Cloud Computing Security: From Single to Multi-Clouds

Abstract:

The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with “single cloud” providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards “multi-clouds”, or in other words, “interclouds” or “cloud-of-clouds” has emerged recently.

This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

Algorithm Used:

Secret Sharing Algorithms:

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the
file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead.

**System Architecture:**

![Diagram of system architecture](image)

**Existing System:**

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with “single cloud” providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards “multiclouds”, “intercloud” or “cloud-of-clouds”.

**Disadvantages:**

1. Cloud providers should address privacy and security issues as a matter of high and urgent priority.
2. Dealing with “single cloud” providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud.

Proposed System:

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient’s medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed.

Advantages:

1. Data Integrity
2. Service Availability.
3. The user runs custom applications using the service provider’s resources
4. Cloud service providers should ensure the security of their customers’ data and should be responsible if any security risk affects their customers’ service infrastructure.

Module Description:

1. Data Integrity
2. Data Intrusion
3. Service Availability
4. DepSKy System Model
Data Integrity:

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux’s distribution servers.

One of the solutions that they propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al. State that this solution can avoid data corruption caused by some components in the cloud. However, Cachinet al. Claim that using the Byzantine fault-tolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place.

Data Intrusion:

According to Garfinkel, another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account’s instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user’s email (Amazon user name) to be hacked (see for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

Service Availability:

Another major concern in cloud services is service availability. Amazon mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user’s web service may terminate for any reason at any time if
any user’s files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers.

**DepSKy System Model:**
The DepSKy system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client’s tasks. Bessani et al. explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing.

**System Configuration:**

- **H/W System Configuration:**
  - **Processor:** Pentium –III
  - **Speed:** 1.1 Ghz
  - **RAM:** 256 MB(min)
  - **Hard Disk:** 20 GB
  - **Floppy Drive:** 1.44 MB
  - **Key Board:** Standard Windows Keyboard
  - **Mouse:** Two or Three Button Mouse
  - **Monitor:** SVGA

- **S/W System Configuration:**
  - **Operating System:** Windows95/98/2000/XP
  - **Application Server:** Tomcat5.0/6.0
<table>
<thead>
<tr>
<th>Category</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front End</td>
<td>HTML, Java, JSP, AJAX</td>
</tr>
<tr>
<td>Scripts</td>
<td>JavaScript</td>
</tr>
<tr>
<td>Server side Script</td>
<td>Java Server Pages</td>
</tr>
<tr>
<td>Database Connectivity</td>
<td>Mysql</td>
</tr>
</tbody>
</table>