GovHack[1]
Team V-SARC
An Accurate and Trustworthy Chatbot for Data Interactions

Proof of Concept
Project Description

Date: August 31, 2025
Project: NTGAssist
Version 1.0

[1]GovHack and the GovHack Logo are registered trademarks of GovHack Australia Limited. The GovHack logo is used here for reference purposes only. All rights in the GovHack name and logo are reserved by GovHack Australia Limited.

Contents

An Accurate and Trustworthy Chatbot for Data Interactions

Our Work

Sources

- GovHack 2025 Backend
- GovHack 2025 User Manual
- GovHack 2025 Frontend

Evidence of Work

Find the Evidence of Work here: Google Drive Folder

Project Description

Project description: The project developed an AI system, implemented as a chatbot, to reliably, transparently, and audibly assist in managing and interacting with government datasets. By combining **Retrieval-Augmented Generation (RAG)**, vectorized metadata, and a tool-calling architecture, the system delivers grounded responses with full audit trails. Advanced AI techniques ensure ethical, accountable, and privacy-preserving outputs. The system enhances government decision-making with over **99% multi-factor confidence scoring**.

Datasets Used

- Australian Government Procurement Statistics
  - AusTender is the Australian Government's procurement information system, where entities publish details of planned procurements, tenders, standing oQers, and awarded contracts in line with Commonwealth Procurement Rules.
- Freedom of Information Statistics
  - The Freedom of Information Statistics dataset contains detailed information on FOI activity reported by Australian Government agencies and ministers. The dataset also records review numbers and estimated costs, with agency-reported staQ time adjusted using a salary multiplier in the Excel version.
- Employee Leave Tracking Data (Kaggle)
  - This dataset records employee leave details for 2024 across various departments, including leave type, duration, entitlements, and balances.

Data Story

Government agencies oversee vast volumes of datasets but often struggle to extract meaningful insights efficiently. Traditional AI chatbots show potential but fail to meet the extremely high accuracy standards required in public sector decision-making, where even a 90

While recent advancements in AI, including large language models with advanced reasoning capabilities, promise sophisticated analysis, they also introduce risks such as hallucination, where outputs may be factually incorrect or unsupported by reliable sources. For government applications, accuracy and verifiability outweigh advanced reasoning; AI systems must provide grounded, scope-limited responses and allow human users to guide interpretation and decision-making.

Our Mission

Government agencies across Australia manage vast volumes of critical data. Despite this, converting these resources into actionable insights remains a major challenge. High-stakes decisions require near perfect accuracy, transparency, and accountability standards that traditional AI often cannot meet.

Current Limitations

1. Accuracy Gap – Commercial AI tools typically achieve around 90% accuracy. For government decisions, this is insufficient; outcomes must meet 99%+ reliability.
2. Hallucination Risk – Generative AI may fabricate information, which is unacceptable when shaping public policy or delivering essential services.
3. Auditability Crisis – Black-box AI outputs lack traceability, making it diQicult to explain or justify decisions.
4. Integration Complexity – Departmental silos prevent seamless cross-functional insights.
5. Trust Deficit – Officials cannot fully rely on AI outputs without verifiable evidence and clear governance.

System Architecture

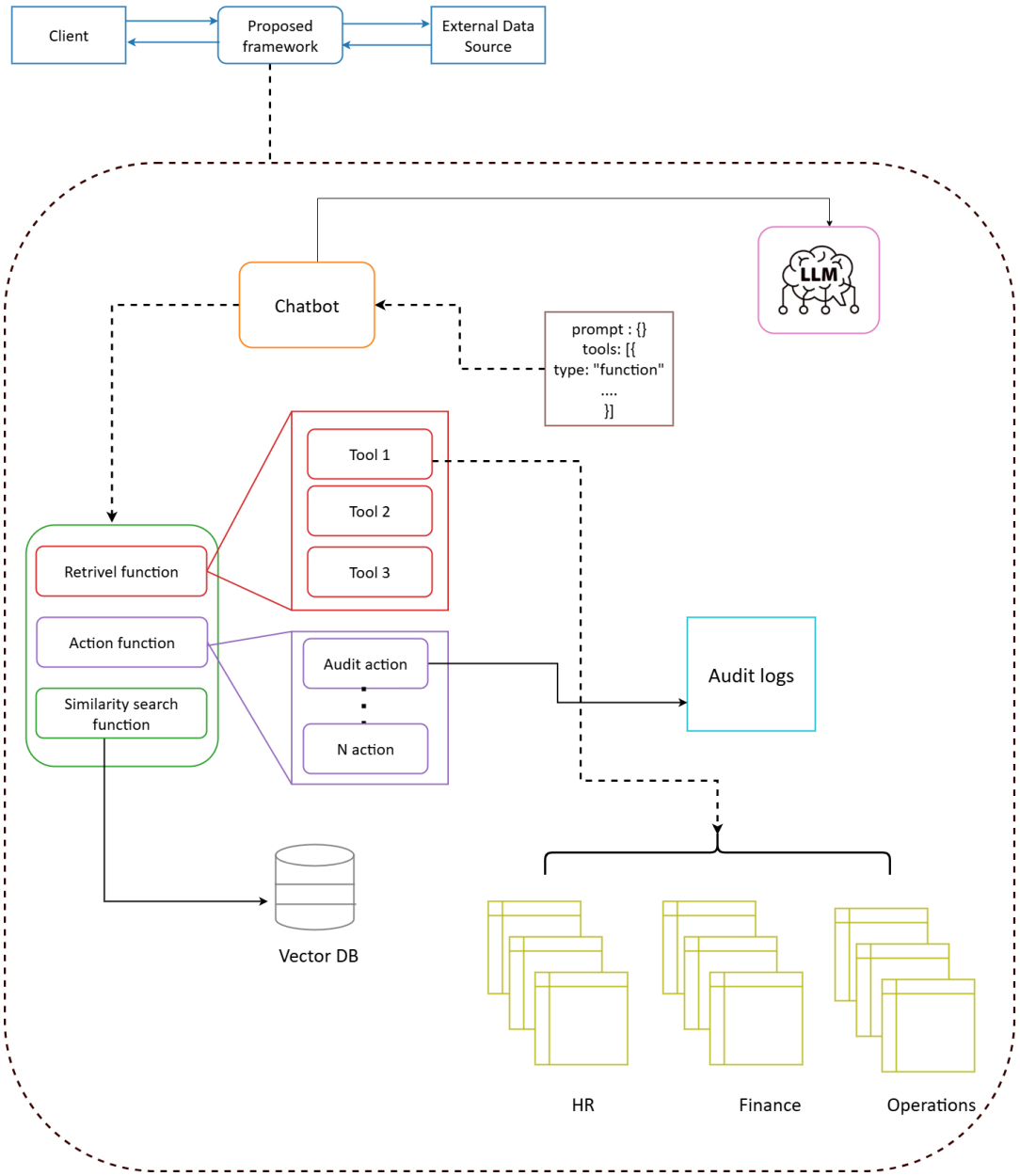

Figure 1: System Architecture Diagram

Our Approach

We designed an AI system focused on **reliability, transparency, and inclusivity**, combining advanced AI techniques with governance measures:

- **Retrieval-Augmented Generation (RAG):** Ensures AI responses are anchored to verified government sources, minimizing hallucination.
- **Conversational interactions** to ensure better engagement.

- **Vectorised Metadata:** Provides contextual understanding and accurate cross- referencing of diverse datasets.
- **Tool-Calling Architecture:** Integrates multiple data sources in a modular and secure way, allowing scalable workflows.
- **Mathematical Aggregation & Statistics:** Supports evidence-based reasoning and quantitative validation of AI outputs.
- **Audit Logging:** Captures all prompts and responses, maintaining a complete history for accountability.
- **Source Referencing:** Every response is linked to original datasets to ensure verifiability.

Key Features & Capabilities

- Multi-Factor Confidence Scoring: Evaluates the reliability of every AI output.
- Plain Language Summaries: Makes complex government information accessible to all literacy levels.
- Cross-Silo Interoperability: Ensures outputs can be reviewed, explained, and justified to meet governance standards.

Objectives We Achieved

	Objective	Proposed Solution / Implementation
1	Conversational data interrogation across multiple government datasets	Build a context with metadata, with references to datasets
2	Trust scoring and vetting mechanisms that validate AI responses	Similarity search and transparency mechanisms: Confidence Scoring, Data Freshness Indicator
3	Grounded, scope-limited responses (no hallucinations about unrelated topics)	Retrieval-Augmented Generation (RAG) AI
4	Transferable framework that works across departments (HR, finance, operations)	Generalized architecture with prompt-back mechanism
5	Suggested question scaffolding to guide users toward productive queries	Conversational RAG with guided prompts
6	Audit trails showing how conclusions were reached	Save fetched data and include detailed logs

Figure 2: System Architecture Diagram

Example Applications and Explanations

1. Finance:
    - Use Case: Detect anomalies in vendor payments or forecast budget compliance.
    - Explanation: The AI system analyzes transactional and financial datasets to flag unusual payment patterns, such as duplicate invoices or unexpected expenditure spikes. It also aggregates historical spending trends to provide accurate forecasts, helping finance teams make informed budgeting decisions

    while reducing risk.

2. Human Resources (HR):
    - Use Case: Analyze leave trends and workforce patterns to support operational planning.
    - Explanation: By examining HR records, timesheets, and leave applications, the AI identifies patterns such as high absenteeism in specific departments or seasonal workforce gaps. This insight helps managers plan staQing levels, improve team productivity, and optimize resource allocation.

3. Operations:

- Use Case: Identify irregularities in procurement or service delivery metrics.
- Explanation: The system evaluates operational data across procurement, logistics, and service records to spot inconsistencies, delays, or inefficiencies. Alerts are generated for potential issues, enabling operational managers to take proactive measures and maintain service quality.

Outcomes Achieved

Our system demonstrates how AI can be safely and e]ectively deployed in government contexts:

- Reduced Misinformation: AI outputs are grounded in verified data, reducing errors.
- Enhanced Transparency: Full audit logs and source references enable accountability.
- Improved Accessibility: Citizens and staQ can interact in natural language and understand outputs in plain English.
- Stronger Collaboration: Cross-agency integration allows unified insights and better-informed decision-making.

Advanced AI Techniques

To deliver reliable and accountable AI services, we leverage cutting-edge technologies:

- Retrieval-Augmented Generation (RAG): Ensures AI responses are accurate and grounded in trusted, authoritative data sources.
- Agent-Based Validation: Autonomous agents review and confirm query results before presenting them, maintaining high standards of accuracy and responsibility.
- Governance and Transparency Dashboards: Monitors AI performance, accessibility, and compliance with ethical principles, providing clear visibility for both government staQ and citizens.

Technology Stack

- Java Runtime - 17 or above
- NPM latest version
- Homebrew
- NPM latest version
- Expo
- React
- GIT
- Docker
- Maven

- Spring Framework

Tools & Softwares

- Canva
- GenAI
- Excel
- Mermaid
- Prezi

AI in Governance

This section addresses the strategic considerations for implementing AI in government, specifically for our AI system that supports accurate, auditable, and trustworthy decision-making. It focuses on:

- Boosting Operational Efficiency
- Improving Transparency
- Multi Factor Confidence Scoring
- Ensuring Ethical Use
- Data Privacy and Security
- Building Public Trust
- Future Adaptations

Boosting Operational Efficiency

Government agencies must scale AI adoption according to organizational maturity, risk tolerance, and AI experience. Key steps include:

- Identify High-Impact Areas: Evaluate where AI can meaningfully enhance workflows, reduce administrative burden, and improve citizen services.
- Risk and Reward Assessment: Consider risks such as data privacy or misinformation, and quantify benefits like time savings, cost efficiency, and improved social inclusion.
- Lean Business Cases: Present concise proposals highlighting costs, benefits, and expected outcomes to secure leadership support.
- Governance Integration: Apply a structured governance framework to ensure compliance with regulations and ethical AI practices.
- Cross-Department Collaboration: Encourage resource and knowledge sharing to maximize efficiency and reduce duplication of effort.

- Pilot Projects: Test AI solutions with proof-of-concept initiatives before full deployment.

Improving Transparency

Transparency is critical for public trust and accountability:

- Governance Dashboards: Provide real-time AI performance insights accessible to officials and citizens.
- Decision Traceability: Log and document all AI outputs, linking responses back to original sources.
- Accountability Assignments: Clearly define responsible stakeholders for AI decisions.
- Practices: Adapt strategies to reflect first-of-a-kind AI solutions, ensuring expert review and integration.

Ensuring Ethical Use

Ethical AI use requires well-defined frameworks and practical measures:

- Alignment with AI Principles: Incorporate human-centred values, fairness, privacy, safety, and transparency.
- Algorithmic Bias Mitigation: Use diverse datasets, perform bias audits, and ensure inclusive design practices.
- Explainable AI: Develop AI systems that can clearly justify their outputs to decision-makers and citizens.
- Documentation & Reporting: Maintain detailed records of development, decisions, and performance metrics.
- Regulatory Oversight: Establish independent monitoring bodies to ensure compliance with ethical standards.
- Remove Personal Identification Informations: Ensure that all data used or displayed in the AI system excludes any personal identifiers to protect privacy and maintain compliance with data protection regulations.

Data Privacy and Security

Protecting sensitive government and citizen data is essential without compromising AI functionality:

- Secure Architecture: Implement encryption, access controls, and model protection to prevent tampering or data theft.
- DevSecOps Integration: Include automated security testing, code audits, and ongoing security training.
- Advanced Measures: Apply red teaming, penetration testing, and treat AI initiatives as first-of-a-kind (FOAK) to identify vulnerabilities proactively.

- Privacy-Preserving Techniques: Leverage differential privacy, federated learning, and homomorphic encryption for safe AI analytics.
- Data Governance: Assign roles like data stewards to oversee proper data management and compliance.

Future Adaptations

To ensure AI systems remain effective and ethical, government agencies should:

- Invest in R&D: Continuously explore emerging AI techniques like multi-agent systems.
- Pilot Emerging Technologies: Test new AI capabilities on a limited scale before wide deployment.
- Enhance Cybersecurity: Strengthen AI-driven defense systems to protect sensitive data.

Retrieval-Augmented Generation (RAG)

- Data Processing: Transforms unstructured content into formats suitable for vectorized storage and efficient retrieval.

Semantic Matching

Recognizes contextually similar terms to deliver more accurate and meaningful responses.

AI Tool Calling

Tool calling (function calling) enables AI models to interact with external APIs or systems, extending their capabilities. Tools are mainly used for information retrieval (e.g., RAG, querying databases, fetching news/weather) and for taking actions. While models can request tool calls with input arguments, the client application executes the calls and returns results, ensuring security.

1. Define the tool in the chat request with a name, description, and input schema.
2. If the model decides to use the tool, it outputs the tool name and input parameters.
3. The application identifies and executes the tool with those parameters.
4. The result is processed by the application.
5. The application returns the result to the model.
6. The model generates the final response using the result as added context.

Spring. (n.d.). *Spring AI: Tools API reference*. Spring. Retrieved August 31, 2025, from https://docs.spring.io/spring-ai/reference/api/tools.html

Vector Database Utilization

- Scalable Access: Handles growing datasets efficiently without compromising retrieval speed.

	Objective	Proposed Solution / Implementation
1	Conversational data interrogation across multiple government datasets	Build a context with metadata, with references to datasets
2	Trust scoring and vetting mechanisms that validate AI responses	Similarity search and transparency mechanisms: Confidence Scoring, Data Freshness Indicator
3	Grounded, scope-limited responses (no hallucinations about unrelated topics)	Retrieval-Augmented Generation (RAG) AI
4	Transferable framework that works across departments (HR, finance, operations)	Generalized architecture with prompt-back mechanism
5	Suggested question scaffolding to guide users toward productive queries	Conversational RAG with guided prompts
6	Audit trails showing how conclusions were reached	Save fetched data and include detailed logs

Figure 3: System Architecture Diagram

- Contextual Awareness: Leverages semantic understanding to provide precise and relevant information.

Governance and Compliance

- Alignment with AI Principles: Ensures operations adhere to standards of fairness, transparency, and accountability.
- Performance Monitoring: Tracks metrics such as accuracy, accessibility, and fairness through a dedicated governance dashboard.

Disclaimer

This software and accompanying documentation are provided strictly for proof-of-concept and demonstration purposes only. The software is experimental and may contain errors; it is not intended for production use. The use of any copyrighted logos, including the GovHack logo, does not imply endorsement, sponsorship, or affiliation. All rights in such logos are reserved by their respective owners. Use of this software is at your own risk, and the authors accept no liability for any damages resulting from its use.

Team Contact Information

Name	Title	Contact information
Team V-SARK		
Ayesh Jayasekara	Team Lead	Email: ejkpac@gmail.com
Chathura Janadara	Member	Email: chathurajanadara97@gmail.com
Ravindu Supun	Member	Email: supunravidu96@gmail.com
Vigneshwaran Palansamy	Member	Email: p.vickey22@gmail.com
Kavini Welarathne	Member	Email: sarakavini18@gmail.com

Thank you! Hope you have enjoyed following through our approach!