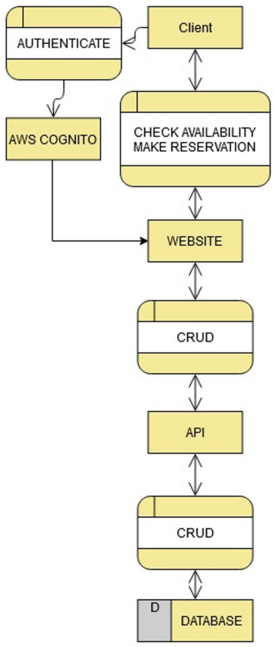
THREAT MODEL

Wat bouwen we?

Data Flows

We bouwen een webapplicatie waarop materiaal kan gereserveerd worden. Deze applicatie bestaat uit de website die een klantvriendelijke interface voorziet, een database die al het beschikbare alsook het uitgeleende materiaal bijhoudt, en een API die de brug vormt tussen de website en de database. Hiervoor worden standaard create, read, update en delete requests gebruikt tussen client, website en api.

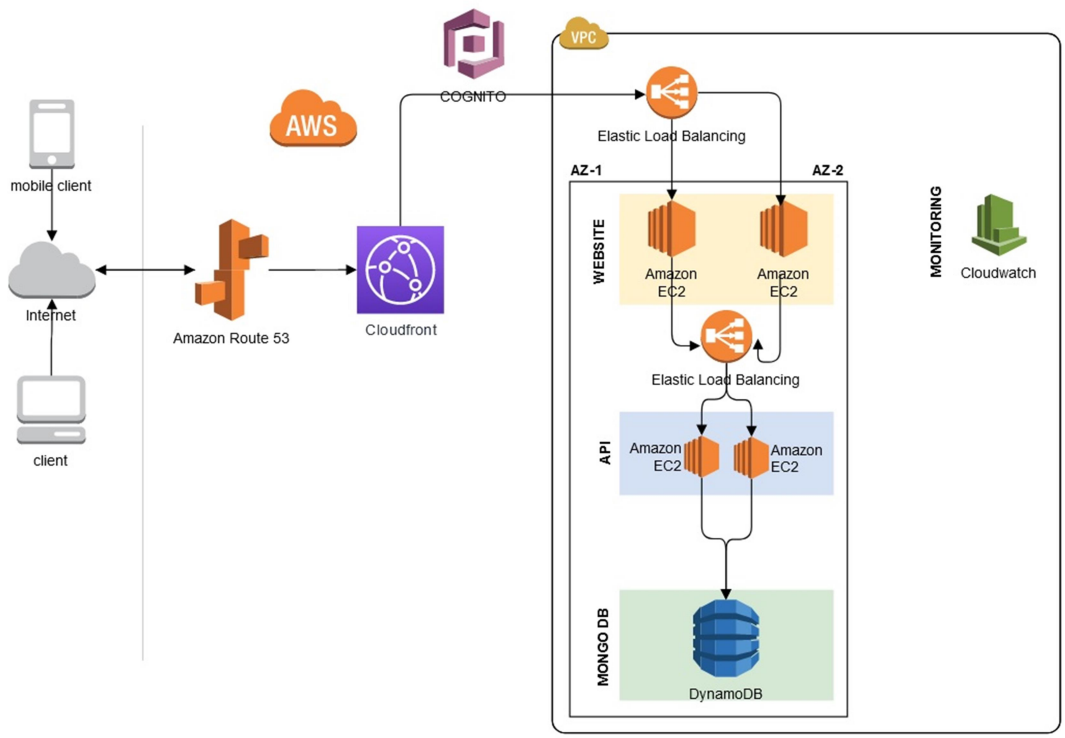


Architectuur

Er wordt gebruik gemaakt van de AWS infrastructuur. (zie onderstaande figuur)
DNS resolutie gebeurt via *Route 53*, die de communicatie doorstuurt naar *Cloudfront* (Caching, DDOS bescherming).
Cloudfront stuurt de requests door naar een *Elastic Load Balancer* (High availability, SSL termination) die deze verdeelt over twee verschillende *EC2 instanties* (= virtuele machines waar de website draait op ASP.NET).
Eventuele authenticatie gebeurt met *Cognito*(Social sign in/eventueel met multi factor authentication).
De requests worden via een andere Load Balancer verdeeld onder twee EC2 instanties waar de API op draait.
Data wordt opgeslaan op *DynamoDB* (High availability, scalability).
Tot slot worden er access logs opgeslaan dankzij *Cloudtrail*, en gebeuren er continu health checks op

Figuur 1

de EC2 instanties dankzij de *Load Balancer*.



Wat kan er mis lopen & hoe wordt het opgevangen?

SPOOFING

De site is enkel bereikbaar via https. Het verkeer is dus geëncrypteerd. Verder maken we gebruik van Cognito. Cognito voorziet bij aanmelden een Json Web Token als signatuur.

TAMPERING

Zoals hierboven vermeld is de site enkel bereikbaar via https, en wordt bij aanmelden een JWT aangemaakt als signatuur.
Binnen de AWS infrastructuur is alle verkeer gefilterd op IP adres (Een EC2 instantie aanvaardt bijvoorbeeld enkel communicatie van het IP adres van zijn Load Balancer).

REPUDIATION

Cloudtrail slaat alle requests op in access logs.

INFORMATION DISCLOSURE

DENIAL OF SERVICE

Cloudfront heeft ingebouwde bescherming tegen DOS aanvallen. Indien deze toch zou falen, kan de

aanval verdeeld worden over de Load Balancers.

PRIVILEGE ESCALATION

De AWS root account is beveiligd met MFA en wordt in principe nooit gebruikt, enkel User Accounts worden gebruikt om AWS services te beheren.

ELEMENT	Spoofing	Tampering	Repudiation	Information disclosure	Denial of Service	Privilege escalation
Website EC2				Mitigate		Mitigate
API EC2				Mitigate		Mitigate
DynamoDB			Accept	Accept	Accept	