# CMS GTA Project

Please include a title and name in the supervisor sections. There is a strict 300-word limit in the project summary section below.

|  |  |  |  |
| --- | --- | --- | --- |
| **First Supervisor** | **Xiao Chen** | | |
| **School/Department** | School of Computing and Mathematical Sciences | | |
| **Email** | Xiao.chen@leicester.ac.uk | **Telephone Ext** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Second Supervisor** | **Ashiq Anjum (Prof.)** | | |
| **School/Department** | School of Computing and Mathematical Sciences | | |
| **Email** | a.anjum@leicester.ac.uk | **Telephone Ext** |  |

|  |  |
| --- | --- |
| **Additional Supervisor** | External |

**Section 2 – *Project Information***

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Title** | **Federated Architectures for Secure Large Language Models** | | |
| **Project Highlights:** | 1. | **Pioneers a three-tiered architecture** integrating blockchain's traceability, federated learning's privacy preservation, and LLMs' generative power to resolve the "impossible triangle" of data privacy, model consistency, and regulatory compliance in distributed AI. | |
| 2. | **Introduces a dynamic knowledge-injection protocol** that hardcodes domain expertise (e.g., medical guidelines) into LLMs via real-time knowledge graph alignment, reducing factual hallucinations in pilot tests. | |
| 3. | **Develops a lightweight blockchain consensus engine** achieving high TPS through sharding and gradient compression, enabling efficient distributed training of models while maintaining full audit trails. | |
| **Project Summary (300 words maximum)** | | | |
| This proposal tackles critical challenges in developing trustworthy AI systems by integrating blockchain, federated learning, and large language models (LLMs) into a unified architecture. While LLMs like ChatGPT and DeepSeek demonstrate transformative potential, centralised AI systems face unresolved issues: data silos impede cross-institutional collaboration, privacy risks conflict with regulations (e.g., EU AI Act), and LLMs’ factual inaccuracies undermine high-stakes applications. Current approaches fail to systematically unify blockchain’s auditability, federated learning’s privacy preservation, and LLMs’ generative capabilities.  The project introduces a **three-tiered architecture** addressing these limitations:   1. **Data Layer**: A zero-knowledge-proof framework for federated learning ensures data authenticity while preventing raw data exposure, countering adversarial attacks via cryptographic verification. 2. **Model Layer**: A knowledge-injection protocol dynamically aligns LLM outputs with domain-specific knowledge bases (e.g., medical codes, legal statutes), significantly enhancing output reliability. 3. **System Layer**: An optimised blockchain consensus mechanism combines sharding and compression techniques to support efficient distributed training of large-scale models while maintaining auditability.   Key innovations include a collusion-resistant data verification method, a neuro-symbolic architecture integrating knowledge graphs with transformers, and a storage-efficient blockchain scheme. Validated through healthcare and financial case studies, the framework streamlines secure data sharing and provides auditable decision trails for regulatory compliance.  Anticipated outcomes encompass open-source tools for trustworthy AI deployment, high-impact publications, and contributions to AI ethics standardisation. By harmonising technological capabilities with ethical requirements, this work establishes a scalable blueprint for AI systems demanding both innovation and accountability, particularly in sensitive domains like medical diagnostics and financial analytics. The architecture’s modular design ensures adaptability across sectors while addressing the core challenges of privacy, accuracy, and transparency in next-generation AI applications. | | | |
| **Supervisor Support Statement (100 words maximum)** | | | This project benefits from the complementary expertise of two supervisors: Dr. Xiao Chen, an experienced researcher in blockchain scalability and privacy-preserving protocols, who brings extensive experience in distributed systems and cryptographic verification, and Dr. Ashiq Anjum, an expert in distributed AI systems, who contributes deep knowledge in AI model optimisation and knowledge integration. Additionally, external support is provided by industry partners, including a major healthcare consortium for real-world data validation and a blockchain infrastructure provider for technical implementation. | |