УДК 004.056

ИССЛЕДОВАНИЕ RAG ПОДХОДОВ В ЗАДАЧАХ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Свиридов Д.А. (Университет ИТМО)
Научный руководитель – научный сотрудник ФБИТ Еритенко Н.А.
(Университет ИТМО)

Введение

Современные большие языковые модели открывают новые возможности в области автоматизации пентеста, так как являются основополагающим звеном этой системы. Однако знания LLM ограничены временем обучения и подвержены проблеме устаревания данных. При этом в области кибербезопасности ежедневно появляются новые уязвимости и техники атак.

Для решения данной проблемы используют RAG, представляющий из себя архитектурный подход к генеративным моделям, который сочетает навыки поиска информации с генеративными возможностями больших языковых моделей [1,2].

Основная часть

Суть предложенного исследования заключается в анализе и сравнении подходов Retrieval-Augmented Generation (RAG) с использованием векторных и графовых хранилищ в задачах автоматизированного тестирования на проникновение. Основной целью является определение оптимальной архитектуры и методов хранения данных, обеспечивающих максимальную релевантность и точность поиска информации в процессе генерации и анализа уязвимостей.

Анализ и проектирование архитектуры RAG. На первом этапе проводится исследование существующих подходов к построению RAG-систем, рассматриваются используемые типы хранилищ и их применимость в задачах пентеста. Особое внимание уделяется сравнению свойств векторных и графовых хранилищ. На основе проведённого анализа проектируются две экспериментальные архитектуры, каждая из которых реализует свой подход к структурированию и поиску данных [3,4].

Разработка и интеграция. На следующем этапе проводится реализация разработанных архитектур и их интеграция с системой автоматизированного пентеста. Для этого создаются конвейеры, обеспечивающие индексацию и семантический поиск информации по заранее подготовленным данным на тему пентеста. В графовом хранилище фокус уделяется анализу связей между уязвимостями, сервисами и эксплойтами, а в векторном быстрой индексации и использованию.

Эксперименты и результаты. В завершающей части работы проводится серия экспериментов по оценке производительности и качества извлечения знаний из различных типов хранилищ. Для этого используются тестовые сценарии автоматизированного пентеста. Результаты позволят определить, какой тип хранилища лучше подходит для RAG в контексте задач кибербезопасности и автоматизации анализа уязвимостей.

Выводы

В ходе работы разработаны и экспериментально сравнены два варианта архитектуры RAG-системы, основанных на векторном и графовом хранилищах знаний, применительно к задачам автоматизированного тестирования на проникновение.

Литература

1. Published CVE Records, [Электронный ресурс]. – URL: https://www.cve.org/about/Metrics, (Дата обращения: 16.02.2026).
2. Arslana M., Cruza C., Ghanema H., Munawarb S. A Survey on RAG with LLM // 28th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems – 2024 – №256 – С. 3781-3790. https://www.sciencedirect.com/science/article/pii/S1877050924021860
3. Gao L., Mialon G., Marti G., Dibaji S. M. Precise Zero-Shot Dense Retrieval without Relevance Labels, [Электронный ресурс]. – URL: https://arxiv.org/abs/2305.14283, (Дата обращения: 16.02.2026).
4. An L., Li C., Xu J. и др. Text2Mol: Cross-Modal Molecule Retrieval with Natural Language Queries, [Электронный ресурс]. – URL: https://arxiv.org/abs/2404.16130, (Дата обращения: 16.02.2026).