Centre for High Performance Computing 2024 National Conference

Contribution ID: **157** Type: **Talk**

A chatbot LLM based access control mechanism

Tuesday, 3 December 2024 11:00 (20 minutes)

Recent Artificial Intelligence(AI) advancements, notably in Large Language Models(LLMs), have enhanced Natural Language Processing(NLP) capabilities like Text-to-SQL. Businesses are increasingly using LLMs for domain-specific applications such as chatbots, but this raises security concerns including data access control. This research addresses these concerns by developing a secure access control mechanism for Text-to-SQL applications. While there exists literature that aims to improve the technical aspects of Text-to-SQL systems, it lacks solutions for access control. This paper proposes a prototype integrating an access control layer within the Text-to-SQL process to ensure secure and authorized data access while maintaining usability and performance. The research is validated through the development of a domain-specific chatbot prototype that demonstrates its effectiveness in mitigating security related access control risks.

Student or Postdoc?

Email address

Co-Authors

CHPC User

CHPC Research Programme

Workshop Duration

Primary authors: ELOFF, Jan (University of Pretoria); STILL, Christian (University of Pretoria)

Presenter: STILL, Christian (University of Pretoria)

Session Classification: ISSA

Track Classification: Cybersecurity / ISSA