DHANVANTH KESAVAN

Phone: +91 - 6381714501 | Email: dhanvanthkesavan@gmail.com | Location: Chennai, India

PROFILE

Versatile, security-conscious Full Stack Engineer with a proven track record of architecting high-performance web applications and enterprise platforms. Specializes in building complex data dashboards, unified control hubs, and financial (BFSI) user interfaces using React and Angular. Expert at bridging robust backend logic (Python Flask, Spring Boot, JSP) with scalable, component-driven client architectures. Highly adept at managing full-lifecycle engineering—including state management, database migrations, deployments, and client-side security hardening (CSP, XSS mitigation, secure context handling) within fast-paced enterprise ecosystems.

TECHNICAL SKILLS

- **Frontend Development:** React (Hooks, Context API, Redux Toolkit), Angular (v14+, TypeScript, RxJS, Services, NgRx), Vue.js, Tailwind CSS, HTML5/CSS3, JavaScript (ES6+)
- **Backend & Databases:** Python (Flask, WSGI), Java (Spring Boot, JSP), MySQL, Oracle, PostgreSQL, Database Migrations
- **Architecture & State:** Component-Driven Design, Client-Side Routing, Single Page Applications (SPA), Asynchronous Payload/JSON Filtering, Axios / Angular HttpClient
- **UI Security Hardening:** Content Security Policy (CSP), XSS/CSRF Mitigation, Clickjacking Protection, Secure Token Storage, Frontend RBAC (View-Trimming)
- **DevOps & Workflows:** Git, Webpack, Vite, NPM/Yarn, Postman, Linux/Unix, Agile Sprint Cycles

PROFESSIONAL EXPERIENCE

Nelito Systems Pvt Ltd | Chennai, India | 2 months

Project: Unified Operations & DevSecOps Control Panel

Scope: End-to-end development of an internal web application consolidating critical DevOps utilities (License File Generator/Decryptor, Secure File Transfer Interface, multi project Patch validation tool, attendance and live resource status monitoring and a SWIFT Messaging LAU utility).

Tech Stack: *Angular, Tailwind CSS, Python Flask (WSGI)*

- Engineered the core application shell using Angular, leveraging lazy loading and routing to decouple isolated sub-tools, optimizing initial bundle size and application load speeds.
- Integrated RBAC & Secure Session Routing: Engineered dynamic client-side Role-Based Access Control (RBAC) to enforce view-trimming and functional restrictions; configured precise route behaviors allowing authenticated operators full file-upload privileges while restricting unauthenticated users strictly to secure download views.
- Asynchronous Processing & State Streams: Implemented RxJS Observables and Behavior Subjects to manage asynchronous payload states, ensuring real-time UI data streaming and responsive status indicators during background file encryption and messaging translation tasks.
- Custom Token Authentication: Structured secure frontend integration for isolated sub-modules, including an protected attendance management portal, utilizing client-side PESTO tokens for stateless session validation, secure context handling, and granular access enforcement.

Nelito Systems Pvt Ltd | Chennai, India | 4 months

Project: "NSmart" BFSI Message Translation Platform

Scope: High-density frontend engineering and client-side security hardening for an enterprise-scale banking application deployed across international divisions for automated SWIFT compliance workflows.
Tech Stack: *Angular, TypeScript, RxJS, Spring Boot REST APIs, MySQL, Oracle*

- Developed responsive UI layers to render and interact with complex relational schemas mapped to database endpoints.
- Advanced Authentication & Access Controls: Spearheaded frontend compliance security by integrating TOTP (Time-Based One-Time Password) multi-factor authentication flows and strict Angular route guards to enforce granular Role-Based Access Control (RBAC) view-trimming based on user permissions.
- Custom End-to-End Encryption (E2EE): Engineered an enterprise-grade client-side encryption pipeline using AES-256 and an ECDH (Elliptic-Curve Diffie-Hellman) key exchange layer; developed custom cryptographic functions to handle key generation directly on the frontend without relying on standard native browser crypto packages, securely transferring keys to the Spring Boot backend with zero exposure risks.
- XSS Mitigation & Hardening: Hardened the application architecture against injection vectors by implementing a strict Content Security Policy (CSP) via dynamic CSP Nonce integration across script tags, completely mitigating XSS, CSRF, and Clickjacking threats on data-heavy financial tracking screens.

Ishta Infotech Pvt Ltd | Chennai, India | 6 months

Project: Enterprise Audit Management Engine

Scope: Full-stack delivery of a multi-tenant dual-portal (Auditor and Client) web application tailored for regulatory governance, evidence tracking, and audit lifecycle management.
Tech Stack: *React, Context API, React Hooks, Tailwind CSS, Python Flask, Database Migrations*

- Architected the frontend interface using React, utilizing functional components, React Hooks (useState, useEffect), and Context API for lightweight, fluid global state management.
- Designed high-density dashboard layouts using Tailwind CSS and engineered the backend layer using Python Flask, handling schema design, migrations, and final deployment.
- Dual-Portal Governance & Live Tracking: Designed and deployed a secure, multi-tenant dual-portal architecture featuring isolated, role-specific layouts for Auditor and Customer dashboards; built real-time tracking modules enabling client stakeholders to track live audit progress, project lifecycles, and operational visibility thresholds.
- Secure Evidence Management & ClamAV Integration: Engineered an asynchronous evidence upload pipeline featuring automated malware sandboxing; integrated open-source ClamAV antivirus scanning to scan all incoming client attachments, blocking malicious files at the application layer before permanent storage.
- Automated PDF Engine & Framework Compliance: Programmed an internal server-side reporting engine that auto-generates professional-grade audit completion PDF summaries; integrated dynamic regulatory auditing controls supporting multi-framework validation and inline scope definition mappings.
- Defensive Architecture & IDOR Mitigation: Implemented robust client-side Angular/React route guards paired with strict server-side Role-Based Access Control (RBAC) checks to completely mitigate Insecure Direct Object Reference (IDOR) vectors across cross-portal transaction endpoints
- Privacy Controls & Admin Overrides: Developed customized customer privacy and data collection acceptance tracking matrices; programmed administrative runtime controls allowing real-time session revocation and instant access suspension from the administrator dashboard directly to the customer portal.

Ishta Infotech Pvt Ltd | Chennai, India | 6 months

Project: Distributed Asset Tracker & Vulnerability Telemetry Platform

Scope: Full-stack development of a centralized monitoring platform displaying live network infrastructure visibility and machine telemetry for over 3,000+ distributed endpoints.

Tech Stack: *React, JavaScript (ES6+), Python Flask, REST APIs, JSON Payload Filtering*

- Multi-Tenant Full-Stack Architecture: Architected and deployed a secure, multi-tenant asset management infrastructure powered by a Python Flask (WSGI) backend and a React client application; implemented granular server-side and client-side Role-Based Access Control (RBAC) to isolate data views and operational capabilities across Admin, Manager, and Associate tiers.
- Cross-Platform Telemetry Agents: Engineered a fleet of lightweight endpoint data collectors, including compiled Go-lang binaries for Windows execution, modular Shell scripts for Linux server distributions, and a dedicated Android application package to securely ingest raw system health, hardware properties, and vulnerability metrics.
- Interactive Visualization & Dashboards: Built high-performance, responsive operational dashboards in React utilizing fluid animations and dynamic charts to track asset exposure; crafted reusable data grids featuring asynchronous client-side payload filtering, universal search, and conditional formatting mapped to real-time risk severity levels.
- Automated Alerting & Lifecycle Management: Integrated an enterprise SMTP email server pipeline to trigger automated, mission-critical operational notifications; programmed background scheduling workers to detect asset drift and instantly flag administrative cases if an endpoint fails to report telemetry for more than 7 consecutive days.
- Access Hardening: Enforced strict perimeter security across all tenant interfaces by embedding multi-factor authentication workflows, including TOTP (Time-Based One-Time Password) MFA verification loops during user session lifecycles.

Ishta Infotech Pvt Ltd | Chennai, India | 3 months

Project: Developer & QA Defect Dashboard

Scope: Full-stack development of an internal bug tracking and resolution ecosystem enabling QA teams to raise defects and engineers to track, fix, and update resolution lifecycles.

Tech Stack: *Java Server Pages (JSP), Java, MySQL, HTML5/CSS3*

- Built the application layer using Java Server Pages (JSP) and managed persistent transactional data stores utilizing a raw MySQL database.
- Programmed a server-side Role-Based Access Control (RBAC) matrix, allowing managers to dynamically assign raised bugs to specific developers, update global project health status indicators, and audit issue resolution velocity.

EDUCATION

Bachelor of Technology (B.Tech) in Computer Science and Engineering

Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology | Chennai, India | Graduation: June 2022

- **Core Focus:** Software Engineering, Web Technologies, Database Management Systems, UI/UX Architecture.