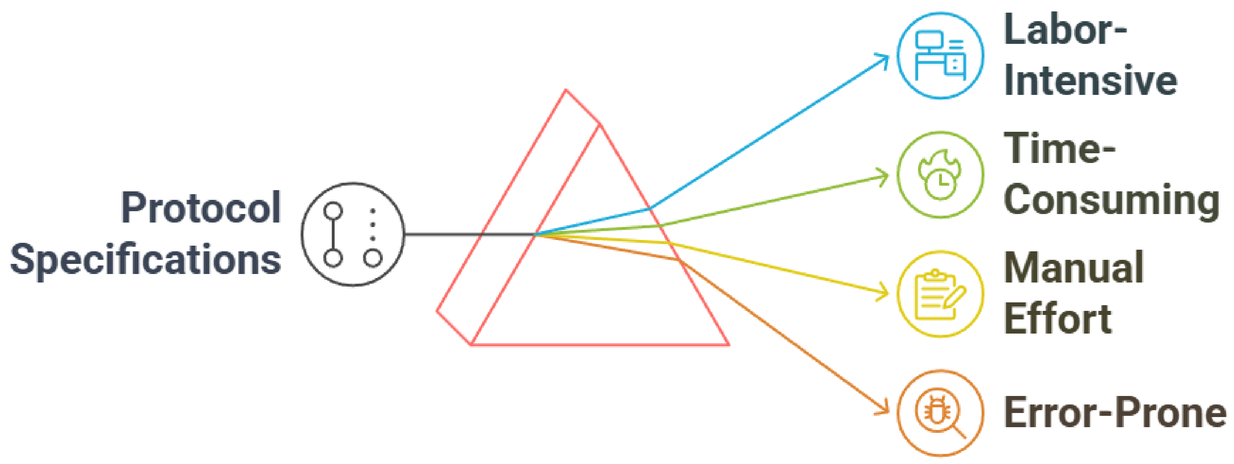
Poster: Automated Security Property Extraction From Protocol Specifications

Hassan Asghar[†], Myeong-Ha Hwang[‡], Jeonghyun Joo[‡], Heewoon Kang[‡], YooJin Kwon[‡],
Kazi Samin Mubasshir[§], Imtiaz Karim[¶], Elisa Bertino[§], Hyunwoo Lee[†]
[†]KENTECH, [‡]KEPRI, [§]Purdue University, [¶]The University of Texas at Dallas

MOTIVATION

Security property extraction is:



This motivates automation of property extraction from natural language specifications.

CHALLENGES & SOLUTIONS

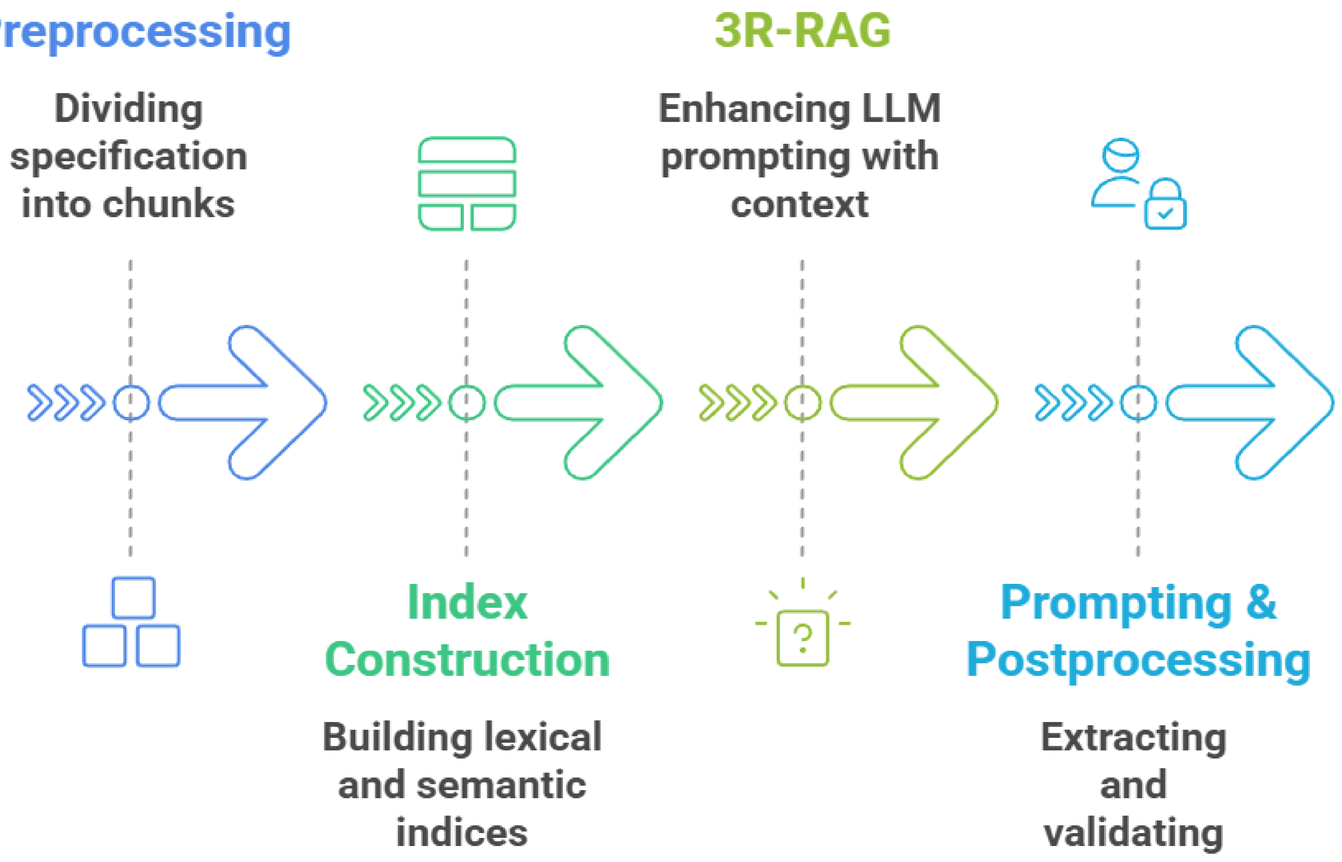
Automating this step is challenging due to the following three reasons:

Challenges	Description	Addressing Challenges (GOALS)
C1: Scalability	Specifications are lengthy, making security details hard to extract.	Targeted filtering excludes irrelevant content.
C2: Heterogeneity	Domain-specific vocabulary hinders automated comprehension.	Domain-specific prompts ensure accurate interpretation.
C3: Implicitness	Security properties are often implied or informally stated.	CoT prompting guides the LLM to reason explicitly.

Guided by these goals, we propose SPARTA, a framework that automatically extracts useful security properties from network specifications by leveraging LLMs and a 3R-RAG pipeline.

APPROACH

We propose a systematic pipeline, SPARTA, that processes specifications, retrieves and structures knowledge, and extracts validated security properties.



EXAMPLE PROMPT TEMPLATE

Security Properties Generation Prompt

Extract Security Properties List **only those lines** that imply or define security properties. *Avoid paraphrasing*. **Reference Example:**
Context:

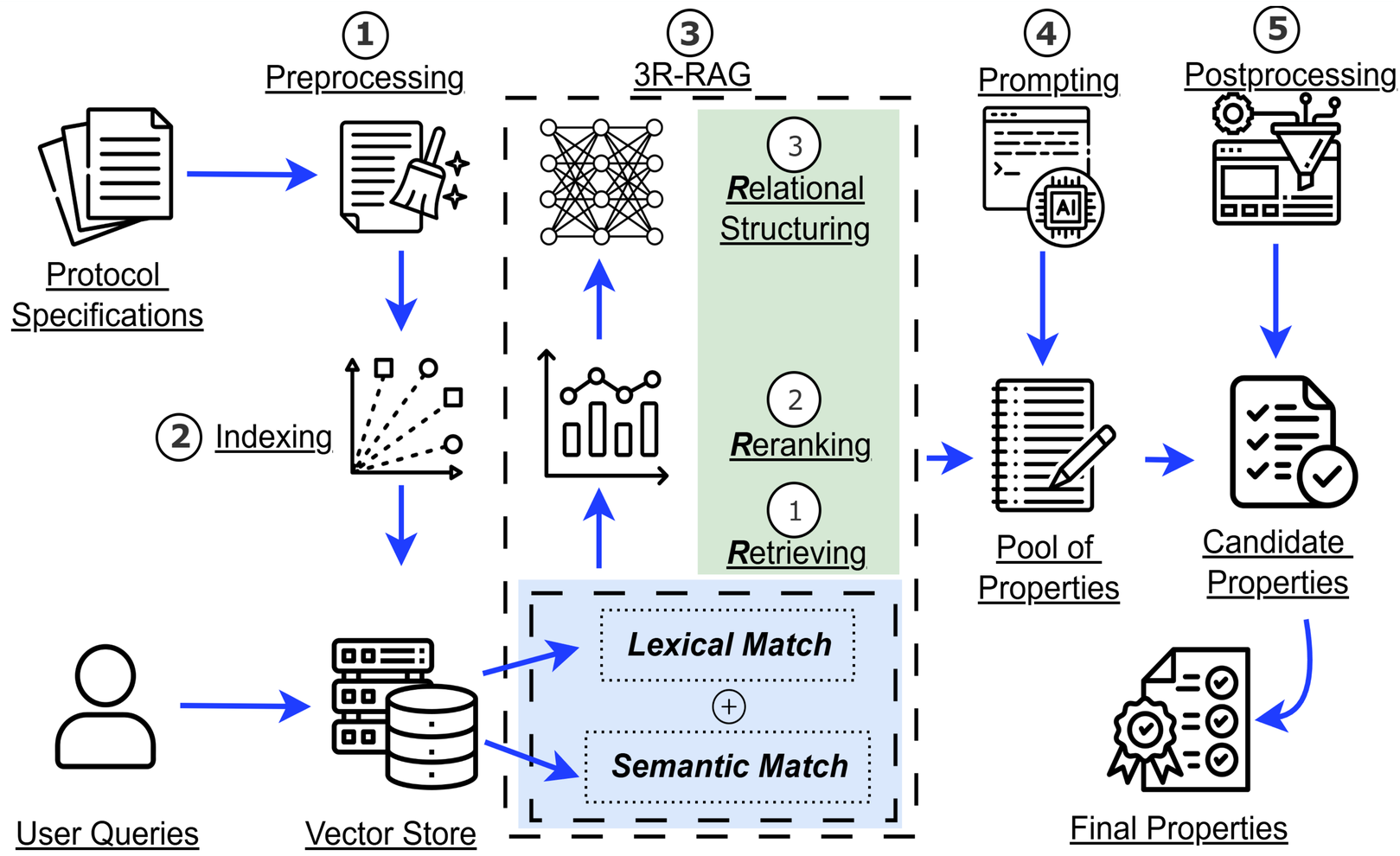
> "If a client PUTs or POSTs a resource to a server containing attributes or elements that instead are to be populated by the server (e.g., href), the server SHALL return an HTTP 400 error..."

Step-by-step Reasoning:
- **Entities:** client, server, resource, href, HTTP method, ACL...
- **Relationships:**
  - client submits → server verifies → may reject
  - method authorization → validated by ACL
- **Evaluation:** "SHALL" indicates a security requirement (validation, authorization logic)

Extracted Security Properties:
1) "If a client PUTs or POSTs a resource... SHALL return an HTTP 400 error."
2) "The HTTP method of an incoming request is checked..."
3) "Authorization is granted if Method, AuthType, and DeviceType are TRUE..."

Instruction: Now apply this process to the given context: **Context:** `<CONTEXT_CHUNK>` **Step-by-step Reasoning: Extracted Security Properties:**

SPARTA FRAMEWORK



FINDINGS & FUTURE WORK

- **Our plans include extending SPARTA to extract implicit properties, systematically aligning formal model properties with their informal counterparts in the specifications, and extending the approach to other protocol specifications (e.g., TLS 1.3 and MQTT).**

Acknowledgement: This work was supported by project R23IA01, "Development of the Information Model Management and Certification System."