COLLEGE CODE: 9504

COLLEGE NAME: Dr.G.U.POPE COLLEGE OF ENGINEERING

DEPARTMENT: CSE

STUDENT NM-ID: 4954207CF1118329552443D44B54854B

ROLL NO. : 45

DATE: 15/09/2025

COMPLETED THE PHASE II
"INTERACTIVE FORM VALIDATION"

SUBMITTED BY,

NAME: SWETHA R

MOBILE NO. : 7708604467

SOLUTION DESIGN AND UNDERSTANDING

TECH STACK SELECTION

For the Interactive Form Validation project, an effective and modern tech stack selection covers frontend, backend, database, and validation libraries/tools to provide seamless, secure, and performant validation. The following tech stack is recommended based on best practices for building interactive validated forms:

Frontend

- React.js — Popular, component-driven JavaScript library for building dynamic user interfaces and reactive forms.
- React Hook Form or Formik — Libraries specialized in managing forms and validations efficiently in React with minimal re-renders.
- Yup — Schema validation library often paired with React Hook Form or Formik for declarative validation rules.
- CSS/SCSS or UI frameworks like Tailwind CSS or Material UI for styling forms responsively and accessibly.

Backend

- Node.js with Express.js — Lightweight backend platform and framework for handling API requests and implementing server-side validation.
- express-validator or Joi — Middleware/libraries for defining robust validation and sanitization rules on incoming data.
- REST API endpoints to communicate validation results and process form submissions securely.

Database

- MongoDB with Mongoose ODM — NoSQL database with flexible schema support. Mongoose allows schema-based validation at the database layer for added data integrity.

Additional Tools & Practices

- ESLint/Prettier for consistent coding style and early error detection.
- Testing frameworks like Jest for unit testing validation logic.
- Accessibility tools to ensure ARIA-compliant validation messaging.
- Use HTTPS/TLS to secure data in transit.

- Employ security best practices such as input sanitization and rate limiting to protect backend from malicious input.

Summary Table

Layer	**Technology/Library**	**Purpose**
Frontend	React.js	Dynamic UI, controlled inputs
Frontend	React Hook Form / Formik	Manage form state and validations
Frontend	Yup	Declarative schema validation
Styling	Tailwind CSS / Material UI	Responsive, accessible form styling
Backend	Node.js + Express.js	Server-side API and validation logic
Backend	express-validator / Joi	Server-side input validation and sanitization
Database	MongoDB + Mongoose	Data storage with schema constraints
Testing	Jest	Unit and integration tests

This tech stack enables building user-friendly, real-time validated forms with robust security and data integrity, supporting modern development workflows and performance optimizations for a better user experience and maintainability.

UI STRUCTURE/ API SCHEME DESIGN

UI Structure for Interactive Form Validation

- Form Layout
    - Use a single-column vertical layout for ease of use and visual scanning.
    - Place labels above input fields to support natural reading flow and reduce eye movement.

    - Clearly mark required fields with an asterisk (*) or "(required)".
    - Group related fields under sub-headers or sections to reduce cognitive load.
    - Use ample white space and subtle borders for input field containers.
- Input Fields and Validation Feedback
    - Provide real-time inline validation that triggers on field blur or after a set number of characters.
    - Show error messages immediately adjacent to the field in red text with a clear icon.
    - Use non-technical, actionable, and concise error messages helping users to fix issues quickly.
    - Show success feedback using green checkmarks or subtle messages next to valid inputs.
    - Provide helper text or tooltips for fields that require explanation (e.g., password requirements).
- Form Interaction
    - Disable the submit button until all validations pass successfully.
    - Use progressive disclosure for long forms (e.g., multi-step form UI) if applicable.
    - Support keyboard navigation and focus states for accessibility.
    - Ensure error/success states are announced by screen readers (e.g., using ARIA live regions).
- Responsive Design
    - Inputs and validation feedback adapt for mobile and tablet screen sizes.
    - Use touch-friendly input sizes and padding.

API Schema Design

- Endpoint: /api/forms/{form_id}/validate
    - Method: POST
    - Request Body: JSON object with key-value pairs for each form field.

json

```
{
  "email": "user@example.com",
  "password": "P@ssw0rd!",
  "username": "user123"
}
```

        - Response Body:

```
json
{
  "is_valid": false,
  "validation_messages": {
    "email": "Please enter a valid email address.",
    "password": "Password must contain at least 8 characters."
  },
  "field_status": {
    "email": "error",
    "password": "error",
    "username": "valid"
  }
}
```

- Endpoint: /api/forms/{form_id}/submit
    - Method: POST
    - Request Body: JSON object with all validated form data.
    - Response Body:

```
json
{
  "success": true,
  "message": "Form submitted successfully."
}
```

- Validation Logic
    - Basic data-type and format validation (e.g., email regex, password strength).
    - Business rules validation (e.g., unique username).
    - Return detailed, field-specific error messages for client display.
    - Support partial validations for real-time feedback as users fill fields.

This structure and schema design ensure a seamless, accessible, and efficient user experience while maintaining robust backend validation and clear communication between frontend and backend

DATA HANDLING APPROACH

- Real-time Data Validation & Feedback:
    - Immediately validate user inputs on the client side to catch errors early.
    - Implement server-side validation for data integrity and security.
    - Provide clear, actionable error messages to guide users effectively.
- Data Quality Management:
    - Validate data formats (e.g., email, phone) and enforce required fields.
    - Sanitize inputs to prevent injection attacks and malformed data.
    - Use normalization and standardization for consistent data (e.g., date formats).
- Data Lifecycle & Storage:
    - Store data securely in an encrypted database with controlled access.
    - Follow data retention policies to delete or archive old/unused data safely.
    - Backup data regularly to prevent loss and enable recovery.
- Privacy & Compliance:
    - Collect only necessary data aligned with privacy regulations (GDPR, CCPA).
    - Ensure transparent privacy notices and obtain user consent where needed.
    - Implement role-based access control limiting data exposure to authorized personnel.
- Integration & Workflow:
    - Integrate smoothly with third-party services (CRM, email marketing) securely.
    - Automate data preprocessing where applicable for efficiency and accuracy.
    - Maintain logs for data submissions and access for audit purposes.
- Usability Enhancements:
    - Pre-fill known user data to improve experience and reduce errors.
    - Use conditional logic to show/hide fields dynamically based on data context.
    - Provide clear instructions and character limits to help users provide valid inputs.

This approach ensures the form data is accurately validated, securely stored, privacy-compliant, and managed throughout its lifecycle, while supporting an optimal user experience and backend reliability.

COMPONENT/MODULE DIAGRAM DESCRIPTION

1. User Interface (UI) Module
    - Responsible for rendering the form fields, labels, validation messages, and submit button.
    - Manages real-time inline validation feedback (on input change/blur events).
    - Communicates with the Validation Module and API Service Module.
    - Handles user interactions, error/success display, and accessibility features.
2. Client-side Validation Module
    - Implements immediate validation rules using JavaScript or React form libraries.
    - Validates input formats, required fields, pattern matching, password strength.
    - Provides quick feedback without waiting for server responses.
    - Passes data to API Service Module for server-side validation when needed.
3. API Service Module
    - Handles communication between UI and backend server via RESTful endpoints.
    - Sends form data for validation (/validate) and form submission (/submit).
    - Processes server validation responses and updates UI accordingly.
4. Server-side Validation Module
    - Resides on backend (Node.js/Express).
    - Re-validates inputs for security, business rules, and data integrity.
    - Returns structured validation errors or success confirmation to API Service Module.
5. Data Storage Module
    - Database layer (e.g., MongoDB) storing validated form data securely.
    - Performs data sanitization and enforces schema rules for stored records.
6. Security and Logging Module
    - Oversees input sanitization, rate limiting, and authorization.
    - Logs validation attempts, errors, and submits for auditing and debugging.

Component Interaction Flow

- User inputs data → UI Module triggers Client-side Validation.
- Client-side Validation passes if OK → API Service Module sends data to server /validate.

- Server processes data → Server-side Validation returns errors or success.
- API Service updates UI with validation status.
- On complete valid form → UI triggers API Service /submit, server stores data.
- Security Module monitors all interactions and logs events.

This modular architecture provides clear separation of concerns for maintainability, security, and scalability while ensuring real-time interactive validation and a smooth user experience.

BASIC FLOW DIAGRAM: INTERACTIVE FORM VALIDATION

1. User Opens Form
    - Form fields are displayed on UI with initial empty state.
    - Submit button is disabled initially.
2. User Inputs Data
    - User types into form fields one by one.
3. Client-side Real-time Validation
    - On each field input or blur event:
        - Validate input format (e.g., email regex, required fields).
        - Show inline error message if invalid.
        - Mark field success if valid (e.g., green check).
    - Disable submit button if any field invalid.
4. Server-side Validation (On-demand)
    - When needed (e.g., blur event or form submit):
        - Send field data or full form data to /validate API endpoint.
        - Server returns validation results with error messages if any.
        - UI updates field statuses accordingly.
5. User Corrects Errors
    - User edits invalid fields based on feedback.
    - Steps 3 and 4 repeat until no validation errors.
6. Form Submit
    - Submit button enabled only if all validations pass.
    - On submit click, send form data to /submit API.

- Server processes submission, stores data, returns success or failure message.

7. Display Final Status
    - Show success confirmation message on success.
    - If submit fails (e.g., server error), display appropriate error message.

This flow ensures smooth, real-time interactive validation with robust server-side checks, enhancing user experience and data integrity.