Title: GovLLM-ZW*: A Policy-Driven Middleware Layer for Privacy, Consent, and Context-Aware LLM Integration in Zimbabwe*

Theme: Harnessing Emerging Digital Technologies for Industrial Transformation and Socioeconomic Advancement in Zimbabwe

Category: Prototype Demonstration

Research Area: Policy, Governance and Sustainable AI

Author Information: Tinavo Chihota

Contact Information: tinavochihota@gmail.com / 078 558 9603

Abstract:

The rapid integration of Large Language Models (LLMs) into enterprise and public sector systems presents critical challenges related to data privacy, governance, consent, and contextual reliability. In Zimbabwe, these risks are heightened by the increasing use of LLMs on sensitive structured and unstructured data without standardized policies, enforcement mechanisms, or safeguards. This exposes personally identifiable information (PII), enables hallucinated or misleading outputs, and produces responses that may not align with local regulatory, cultural, or domain-specific contexts, while also raising concerns around unauthorized data usage and lack of user consent.

This prototype demonstration presents GovLLM-ZW, a middleware-based data governance layer designed to securely mediate interactions between enterprise systems and LLMs. The architecture enforces end-to-end controls across the AI pipeline, including automated anonymization of PII in both structured datasets and unstructured text, consent management mechanisms to ensure data is processed only with appropriate authorization, role-based access control, and configurable policy engines that allow organizations to define and enforce rules, compliance requirements, and acceptable usage standards aligned with data protection principles. The system incorporates context-aware input filtering, output validation, and response restructuring to reduce harmful or inaccurate outputs.

To enhance reliability, the middleware integrates retrieval-augmented generation (RAG) pipelines that ground model responses in trusted and locally relevant knowledge sources. Additional components include fact-checking mechanisms, response validators, and comprehensive audit logging to ensure traceability, accountability, regulatory compliance, and verifiable consent tracking. The design also supports extensible control points where institutions can introduce domain-specific policies, validation workflows, and governance rules.

The demonstration will showcase the working middleware layer, including real-time data anonymization, consent enforcement, controlled LLM interactions, and monitored outputs through interactive dashboards. By embedding privacy preservation, consent management, policy enforcement, and verification directly into the LLM interaction lifecycle, GovLLM-ZW mitigates risks of data leakage, misinformation, and non-compliance. The proposed approach demonstrates how middleware-driven governance can enable secure, trustworthy, and context-aware AI adoption, contributing to sustainable digital transformation and socioeconomic advancement in Zimbabwe.