Risk Analysis and Security Design

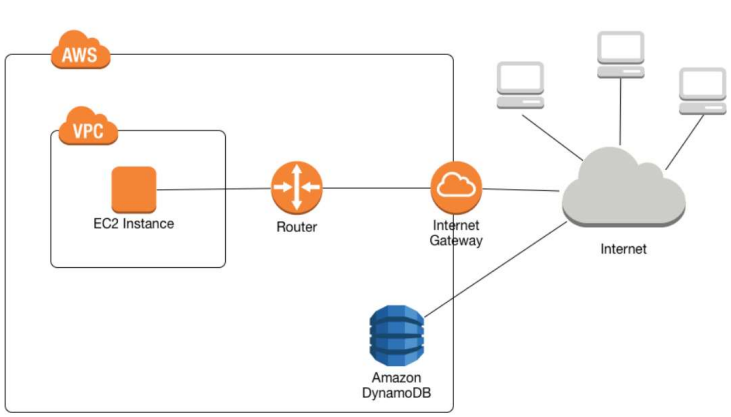
Background:

Our website is hosted by **AWS EC2** instance and involves data transfer between website database and AWS services

Cloud Security:

Risk Description	Risk Rating	Recommendation
heavy workload: At some point, the load on the application will be far greater than usual	medium	Setup an Auto Scaling group of EC2 instances, choose the minimum capacity and maximum capacity
the hardware in a certain region may go down	High	Implement multi-AZ. For example, deploy 2 instances in Availability Zone 1 and another 1 instance in Availability Zone 2
unauthorized access to our EC2 instances	High	Setup AWS VPC for our instances, a firewall policy that controls inbound and outbound traffic.
unauthorized third party access our website extract data from our application	High	• Use a domain name • Data will be transferred between the website and the AWS server, to protect credentials and sensitive information from unauthorized third party, we should use encryption: SSL/TLS • We should manage the credential used to connect our AWS services and website, use a secure password and do not share it • Manage the IAM role and policies attached to role

Schema:



References:

VPC endpoints:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html

Infrastructure security:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/infrastructure-security.html#control-network-traffic

Resilience:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/disaster-recovery-resiliency.html