**Cloud Computing Challenges – Security and Cost**

Made by:

1-Fernando kakony Cueit21004

2-Shlama Bello Cueit21016

2-Ibrahim abdoonee Cueit21006

**Introduction**

Cloud computing is a type of internet based computing which provides services and resources via the internet either by public provider or a private cloud, some common issues individuals run into when dealing with cloud computing is first the security threats and second the cost on implementing or maintaining the cloud services. Through this report we will discuss both the security and cost problems of the cloud computing.

**Security threats in cloud computing**

* According to the research (Bollinadi, 2017).Some of the security threats in cloud computing include:

1. Data Breaches: with vast amount of data stored in cloud servers they become the main target for hackers.
2. Compromised Credentials and Broken Authentication: weak authentication methods such as password management can lead to data breaches.
3. Hacked interfaces and API’s: weaknesses in cloud service interfaces and API’s can expose vulnerability can affect security aspects.
4. Exploited System Vulnerability: bugs in systems can lead to data crashes or even virus infections.
5. Account Hijacking: sharing credentials or data with third –party vendors can lead to account hijacking.
6. Malicious Insider: insider threats from employees or associates with access to sensitive information can pose significant risks.
7. Cloud Service Abuses: Hackers may abuse cloud services to disrupt environments, leading to system shutdowns or data loss
8. DOS Attacks: Denial of Service (DOS) attacks can severely impact system performance and increase operational costs.

* As it mentioned in this article posted on (dig8ital, 2023). The role off services providers and users in ensuring a secure cloud environment is:

1. **Cloud Provider** typically takes responsibility for securing the infrastructure, such as servers, networking, and physical data centers. Meaning there job is insuring the cloud platform is protected from external threats.
2. **Customer** are accountablefor securing theirdata, applications, and configurations with in the cloud. This includes access control, encryption.

* Preventive measures that could prevent a breach:

1. Data Encryption: implement End-to-End encryption for data stored in cloud to ensure that even if unauthorized access occurs the data remains safe.
2. Multi-Factor Authentication (MFA): this helps prevent unauthorized access in case credentials are compromised.
3. Access control Policies: implement access control policies to restrict access to sensitive data.
4. Strong Password Policies: enforce strong password including requirements for minimum length, complexity, and regular password changing.
5. API Security: make sure that’s interface and API’s used to manage cloud services are properly secured with authentication mechanisms, encryption to prevent data breaches.
6. Employee Training and Awareness: Provide comprehensive security awareness training to employees to educate them about common security threats, such as phishing attacks and social engineering, and how to recognize and respond to them effectively.
7. Third-Party Risk Management: Assess and monitor the security practices of third-party vendors and service providers that have access to the cloud environment to ensure they meet security standards and do not introduce additional risks.

* Which deployment models provide more security?

To explain this it really depends on the organizations security requirement, cost, and application.

1-Public Cloud:

* Shared responsibility model with the CSP responsible for infrastructure security.
* Economies of scale and robust security measures provided by leading providers.
* Global compliance standards and scalability/flexibility benefits.

2-Private Cloud:

* Dedicated infrastructure with enhanced privacy and control.
* Isolation and segmentation for increased security.
* Custom security policies tailored to unique requirements.

3-Hybrid Cloud:

* Combines benefits of public and private clouds.
* Flexibility in workload placement and scalability.
* Enhanced disaster recovery and redundancy.
* Requires effective security orchestration and management.

Though each model has its benefits it is known that private cloud provides the best security since it’s on premise.

**Cost in cloud computing**

* According to the research (Al-Roomi, 2013) the cost of models in cloud computing vary from one model to another.

The following are the most pertinent factors that influence pricing in cloud computing

1. Initial costs. This is the amount of money that the service provider spends annually to buy resources.
2. Lease period. This is the period in which the customer will lease resources from the service provider. Service providers usually offer lower unit prices for longer subscription periods.
3. QoS. This is the set of technologies and techniques offered by the service provider to enhance the user experience in the cloud, such as data privacy and resource availability. The better QoS offered, the higher the price will be.

4. Age of resources. This is the age of the resources employed by the service provider. The older the resources are, the lower the price charged will be. This is because resources can sustain wear over time, which reduces their financial value.

5. Cost of maintenance. This is the amount of money that the service provider spends on maintaining and securing the cloud annually.

* Here are several common cost models used in the cloud, which you can combine depending on your needs.

1-Pay-As-You-Go

In this model, cloud services are billed per actual usage. Cloud services may bill for utilization of computing power, storage, networking, or other resources. The advantage is that you only pay for actual usage, and can scale down resources when needed. The downside is that as you add more resources to your cloud deployment, ongoing costs can quickly skyrocket.

2-Prepaid/Fixed Subscriptions

In a subscription-based model, cloud customers pay for services upfront. Subscription prices deliver a predetermined package of services for a specified time. The longer the period, the lower the price.

Subscription pricing is common for cloud services that combine multiple hardware and software elements, like platform as a service (PaaS) and software as a service (SaaS). Most cloud providers also offer subscription-based pricing for customers with high spend, allowing them to enter into a corporate discount plan, where they commit to a certain level of cloud spend and receive a discount on some or all of their cloud services.

3-Reserved Instances

Reserved instances allow companies to commit to cloud resources for a long period of time, typically 1 or 3 years. The longer the discount, and the more the company is prepared to pre-pay at the beginning of the period, the greater the discount. A three-year term is usually the most cost effective. Cloud providers typically offer discounts of 50-75% compared to pay-as-you-go rates for reserved instances with the same capabilities.

Reserved instances are suitable for steady state loads and long running systems. However, organizations should not use reserved instances for peak loads. Instead, reserved capacity should be used for core components of the system, and additional capacity required during peaks should be handled using pay-as-you-go or spot instances.

4-AWS Savings Plan

Similar to reserved instances, Savings Plans are a flexible pricing model that allows organizations to enjoy lower than on-demand pricing, in exchange for a one-year or three-year specific usage commitment. The commitment is expressed in terms of spend per hour on Amazon services.

AWS offers three types of Savings Plans:

* Compute Savings Plans – apply to all usage of Amazon compute services usage, including EC2, AWS Lambda and Fargate.
* EC2 Savings Plans – applies only to usage of Amazon EC2 instances.
* SageMaker Savings Plans – applies only to SageMaker usage.

Savings plan offer three payment methods:

* No upfront – does not require an upfront payment, bills customers according to actual usage each month. This grants the minimal savings plan discount.
* Partial upfront payment – with this option, more than half of your contract is prepaid and the rest is billed monthly, which grants an additional discount.
* Full upfront payment – the full commitment is paid up front, which grants the deepest discount.
* Cloud Cost Management Strategies

Cloud cost management enables businesses manage the costs associated with cloud technology, maximize the return on investment in cloud technology, and increase efficiency.

Here are some of the strategies used to manage cloud costs:

* Budget control: as a first step, organizations must establish budgets for cloud services and ensure teams are aware of them, and cannot exceed the budget for their specific project.
* Right sizing: ensuring compute instances, storage volumes and other services are provisioned at the level actually required by the business.
* Auto scaling: scale resources up and down dynamically according to application demand, ensuring you only pay for extra cloud resources during peak usage.
* Scheduling: many cloud services are not required 24/7, and can be scheduled to shut down when not needed.
* Detecting unused resources: compute instances, storage volumes, load balancers, snapshots, and many other resources can easily be created and forgotten. Organizations must be able to scan their cloud deployment for unused resources and delete them to conserve costs.
* Smartly applying discounts: discounted pricing models like reserved instances and spot instances can significantly drive down cloud costs, but they must be used appropriately.
* Cloud Cost Optimization Tools:

Automated tools are available which can retrieve metrics from APIs, report on cloud consumption and costs, and make changes to services as necessary. There are two main types of tools—first party tools provided directly by the cloud provider, and third party tools from external vendors.

1. First Party Tools:

All public cloud platforms provide cost management tools. These tools are highly integrated with the cloud platform, and are available out of the box without a special deployment effort. Some of these tools are free to use, while others are billed on a pay-per-use model.

In many cases, these basic tools are the fastest way to start managing your cloud costs. However, they have several limitations, which are addressed by third party tools:

* Limited functionality: most first-party tools are limited in their ability to identify wasted costs and maximize savings using multiple cost models.
* Limited to one vendor: most first-party tools only work with one cloud provider, and are not suitable for organizations that require multi-cloud cost management.
* Conflict of interest: a cloud provider is, in the end, interested in maximizing profits. On the one hand, cloud providers do want to help clients run applications in a cost-effective manner, to increase usage and retention. On the other hand, cloud providers want to maximize consumption of cloud services and may not always offer the optimal solution for the cloud customer.

2-Third Party Tools:

Third-party cost management tools can address the functional limitations of first party tools, and commonly provide multi-cloud cost management. Most of these tools are built to reduce cloud costs across a variety of cloud services and workloads, providing clear return on investment (ROI).

**Conclusion**

Security remains a central concern in cloud computing due to various potential vulnerabilities, spanning from data breaches and compromised credentials to internal threats and misuse of services. Nevertheless, proactive steps such as encrypting data, implementing multi-factor authentication, establishing access controls, and providing thorough employee training can substantially alleviate these risks. Moreover, the choice of deployment model—whether public, private, or hybrid—plays a pivotal role in determining the security level, with private cloud often perceived as offering the highest security due to its localized nature.

Conversely, financial aspects are also crucial factors influencing cloud computing adoption and usage. Various elements such as upfront costs, lease durations, service quality, resource age, and maintenance expenses contribute to the pricing models offered by cloud providers. Understanding these elements and comparing pricing structures can assist organizations in making informed decisions regarding cloud adoption, ensuring optimal cost efficiency while meeting their operational needs.

Overall, while cloud computing presents unparalleled advantages in terms of scalability, flexibility, and efficiency, addressing security challenges and optimizing expenses are imperative for organizations to fully harness the potential of cloud technology and drive sustainable growth and innovation. By implementing robust security measures and prudent cost management strategies, businesses can leverage cloud computing to expedite digital transformation and accomplish their objectives effectively.

**References**

Al-Roomi, M., Al-Ebrahim, S., Buqrais, S., & Ahmad, I. (2013). Cloud computing pricing models: a survey. International Journal of Grid and Distributed Computing, 6(5), 93-106.

Cloud Computing: Security Issues and Research Challenges <https://www.jncet.org/Manuscripts/Volume-7/Issue-11/Vol-7-issue-11-M-12.pdf>

THE IMPORTANCE OF CLOUD SECURITY ARCHITECTURE: ENSURING YOUR DATA’S PROTECTION

[https://dig8ital.com/post/secure-cloud-architecture/ - :~:text=The%20cloud%20provider%20typically%20manages,configurations%20within%20the%20cloud%20environment.](https://dig8ital.com/post/secure-cloud-architecture/#:~:text=The%20cloud%20provider%20typically%20manages,configurations%20within%20the%20cloud%20environment.)

Cloud Cost: 4 Cost Models and 6 Cost Management Strategies

<https://spot.io/resources/cloud-cost/cloud-cost-models-management-strategies/>