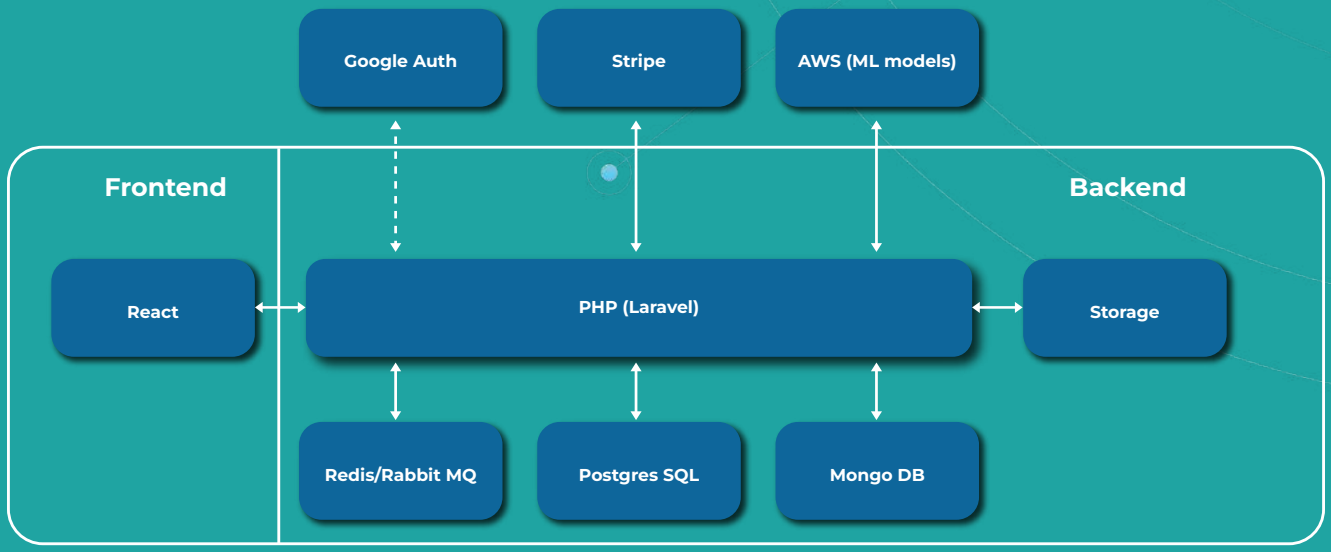
altris AI

SECURITY DOCUMENTATION

ARCHITECTURE DIAGRAM

The architecture diagram of the Altris web platform is presented below:



1.BACKEND

Contains all business-logic, API-layer, and produces jobs for examination queue (RabbitMQ).
Developed on the PHP (Laravel framework).

Server architecture:

a PostgreSQL database
This database is related to all **user data** that is stored on a local server. All additional encryption processes on a Backend server are related to this database.

b MongoDB
Database that is related to all images (scans) presented on a platform.

c Redis/RabbitMQ
Key-value storage and queue “manager” for blockings and simple caching implementation.

d Storage
Storage on the local instance. Is used for collecting system data like configs or keys.

Integrations:

a Google Authentication
Integrated for a more user-friendly experience.
Documentation is presented here - oauth2

b Stripe
Integrated for the payment functionality.
Documentation is presented here - Stripe api

c Artificial Intelligence edpoints
Integrated for non-user data management.
All **endpoints** are located on AWS instances.

2.FRONTEND

Front-end side developed on the React.js framework. Placed on **the same** AWS instance. It “communicates” with the back-end through API. Also, all HTTP responses are **Gziped** for minimize traffic and speed up.

All data management (between Frontend and Backend parts) is secured via HTTPS encryption.

ENCRYPTION

1 Password Encryption

Database user passwords and passwords of all users of the Altris platform are stored as hashes (determined by the setting **password_encryption**), so the administrator cannot determine the actual password assigned to the user. If SCRAM or MD5 encryption is used for client authentication, the unencrypted password is never even temporarily present on the server because the client encrypts it before being sent across the network. SCRAM is preferred, because it is an Internet standard and is more secure than the PostgreSQL-specific MD5 authentication protocol.

2 SSL Host Authentication

Both the client and server have provided SSL certificates to each other. It takes some extra configuration on each side, but this provides stronger verification of identity than the mere use of passwords. It prevents a computer from pretending to be the server just long enough to read the password sent by the client. It also helps prevent “man in the middle” attacks where a computer between the client and server pretends to be the server and reads and passes all data between the client and server.

3 Client-Side Encryption

If the system administrator for the server's machine cannot be trusted, it is necessary for the client to encrypt the data; this way, unencrypted data never appears on the database server. Data is encrypted on the client before being sent to the server, and database results have to be decrypted on the client before being used.

4 User data encryption in PostgreSQL via pgcrypto

The pgcrypto module provides cryptographic functions for PostgreSQL. This module is considered “trusted”, that is, it can be installed by non-superusers who have CREATE privilege on the current database.

5 **Data Encryption at rest**
Data At Rest Encryption (DARE) is the encryption of the data that is stored in the databases and is not moving through networks. Within Altris AI architecture, data at rest including offline backups are protected.

6 **End-user devices encryption.**
We suggest implementing it on the client's side to ensure that end-user devices – laptops for all employees, contractors who have access to data records (in particular software developers) are encrypted regardless of whether personal data is stored there or not. This will mitigate the risk of data breaches since everyone is providing services remotely and data is not stored onsite; laptops are taken to the public spaces and can be easily stolen and data will be compromised.

Important
Altris AI stores all patient's data in a separate DB. Data is encrypted and can not be accessed by anybody, except users of according account

ADDITIONAL DATA PROTECTION:

1 **Activity Logging**
All user activity logs and records are saved. Implemented to track the user behavior and identify suspicious activity as a precondition to possible data breach. So in case of potential breaches, unexpected activity or offensive actions from the employee's side, the Account Holder will be able to request logs for further actions.

2 **Data Dumps**
Up to Account Holder request Altris AI can provide data dump.

3 **Data deletion**
After data is deleted from the system in case of account deletion Altris AI will no longer be saving any client's data.

4 **Data Pseudonymization.**
Stored data in Altris system is completely pseudonymized. All data is divided in two databases: one with ids, the other one – with original records which are encrypted.