cloud_Computing_Security_Issues_and_Challenges_A_Survey

[10] Research in Cloud Security: Problems and Prospects. http://www.tjprc.org/publishpapers/2-14-1375100443-33.%20Recent%20advances.full.pdf