Module – 4(Resource Management and Security)

1.Resource Monitoring Techniques

Cloud computing provides elastic, scalable resource sharing service by resource management. Resource monitoring and prediction are the foundation to achieve resource automation, high performance management in cloud computing environment. This paper addresses the resource monitoring and prediction problem in cloud computing environment, designs and implements an adaptive resource monitoring framework for cloud computing, and presents a resource prediction mechanism based on Vector Auto Regression (VAR) by the correlation between various resources. Related experiments show that the proposed resource monitoring framework can effectively monitor the resource usage in cloud computing environment, and prediction mechanism based on vector auto regression compared to other prediction mechanism could be more effective to predict resource usage.

2.How to access compute (windows and linux) from internet ? describe tools and its security

Remote Desktop Protocol Method is the most straightforward way to connect to a Linux desktop from your Windows computer. RDP is a protocol used to connect remote desktop computers to the internet. After typing “rdp” into the search box, the Remote Desktop software can be installed on your Windows computer.

The RDP software must be installed on your Windows machine in order for this to occur. After the software has been installed, click the “Remote” tab to begin using it. Click on the “Connections” button in the “Remote” tab to connect to a remote computer. When you are in the “Connections” window, click on the “Add Connection” button. The

“Add Connection” window will display the “RDP” radio button; under “Next,” you will see the “RDP” button. You can find the Ubuntu machine by typing its name into the “Server Name” window and clicking the “Next” button. To view the status of your Ubuntu machine’s port, go to the “Port” window and type the port number. To change the user’s username on your Ubuntu machine, double-click it and choose “User Name.” You can change the password for a user on an Ubuntu machine by typing it into the “Password” window and clicking the “Next” button. When prompted to specify the name or IP address of the Ubuntu machine, click “Next.” The “Remote Host Port” window can be accessed by clicking “Next” in the “Remote Host Port” box. If the Remote Desktop Session Name window does not exist, enter the name of the Ubuntu session you wish to use and click the “Next” button. When you click the “Next” button on the “Remote Desktop Session Port” window, you will be taken to the Ubuntu session’s remote desktop. The “Finish” button is located in the “Advanced” section of the “Advanced” window.
When the connection is complete, you will be able to log in to your Ubuntu machine using the credentials you’ve entered in the “Remote Desktop Session Name” and “Remote Desktop Session Port” windows.

Linux’s and Windows’ support for network security and protocols are comparable. Both include support for IPSec, an open standard for cryptography-based protection at the IP layer. IPSec verifies the identity of a host or end point and ascertains that no modifications were made to the data during transit across the network and encrypts data.

3.Encryption Technologies and Methods

Data encryption in the cloud is the process of transforming or encoding data before it’s moved to cloud storage. Typically cloud service providers offer encryption services — ranging from an encrypted connection to limited encryption of sensitive data — and provide encryption keys to decrypt the data as needed.

For instance, Office 365 Message Encryption is a built-in service that encrypts all messages — both inside and outside of the platform. Encryption services like these prevent unauthorized free access to your system or file data without the decryption key, making it an effective data security method.

Keeping information secure in the cloud should be your top priority. Just taking a few preventative measures around data encryption can tighten security for your most sensitive information. Follow these encryption tips to lock down your information in the cloud.

Encrypt Data Before You Upload It

If your cloud service does not automatically encrypt data before it's uploaded, make sure to encrypt these files beforehand. You can find a third-party encryption tool that will apply passwords and encryption to files after you are finished editing so they are encrypted before upload.

Secure Access With Cloud Cryptography

Cloud cryptography is another way to secure your cloud computing architecture. Cloud computing service providers like Azure employ cryptography to offer a layer of information security at a system level and enables secure access to whoever needs shared cloud services. This layer of encryption is based on the Quantum Direct Key system, which is an advanced system of symmetric encryption keys. Users receive a public and private key pair with a specific ID. Cryptographic cloud computing can also minimize network congestion.

Protect Data at Rest & In Transit With a Cloud Access Security Broker

A cloud access security broker (CASB) is another way you can encrypt data and control your own keys. A CASB offers a single point of visibility and access control into any cloud app in a large enterprise. The control comes through contextual access control, encryption for data at rest and leakage protection of data. A CASB mediates the connections between cloud apps and the general public through several API connectors and proxies.

Maximize Data Security in the Cloud

Beyond encrypting cloud data at the file level, use these cloud data security tips for more protection:

Back Up Your Cloud Data Locally

Although cloud services providers offer redundancy and instant backups, you should always backup your most important data locally — whether on a secured server or laptop. If your cloud-saved data gets lost or corrupted, you can rely on locally backed-up versions. You can also choose to back up your data on a separate cloud. For instance, you might use Dropbox exclusively but backup important files on Google Drive.

Use Encryption Through Your Cloud Services Provider

Many cloud providers offer encryption services to safeguard your data when using their cloud storage. Local encryption will offer an extra layer of security because decryption is necessary before accessing the files or data. Encrypting data at rest is great, but also encrypting data in transport is even better. Find out what type of encryption your cloud services provider can offer.

Map Your Security Needs for Your Cloud Deployment

You should identify the data you need encrypted, and map out a plan with your cloud service provider to prioritize sensitive data. If your sales team is using the cloud for video presentations and graphics accessible for public use, only the account information should be encrypted. Other teams using the cloud to share documentation and source code would require end-to-end encryption at the file level.

Understand the Details of Service Before Working With a CSP

The user agreement usually outlines the details of your plan. Ask about any details left out of the user agreement to clarify how, when and where your data is stored, especially if using a public cloud. Make sure to search for anything that could violate your company's privacy policy.

4.Describe network security in cloud, compute security and storage security

Cloud network security is a branch of cybersecurity that focuses on **ensuring the security of cloud computing systems.** You can generate, process, and store many business and personal data, like financial and credit card data using cloud network security systems.

Cloud network security also includes all aspects of securing every component in the cloud, from virtual machines, through configurations, to applications and data. The purpose behind cloud security is to **shift the risk of data loss, unauthorized access, and service interruption**. It also helps you avoid **performance degradation, data breach**, and anything compromising your system in the cloud.

Cloud security **enhances your company's knowledge in protecting cloud-based digital assets**. When you apply this knowledge, you also

improve your company's ability to comply with data privacy/protection laws and regulations.

Now that you know what cloud network security is, I'll guide you through **5 reasons why cloud security is important** for your company.

Why Is Cloud Network Security Important?

Adding cloud security as a business priority might seem unnecessary and impractical, but it's not. Check out 5 reasons why cloud network security is important below:

1. Reduces Business Risk

As you migrate workloads to the cloud, you increase your attack surface. Why? Before, you only had to worry about potential threats and vulnerabilities in your on-premise IT infrastructure, which impacted business operations. Now, you also have to contend with similar concerns in your private, public, and hybrid clouds. When you adopt cloud security, you **reduce risks in those areas**.

2. Protects Data

Cloud environments generate, process, and store huge amounts of data every day. In fact, predictions say that by 2025, **100 zettabytes**, or 50% of the world's data at that time (up from 15% in 2015), will be stored in the cloud. Some of that will be sensitive data, e.g., personal data, financial data, trade secrets, credit card data, etc. Your company also needs cloud security to **ensure the confidentiality, integrity, and availability of that data.**

3. Increases Reliability and Availability

A significant part of your business processes run in the cloud, so you need to constantly keep the cloud services driving those processes reliable and available. Cloud security also helps you **prevent processes from being deliberately or accidentally corrupted or disrupted**.

4. Ensures Regulatory Compliance

Data protection/privacy laws and regulations cover certain types of data stored in the cloud. These laws could be the Payment Card Industry Data Security Standard (PCI DSS), the US Health Insurance Portability and Accountability Act (HIPAA), and the EU General Data Protection Regulation (GDPR), among others. When you implement cloud security best practices, you **increase your chances of staying compliant** with these mandates.

5. Reduces Costs

The price of a single data breach costs you much more than cloud security initiatives. Data breaches are more likely to happen in the absence of cloud security. In the **2021 Cost of a Data Breach Report**, the average total cost was already estimated to be at $4.24M, with the average cost of a mega-breach (50-65 million records) already at $401M. That means you'll have to spend on potential lawsuits, legal and regulatory fines/penalties, data breach notifications, and other related costs. You'll also **suffer a loss of opportunity** and a severely damaged reputation.

Indeed, you shouldn't take cloud security's importance lightly. That said, I should say the road to a secure cloud environment has bumps and potholes. In the next section, I'll tackle the top 4 challenges you'll likely face along the way.