

# LIST OF FIGURES

|     |                                                                                     |     |
|-----|-------------------------------------------------------------------------------------|-----|
| 1.1 | AIM-CTI conceptual framework . . . . .                                              | 7   |
| 1.2 | Integration of LLMs and RAG within the CTI-CMM framework . . . . .                  | 11  |
| 2.1 | CTI Life Cycle . . . . .                                                            | 18  |
| 3.1 | A representative instance of the RAG process . . . . .                              | 35  |
| 3.2 | Architecture of LLM-Enhanced Cyber Threat Intelligence System . . . . .             | 36  |
| 3.3 | The CTI GraphRAG Architecture . . . . .                                             | 39  |
| 3.4 | Prototype Development Flowchart . . . . .                                           | 41  |
| 3.5 | AIM-CTI System Architecture . . . . .                                               | 49  |
| 3.6 | STIX-Based Entity-Relationship Model . . . . .                                      | 59  |
| 3.7 | Entity-Relationship Data Model . . . . .                                            | 60  |
| 3.8 | Neo4J Database Schema . . . . .                                                     | 63  |
| 3.9 | Neo4J Database Relationships . . . . .                                              | 64  |
| 4.1 | Evaluation Metric Overall Score Comparison Between Hybrid RAG and ChatGPT . . . . . | 88  |
| 4.2 | CTI Maturity Evaluation . . . . .                                                   | 97  |
| 4.3 | CTI Gauge Evaluation . . . . .                                                      | 99  |
| 4.4 | CTI Gauge Evaluation . . . . .                                                      | 102 |
| 4.5 | Cypher Injection Attack Attempt Blocked by Security Measures . . . . .              | 105 |