Zijun (Marshall) Zhang

- Phone - Portfolio - Email - Linkedin - Github

TECHNICAL SKILLS

Programming Languages: TypeScript, Python, SQL
Web & APIs: React, Next.js, Node.js, NestJS, RESTful APIs
Databases & Storage: PostgreSQL, MySQL, MongoDB, Redis
Cloud & DevOps: Docker, AWS (EC2, S3, RDS), GitHub Actions (CI/CD), Linux, Git
Testing & Tooling: Jest, Supertest, React Testing Library, ESLint, Prettier
Machine Learning & LLMs: PyTorch, Scikit-learn, NumPy, Pandas, Hugging Face Transformers
LLM Security & Trustworthy AI: Model Unlearning, Membership Inference, Adversarial Robustness & Evaluation, Privacy-preserving ML, Model Auditing

EDUCATION

The University of Melbourne — **Melbourne, Victoria, Australia**
Doctor of Philosophy - Engineering and IT — *Dec 2025 - Present*

The University of Melbourne — **Melbourne, Victoria, Australia**
Master of Computer Science — *Mar 2024 - Dec 2025*

The University of Melbourne — **Melbourne, Victoria, Australia**
Bachelor of Science in Computing and Software Systems — *Mar 2021 - Dec 2023*

WORK EXPERIENCE

Software Engineer
Techman Launch Pty Ltd, Melbourne, Australia — *May 2025 - Present*

- Shipped 8+ end-to-end features across a React frontend and backend APIs on AWS, lifting client Net Promoter Score from 7.6 to 8.7 over two quarters.
- Designed and maintained a Docker- and GitHub Actions–based CI/CD pipeline, shrinking the release cadence from bi-weekly to daily and reducing regression defects by 30%.
- Established an automated testing strategy with Cypress end-to-end tests for the React frontend and xUnit integration tests for backend services (200+ cases, ˜90% coverage), cutting manual QA effort by 50%.

Software Engineer Intern
Industrial and Commercial Bank of China, Melbourne, Australia — *Dec 2023 - Feb 2024*

- Optimised high-volume SQL queries and integrated Redis caching, reducing average transaction latency by 20% on core banking workflows.
- Redesigned the internal user interface with clearer information hierarchy and real-time validation, cutting form submission error rates by 15%.
- Coordinated cross-functional launch of a new KYC microservice with backend, operations, and compliance teams, delivering 1 week ahead of the regulatory deadline.

Data Engineering and Testing Intern
Alibaba, Yunnan, China — *Dec 2022 - Feb 2023*

- Developed and deployed an LSTM-based demand-forecast model that improved safety-stock accuracy by 10%, reducing stock-out incidents for key SKUs.
- Automated data-pipeline validation with Airflow and PyTest, reaching ˜98% test coverage and preventing critical data outages.
- Led code reviews across 5 repositories, resolving 30+ critical issues and raising team adoption of testing and linting standards.

PUBLICATIONS

- **When Forgetting Reveals: Black-Box Inversion Attacks on Unlearning in Large Language Models**, Proceedings of ESORICS Workshop on Secure and Trustworthy Machine Unlearning Systems (STMUS 2025). Demonstrated the first systematic subject-level black-box unlearning inversion attack on LLMs, showing that modern unlearning methods leave detectable behavioral “fingerprints” exploitable for privacy leakage. Developed a discrepancy-based attack pipeline using probe-query pairs and an LLM judge (Gemini 2.5 Pro) to identify removed subjects from a 100-candidate pool. Evaluated GA, DPO, NPO, and RT across LLaMA-3 8B and Phi-3 Mini-4K, achieving up to 72% Top-1 accuracy (vs. 1% random).