Knowledge Graph for Threat Intelligence:

KG4TI : A Knowledge Graph Approach to Strengthening Threat Intelligence in Nigeria

Emmanuel Innocent Umoh, Sanju Tiwari, Kusum Lata

Sharda University, Greater Noida, UP. India.

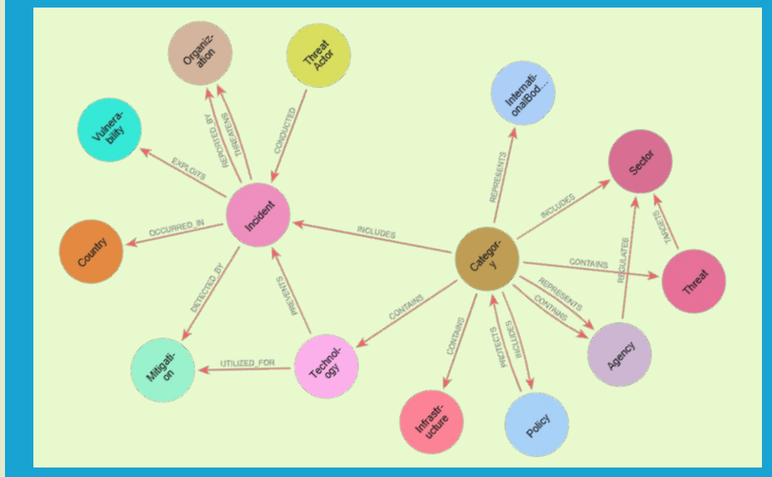
Introduction

The research introduces the increasing sophistication of cyber threats in Nigeria, emphasizing the need for advanced detection and mitigation strategies. Traditional rule-based cybersecurity methods are no longer sufficient to handle the dynamic nature of modern cyber threats. As a solution, the study proposes a Knowledge Graph (KG) approach, leveraging Neo4j, a graph database designed to represent and analyze cyber threat data more effectively.

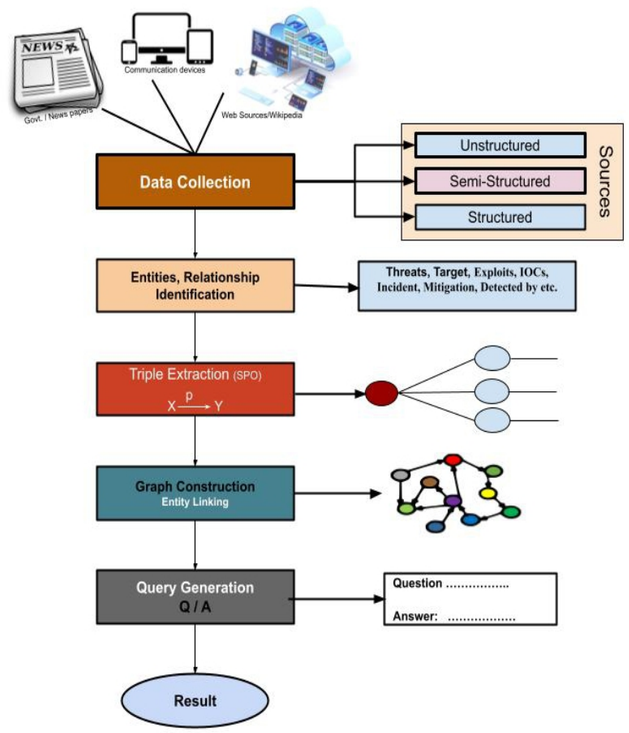
Purpose

The primary objective of this research is to develop a Nigeria-centric Knowledge Graph for Threat Intelligence (KG4TI). This system aims to enhance situational awareness and improve decision-making in Nigeria's cybersecurity landscape. By integrating various sources of cyber threat intelligence into a single, dynamic framework, the study seeks to address the limitations of existing fragmented and static cybersecurity systems.

No	Queries	Answers
1	What are the main cyber threats facing Nigeria?	Malware
2	Who are the major threat actors in Nigeria?	Cybercriminals
3	What sectors in Nigeria are most vulnerable to cyberattacks?	Finance
4	What is the impact of financial fraud on Nigeria's economy?	GDP Loss
5	How does the Nigerian government track cybercriminals?	Surveillance
6	What types of cyberattacks are common in Nigeria?	Phishing / Social Engineering
7	What role does social engineering play in Nigerian cybercrime?	Manipulation
8	What preventive measures are used against cyber threats in Nigeria?	Firewalls
9	What laws regulate cybersecurity in Nigeria?	Cybercrime Act
10	What cybersecurity agencies operate in Nigeria?	NITDA /
11	How do Nigerian businesses protect against ransomware?	Backups
12	What are the major hacking groups in Nigeria?	Anonymous / OpNigeria
13	How does cybercrime impact Nigerian banks?	Fraud / Losses



KG4TI Proposed Methodology



Methodology

The study outlines a structured approach to constructing the knowledge graph. It begins with data collection from multiple sources, including regulatory reports, threat feeds, and social media. The extracted data is then structured into subject-predicate-object triples, which are stored and processed using Neo4j. By applying graph analytics, relationships between cyber threats, vulnerabilities, and attack vectors are visualized, providing deeper insights for threat detection and mitigation.

Graph Construction

The Knowledge Graph is built using Neo4j, mapping relationships between cyber threats, actors, and vulnerabilities. The graph structure enables better analysis of attack patterns and facilitates predictive threat intelligence. The construction process also integrates multiple cybersecurity data sources, enhancing the accuracy and relevance of Nigeria's cyber threat analysis.

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
Vulnerability	ASSOCIATED WITH (from Incident to Vulnerability)	Malware → "exploits" → Vulnerability
Location	OCCURRED IN (from Incident to Location)	Threat Actor → "associated with" → Cybercrime Group

Result

The implementation of KG4TI has shown promising results in identifying cyber threats, their sources, and affected sectors in Nigeria. The structured representation of threat actors, attack types, and vulnerabilities has improved the accuracy of cybersecurity analysis and decision-making processes.

Conclusion

It demonstrates how a structured and interconnected threat intelligence system can offer better situational awareness and proactive cybersecurity measures. However, challenges such as data quality, integration complexities, and compliance with cybersecurity regulations must be addressed to ensure the effective adoption of the KG4TI framework.