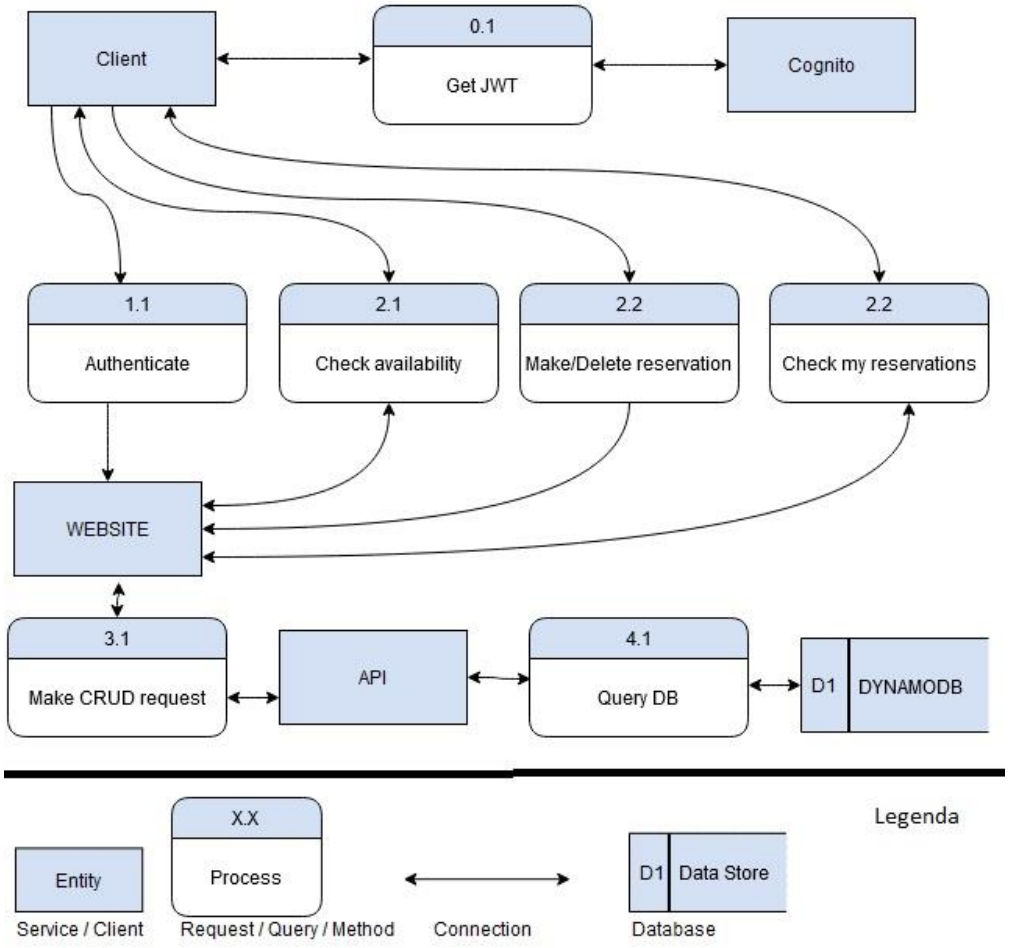
THREAT MODEL

Wat bouwen we?

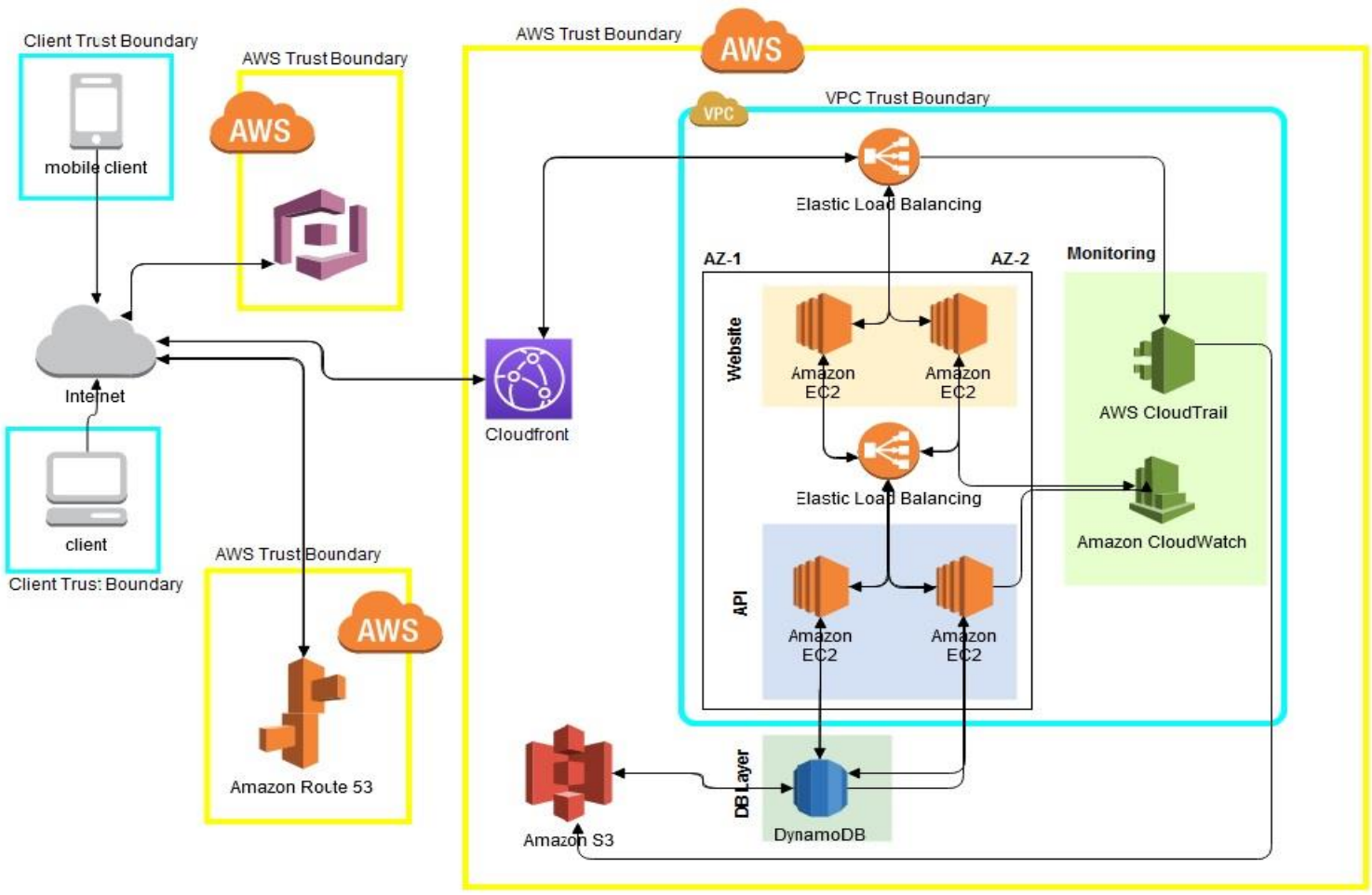
Data Flows

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 fig. 2)
DNS resolutie gebeurt bij *Route 53*.
Webrequests van de client worden gestuurd 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.
Records van data wordt opgeslaan op in een NoSQL serverless database: *DynamoDB* (High availability, scalability).
Deze records kunnen ook verwijzen naar data opgeslaan in *S3*.
Cloudwatch houdt het resourcegebruik van de EC2 instanties in het oog en verstuurt een bericht wanneer het resourcegebruik abnormaal hoog of laag wordt.
Binnenin AWS staan er tussen alle verschillende services die met elkaar communiceren *security groups*. Deze zorgen ervoor dat enkel internetverkeer van bepaalde ip addressen wordt aanvaard.
Tot slot worden er access logs opgeslaan dankzij *Cloudtrail*, en gebeuren er continu health checks op 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. De client vraagt bij Cognito een Json Web Token aan en kan hiermee aanmelden bij de applicatie.

TAMPERING

Zoals hierboven vermeld is de site enkel bereikbaar via https. SSL termination gebeurt bij de Load Balancer die voor de Website EC2 instances staan.
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

- De informatie wordt opgeslaan in S3. Door middel van AWS 'security groups' staat s3 enkel open voor communicatie met DynamoDB, die op zich weer enkel bereikbaar is via de IP addressen van de EC2 instanties, die op hun beurt enkel bereikbaar zijn via de IP addressen van hun load balancers. De info op S3 is dus in principe dichtgetimmerd voor alle queries/requests behalve die requests die via de website van de API zelf komen.
- Als aangemeldde gebruiker heb je via de website enkel toegang tot queries die betrekking hebben op je eigen reservaties, of queries die het beschikbare materiaal weergeven. Je hebt geen toegang tot queries die informatie over andere gebruikers zouden kunnen vrijgeven.
- Als niet aangemeldde gebruiker heb je enkel toegang tot queries die het beschikbare materiaal weergeven.

DENIAL OF SERVICE

Cloudfront heeft ingebouwde bescherming tegen DOS aanvallen. Indien deze toch zou falen, kan de aanval verdeeld worden over de Load Balancers.
Cloudwatch monitort het resource gebruik van de EC2 instanties. Deze stuurt een waarschuwing wanneer het resourcegebruik abnormaal hoog wordt (parameters zelf te bepalen).

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	Cognito, Cloudfront	Load Balancer, Security groups	Cloudtrail	Security Groups, Application architecture	Cloudfront	Cognito
API	Security groups	Security groups	Accept	Security Groups	Cloudwatch	Mitigate
DB	Security groups	Security groups	Accept	Security Groups	Cloudwatch	Mitigate