CSE 550 50/51 Group 2, Final Review
Carlos Cabrera
Adam Ma
Sam Kist
Cody “Turbo” Nichols
Griffin Myslow
Youssef Sheta

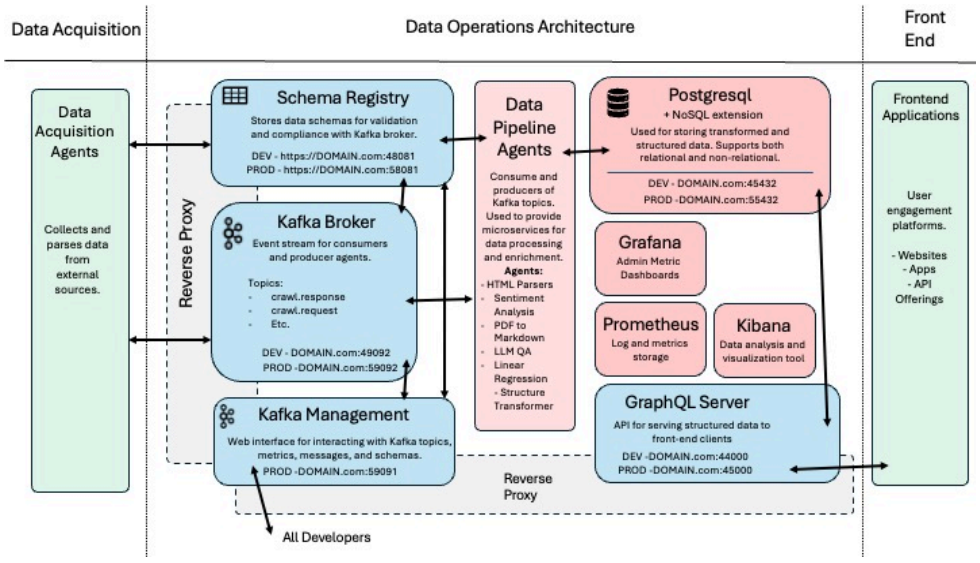
Define Objectives:
"Don't Bet On" (DBO) helps users avoid selecting underperforming NFL players by combining traditional performance metrics with **non-traditional data**, such as late-night activities, social media engagement, dating, lifestyle impacts, and more. These provide unique contextual explanations of how off-field factors influence player performance.

Reason for Problem Selection:
DBO addresses gaps in fantasy sports and betting platforms by integrating **non-traditional data** and allowing users to contribute their own knowledge to enhance player performance insights. This holistic approach, considering human and emotional factors, is important for users seeking a broader view.

An analysis of 18 companies (including sports betting, fantasy platforms, data providers, and media) revealed that most rely on traditional data like statistics, injury reports, and betting odds. Only 3 companies leveraged non-traditional data, such as RFID and AI technologies used by Zebra Sports and NFL Next Gen Stats for real-time on-field player data, and Unabated, which provided insights into real-time betting activities. Most of these services focused on passive consumption (e.g., player rankings, news) rather than user engagement. Only Sleeper and Unabated fostered user participation.

DBO aims to address both of these gaps—non-traditional data integration and user engagement—on a smaller scale.

Software Design:



Risk Matrix:

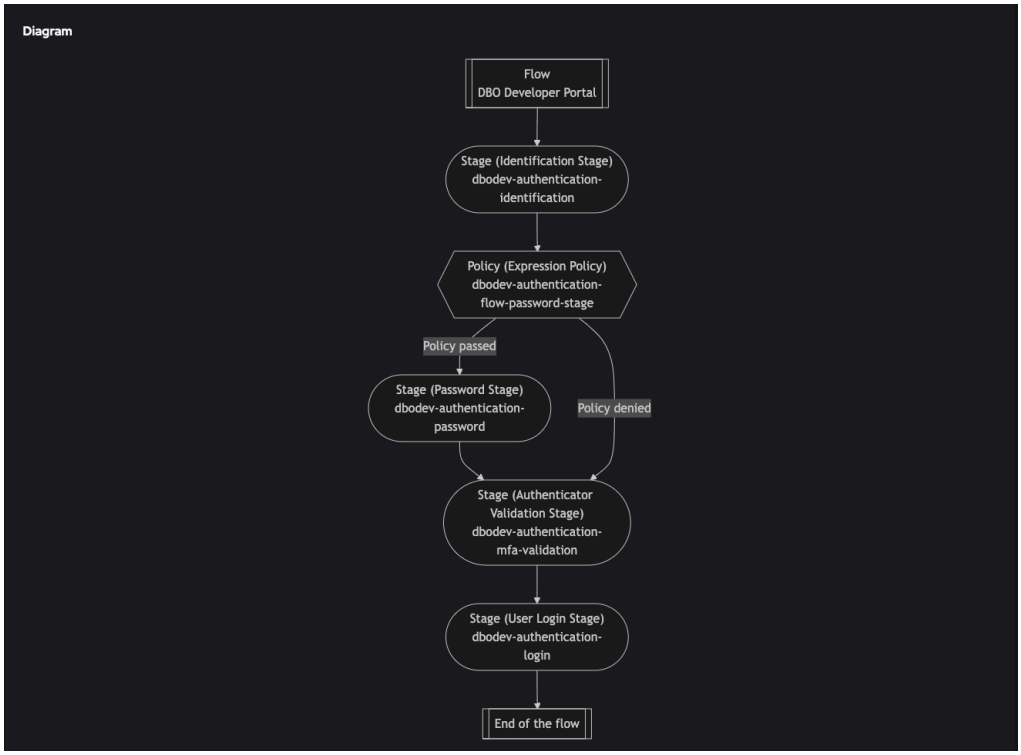
RISK MATRIX

RISK RATING KEY	LOW	MEDIUM	HIGH	EXTREME
	0 - ACCEPTABLE OK TO PROCEED	1 - ALARP as low as reasonably practicable TAKE MITIGATION EFFORTS	2- GENERALLY UNACCEPTABLE SEEK SUPPORT	3- INTOLERABLE PLACE EVENT ON HOLD

LIKELIHOOD ↓ / SEVERITY →	ACCEPTABLE LITTLE TO NO EFFECT ON EVENT	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	UNDESIRABLE SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	INTOLERABLE COULD RESULT IN DISASTER
IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW - 1 -	MEDIUM -4 -	MEDIUM - 6 -	HIGH - 10 -
POSSIBLE RISK WILL LIKELY OCCUR	LOW - 2 -	MEDIUM -5 -	HIGH - 8 -	EXTREME - 11 -
PROBABLE RISK WILL OCCUR	MEDIUM - 3 -	HIGH -7 -	HIGH - 9 -	EXTREME - 12 -

We chose a Behavioral design pattern as we split into three teams working on three different sections/objects of the project. We will then have to collaborate to have the objects/sections interact and talk to each other. This allows us to split the work evenly among four people

Our Authentication Process:



Example of API pull from SportsDataIO in Java:

```java
// Method to pretty print the JSON response
private static void prettyPrintJson(String jsonResponse) throws IOException {
    // Create an ObjectMapper instance
    ObjectMapper objectMapper = new ObjectMapper();

    // Parse the JSON into a JsonNode tree
    JsonNode rootNode = objectMapper.readTree(jsonResponse);

    // Pretty print the first 2 players (or fewer if not available)
    if (rootNode.isArray() && rootNode.size() > 0) {
        System.out.println("Pretty Printed JSON for First 2 Players:");
        for (int i = 0; i < Math.min(2, rootNode.size()); i++) {
            JsonNode player = rootNode.get(i);
            String prettyPlayerJson = objectMapper.writerWithDefaultPrettyPrinter().writeValueAsString(player);
            System.out.println("Player " + (i + 1) + ":");
            System.out.println(prettyPlayerJson);
            System.out.println("------------------------------");
        }
    } else {
        System.out.println("No players found.");
    }
}
```

Security:

Overall Security Model
Infrastructure and services are designed with security and data regulation in the mind from the start.

Use LXC for internal services with no access to internet, and minimal remote attack service
- Use VM for isolation
    - VM for each group of isolated services
    - Podman rootless containers exposed services
    - go-audit rules for detecting threats
    - opentelemetry agent collector and ship to prometheus or jagger (or allow scrape)

<u>OpenID Connect Authentication and Authorization</u>
Applications, infrastructure, and machine-to-machine services are secured via integration with Authentik. This framework helps provide AUTHENTICATION and AUTHORIZATION to use services via providers such as LDAP, RADIUS, PROXY BASIC AUTH, and our most used standard OAUTH2.

OAUTH2 allows us to use temperate JSON Web Tokens (JWT) to allow authenticated users very specific permissions (AUTHORIZATION) for each application. Since these tokens are short-lived, any compromise of a user's token would only be valid for 12 minutes before the user would need to reauthenticate.

Scalability and Performance:
- Containers and microservices infrastructure and architecture
- Proxmox is used at the virtual machine and container management and orchestrator
- Individual apps are deployed in containers across infrastructure, apps that require scale simply deploy another container
- Apps that have micro processes use Kubernetes to manage the application state

- This solution allows us to scale horizontally and or vertically, using our own computers/servers or being able to interface with cloud providers

Design and explain the software with scalability and performance in mind to handle future growth and user demands given economical and time constraints.

Legal and Compliance Considerations:

- Need to ensure information is gathered from legal and credible sources
- Need to reduce spread of incorrect information
- Libel and Slander (legal team??)
- Respect Robots.txt and Terms of Service