level™

Technical overview

ELITE COMPANY

Contents

1. Introduction

Level is a scalable, rules-driven, cognitive decisioning platform that can be used to add extra functionality to existing software and systems, or to develop novel applications that function independently. It is system-agnostic, meaning it can integrate with all software and systems, regardless of vendor or physical location.

Applications that are developed using the Level platform are mobile-friendly and web-based, meaning, if needed, they can be accessed 24/7 from any device and any location. Applications are designed to be user-friendly, accessible and intuitive, so users need very little training. The whole organisation can begin using the new applications from day one.

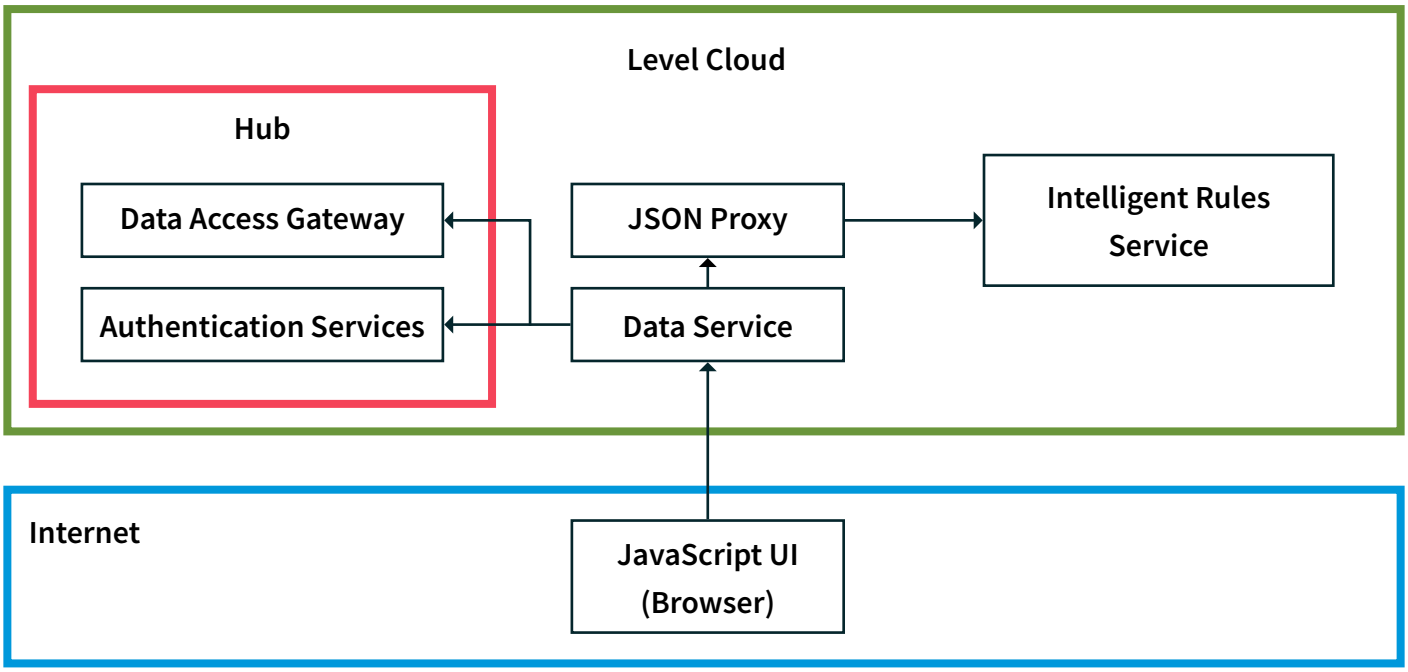
This document describes the high-level design of the Level platform and is intended to give an overview of the technologies used. For more information, contact hello@level.global.

2. Components

The platform consists of two main parts:

- A Java web application – the controller that passes data between the Data Access Gateway, the Intelligent Rules Service and the UI
- An HTML5/JavaScript mobile-optimised front-end

The structure of these components are as follows:



Each of these components has been specifically chosen to ensure that the Level platform is system and vendor-agnostic, meaning it can integrate with any and all software and systems that may already be in use. A brief description of each of the components is provided below.

2.1. Data Service

In MVC terms, the Intelligent Rules Service is the model, the JavaScript client is the view, and Data Service is the controller. The Data Service is the communication centre of the platform and is the component through which all others communicate.

2.2. JavaScript UI

The front-end is really its own application altogether. It has been developed using AngularJS, a JavaScript framework for building complex applications that run in the browser. This approach limits the interaction with the server by loading resources only as needed, rather than on every user interaction as in a traditional Java web application (e.g. JSP). This application's primary purpose is to allow users to interact with the Intelligent Rules Service.

2.3. JSON Proxy

The JSON Proxy translates the Intelligent Rules Service's SOAP interface to a REST-like JSON interface. This allows the JavaScript client to consume messages received by the Intelligent Rules Service directly and efficiently, without the need for further translation.

2.4. Hub Authentication Services

The Hub Authentication Services application authenticates and authorises the user on the system.

2.5. Data Access Gateway

The Data Access Gateway is the source of all user-related data that passes through the Data Service. It comprises a set of REST services that give secure access to relational database storage, together with programs built to convert between file data and relational data. It is capable of forming complex data structures, and the way in which those structures are represented is highly configurable.

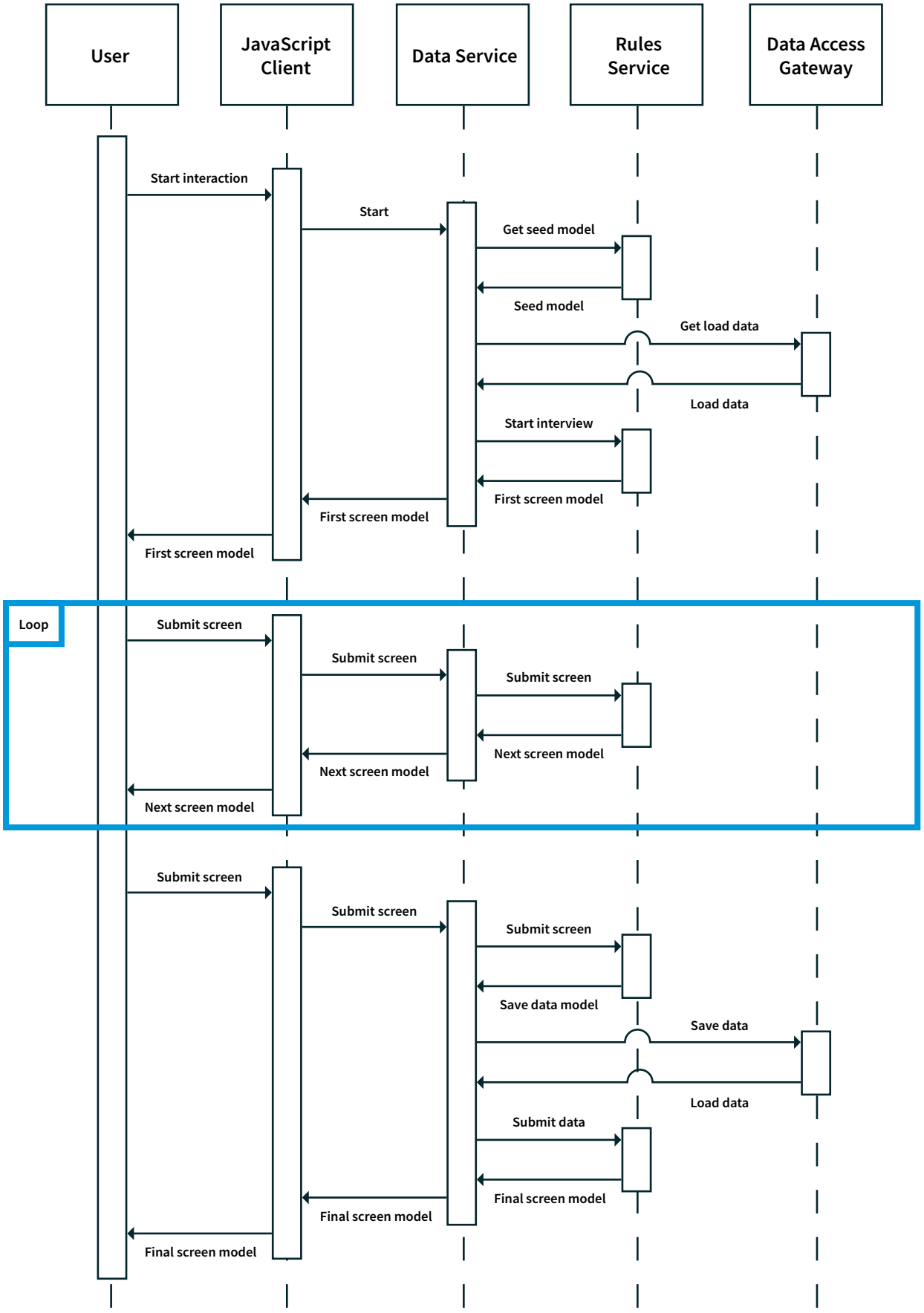
2.6. Intelligent Rules Service

The Intelligent Rules Service (IRS) is the cognitive element of the platform. Human thinking and decision-making processes are configured in the form of rules and each collection of related rules is called a Rulebase. When Rulebases are ready to be used, they are deployed to the IRS, and the user is then able to interact with the service via the UI as if they were interacting with a human expert.

The IRS exposes access to the Rulebase via a web service, and the user interacts with it through an iterative screen-by-screen process. The user answers a variety of questions on each consecutive screen, and the IRS tailors the experience to that user based on their responses. Once enough data has been gathered, or the Rulebase has reached its desired conclusion, the process ends and the appropriate next step is initiated.

One of the advantages of this process is that the user is only presented with questions that are relevant to them, and they are never required to provide data that already exists in the system in some form. In this manner, the Level platform ensures that the user takes the simplest, most efficient route to the desired conclusion, removing opportunities for error or confusion.

2.7. User Interaction Sequence



3. Access Control

3.1. Web Security

3.1.1. Full Site HTTPS

By default, all connections from the user to the site are encrypted using HTTPS.

3.1.2. HTTP Strict Transport Security (HSTS)

HSTS is a setting on a website which signals to the browser that this website will only ever use HTTPS for all of its connections. Attacks exist which attempt to trick the browser into communicating over an insecure channel, allowing for eavesdropping. With HSTS enabled, the browser enforces HTTPS for all connections.

3.1.3. Secure Cookie

The platform will ensure that its session cookie is only ever transported over HTTPS by setting the HTTPS flag on the cookie itself. Also, because the cookie will be issued by the platform and not used elsewhere, the cookie's domain setting will be as specific as possible.

3.1.4. Content Security Policy (CSP)

Level has a strict content security policy that helps protect users from many known vulnerabilities. Like HSTS, CSP is a way of configuring the website that signals to the browser what kind of activity to expect and what activity to block.

4. Security Assumptions

By default, the platform employs the latest web security standards used by any major website (e.g. Facebook or Gmail). However, this is not without risk, and much of the security of the system as a whole is determined by how much functionality is exposed and the precautions individuals take to protect their accounts.

Aside from what is offered as standard, other measures can be taken to increase the security of the system including mobile VPNs, device-specific registration, company policies for device passwords and encryption, policies for lost devices, and so on.

Level will work with the client to ensure that the level of security is appropriate to the level of risk.

5. Device Compatibility

Due to the wide range of mobile operating systems and incompatibility between them, the UI conforms to web standards. Applications created using the Level platform are mobile-friendly, app-like websites, which avoid the need to provide OS-specific applications. The UI was designed to be usable on any modern web browser platform including: Internet Explorer 11+, Edge, Chrome, Safari, Firefox, Android 4.2+ and iOS 8+.

5.1. Mobile device loss

If a user's mobile device is lost or stolen, it should be treated no differently than the loss of a laptop or PC. If the user has not saved their credentials in the web browser, there is no security risk. If the credentials were saved, but the device is encrypted and has a strong OS password, then there is a very low security risk, but the user should change their password as a precaution. If the user saved their credentials and did not secure their device, then the user MUST change their password immediately.

level™

Get in touch

If you'd like more information we'd love to hear from you

hello@level.global
+44 1463 710816

ELITE COMPANY