QUESTION 1.

Compare and contrast the security features and controls of different cloud providers (E.g. AWS, Azure and Google cloud).

The security features and controls offered by major cloud providers like AWS, Azure, and Google Cloud have a Shared Responsibility Model

Foundation: All cloud providers operate on a shared responsibility model. They secure the underlying infrastructure that's security of the cloud, while customers are responsible for securing their own data, applications, and operating systems.

Key Security Features and Controls

Feature/Control	AWS	Azure	Google Cloud
Identity and Access Management (IAM)	1) Fine-grained access control using roles, policies, and groups. 2) Multi-factor authentication (MFA) support.	1. Role-based access control (RBAC) with granular permissions. 2. Azure Active Directory for identity management.	1) IAM roles and service accounts for access control. 2) Integration with Google Workspace and Cloud Identity.
Data Protection	1. Encryption at rest and in transit. 2. Key management services (KMS).	1. Encryption at rest and in transit. 2. Azure Key Vault for key management.	1. Encryption at rest and in transit. 2. Cloud Key Management Service (KMS).
Network Security	1. Virtual Private Cloud (VPC) for network isolation. 2. Security groups and network ACLs for firewalling.	1. Virtual Network (VNet) for network isolation. 2. Network Security Groups (NSGs) for firewalling.	1. Virtual Private Cloud (VPC) for network isolation. 2. Firewall rules and network tags.
Compliance and Certifications	1. Extensive compliance certifications (e.g.,	1. Wide range of compliance	1. Strong compliance certifications (e.g., ISO

	ISO 27001, SOC 2, PCI DSS, HIPAA).	certifications (e.g., ISO 27001, SOC 2,	27001, SOC 2, PCI DSS, HIPAA).
Security Monitoring and Threat Detection	1. CloudTrail for API logging and auditing. 2. GuardDuty for threat detection.	1. Azure Activity Log for auditing. 2. Azure Security Center for threat detection and vulnerability	1. Cloud Audit Logs for auditing. 2. Cloud Security Command Center for threat detection and security health analytics.

Other Important Considerations that we can also look at

- **Automation:** All providers offer tools for automating security tasks, such as vulnerability scanning, patch management, and incident response.
- **Serverless Security:** Providers are enhancing security for serverless environments with features like function-specific IAM roles and integrated security scanning.
- **Confidential Computing:** Emerging technologies like Intel SGX and AMD SEV enable the encryption of data in use, adding an extra layer of protection for highly sensitive workloads.

Choosing the Right Provider

The best cloud provider for security depends on your specific needs and priorities.

Consider factors like:

- **Compliance requirements:** Ensure the provider has the necessary certifications for your industry.
- **Workload sensitivity:** Evaluate the provider's capabilities for protecting your specific types of data and applications.
- **Integration with existing systems:** Choose a provider that integrates well with your current security tools and processes.
- **Security expertise:** Assess your team's familiarity with the provider's security offerings and the level of support available.

QUESTION 2.

Develop a cloud security policy for a fictional organization, including policies for data classification, access control, and incident response.

Here is the Cloud security policy framework for Venite University Iloro-Ekiti

Planning and Scoping for Venite University Iloro-Ekiti

1) **Organization Profile:** Venite University Iloro-Ekiti is a fictional private university in Nigeria. Its data includes student records, faculty research, financial information, and administrative data. It utilizes cloud services for student portals, online learning platforms, and research data storage.
2) **Stakeholders:** Include the Vice-Chancellor, IT Director, Registrar, Faculty Heads, Legal Counsel, and Student Representatives.
3) **Scope:** This policy applies to all cloud services used by Venite University, including student portals, online learning platforms, research data storage, and administrative systems. It covers all data stored and processed in these cloud environments.
4) **Regulatory and Legal Requirements:** Venite University must comply with Nigerian data protection laws, educational regulations, and potentially international research data sharing agreements.

Policy Development

Introduction:

This policy establishes the guidelines for securing cloud computing resources and data at Venite University Iloro-Ekiti.

Objective:

Its objective is to protect the confidentiality, integrity, and availability of university data, ensure regulatory compliance, and mitigate security risks.

Scope:

This policy applies to all cloud services used by Venite University, encompassing student portals, online learning platforms, research data storage, and administrative systems. It covers all data stored and processed within these cloud environments.

Roles and Responsibilities:

Chief Information Security Officer (CISO): Oversees cloud security strategy and policy.

IT Department: Manages cloud infrastructure and implements security controls.

Data Owners (e.g. Registrars, Faculty Heads): Responsible for the security of their data.

Cloud Users (Faculty, Students, Staff): Adhere to security policies.

Data Classification:

- Public: University website, research publications.
- Internal: Student directories, internal communications.
- Confidential: Student academic records, financial data.
- Restricted: Research data with sensitive findings, personal identifiable information (PII).

Access Control

- RBAC: Implement role-based access control.
- MFA: Require multi-factor authentication for all users accessing sensitive data.
- Least Privilege: Grant users only the necessary permissions.
- Regular Reviews: Conduct quarterly access reviews.
- Password Policy: Force strong passwords and regular changes.

Data Protection:

- Encryption: Encrypt data at rest and in transit.
- Backup and Recovery: Implement daily backups and test recovery procedures.
- DLP: Use data loss prevention tools to prevent data leaks.

Incident Response:

a) Incident Response Plan: Develop a plan for security incidents.
b) Incident Reporting: Establish a clear reporting process.

Security Awareness and Training:

Conduct annual security awareness training for all users.

Provide phishing awareness training.

Compliance

List Nigerian data protection laws and educational regulations. Include any relevant international standards.

Policy Enforcement, Review and Updates

Consequences for policy violations must be stated, Review and update the annually.

Review and Approval

Distribute the policy to stakeholders for feedback.

Revise the policy based on feedback.

Obtain approval from the Vice-Chancellor and governing board.

Implementation and Communication

- Communicate the policy to all university members.
- Conduct training sessions and Implement security controls.
- Conduct regular audits and monitoring.

Other Key Cloud Security Considerations to be implemented

- Access Control (SAML, XACML): Implement robust access control using industry standards.
- Data Protection (Homomorphic Encryption): Explore advanced encryption methods for sensitive data.
- Threats: Address threats like account hijacking, data loss, and insider threats.
- Unknown risk profile: Implement logging and monitoring to reduce the unknown risk profile.

QUESTION (3)

The analysis of a real-world cloud security breach or incident with root cause and recommended mitigation using case study of Flutter wave.

Incident Overview in February 2023, reports emerged that Flutter wave had suffered a security breach that led to unauthorized transactions affecting multiple customers. The breach involved hackers exploiting vulnerabilities in the company's cloud-based financial infrastructure to move funds fraudulently. Over ₦2.9 billion was allegedly transferred to various bank accounts before the incident was contained.

Root Causes

1) API Security Vulnerabilities: Weaknesses in Flutter wave's API allowed attackers to initiate unauthorized fund transfers.

2) Lack of Strong Authentication Measures: Insufficient multi-factor authentication (MFA) protocols made it easier for attackers to access sensitive systems.
3) Delayed Incident Detection: The breach was not immediately identified, allowing the attackers time to execute multiple fraudulent transactions.
4) Weak Internal Access Controls: Some reports indicated that insider threats or poor privilege management may have played a role in the attack.

Mitigation Strategies

1. Enhance API Security: Implement strict API security measures, including rate limiting, token-based authentication, and regular penetration testing.
2. Implement Robust Multi-Factor Authentication (MFA): Strengthening user authentication mechanisms can prevent unauthorized access to critical financial systems.
3. Deploy Real-Time Fraud Detection Systems: Advanced AI-driven fraud detection tools can identify and block suspicious transactions before they escalate.
4. Restrict Internal Access Controls: Using the principle of least privilege (PoLP) for internal employees can limit the risk of insider threats.
5. Regular Security Audits: Conducting frequent security audits and penetration testing can help detect and address vulnerabilities before they are exploited.
6. Improve Incident Response Protocols: A well-defined incident response plan ensures rapid detection and containment of security breaches.

Conclusion: The Flutter wave breach highlights the critical need for enhanced security measures in Nigeria's fintech sector. Strengthening API security, enforcing multi-factor authentication, and implementing real-time fraud detection are essential steps to safeguard customer funds and maintain trust in digital financial platforms.

Another Case Study Analysis: Uber Cloud Security Breach

Introduction The Uber cloud security breach of 2022 is a notable example of how poor security hygiene and social engineering can lead to significant data exposure. The breach compromised internal systems, exposing sensitive company data and internal communications. This case study analyzes the root causes and recommends mitigation strategies.

Incident Overview in September 2022, an attacker gained access to Uber's internal systems by targeting an employee with social engineering tactics. The attacker tricked the employee into approving a multifactor authentication (MFA) request, allowing access to Uber's VPN. This access enabled lateral movement within the cloud environment, leading to the compromise of several internal systems, including Slack, AWS, and Google Workspace.

Root Causes

1. Social Engineering Exploitation: The attacker used phishing tactics to manipulate an employee into granting access.
2. Weak MFA Implementation: The use of push-based MFA without additional verification made it susceptible to approval fatigue attacks.
3. Lack of Robust Privilege Controls: Once inside, the attacker could escalate privileges due to insufficient access restrictions.
4. Insufficient Logging and Monitoring: Uber did not immediately detect the breach, allowing the attacker to explore internal systems unnoticed.

Mitigation Strategies

1. Strengthen MFA Policies: Implement phishing-resistant MFA methods, such as FIDO2 security keys, to prevent social engineering attacks.
2. Enhance Employee Security Awareness: Regular security training and simulations can help employees recognize and avoid social engineering attempts.
3. Implement Strict Privilege Access Management: Adopting least privilege access and regularly reviewing permissions can limit the damage caused by an attacker.
4. Deploy Advanced Monitoring Solutions: Real-time security monitoring and behavioral analytics can help detect unauthorized access attempts quickly.
5. Adopt a Zero Trust Security Model: Ensuring continuous authentication and verification for all users can prevent attackers from easily moving within the network.
6. Conduct Regular Security Audits: Frequent penetration testing and audits can uncover vulnerabilities before they are exploited by malicious actors.

Conclusion The Uber breach underscores the importance of strong authentication measures, proactive security monitoring, and effective employee training in preventing cloud security incidents. By implementing these mitigation strategies, organizations can bolster their security posture and better protect sensitive data from cyber threats.