

Building a cybersecurity advisory chatbot for general users.

Ha The Dat

Abstract: The project focuses on developing an intelligent virtual assistant to enhance awareness and support non-technical users in avoiding cybersecurity risks. The system uses a large language model (LLM) combined with Retrieval-Augmented Generation (RAG) techniques to provide accurate, up-to-date security solutions for phishing, malware, and password management. The chatbot is deployed on a web platform, enabling users to easily access complex security knowledge through natural language.

Keywords: Chatbot, Cybersecurity, RAG, Artificial Intelligence

References

- [1] Cục An toàn thông tin, "Báo cáo tình hình an toàn thông tin mạng Việt Nam năm 2024," 2024. [Online]. Available:
- [2] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in Proc. NAACL-HLT, 2019.
- [3] A. Vaswani et al., "Attention Is All You Need," in Proc. NeurIPS, 2017.
- [4] D. Jurafsky and J. H. Martin, Speech and Language Processing, Stanford University, 2020.
- [5] R. Bace and P. Mell, "Intrusion Detection Systems," NIST, 2001.