KABALE UNIVERSITY

FACULTY OF COMPUTING LIBRARY AND INFORMATION SCIENCE

COURSE UNIT : CLOUD COMPUTING

PROGRAME : BCS

CODE : BCS 1101

YEAR : ONE

NAME : MUHEREZA ALOUZIOUS

REGNO : 2024/A/KCS/5193/G/F

Qn.1

You are the chief Technology Officer of a mid-sized Company that currently operates with a traditional on-promises IT infrastructure. The company is considering transitioning to cloud computing to improve scalability and reduce costs. However, the CEO is concerned about potential security risks and Vendor lock-in.

1(i)

How would you approach the transition to cloud Computing to address the CEO's Concerns?

Introduction;

Moving to cloud computing can help our company grow faster and save money, but we need to be careful about security risks and getting stuck with one provider. With the right plan, we can take advantage of the cloud's benefits while staying safe flexible. This way, we'll get the best of both worlds without putting the company at risk.

The following are how I would approach the transition to cloud computing to address the CEO's concerns;

(a) Vendor Lock-In Concerns.

It occurs when a company becomes dependent on a single cloud provider making it difficult or costly to migrate to another cloud service provider.

The CEO's concern is clear but you can minimize this risk with the following.

1. Multi - Cloud strategy: In place of relying on a single cloud service like Amazon Website software (AWS), implement a multi - cloud strategy where different services are spread among multiple cloud providers like Microsoft Azure, Google Cloud, AWS

Benefits

This will ensure the company can easily transfer tasks or responsibilities between cloud providers and prevent total reliance on one provider resources.

Minimization of Vendor Lock - In.

If one cloud provider experiences a data loss, the company can move its operations to another cloud provider without meaningful shutdown or interruption.

2. Cross - Cloud Tools like Docker, Kubernetes.

They help services that can work smoothly with different cloud Computing platforms such as Google Cloud, Azure and AWS without any restrictions.

Benefits.

They allow users to take full advantage of the unique features and can choose the provider that best meets their needs without worrying about weather the tool they are using will work properly or not.

Mitigation of Vendor Lock - In.

Since there are cross cloud tools, users avoid using special features that only work on a specific provider, so users can easily switch between different cloud services if needed.

This gives them more flexibility and freedom.

3. Open Standard and Data Portability. This ensures that any data stored in the cloud can easily be transferred in a portable format like Extensible Markup Language (EML).

Benefits.

Enables the users to move data between different platforms without loosing it or having to manually re-enter it.

Minimization of Vendor Lock-in.

Data Portability ensure that data can be transfered without interruption incase in the process of changing the cloud provider.

(b) Security Risks Concern.

These are potential problems that can make information to attacks like weak passwords.

These risks can be minimized through well-defined Security practices as follows.

1. Strong Encryption: Implement encryption for all data both when data is being sent and when data is stored somewhere.

Benefits.

Even if someone tries to open it, they cannot read the contents without the correct key. This keeps Company information safe from unauthorized access.

Mitigation Of Security Risks.

Encryption of data importantly reduces the risk of data attack thus protecting important and private data that belongs to the company.

2. Cloud Security Tools: Utilize the cloud providers monitoring tools such as AWS Security Hub, Azure security centre to constantly watch or oversee for potential threats.

Benefit.

It helps to keep data and systems safe constantly watching for security threats.

Reduction of Security Risks.

Active monitoring tools help to detect and respond to security issues or cases before they become serious attacks.

3. Identify and Access Management. Tools from cloud Providers help to control who can use the company's cloud resources and what they can do with them.

Benefit.

This helps to protect sensitive information by making sure only authorized people can access it.

Mitigation of Security Risk.

It ensures that right people have the right level of access to do their job.

Conclusion.

To ease the CEO's Concerns a balanced approach to cloud adoption is essential. The multi-cloud and use of cross-cloud tools can minimize the risk of Vendor Lock-in while strong encryption and cloud security tools address security risks. By presenting strategies I can demostrate that the transition to cloud Computing can be done in a flexible way allowing the company to benefit from scalability and Cost reduction.

3(ii)

Outline a strategy that balances the benefits of cloud adoption with the risks of security and Vendor lock in.

Introduction

Cloud Computing offers many benefits like saving money and being more flexible, but there are risks such as security problems and relying too much on one provider. A balanced strategy will help us enjoy these benefits while reducing security risks and avoiding Vendor lock in in the following ways;

1. Hybrid Cloud Approach. This combines a Company's own services with cloud services. This gives the Company flexibility to move some of its operations to the cloud while still keeping important or sensitive information on their own secure servers.

Risk mitigation.

Critical data can be stored on local servers for better security and less sensitive data are moved to the cloud.

2. Use of strong Security Practices. Cloud providers offer strong security tools to help to keep your data safe. There inculde things like encryption which moves company's data to only authorized people can read it and ensures the only people have access to the information.

Risk Reduction.

To reduce risks make sure all data is encrypted and people need more than just a password to log in like a Code. Finally do regular checks to find and fix any weakness in the system.

3. Choose across - Cloud Tools. That help to control who can access the cloud resources of the company.
Risk Mitigation:
Using these tools makes it easy to move applications between different cloud providers further reducing Vendor lock-in.

4. Adopt A multi - Cloud strategy. Through using more than one Cloud provider eg AWS Google Cloud and Microsoft Azure.
The Company is able to migrate to different cloud providers.
Risk Minimization.
A company can move its operations to another cloud provider without interruption incase one Cloud provider experiences a data loss.

Conclusion:

By using a balanced strategy, we can take full advantage of cloud Computing benefits while minimizing the risks. With a multi-cloud strategy, across-cloud Tools and hybrid cloud approach, we can Protect the Company and Keep our option open for the future.

Qn 2.

Your company has decided to expand its digital infrastructure by adopting cloud computing. The IT team is debating whether to implement a multi-cloud strategy where services from different cloud providers are used or a hybrid cloud strategy, where on-promises infrastructure is integrated with cloud services.

(i) Evaluate the pros and cons of both multi-cloud and hybrid cloud strategies in the context of your company's needs. Recommend the best approach and Justify your decision.

Introduction.

With modern technology, businesses use cloud computing to save time, money and spend less. Is a multi-cloud strategy or a hybrid cloud strategy the way to go. The following will help us to understand our options and make a decision by comparing.

The following are the pros of a hybrid cloud strategy.

A hybrid cloud strategy mixes public and Private cloud services. This setup gives business more control because they can choose where to store their data and run their applications based on what they need for example They can use private cloud for sensitive information and public for less sensitive tasks.

With a hybrid Cloud strategy a business can easily adjust their cloud resources to match their needs. If they need more capacity they can use public cloud resources while keeping some they in private cloud. This means they can quickly respond to changes in the market without being stuck with one cloud provider.

Improved Security. The business keep their sensitive data on a private cloud which is more secure. They use the public cloud for other tasks that don't need extra security. This way they get the extra protection for their important data while still enjoying the benefits of the public cloud.

Cost-effectiveness. They can save money because they combine public and private clouds company can use the public cloud for things that don't need special security and the private for more sensitive data. This way they get the benefits of both types of clouds without paying extra for unnecessary features leading to over all costs.

The following are the cons of a hybrid cloud strategy.

Vendor lock-in happens. When a business becomes too reliant to one cloud provider This dependence can make it hard to switch to a different provider. This limit the company options and flexibility in finding the best solutions for their needs.

Potential Security risks. Even though a hybrid clouds can be more secure, there is still a risk of data attacks or security problems if the right protections aren't in place. It is important to setup strong security measures to keep everything safe.

On going Costs. Hybrid cloud setups can be expensive to maintain because they need regular investment in equipments up keep and support. This on going spending can be a financial challenge for some organisations.

The following are pros and cons of a multi-cloud strategy.
A multi-cloud strategy involves using multiple cloud computing services with different providers like AWS, Azure and Google Cloud. This approach offers more advantages as follows.

Avoids Vendor lock-in. Using multi-cloud providers helps a business to avoid relying too much on just one provider. This way they are not stuck with one provider services. It gives them more flexibility and can save money by allowing them to choose the best options from different providers.

Increased flexibility: A multi-. cloud strategy allows for more flexibility in choosing the best services for specific tasks as different providers may offer different strengths and capabilities.

Enhanced innovation. Using multi-cloud strategy allows the company to access newest technology and features from each one. This helps them stay up to date with the latest advancements. which can lead to better performance and keeps them a head of their competition.

Cost - effectiveness: Using multi - cloud strategy a Company can save money because it can choose the best prices and services from each one. This way they can find the most cost effective option for their specific needs and workloads leading to overall lower costs.

The following are the cons of a multi - cloud strategy.

Increased Complexity. Managing multiple cloud providers can be more complicated than using just one because you have to handle different systems and services from each provider. This means more effort is needed to make everything work together smoothly and to keep track of how things are running across different platforms.

Increased Costs. Using a multi - cloud strategy can sometimes lead to extra costs because managing and combining different services can be complicated. Company might need to spend more on training support and security and they might face other issues that add to the overall costs.

Potential for Vendor Disagreements. There can be conflicts between them especially if they offer similar services or managing these issues can require careful handling and negotiation to keep a good working relationship with all the providers.

Potential for Vendor lock - in. Even with a multi cloud strategy, there is still a risk of becoming to dependent on certain cloud providers. This can happen if an organisation invests heavily in one provider and when trying to move to another provider it faces challenges.

After evaluating both a multi-cloud strategy and a hybrid-cloud strategy, its clearly that each has its own advantages and challenges. The multi-cloud approach offer flexibility and reduces vendor lock-in but on the other hand, the hybrid-cloud strategy provide a balanced solution by combining the strength of on-promises infrastructure with cloud services offering flexibility, cost efficiency.

Given our company's need to balance sensitive data protection with reliable resources.
I recommend a hybrid cloud strategy the better choice. It allows to keep sensitive data and critical systems secure and under our control while taking advantage of cloud benefits for scalability and flexibility.

Qn 3.

After a successful initial migration to the cloud, your company notices that cloud costs are increasing more rapidly than expected. The finance department is concerned about cost overruns and is questioning whether the move to the cloud was financially beneficial.

(i) Analyze the potential reasons for the unexpected increase in cloud costs.

(ii) Propose strategies to optimize cloud spending while maintaining the benefits of cloud scalability and flexibility.

Introduction:

After moving a company to the cloud, the company notices there are rising faster costs than expected. The finance team is worried about spending too much and doubts if the move to the cloud was a good idea. To keep cloud migration financially smart, its important to find out why the cots are going up unexpectedly. Lets look at what might be the cause of the increase in cloud expenses.

Unused Resources. If you have resources like servers or storage that are not being used and still we again pay for them even though they are still idle. This leads to unnecessary spending which can add up quickly.

Inadequate Monitoring. If the company don't regularly check and adjust its cloud setup it might end up paying for the things it don't need.

Vendor lock-in happens. When a company relies so much on one provider that switching to another would be difficult or costly. And the company will keep paying more because moving to another provider would be too complex.

Increased in demand. When there is unexpected increase in usage like more customers suddenly visits company's website. The cloud automatically adds more resources to handle extra demand. However more resources also mean higher costs.

Premium services. A company can be using more expensive options or features that cloud providers offer. Sometimes companies use these higher-cost services even though they don't really need them for their tasks. This can lead to paying more money than necessary. By choosing only the basic services that fit the actual needs, companies can save on cloud costs.

The following are the strategies to optimize cloud spending while maintaining the benefits of cloud scalability and flexibility.

Monitor and Optimize. It is important to regularly check how much the company is using and how much it costs. There are tools that can show the company exactly where its money is going like which services are costly the most and make adjustments to save money.

Turn off unused Resources. The Company should regularly monitor and shutdown services that aren't being used to avoid paying for the things they don't need. This helps to reduce and lower the overall costs.

Right Size Resources. Ensure the Company only pays for what it actually needs by adjusting resource size based on demand. This way if demand goes up or down its costs will match their usage.

Use of multi-Cloud approach. Ensure the Company look for other cloud providers to see if they offer better prices or services. This way, it will not stuck with just one provider who might change more. It also gives it more power to negotiate better deals.

Conclusion.

By doing these things for example turning off unused resources, Right size resources the Company will keep Cloud costs down while still benefiting from the Cloud's flexibility and ability to scale up when needed.

Qn 4:

A government agency is tasked with storing and analyzing large amounts of citizen data.

(i) What cloud computing solutions can help the agency manage and process this data effectively?

Introduction:

When a government agency handles alot of citizen data, it needs to use the right cloud services to store and analyze this information. It also must follow strong security rules to keep the data safe and meet legal requirements.

There are several cloud computing solutions that can help a government agency manage and process large amounts of citizen data effectively. Some of these include:

Amazon Web Services (AWS). Is a platform popular that provides many tools and services for storing, processing and analyzing data. It can handle large amount of data and grow as you need increase. Additionaly AWS meets various government solutions so it can be used by the government agencies while staying compliant with the law.

Azure or Microsoft Azure. Is a cloud platform similar to AWS. It provides tools and services for storing processing and analyzing data. Azure can easily ~~analyzes~~ data scale up or down based on your needs keeps your data safe and secure and meets government regulations.

Google Cloud Platform (GCP) Is a set of online tools that help organizations store, analyze and understand large amounts of data. For a government agency, GCP can be used to keep data safe, process it quickly, and use smart technology to find useful patterns and insights.

Machine Learning and AI: AWS sagemaker or Google AI platform are tools that use machine learning and artificial intelligence to analyze data and make predictions. They help find patterns and insights in large amounts of data which can be useful for making decisions and solving problems.

(11)

What security and Compliance measures should be Considered?

When it comes to managing and processing citizen data, it is important for a government agency to consider several security and compliance measures. Some of these measures include;

Data Encryption: Encrypting data: Puts data in a secure lockbox so that only people with the right key can see it. This is very important for keeping sensitive citizen information safe when it's stored or sent over the internet.

Access Control: This is like setting up rules to make sure only the right people can see or use the citizen data. This can be done by checking who they are, giving different access levels based on their role and using extra security steps like passwords and codes to confirm their identity.

Privacy and Data Protection. The agency needs to follow all the rules and about keeping people's data private and safe. Theses rules help to protect citizen data and prevent legal problems.

Backup and Recovery. Regularly saving copies of data so it don't lose it if something goes wrong. Having a recovery plan means being ready to restore the data quickly if there's a problem.

Conculusion:
A government agency handle alot of sensitive data like numer and financial details, which needs strong security and legal protection. Cloud computing offers a flexible and cost-effective way to manage this data. However, its crucial to ensure that the data remains secure and complies with laws. The above cloud solutions can help and the key security measures needed to protect citizen data and maintain trust.

References:

Venkatesan, R, & Plummer, D.C. (2017)
Cloud Computing: A Comprehensive Overview.

S.S Iyengar and R.G. Raji
Cloud Computing: A Review of Literature.

A.K. Singh and A.K. Misra. Cloud Computing
A Review and Future Directions.