KG4TI: A Knowledge Graph Approach to Strengthening Threat Intelligence

March 13, 2025

Abstract

The cybersecurity infrastructure faces increasing sophistication in cyber threats, requiring advanced approaches for detection and mitigation. Traditional rule-based threat intelligence systems are inadequate due to the dynamic nature of cyber threats. This study introduces a Knowledge Graph (KG)-based approach leveraging Neo4j for modeling and analyzing cyber threats. The framework integrates multiple data sources, such as threat reports and Indicators of Compromise (IOCs), into a structured graph database, improving threat intelligence and proactive cybersecurity strategies.

Keywords: Threat Intelligence, Knowledge Graph, Entity Extraction, Entity Linking

1 Introduction

Cyber threats are becoming increasingly complex, requiring advanced methodologies for detection and mitigation.[3] Traditional security models rely on static rule-based systems that struggle to handle dynamic attack patterns. [1] Knowledge Graphs (KGs) offer a structured way to represent cybersecurity relationships, improving threat detection, actor profiling, and anomaly identification.[2] This study focuses on applying KG technology to enhance cybersecurity frameworks.[6] Several studies have explored the use of Knowledge Graphs in cybersecurity. The very latest papers from other researchers are being referenced in the course of this work, such as Mishra et al. [4] integrated PageRank with Large Language Models (LLMs) to update Security Knowledge Graphs dynamically. Mouiche and Saad [5] applied NLP techniques to extract entities from threat intelligence. However, there is limited research focusing on localized cybersecurity applications. This study addresses this gap by creating a threat intelligence Knowledge Graph. The major contribution of this work is stated here:
-Acquiring data to develop a Knowledge Graph for Cyber Threat Intelligence.
-Integration of multiple data sources into a unified threat intelligence framework.
-Application of entity extraction and graph analytics to identify relationships

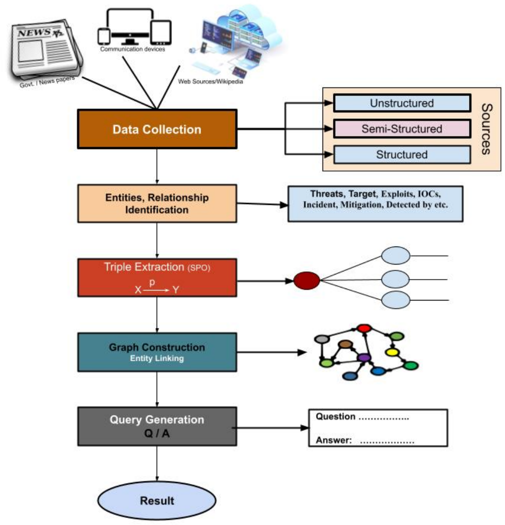

Figure 1: KG4TI Proposed Methodology

between cyber threats.
-Utilization of Neo4j for scalable threat detection and intelligence sharing.

2 Methodology

Data Collection: Sources include threat intelligence feeds, vulnerability databases, incident reports, and open source intelligence (OSINT). Data pre-processing involves cleaning and structuring raw cybersecurity data. Figure 1 has presented the proposed methodology to construct Knowledge Graph for Threat Intelligence.
Entity and Relationship Extraction: Entities such as threat actors, malware, vulnerabilities, and attack patterns are extracted. Relationships are modeled as subject-predicate-object triples (e.g., Threat Actor → targets → Banking Sector).
Graph Construction: Neo4j is used to construct the KG, representing the entities and relationships of cybersecurity. Querying and visualization provide information on attack patterns and threat actor behavior.

3 Results

A total of 300 entities and 500 relationships have been modeled in the Knowledge Graph. The constructed graph responds successfully to 85% of security queries accurately. Approximately 40% of these correct responses contain insights that are not readily available on search engines such as Google. Improved

Table 1: Entities, Relations and Triple Examples

Entities	Relationships	Triple Generation Examples.
ThreatActor	TARGETS (from ThreatActor to Organization)	Threat Actor → "targets" → Banking Sector
Incident	RESPONDS TO (from Organization to Incident)	Malware → "detected by" → Antivirus Software
Location	OCCURRED IN (from Incident to Location)	Threat Actor → "associated with" → Cybercrime Group
AttackType	CONDUCTED (from ThreatActor to Incident)	APT28 → Responsible For → 2016 U.S. Election Hacking
Mitigation	MITIGATED BY (from Vulnerability to Mitigation)	SQL Injection → Mitigated by → Regular Software Updates.

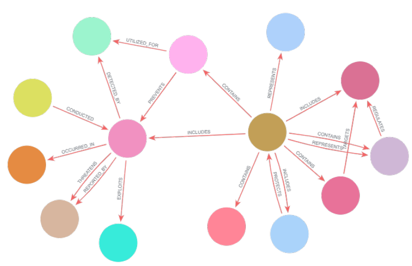

Figure 2: Graph Construction

Table 2: Query Generation

No	Queries	Answers
1	What are the main cyber threats in 2025?	Malware / Ransomware
2	Who are the major threat actors ?	Hacktivists / Insider Threats / Cybercriminal Groups
3	What is the impact of financial fraud on Nigeria's economy?	GDP Loss
4	What industries are prime targets for cybercriminals?	Financial Institution

situational awareness through structured threat intelligence. Enhanced detection of emerging cyber threats by linking disparate data sources. Faster and more effective cybersecurity responses using graph analytics. Visualization of cyber threat actors and their attack patterns.

4 Conclusion

This study demonstrates the effectiveness of Knowledge Graphs in cybersecurity threat intelligence. By integrating diverse threat intelligence sources, KGs offer a structured, scalable, and real-time analysis framework. Future work will focus on real-time threat detection and integration with global threat intelligence frameworks such as MITRE ATT&CK.

References

[1] Bin Chen, Hongyi Li, Di Zhao, Yitang Yang, and Chengwei Pan. Quality assessment of cyber threat intelligence knowledge graph based on adaptive joining of embedding model. *Complex & Intelligent Systems*, 11(1):1–14, 2025.

[2] Paolo Falcarin and Fabio Dainese. Building a cybersecurity knowledge graph with cybergraph. In *Proceedings of the 2024 ACM/IEEE 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) and 2024 IEEE/ACM Second International Workshop on Software Vulnerability*, pages 29–36, 2024.

[3] Romy Fieblinger, Md Tanvirul Alam, and Nidhi Rastogi. Actionable cyber threat intelligence using knowledge graphs and large language models. In *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 100–111. IEEE, 2024.

[4] Chinmaya Mishra, Himangshu Sarma, and M Saravanan. Pagellm: Incremental approach for updating a security knowledge graph by using page

ranking and large language model. *Information Processing & Management*, 62(3):104045, 2025.

[5] Inoussa Mouiche and Sherif Saad. Entity and relation extractions for threat intelligence knowledge graphs. *Computers & Security*, 148:104120, 2025.

[6] Jian Wang, Tiantian Zhu, Chunlin Xiong, and Yan Chen. Multikg: Multi-source threat intelligence aggregation for high-quality knowledge graph representation of attack techniques. *arXiv preprint arXiv:2411.08359*, 2024.