COVID-19 Data Tracker System Architecture (Monolith)

A. Monolith Components:

1. **Express.js Server:**
   - Handles incoming HTTP requests and routes.
   - Manages API endpoints for data extraction and visualization.
2. **Data Processing:**
   - Extracts COVID-19 data from the chosen API source.
   - Parses and processes data for storage and visualization.
3. **Data Storage (MySQL):**
   - Stores extracted data efficiently.
   - Provides querying capabilities for data retrieval.

B. Database Layer:

1. **MySQL Tables**
2. **Database Schema:**
   1. **us_daily_data Table:**
      - date (Primary Key)
      - states
      - total_cases
      - total_testing
      - hospitalized_currently
      - in_icu_currently
      - on_ventilator_currently
      - total_deaths
   2. **state_daily_data Table:**
      - date (Primary Key)
      - state
      - total_cases
      - total_testing
      - hospitalized_currently
      - in_icu_currently
      - on_ventilator_currently
      - total_deaths

D. Security Layer

To ensure the security of the COVID-19 Data Tracker system, the following measures are implemented:

- A proper authorization system is employed to control access to sensitive data and functionalities.

H. API Contracts

A. Data Extraction:

1. **National Data**
   a) **Endpoint:** '*/daily*'
   b) **Purpose:** Retrieve historic COVID-19 data for the entire US.
2. **Single-Day Data:**
   a) **Endpoint:** *'/daily/{date}'*
   b) **Purpose:** Retrieve COVID-19 data for a specific date in the US.
3. **Historic Data for a State:**
   a) **Endpoint:** *'/states/{state-code}/daily'*
   b) **Purpose:** Retrieve historic COVID-19 data for a specific state.
4. **Single-Day Data for a State:**
   a) **Endpoint:** *'/states/{state-code}/{date}'*
   b) **Purpose:** Retrieve COVID-19 data for a specific date and state.

*(The {date} will have the ISO format structure.)

I. Security Measures and Compliance

- All data transmission is secured using HTTPS (TLS/SSL) encryption to safeguard the integrity and privacy of the exchanged information.
- Comprehensive input validation and sanitation procedures are in place to mitigate the risk of injection attacks and other security vulnerabilities.
- A Centralized Error Handler is implemented to maintain security by handling and responding to errors gracefully.

J. Deployment Environments

The COVID-19 Data Tracker system will be deployed using the following environments and tools, each chosen for its specific benefits:

- **MySQL Database Deployment:** The MySQL database will be hosted on Azure's reliable and scalable platform, utilizing Azure Database for MySQL. This ensures high availability, scalability, and managed database services that are crucial for storing and managing COVID-19 data.

- **Application Deployment:** The application will be deployed on Heroku, a powerful cloud platform that simplifies the deployment and management of applications. The selected Docker image (**node:20.3.1-slim**) enhances security by offering a lightweight and well-maintained environment for running the application.