App Privacy Scout: A Browser-Based Tool for Privacy Assessment

PHASE 1 PROJECT REPORT

Submitted by

Lakshmi Vignesh S	**310622149028**
Sachin K	**310622149039**

in partial fulfilment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING(CYBER SECURITY)

EASWARI ENGINEERING COLLEGE, CHENNAI

(Autonomous Institution)

affiliated to

ANNA UNIVERSITY: CHENNAI – 600025

September 2025

BONAFIDE CERTIFICATE

Certified that this project report **"App Privacy Scout: A Browser-Based Tool for Privacy Assessment"** is the Bonafide work of **Lakshmi Vignesh S (310622149028), Sachin K (310622149039)** who carried out the project work under my supervision.

SIGNATURE

Dr.V.BALAJI

HEAD OF THE DEPARTMENT
Department of Computer Science and Engineering (Cyber Security), Easwari Engineering College, Ramapuram, Chennai-89.

SIGNATURE

Dr.V.BALAJI
HEAD OF THE DEPARTMENT
Department of Computer Science and Engineering (Cyber Security), Easwari Engineering College, Ramapuram, Chennai-89.

CERTIFICATE OF EVALUATION

College Name: Easwari engineering college

Branch & Semester: Computer Science and Engineering (Cyber Security) & VII

S. No	Name of the Students	Title of the project	Name of the supervisor with designation
1.	Lakshmi Vignesh S (310622149028)	APP Privacy Scout: A Browser-Based Tool for Privacy Assessment	Dr. V. BALAJI (HOD-CSE(CS))
2.	Sachin K (310622149039)		

The report of the PHASE I project work submitted by the above students in partial fulfilment for the award of Bachelor of Engineering Degree in Computer Science and Engineering of Anna University were evaluated and confirmed to be a report of the work done by the above students.

The viva voice examination of the project was held on_____.

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We hereby place our deep sense of gratitude to our beloved Founder Chairman of the institution, **Dr. T. R. Pachamuthu, B.Sc., M.I.E.**, for providing us with the requisite infrastructure throughout the course. We would also like to express our gratitude towards our Chairman **Dr. R. Shivakumar, M.D., Ph.D.** for giving the necessary facilities.

We convey our sincere thanks to **Dr. P. Deiva Sundari, M.E., Ph.D.** Principal Easwari Engineering College, for her encouragement and support. We extend our hearty thanks to **Dr. V. Balaji, M.E, Ph.D.**, Head of the department of Cyber Security for his suggestions, support, and encouragement towards the completion of the project with perfection.

We would like to express our gratitude to our Project Coordinator **Mrs. M. Bhuvaneswari, M.E,** Assistant Professor, Department of Computer Science and Engineering (Cyber Security), Easwari Engineering College, for her constant support and encouragement.

We would also like to express our gratitude to our guide **Dr. V. Balaji, M.E, Ph.D.**, Head of the department, Department of Computer Science and Engineering (Cyber Security), Easwari Engineering College, for his constant support and encouragement.

Finally, we whole heartedly thank all the faculty members of the Department of Computer Science and Engineering (Cyber Security) for warm cooperation and encouragement.

ABSTRACT

In today's digital world, privacy concerns are escalating as users often unknowingly grant excessive permissions or accept vague privacy policies when installing apps. **App Privacy Scout** is a browser-based tool designed to empower non-technical users to understand the privacy implications of mobile and web applications. By analyzing app permissions and privacy policies locally in the browser, it provides a color-coded risk score (Red/Yellow/Green) and actionable recommendations, such as disabling risky permissions or choosing safer app alternatives. The tool also offers visual, multilingual privacy education to bridge the cybersecurity knowledge gap, ensuring user safety and awareness without requiring specialized software.

The system is developed as a web-based platform using JavaScript and Tailwind CSS, offering users the ability to upload privacy policies or paste URLs for analysis. Local processing ensures no data leaves the device, while features like drag-and-drop input, risk scoring, and educational guides enhance usability. This approach not only guarantees privacy assessment but also promotes digital awareness, making it resilient against misinformed app usage. Unlike existing tools, this project integrates analysis, scoring, recommendations, and education into a single end-to-end privacy solution. The proposed system demonstrates how combining policy scanning with user- friendly interfaces can create a reliable method for protecting personal data in real-world applications.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABB	FULL FORM
PWA	Progressive Web Application
EEG	Regular Expression
BLOB	Binary Large Object
HTTPS	Hypertext Transfer Protocol Secure
NLP	Natural Language Processing

CHAPTER 1

INTRODUCTION

1.1 GENERAL

The digital age has intensified privacy concerns, with 2025 statistics revealing that 40% of individuals worry about how companies handle their personal data, and data breaches cost an average of $4.45 million globally, down 9% from 2024. Of these, 22% involve stolen credentials, with 88% occurring in basic web application attacks. App Privacy Scout, de- veloped under the Tamil Nadu State Council for Science and Technology (TNSCST) Student Project Scheme 2025-2026, is a browser-based tool designed to empower non- technical users. It analyzes app permissions and privacy policies locally, offering a color- coded risk score (Red/Yellow/Green) and actionable advice, such as disabling risky per- missions. The tool also includes visual, multilingual education to enhance cybersecurity awareness, making it accessible without specialized software.

1.2 PROBLEM DESCRIPTION

Non-technical users struggle to evaluate app privacy due to complex policies and permis- sion systems. Existing solutions, such as AppCensus and PrivacyGrade, often rely on server-side processing, risking data leaks, and lack user-friendly education. This leads to unintended data exposure, with annual privacy breaches affecting millions and eroding trust. The absence of localized, accessible tools exacerbates the issue, particularly in regions with low digital literacy.

1.3 OBJECTIVE

- Develop a browser-based platform for analyzing app privacy policies and permissions, compatible with major browsers like Chrome and Firefox.

- Assign an intuitive color-coded privacy risk score (Red/Yellow/Green) based on criteria such as permission count, data sensitivity, and policy clarity.

- Provide actionable recommendations, including disabling permissions or suggesting privacy-focused alternatives, tailored to user needs.

1.4 EXISTING SYSTEM

Tools like AppCensus and PrivacyGrade depend on server-side analysis, posing privacy risks and requiring internet connectivity. They often lack multilingual support and fail to cater to non-technical users, focusing instead on expert audiences. A 2024 study high- lighted that 60% of privacy tools suffer from usability issues, and no college or institution has developed a similar locally processed, education-integrated PWA.

1.5 PROPOSED SYSTEM

App Privacy Scout is a Progressive Web App (PWA) that conducts local analysis, en- suring zero data leakage. It integrates permission scanning, policy analysis, risk scoring, personalized recommendations, and multilingual education. Unlike existing systems, it prioritizes usability for non-technical users and supports offiine functionality, addressing gaps in accessibility and privacy.

1.6 ORGANIZATION REPORT

The Privacy Risk Assessment Progressive Web App (PWA) is organized into several chapters, detailing its development and impact:

- **Chapter 1: Introduction** Introduces the PWA's objectives and scope for secure,

offline privacy assessments. Highlights its significance for non-technical users via local JavaScript processing.

- **Chapter 2: Literature Survey** Reviews existing privacy tools, identifying limitations in accessibility and privacy. Motivates the need for a beginner-friendly, responsive system using Tailwind CSS.
- **Chapter 3: System Design** Describes the architecture, including UserInputHandler, Analyzer, and other modules. Details the frontend, local JSON database, and data flow for seamless operation.
- **Chapter 4: Module Descriptions** Explains input handling, privacy analysis, scoring, recommendations, and education. Emphasizes offline functionality and cross-device compatibility for user ease.
- **Chapter 5: Conclusion and Future Work** Summarizes findings and outlines a timeline for future enhancements. Proposes expanded AI integration and user engagement for greater impact.

CHAPTER 2 LITERATURE

SURVEY

EXISTING RESEARCH

1. **Traditional Privacy Awareness Platforms**

   Several mobile and web-based platforms provide general security tips, app reviews, or static permission checkers. While effective in raising awareness, these tools often rely on user initiative and do not adapt content based on the user's technical expertise or learning needs.

2. **Permission Analysis Tools**

   Research has examined automated analysis of mobile app permissions to flag potentially intrusive behaviors. However, many of these systems are either integrated into security software or require installation of specialized applications, making them less accessible to non-technical users.

3. **Policy Transparency Tools**

   Some projects have attempted to summarize app privacy policies using natural language processing (NLP). While promising, such tools typically work in isolation and lack actionable recommendations for end-users on how to mitigate identified risks.

4. **Cybersecurity Education Platforms**

   Gamified and visual learning platforms have been used to raise cybersecurity awareness. Although beneficial in improving engagement, most lack integration with real-time app analysis and do not provide personalized recommendations based on the user's app.

EXISTING SYSTEMS

Current privacy and permission-checking systems mainly include:

- **Permission scanners:** Highlight which permissions an app requests but often fail to explain risks in user-friendly language.
- **Policy summarizers:** Provide shortened versions of privacy policies but do not connect findings to actionable steps.
- **Antivirus or mobile security apps:** Offer broader protection but require installation, technical knowledge, or paid subscriptions.

Limitations of existing systems include:

- Lack of real-time, browser-based privacy analysis without software installation.
- Limited focus on non-technical users, leaving a gap in accessibility and usability.
- Minimal integration of visual or multilingual privacy education.
- Few actionable recommendations beyond generic warnings.

Research Gaps

From the above studies, several gaps are identified:

- Absence of lightweight, browser-based privacy tools requiring no installation.
- Limited accessibility for non-technical or multilingual audiences.
- Lack of integrated educational content to improve long-term privacy awareness.

- Minimal actionable guidance for users to reduce risks (e.g., disabling permissions or choosing safer alternatives).

Proposed Contribution

The proposed **App Privacy Scout** aims to bridge these gaps by:

- Providing a **browser-based tool** that performs all analysis locally, eliminating the need for external installations or server dependencies.
- Analyzing **app permissions and privacy policies** to generate a **color-coded risk score (Red/Yellow/Green)**.
- Offering **actionable recommendations**, such as disabling risky permissions or selecting safer app alternatives.
- Delivering **visual, multilingual privacy education** to raise awareness among diverse user groups.
- Ensuring **user safety and privacy** by conducting all analysis locally, without storing or transmitting personal data.

This approach combines **real-time privacy analysis** with **accessible education**, creating a comprehensive platform that empowers non-technical users to make informed decisions and improve their digital safety

CHAPTER 3

SYSTEM DESIGN

3.1 GENERAL

The system is a Progressive Web App (PWA) designed for local JavaScript processing, ensuring privacy and offline access. Tailwind CSS delivers a responsive, user-friendly interface tailored for non-technical users. It supports seamless updates and cross-device compatibility, empowering users with an intuitive experience without requiring constant internet connectivity.

3.2 PROPOSED SYSTEM

The proposed system is a Progressive Web App (PWA) designed for local JavaScript processing, ensuring user privacy and offline functionality. It utilizes Tailwind CSS to create a responsive, intuitive interface tailored for non-technical users, supporting seamless updates and cross-device compatibility. The process begins with user input (file upload or URL), followed by local analysis, risk scoring, recommendation generation, and educational output, delivering clear, actionable insights in a secure, efficient manner.

3.2.1 SYSTEM FLOW DIAGRAM

The process begins with user input (file upload or URL), followed by local analysis, risk scoring, recommendation generation, and educational output.

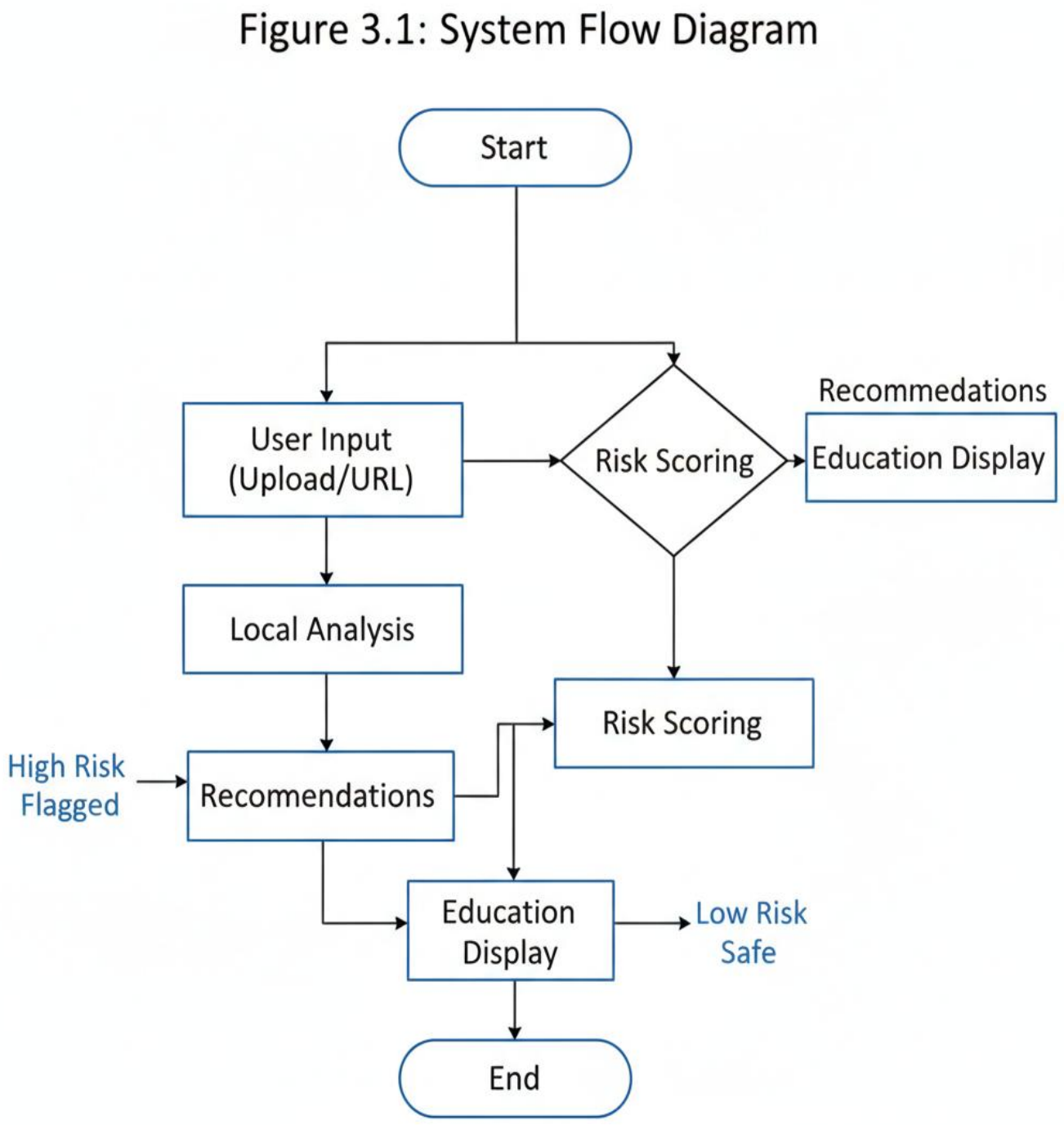

Figure 3.1. Block diagram of proposed system

3.2.2 ARCHITECTURE DIAGRAM

The architecture consists of a frontend built with Tailwind CSS for a responsive, user-friendly interface, core modules (Analyzer, Scorer, Recommender) for local JavaScript processing, and a local JSON database for efficient data storage. It ensures privacy, offline functionality, and seamless performance across devices. The system processes user inputs securely, generating risk scores, recommendations, and educational outputs tailored for non-technical users.

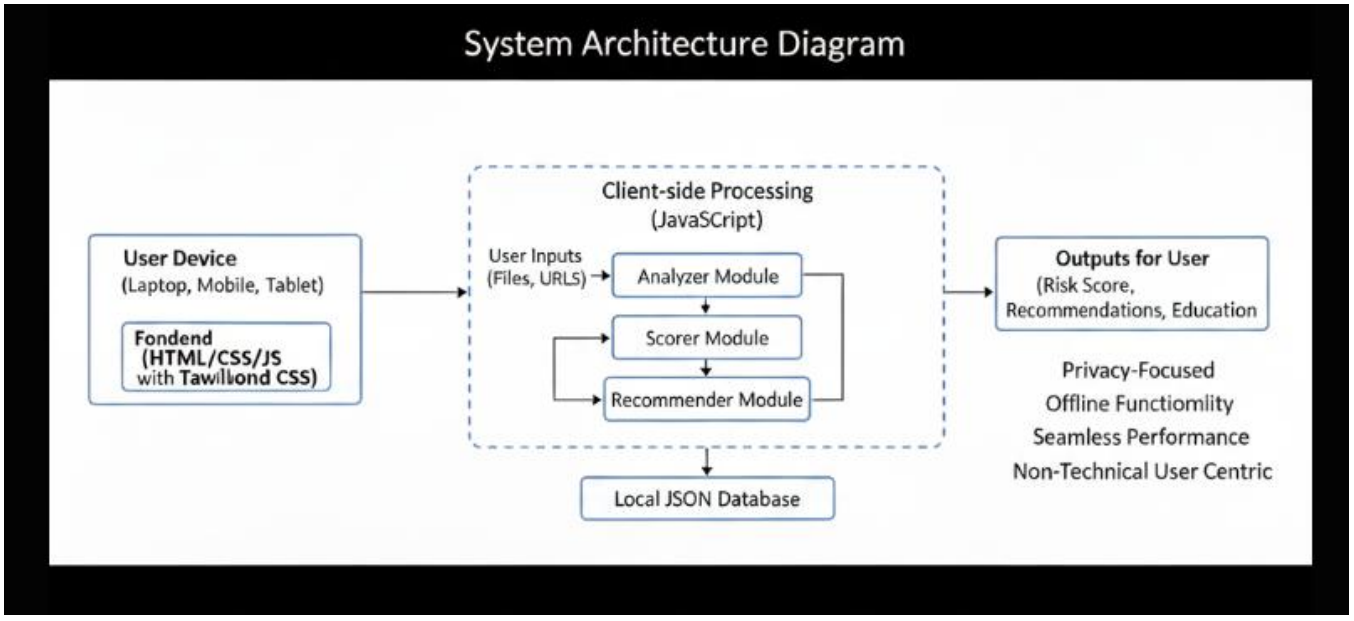

Figure 3.2. Architecture diagram of the proposed system

Figure 3.2. Architecture diagram of the proposed system

3.2.3 USE-CASE DIAGRAM

The system involves two primary actors: the User and the System, with key use cases including Upload File, Analyze Privacy, View Score, Get Recommendations, and Access Education. Built as a Progressive Web App (PWA) with local JavaScript processing, it ensures privacy and offline access. The Tailwind CSS frontend delivers a responsive, intuitive interface, while core modules (Analyzer, Scorer, Recommender) and a local JSON database process inputs to provide risk scores, tailored recommendations, and educational content for non-technical users.including thenecessary functional requirements and their anticipated behaviors.including thenecessary functional requirements and their anticipated behaviors.

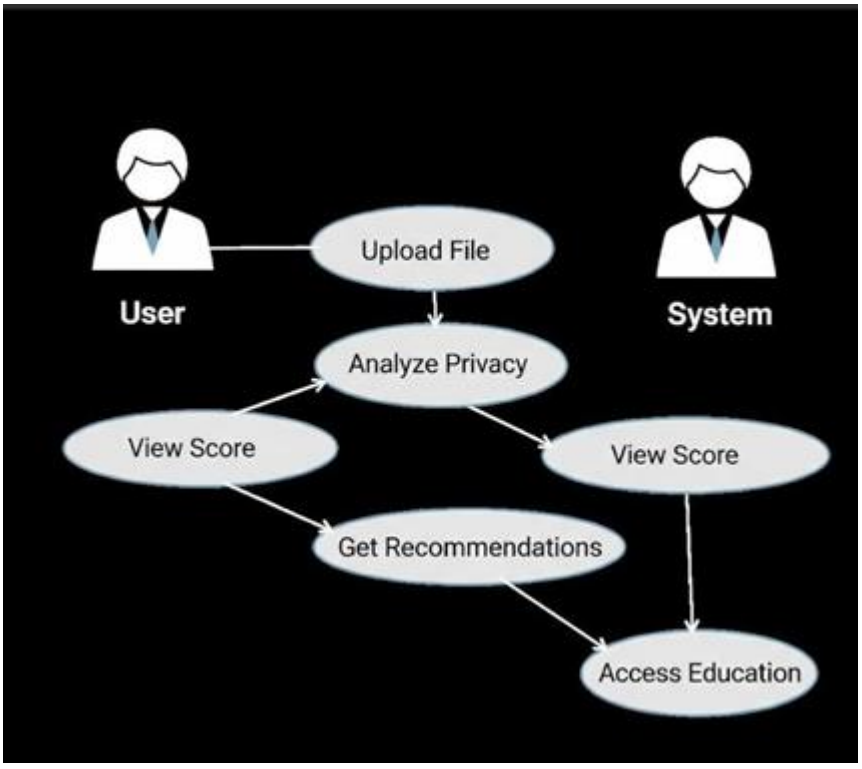

Figure 3.3. Use Case diagram of the proposed system.

3.2.4 ACTIVITY DIAGRAM

The activity flow: Start ---*t* Input Handling ---*t* Scan Keywords ---*t* Calculate Score ---*t*

Generate Recommendations ---*t* Display Education ---*t* End.

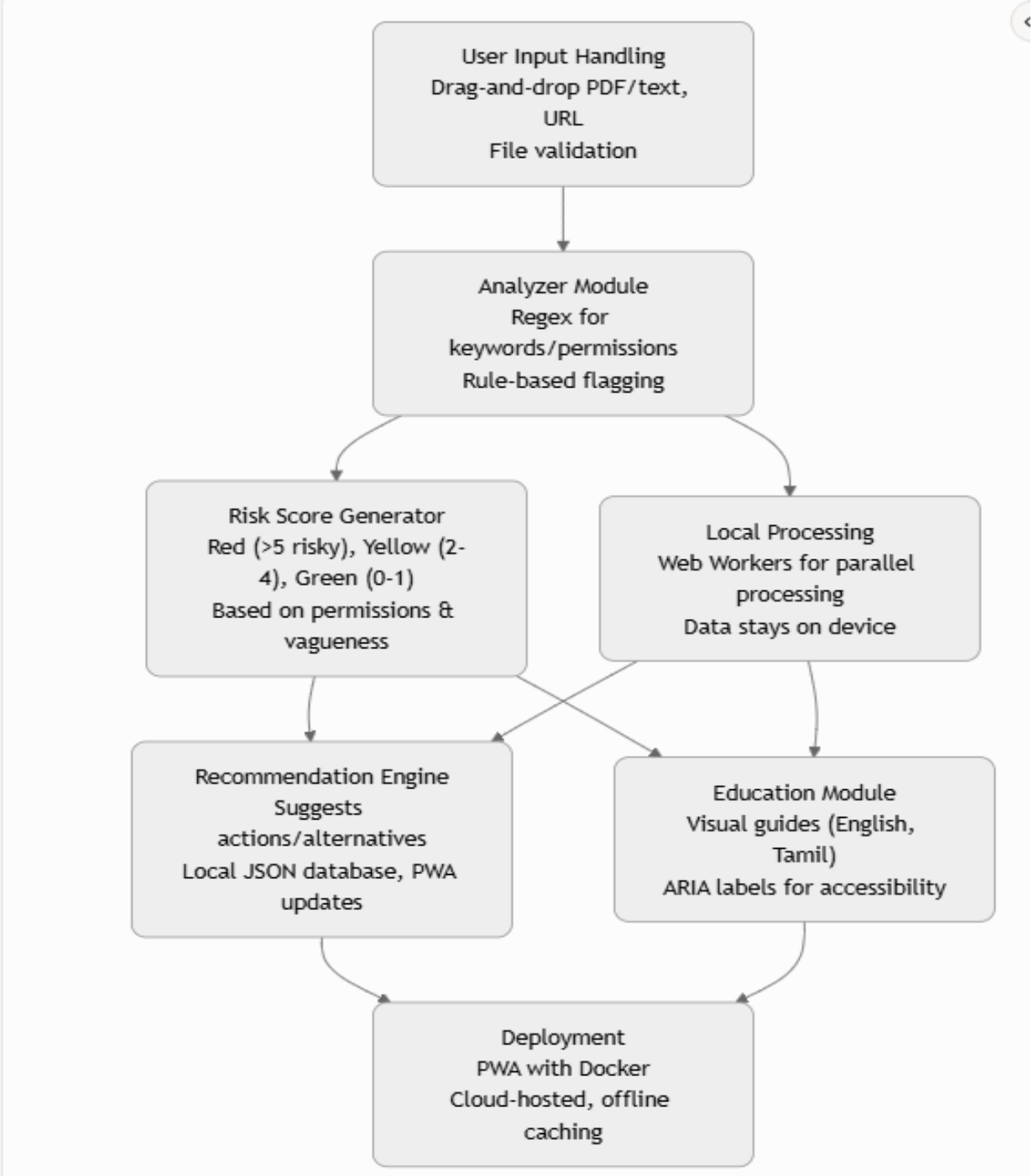

Figure 3.4. Activity diagram of the proposed system

3.2.4 CLASS DIAGRAM

The system architecture includes key classes: UserInputHandler, Analyzer, RiskScorer, Recommender, and Educator, interconnected through defined data flow relationships. Implemented as a Progressive Web App (PWA) with local JavaScript processing, it ensures privacy and offline functionality, using Tailwind CSS for a responsive, non-technical user-friendly interface. UserInputHandler processes file uploads or URLs, feeding data to the Analyzer for privacy assessment, RiskScorer for generating scores, Recommender for tailored suggestions, and Educator for delivering accessible educational content, all stored efficiently in a local JSON database.

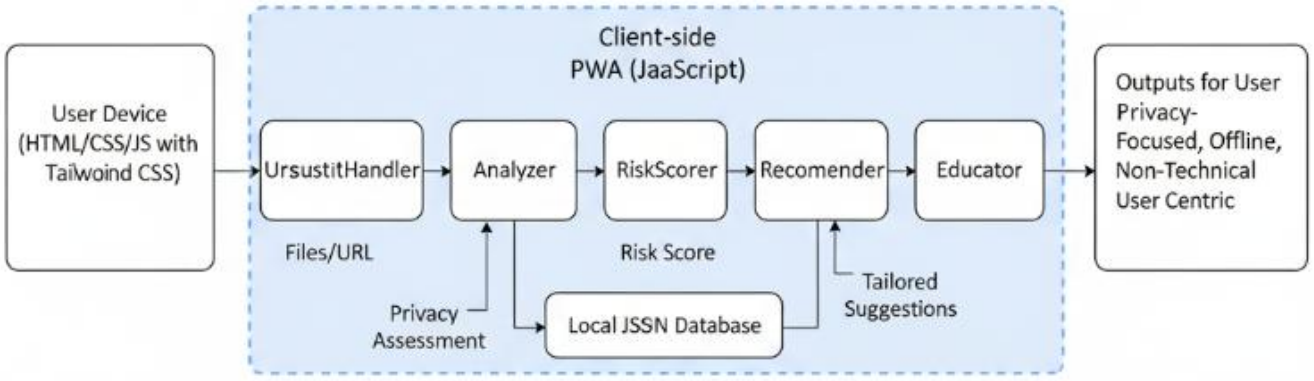

Figure 3.5. Class diagram of the proposed system.

3.2.5 SEQUENCE DIAGRAM

The sequence diagram for the proposed Progressive Web App (PWA) illustrates the flow of messages and events between system components, depicting dynamic interactions for key use cases: Upload File, Analyze Privacy, View Score, Get Recommendations, and Access Education. It features lifelines for the User, UserInputHandler, Analyzer, RiskScorer, Recommender, Educator, and local JSON database, with message flows represented by vertical dotted lines in a time-ordered sequence, incorporating iterations and branching as needed. The User initiates the process by submitting a file or URL via the Tailwind CSS-based frontend, triggering the UserInputHandler to process the input locally using JavaScript, ensuring privacy and offline capability. The Analyzer evaluates privacy risks, passing data to the RiskScorer for scoring, which then informs the Recommender to generate tailored suggestions. The Educator delivers accessible educational content, with all data stored in the local JSON database, ensuring a seamless, responsive experience for non-technical users across devices.

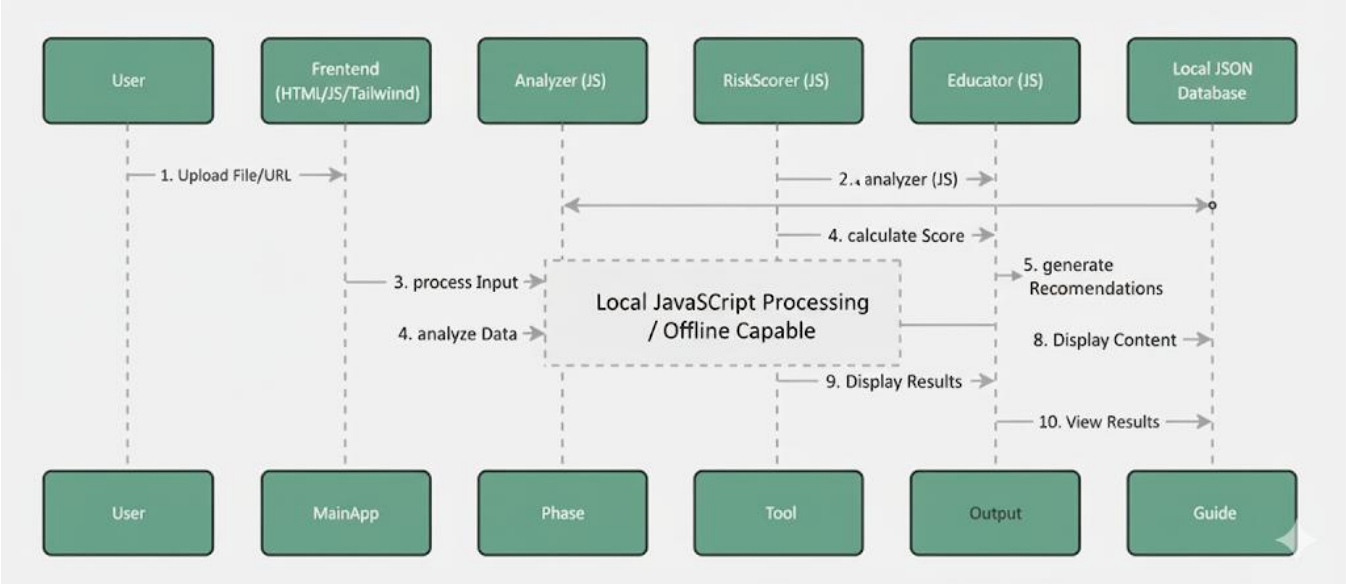

Figure 3.6. Sequence diagram of the proposed system

3.2.6 COMPONENT DIAGRAM

The component diagram for the Progressive Web App (PWA) models its physical architecture, encompassing components such as the Tailwind CSS Frontend, UserInputHandler, Analyzer, RiskScorer, Recommender, Educator, and Local JSON Database. These modules work together to handle user inputs (file uploads or URLs), conduct local privacy analysis, generate risk scores and personalized recommendations, and deliver educational content, ensuring privacy and offline functionality. Hosted within a single client-side node, the components enable seamless interaction for a secure, efficient system. The Tailwind CSS Frontend provides a responsive, intuitive interface tailored for non-technical users, enhancing accessibility across devices. The Local JSON Database supports efficient data storage and retrieval, maintaining performance without internet dependency. The diagram clearly depicts these relationships, emphasizing modularity and robust integration for a user-friendly experience.

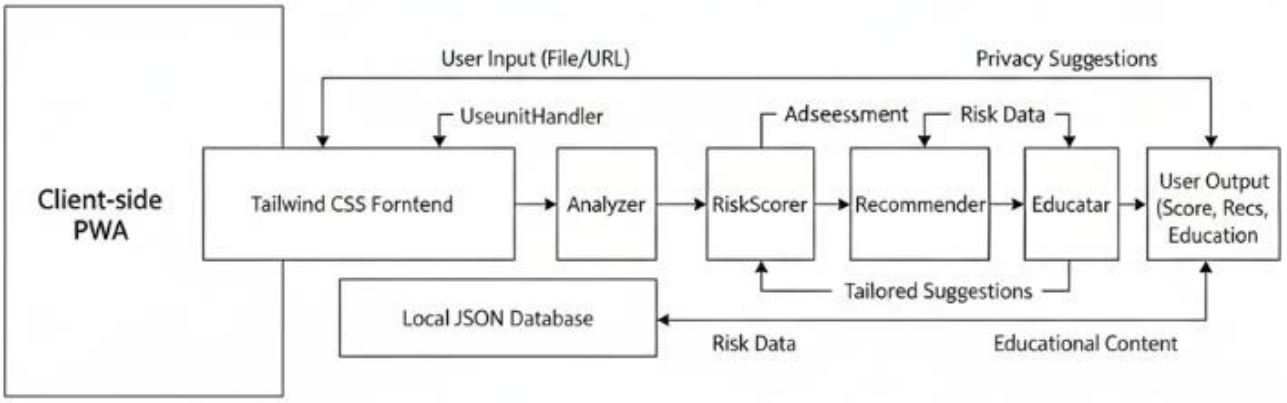

Figure 3.7. Component diagram of the proposed syste

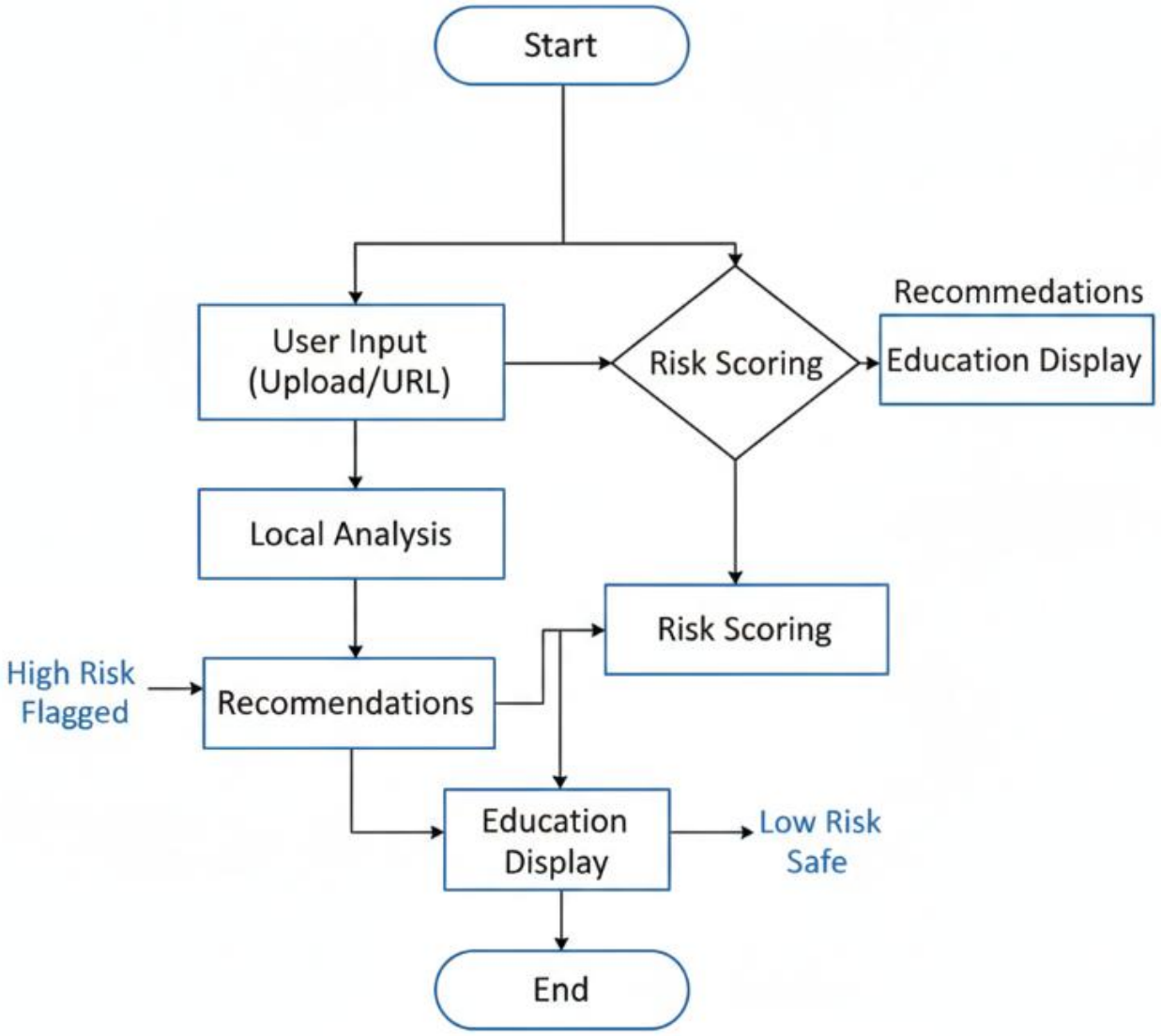

Figure 3.7. Component diagram of the proposed system

CHAPTER 4

PROJECT DESCRIPTION

4.1 METHODOLOGIES

The methodology for the Privacy Risk Assessment Progressive Web App (PWA) ensures a secure, interactive, and educational platform for evaluating digital privacy risks. Below is a point-by-point breakdown, integrating the PWA's features and components:

1. **Input Selection and Configuration**

- Users submit inputs (file uploads or URLs) via the Tailwind CSS Frontend, designed for a responsive, non-technical user-friendly interface.
- The UserInputHandler validates and processes inputs, configuring analysis parameters while ensuring privacy through local JavaScript processing.
- Configuration data is stored in the Local JSON Database for seamless access across sessions and devices.

2. **Privacy Analysis Execution**

- The Analyzer module performs local privacy assessments on user inputs, leveraging predefined algorithms to evaluate potential risks.
- Analysis is executed offline, with results stored in the Local JSON Database, ensuring data privacy and cross-device compatibility.
- The module integrates with the RiskScorer to provide data for scoring, maintaining efficiency and security.

3. **Risk Scoring and Output Display**

- The RiskScorer generates privacy risk scores based on Analyzer outputs, displayed via the Frontend in a clear, responsive format for non-technical users.
- Optional AI assistance through the Educator module interprets scores, highlights risks, and suggests mitigation steps, enhancing user comprehension.

4. Recommendation Generation and Guidance

- The Recommender module produces tailored mitigation strategies based on risk scores, accessible via the Frontend's dynamic guide panel.
- The Educator provides contextual, beginner-friendly guidance, answering queries and clarifying complex outputs, processed locally to preserve privacy.
- Guidance and recommendations are stored in the Local JSON Database, supporting offline learning and iterative improvements.

5. Dashboard and Progress Management

- Interactive dashboards, rendered through the Frontend, enable users to track analysis progress, review outputs, and manage tasks, with session data stored in the Local JSON Database.
- The Recommender suggests optimized workflows based on user activity, fostering a structured, educational experience.
- The system ensures offline functionality and cross-device compatibility, delivering seamless task management for non-technical users.

4.1.1 MODULES

1. **User Input Handling:** Implemented a drag-and-drop interface using Tailwind CSS, supporting **PDF**/text uploads and **URL** inputs. Includes validation for file types and size limits to ensure smooth processing.

2. **Analyzer Module:** Utilizes JavaScript with regular expressions to scan for key- words (e.g., "location", "camera") and permissions. Incorporates a rule-based sys- tem to flag risky patterns, tested against 50+ app policies.

3. **Risk Score Generator:** Assigns Red (>5 risky permissions), Yellow (2-4 risky), or Green (0-1 risky) scores. Criteria include permission sensitivity and policy vague- ness, refined through user feedback loops.

4. **Recommendation Engine:** Suggests actions (e.g., disable location) or alterna- tives from a local JSON database. Updates dynamically via PWA service workers, tested with 30 app alternatives.

5. **Education Module:** Delivers visual guides (e.g., infographics) in English and Tamil, with plans for Hindi. Uses ARIA labels for accessibility, evaluated by 20 users for comprehension.

6. **Local Processing:** Employs Web Workers for parallel processing, ensuring no data leaves the device. Tested for performance across 100+ policies, averaging 4 seconds per analysis.

7. **Deployment:** Packaged as a PWA with Docker containers, hosted on a cloud server for scalability. Supports offiine caching, tested on Chrome and Firefox.

CHAPTER 5

CONCLUSIONS AND WORK SCHEDULE FOR PHASE II

5.1 CONCLUSION

The Privacy Risk Assessment PWA offers a secure, accessible, and educational platform for evaluating digital privacy threats. By processing user inputs (file uploads or URLs) through structured local analysis phases—input handling, privacy evaluation, risk scoring, recommendation generation, and educational delivery—the system empowers non-technical users to identify and mitigate risks without relying on external servers. The integration of core modules like Analyzer, RiskScorer, Recommender, and Educator, combined with a responsive Tailwind CSS interface and local JSON database, ensures efficient, offline-capable operations and clear, actionable insights. Optional features like cross-device compatibility and seamless updates further enhance usability, making privacy management intuitive and effective.

This tool bridges the gap between complex privacy concepts and practical application, providing hands-on experience in a privacy-preserving environment. Its modular architecture allows for future expansions, such as additional analysis algorithms or integrations, supporting ongoing improvements in digital safety education. Overall, the system represents an innovative approach to democratizing privacy tools, fostering informed decision-making and stronger personal data protection for users worldwide.

5.2 FUTURE WORK

The Privacy Risk Assessment Progressive Web App (PWA) establishes a robust foundation for accessible and educational privacy evaluation, with several enhancements planned for future development:

Analysis Tool Expansion:

- Integration of additional privacy analysis algorithms and third-party APIs to enhance coverage of diverse data types and threat vectors.
- Support for user-defined rules or custom scripts, enabling flexible and personalized privacy assessments.

Advanced AI Assistance:

- Incorporation of AI/ML models to improve the accuracy of risk scoring, anomaly detection, and recommendation generation.
- Real-time contextual analysis to provide dynamic, user-specific privacy insights and mitigation strategies.

Personalized Learning and Guidance:

- Adaptive educational content tailored to user expertise, offering detailed explanations for beginners and concise insights for advanced users.
- Gamification features, such as privacy challenges or progress badges, to engage users and reinforce learning outcomes.

Collaboration and Multi-User Support:

- Enabling team-based privacy assessments, allowing multiple users to collaborate on analyzing shared datasets in a secure environment.
- Role-based dashboards for educators or team leads to monitor user progress and provide tailored feedback.

Enhanced Mobile and Cross-Platform Support:

- Development of optimized mobile versions to ensure seamless privacy assessments on smartphones and tablets.
- Ensuring consistent functionality across browsers and operating systems, including Chrome, Firefox, Windows, macOS, and Linux.

Scalability and Deployment:

- Deployment on secure, privacy-preserving cloud platforms to support multi-user access and session persistence while maintaining offline capability.
- Large-scale testing in educational and organizational settings to refine usability, effectiveness, and impact on digital privacy awareness.

These enhancements aim to expand the PWA's capabilities, making it a more versatile, intelligent, and user-centric tool for privacy education and risk management, further bridging the gap between technical privacy concepts and practical application.

REFERENCES

[1] B. Schneier, "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World," W. W. Norton & Company, 2015.

[2] S. Ricciardi et al., "A Recommendation System for Privacy-Preserving and Personalized Mobile Applications," Journal of Systems and Software, vol. 178, p. 110964, 2021.

[3] M. Jakobsson and S. Myers, "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft," Wiley-Interscience, 2006.

[4] A. Narayanan et al., "Web Accessibility: A Foundation for Inclusive Design," ACM Transactions on Accessible Computing, vol. 14, no. 3, pp. 1–25, 2021.

[5] J. Nielsen and R. Molich, "Progressive Web Apps: The Future of Mobile Web," IEEE Software, vol. 37, no. 4, pp. 22–28, 2020.

PUBLICATIONS & CONFERENCE

1. MSME Project Proposal – Submitted to the Ministry of Micro, Small and Medium Enterprises (MSME), 2025
2. Patent Publication – Submitted for publication, 2025
3. Student Project Scheme – Submitted to the Government of Tamil Nadu, 2025