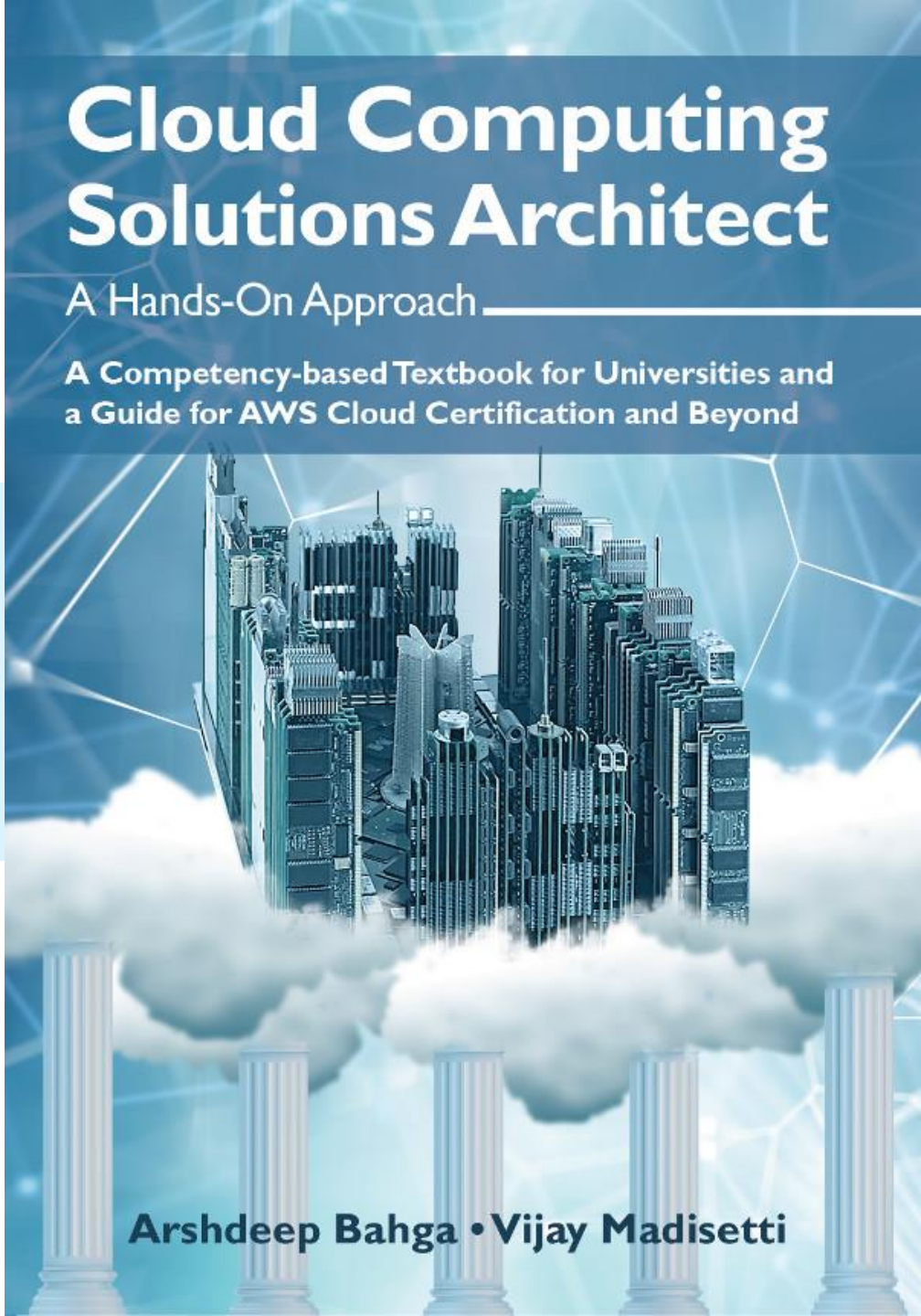
Chapter 17

Applying the Security Pillar



Security Pillar

- The Security pillar includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.
- Within the Security pillar, there are five best practice areas:
  - Identity and Access Management
  - Detective Controls
  - Infrastructure Protection
  - Data Protection
  - Incident Response

Design Principles for Security Pillar

- Implement the principle of least privilege and centralize privilege management.
- Enable traceability, collect logs and metrics, and monitor all changes to your environment.
- Apply security at all the layers of your application (for instance, load balancer, instances, and operating system).
- Protect data in transit and at rest
- Reduce or eliminate the need for direct access to data and manual processing of data.
- Have an incident management process and automate detection and recovery from security events.

Best Practice Area: Identity and Access Management

- The Identity and Access Management best practice area highlights the importance of ensuring that only authorized and authenticated users can access your resources and do so only in an intended manner.
- To manage your credentials and authentication, you must define identity and access management configurations.
- The AWS root user must be secured by using multi-factor authentication (MFA) and by limiting its use.
- Enforcement of access controls should be automated. Where possible, use a federated identity provider or directory service to authenticate all users in a centralized place.
- Enforce password requirements and rotate credentials regularly.
- Credentials must be audited to ensure the defined controls such as MFA are enforced.
- To control human access, the access requirements for users should be defined based on job function, and only the least privileges should be granted to reduce the risk of unauthorized access.
- To control programmatic access, you should clearly define access requirements for programmatic access and grant only the least privileges.

Pillar II: Security - Best Practice Area: Identity and Access Management	
Consideration	**Best practice**
Manage credentials and authentication	Define identity and access management requirements
	Secure AWS root user
	Enforce use of multi-factor authentication
	Automate enforcement of access controls
	Integrate with centralized federation provider
	Enforce password requirements
	Rotate credentials regularly
	Audit credentials periodically
Control human access	Define human access requirements
	Grant least privileges
	Allocate unique credentials for each individual
	Manage credentials based on user lifecycles
	Automate credential management
	Grant access through roles or federation
Control programmatic access	Define programmatic access requirements
	Grant least privileges
	Automate credential management
	Allocate unique credentials for each component
	Grant access through roles or federation
	Implement dynamic authentication

Best Practice Area: Detective Controls

- The Detective Controls best practice area highlights the importance of using detective controls to identify a potential security threat or incident.
- To detect and investigate security events, you should capture and analyze logs and metrics.
- Requirements for collecting logs and metrics and requirements for alerts should be defined.
- Logs must be collected and analyzed centrally to detect any anomalous access patterns and malicious activities, and alerting should be automated on key indicators.
- To defend against emerging security threats, you should keep up to date with security best practices and security threats.

Pillar II: Security - Best Practice Area: Detective Controls	
Consideration	**Best practice**
Detect and investigate security events	Define requirements for logs
	Define requirements for metrics
	Define requirements for alerts
	Configure service and application logging
	Analyze logs centrally
	Automate alerting on key indicators
	Develop investigation processes
Defend against emerging security threats	Keep up to date with organizational, legal, and compliance requirements
	Keep up to date with security best practices
	Keep up to date with security threats
	Evaluate new security services and features regularly
	Define and prioritize risks using a threat model
	Implement new security services and features

Best Practice Area: Infrastructure Protection

- The Infrastructure Protection best practice area highlights the importance of protecting your network and compute resources.
- To protect your networks, you should define your network protection requirements and limit the exposure of your application's resources to the Internet.
- Configuration management and network protection should be automated.
- Traffic should be controlled at all layers.
- To protect your compute resources, you should define protection requirements for compute resources.
- Configuration management and compute protection should be automated.
- Where possible, you should use managed services such as Amazon RDS for database instead of managing your databases on EC2 instances.

Pillar II: Security - Best Practice Area: Infrastructure Protection	
Consideration	**Best practice**
Protect your networks	Define network protection requirements
	Limit exposure
	Automate configuration management
	Automate network protection
	Implement inspection and protection
	Control traffic at all layers
Protect your compute resources	Define compute protection requirements
	Scan for and patch vulnerabilities
	Automate configuration management
	Automate compute protection
	Reduce attack surface
	Implement managed services

Best Practice Area: Data Protection

- The Data Protection best practice area highlights the importance of protecting your data in transit and at rest.
- To classify your data according to the levels of sensitivity, you should define the data classification requirements and protect data according to its classification level.
- The identification and classification of data should be automated.
- To protect your data at rest, you should define data management and protection at rest requirements.
- Data at rest must be encrypted, and the encryption keys must be stored securely and rotated with strict access control.
- Users should be prevented from directly accessing sensitive data; instead, access to data should be provided indirectly through dashboards and other tools.
- To protect your data in transit, you should define requirements for data protection in transit.
- All data in transit must be encrypted using protocols such as TLS, and the encryption keys and certificates must be stored securely.

Pillar II: Security - Best Practice Area: Data Protection	
Consideration	**Best practice**
Classify your data	Define data classification requirements
	Define data protection controls
	Implement data identification
	Automate identification and classification
	Identify the types of data
Protect your data at rest	Define data management and protection at rest requirements
	Implement secure key management
	Enforce encryption at rest
	Enforce access control
	Provide mechanisms to keep people away from data
Protect your data in transit	Define data protection in transit requirements
	Implement secure key and certificate management
	Enforce encryption in transit
	Automate detection of data leak
	Authenticate network communications

Best Practice Area: Incident Response

- The Incident Response best practice area highlights the importance of putting processes in place to respond to and mitigate the potential impact of security incidents.
- To respond to security incidents promptly, you should identify the key personnel and external resources for incident response and provide them with the right tools so that appropriate responses can be made.
- You should create incident response plans and automate containment of an incident to reduce the response time and impact.

Pillar II: Security - Best Practice Area: Incident Response	
Consideration	**Best practice**
Respond to an incident	Identify key personnel and external resources
	Identify tooling
	Develop incident response plans
	Automate containment capability
	Identify forensic capabilities
	Pre-provision access
	Pre-deploy tools
	Run game days

Recipe for Security Pillar

- This recipe uses AWS IAM for securely controlling access to AWS services and resources used by the photo gallery application.
- For user directory and authentication, Amazon Cognito service is used.
- The application is implemented in Python and uses the Flask web framework.
- The application is deployed on an Amazon EC2 instance.
- The photos uploaded to the application are stored in an Amazon S3 bucket.
- The records of photos are maintained in a MySQL database instance on Amazon RDS.