2nd INTERNATIONAL CONFERENCE ON
Artificial Intelligence
31 May - 1 June 2026

IICAI
Second International Interdisciplinary Conference on Artificial Intelligence

An Automated Modular Framework for MITRE ATT&CK Mapping

Alireza Katani
M.Sc. Graduate in Computer Engineering
a.katani@ec.iut.ac.ir

Abstract

Tagging cybersecurity artifacts with MITRE ATT&CK techniques—across diverse textual sources such as logs, detection rules, attack descriptions, adversarial procedures, and technique-specific defensive strategies—is fundamentally an analytical and knowledge-intensive task. Given the continuous large-scale generation of such security texts, manual mapping imposes significant time and operational costs on security analysts and engineers. In this study, we propose a modular automated framework that leverages a fine-tuned lightweight large language model (LLM) in combination with a Retrieval-Augmented Generation (RAG) module to perform intelligent MITRE ATT&CK tagging. The proposed approach reduces human workload, improves consistency in technique identification, and enables scalable, organization-deployable automation of security analysis workflows

Research Method

- Fine-tune a lightweight LLM (PHI-3.5 Mini) for MITRE ATT&CK technique tagging.
- Preprocess and structure diverse cybersecurity datasets (Splunk ES, MITRE datasets, Sysmon, Elastic rules, Hugging Face datasets).
- Integrate a Retrieval-Augmented Generation (RAG) module to provide domain-specific context.
- Encode inputs and MITRE techniques using ATT&CK-BERT embeddings.
- Apply Few-Shot prompting to handle underrepresented patterns.
- Evaluate model performance using a two-stage process: RAG-only retrieval and RAG + fine-tuned LLM inference.
- Use standard classification metrics (Weighted Precision, Recall, F1, and Accuracy) to assess technique tagging.

Conclusion

- This research addresses the limitations of manual and rule-based MITRE ATT&CK tagging in large-scale security environments.
- The proposed lightweight LLM + RAG framework enables automated, scalable, and semantically aware technique mapping.
- Beyond technique identification, the model provides contextual explanations and supplementary attack insights, supporting informed decision-making by security analysts.
- The system eliminates the need for manual mapping and rigid rule-based approaches while maintaining high adaptability.
- Due to its lightweight architecture and OS-level security awareness (PHI-3.5), the model can be deployed locally within organizations, preserving data privacy.
- The embedded operating system knowledge also assists experts in troubleshooting cases where alerts originate from misconfigurations rather than real attacks.

The Purpose Of The Research

Problems:

- Traditional mapping of security events to MITRE ATT&CK is manual, time-consuming, and costly.
- Current methods rely on expert interpretation and rigid rules, limiting adaptability to new logs and attack patterns.Unstructured data, such as raw logs and incident reports, are often underutilized.

Proposed Solution:

- Develop an automated, intelligent framework using semantic analysis and LLM/RAG methods to efficiently map diverse security data to MITRE ATT&CK techniques, reducing analyst workload and improving coverage.

Practical Results

- Evaluated on 367 MITRE ATT&CK techniques, with at least 3 distinct examples per technique, using attacker-centric ART rules.
- RAG module: 255 events/sec; LLM + RAG: 6 events/sec with better accuracy.
- Higher precision, recall, F1, and accuracy vs. CyberBench LLaMA models.
- Outperforms RAM; keeps data internal, no external services needed.
- Covers diverse sources: logs, rules, attack procedures.
- Provides consistent and automated MITRE technique tagging, reducing analyst workload and manual effort.

References

[1] MITRE, “ATT&CK Framework,” 2024.

[2] Red Canary, “Atomic Red Team,” 2024.

[3] Microsoft, “Phi-3 Technical Report,” 2024.

[4] Elastic, “Detection Rules,” 2024.

[5] H. C. Nguyen, “CTI-to-MITRE Dataset,” 2024. [Online]. Available: https://huggingface.co/dattaraj/security-attacks-MITRE