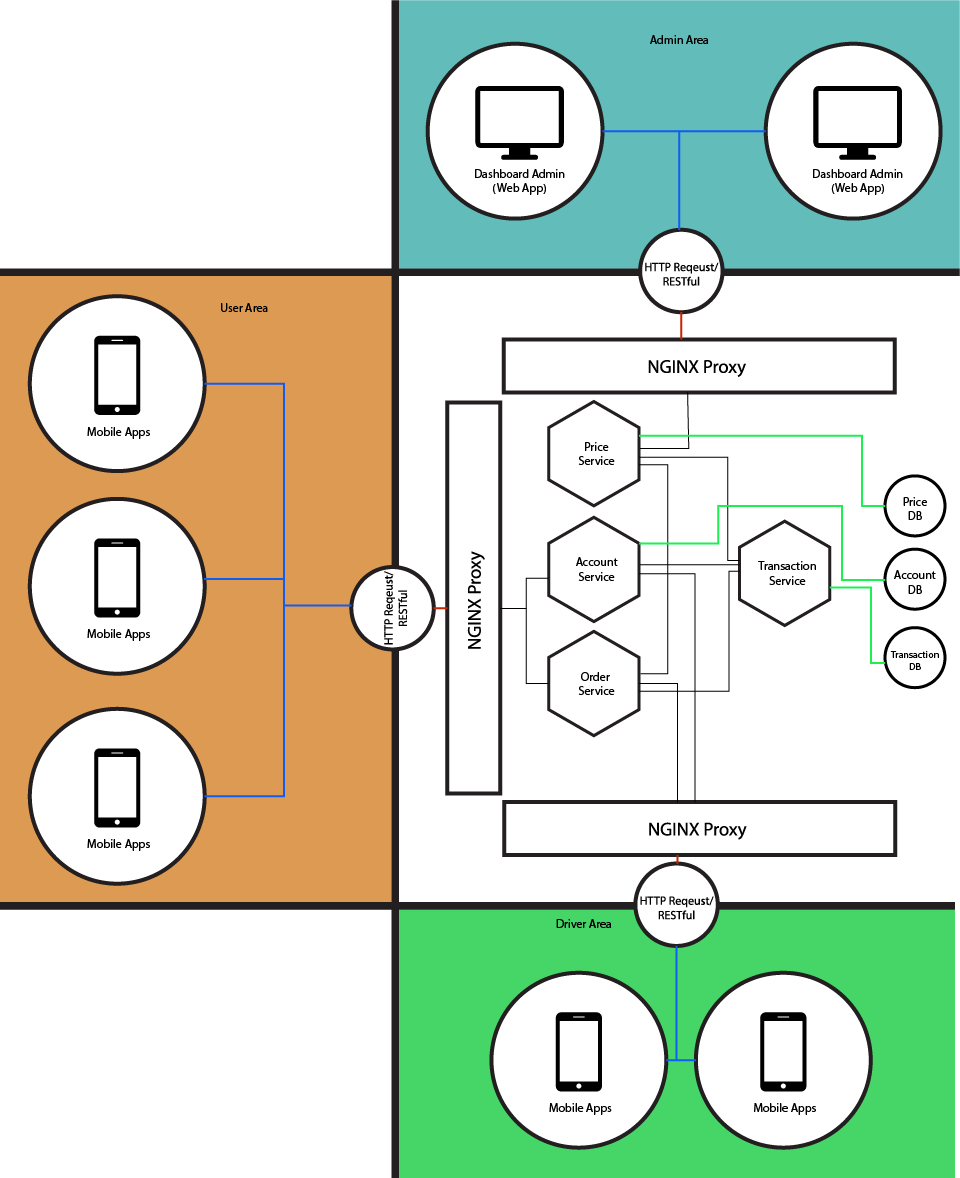
Nama : Arief Ditia Faltah

Soal No. 1



Pada design webservice saya menggunakan komunikasi REST agar aplikasi(client) dan webservice dapat saling terhubung dan berbagi data. Untuk bahasa pemrograman backend saya menggunakan Node.js dan database yang digunakan adalah MongoDB. Setiap komunikasi HTTP Request yang datan akan ditangani oleh NGINX Proxy yang nantinya akan meneruskan kepada port dimana aplikasi webservice tersebut berjalan. Aplikasi webservice yang terhubung dengan database akan menggunakan redis sebagai metode cache agar komunikasi menjadi lebih cepat. Pada saat deployment webservice yang berupa microservice akan berjalan di atas Docker Cointainer agar memudahkan scalling dan maintenance

Soal No.2

Dalam menangani pengiriman data, terdapat beberapa jenis pengamanan yang berjalan pada fase komunikasi yang berbeda namun memiliki kepentingan yang sama.

1. APP Key

Agar membatasi tidak semua orang dapat mengakses Webservice dari aplikasi digunakan APP Key. APP Key adalah sebuah kunci yang di hasilkan melalu proses hash pada Webservice. Setiap Komunikasi HTTP Request yang dilakukanan client, Webservice akan meminta APP Key untuk mengenali apakah client tersebut merupakan client yang seharusnya mendapatkan response dengan benar. Pengamanan ini adalah pengamanan ranah aplikasi(client) dan webservice saat akan memulai komunikasi.

1. Token Based Authentication

Saat komunikasi antara apilkasi(client) dan webservice telah berhasil dilalui, sebuah aplikasi tentu akan melakukan banyak komunikasi dengan server. Banyak celah keamanan yang terjadi pada fase ini. Dapat digunakan Token Based Authentication seperti JSON Web Token. Dimana setiap komukasi selain memiliki APP Key juga akan memiliki token untuk melakukan request. Panjang token dapat diatur, semakin panjang dan rumit maka akan semakin baik untuk keamanan. Pengamanan ini adalah pengamanan pada pada fase komunikasi telah terjadi antara aplikasi(client) dan webservice.

1. SSL/TLS/HTTPS

Penggunaan layanan SSL/TLS/HTTPS baik di implementasikan agar setiap data yang dikirim melalui metode POST di enkripsi. Pada umumnya saat pengguna akan masuk ke dalam aplikasi, pengguna akan memasukkan email dan password mereka. Fase ini memiliki kerentangan dimana data dapat di Sniffing dengan tools seperti WireShark. Penggunaan Protokol HTTP yang aman (HTTPS) dapat mengurangi ancaman saat terjadi pencurian identitas login.

Soal No.3

Pada soal no.3 saya menggunakan Node.js dan JsonWebToken sebagai bahasa pemrograman dan metode pengaman komunikasi. Berikut adalah screenshoot setiap testnya melalui aplikasi postman.

