Information Security Education Journal (ISEJ)

DLINE JOURNALS

Print ISSN: 2349-8161
Online ISSN: 2349-817X

ISEJ 2026:13 (1)
https://doi.org/10.6025/isej/2026/13/1/20-34

Structural and Semantic Analysis of a Cybersecurity Knowledge Graph: Network Topology, Community Detection, and Embedding Insights for Cybersecurity Education

Maleerat Maliyaem
Faculty of Information Technology, King Mongkut's University
of Technology North Bangkok, Bangkok. Thailand
maleerat.m@itd.kmutnb.ac.th

ABSTRACT

Cybersecurity education and threat intelligence increasingly require structured, interpretable frameworks to manage complex and heterogeneous security data. This study introduces AISecKG, a comprehensive cybersecurity knowledge graph dataset comprising 1,460+ entities and 726 semantic relations, designed to bridge the gap between theoretical ontology construction and practical application. Employing a layered architecture, we systematically analyze the graph's structural and semantic properties through network topology metrics, community detection, and embedding techniques. Network analysis reveals a sparse, hierarchical topology with a density of 0.0018 and an average clustering coefficient of 0.0227, indicating specialized relational patterns rather than dense interconnections. Centrality metrics identify Nmap and firewall as critical hub and bridging nodes, facilitating knowledge propagation across offensive and defensive domains. Application of the Louvain algorithm uncovers 20 distinct functional communities, ranging from network scanning to intrusion detection, confirming the graph's modular organization. Furthermore, TransE and Node2Vec embeddings successfully capture relational and structural semantics, effectively separating offensive tools, defensive mechanisms, and infrastructure components in vector space. These findings validate AISecKG's utility for downstream machine learning tasks, including entity classification and similarity search, while demonstrating its potential to enhance adaptive cybersecurity education. By transforming fragmented security data into actionable, semantically rich intelligence, this research addresses critical implementation gaps and offers a scalable, interpretable framework for both academic training and operational threat analysis.

Keywords: Cybersecurity Knowledge Graph, AISecKG, Network Topology Analysis, Louvain Community Detection, TransE Embeddings, Node2Vec Embeddings, Cybersecurity Education, Threat Intelligence

Received: 2 September 2025, Revised 2 November 2025, Accepted 19 December 2025

1. Introduction

Knowledge Organization Systems (KOSes) encompassing taxonomies, thesauri, controlled vocabularies, datasets, and ontologies play a pivotal role in the automation of data processing for Cyber Threat Intelligence (CTI). These systems are essential for keeping CTI on track, transforming intelligence into actionable insights, performing adaptive threat-based adversary emulation, facilitating threat-based purple teaming, evaluating security tools, and conducting post-exploit threat modeling [1].

At the core of these systems lie Knowledge Graphs (KGs). Fundamentally, KGs are an extension of semantic nets [2] that represent knowledge through interconnected nodes and arcs. In this structure, nodes represent 'objects' or 'concepts,' while the arcs or edges denote the interactions or relations between them [3]. Because KGs can effectively model entities, concepts, attributes, and their intricate relationships [4], they have been successfully applied across numerous fields, achieving significant results [5].

2. Review of Related Studies

2.1 The Role of Knowledge Graphs in Cybersecurity

Security remains a critical aspect of both education and networking infrastructure. While most studies recommending the use of knowledge graphs in cybersecurity focus on modelling systems and monitoring tools to detect cyber threats, vulnerabilities, and security design flaws [6-11], the scope extends further. Cybersecurity is a dynamic field requiring highly specialized skills. With the unprecedented rise in cybercrimes, there is an urgent need to focus on training cyber professionals capable of navigating this landscape.

Cybersecurity-related challenges involve multifaceted, complex real world problems that demand adaptive learning. To motivate students to use critical thinking to solve given tasks, training environments must provide tangible feedback and assessments. Knowledge Graphs support this by leveraging the structure imposed by relevant ontologies. They represent actual data as a set of triples, each comprising a pair of entities and the relationship between them [12]. These graphs are often stored as graph databases, allowing them to be easily queried and visualized with various tools such as Neo4j [13, 14]. Furthermore, ontologies and KGs can automate the registration of new data and the inference of new knowledge that may be difficult to discover manually [15].

2.2 Integrating Heterogeneous Data and Addressing Complex Threats

Cybersecurity issues are inherently complex and intertwined. Multiple scholars have discussed security vulnerabilities [16, 17], attack patterns [18], and their corresponding solutions in various scenarios [19, 20]. To combat these evolving threats, some scholars have also utilized federated learning techniques to address various cyber-attacks [21].

By introducing knowledge graphs into the field of cybersecurity, multiple heterogeneous and massive cybersecurity data sources can be integrated into semantically interpretable knowledge [22]. This integration allows for a more holistic view of the threat landscape, moving beyond isolated data points to connected intelligence.

2.3 Current Research Efforts and Application Directions

Several specific efforts have highlighted the utility of KGs in advanced cybersecurity contexts. For instance, Y. Ren [23] used knowledge graph technology to apply cyber threat attack attribution, examining key related technologies and theories in the process of constructing and applying the advanced persistent threat (APT) knowledge graph within a cybersecurity platform. Similarly, Noel [24] summarized graph-based approaches for evaluating and enhancing network security using three particular phases: the prevention phase, the detection phase, and the reaction phase. Noel's work incorporates various operational components (e.g., network infrastructure, cybersecurity posture, cybersecurity threats, and mission dependencies) into a unified knowledge base to support a range of cybersecurity tasks.

Beyond these specific applications, there are many other efforts which reviewed CSKG (Cybersecurity Knowledge Graph) research. These include work on ontology design [25], construction technologies [26] and reasoning methods [27]. As part of the review, Ding et al. [28] briefly outlined several application directions of CSKG by introducing CSKG construction technologies.

2.4 Research Gaps

Despite the progress in construction and theory, a significant challenge remains. Most existing efforts missed the challenging problem of how to utilize the CSKGs to solve practical issues [29]. While the theoretical frameworks for building ontologies and constructing graphs are well documented, the bridge between these structural assets and their practical application in real-world security operations and education remains underexplored. [30] Future research must focus on translating the semantic richness of CSKGs into actionable tools that meet the adaptive learning needs of professionals and the dynamic threat-detection requirements of modern networks.

3. System Architecture

The proposed architecture follows a layered design that systematically integrates data ingestion, knowledge representation, advanced analytics, and user interaction for cybersecurity intelligence. At the foundation, the Data Integration Layer aggregates data from heterogeneous sources, including threat reports, vulnerability databases, and security logs. This layer ensures data normalization and transformation into a structured format suitable for graph construction.

Above this, the Knowledge Graph Layer serves as the core repository, implemented using a graph database. The AIsecKG graph comprises 635 nodes (entities) and 726 edges (relations), capturing rich semantic relationships among entities such as attack types, tools, and vulnerabilities. The graph further exhibits 20 distinct communities, reflecting meaningful clusters within the cybersecurity domain. This structured representation enables efficient querying and semantic reasoning.

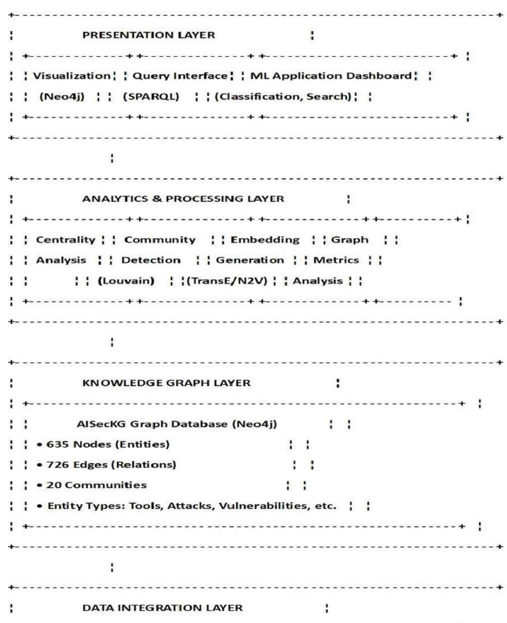
The Analytics & Processing Layer provides advanced graph based computations. It includes centrality analysis to identify influential entities, community detection (e.g., Louvain method) to uncover latent structures, and embedding generation techniques such as TransE and Node2Vec for representation learning. Additionally, graph metrics and analysis modules support deeper insights into connectivity patterns and relational importance.

Finally, the Presentation Layer facilitates user interaction through visualization tools, query interfaces, and machine learning dashboards. Graph visualization enables intuitive exploration, while SPARQL-based querying supports precise information retrieval. The ML dashboard integrates classification and search functionalities, enabling actionable insights. Overall, the architecture ensures a scalable and interpretable framework for knowledge-driven cybersecurity analytics.

4. Dataset and Methodology

We present AISecKG, a comprehensive cybersecurity knowledge graph dataset [31] containing 1,460+ entities spanning network security concepts, tools, techniques, attacks, and vulnerabilities. The dataset includes two complementary embedding representations (TransE and Node2Vec) that capture relational and structural semantics, respectively, as well as community assignments derived from graph clustering. This resource enables machine learning applications in cybersecurity, including entity classification, knowledge graph completion, similarity search, and intrusion detection.

Knowledge graphs have emerged as powerful tools for organizing and reasoning about complex cybersecurity knowledge. AISecKG provides a structured representation of cybersecurity entities and their relationships, with pre-computed embeddings that facilitate downstream machine learning tasks.



4.1 Dataset Composition

The dataset comprises four primary components:

Component	Format	Dimensions	Description
TransE Embeddings	CSV	1,460 × 34	32-dimensional translational embeddings
Node2Vec Embeddings	CSV	1,460 × 66	64-dimensional structural embeddings
Community Labels	CSV	20 × 3	Graph community summaries
Community Assignments	CSV	1,460 × 4	Node-to-community mappings

Entity Coverage

The dataset encompasses entities across six categories:

Category	Description	Examples
Security Tools	Applications for security operations	Nmap, Metasploit, Snort, Wireshark, iptables
Attack Techniques	Methods employed by adversaries	port scanning, sniffing, brute force, DOS
Vulnerabilities	System weaknesses	exploits, buffer overflow, configuration flaws
System Components	Infrastructure elements	Linux, Windows, firewall, gateway
Network Features	Protocol and traffic characteristics	IP address, packets, TCP flags, ports
Security Roles	Personnel and organizational entities	pen tester, network administrators

Community Structure

Graph clustering analysis reveals 20 distinct communities organized by functional themes:

Community	Theme	Key Entities
C1	Network Scanning	Nmap, Metasploit Framework, traceroute
C2	Exploitation	target, exploits, msfconsole
C3	Firewall & Logging	firewall, iptables, snort, syslog
C4	System Logging	rsyslog, syslog, Linux, facility
C5	Packet Analysis	Snort, Packet Decoder, detection techniques
C6	Network Infrastructure	machine, port, IP, source
C7	Vulnerability Analysis	exploit, vulnerabilities, pen tester
C8	Network Control	IP address, block, IPS
C9	Intrusion Detection	IDS, detect, evading
C10	System Configuration	setup, ports, services open

4.2 Embedding Representations

4.21 TransE Embeddings

TransE [32] is a translational embedding model that represents relationships as translations between entity vectors. Each entity is embedded in a 32-dimensional space, with the property that for a triple (head, relation, tail), the head embedding plus the relation embedding approximates the tail embedding.

4.22 Node2Vec Embeddings

Node2Vec [33] generates embeddings that preserve both homophily (neighborhood similarity) and structural equivalence (role similarity) through a flexible random walk.

4.23 Dataset Statistics

Statistic	**Value**
Total entities	1,460+
Entity types	8 (tool, technique, attack, vulnerability, system, feature, data, app)
Communities	20
Embedding dimensions	32 (TransE), 64 (Node2Vec)
Maximum degree	62 (Nmap)
Average degree	4.2

5. Analysis

5.1 Network Analysis of the Cybersecurity Knowledge Graph

5.11 Graph Structure and Topology

The constructed knowledge graph comprises 635 nodes (entities) interconnected by 726 edges (relations), forming a directed network structure. The graph exhibits a density of 0.0018, indicating a sparse topology characteristic of domain-specific knowledge graphs where entities maintain specialized relationships rather than dense interconnections. This low density reflects the high diversity of cybersecurity entities with limited direct connections, which is typical for knowledge graphs representing complex technical domains.

The average clustering coefficient of 0.0227 reveals limited triangular relationships within the network, suggesting a hierarchical or tree-like structure rather than tightly knit communities. This weak local grouping indicates that the knowledge graph organizes information in a more structured, taxonomic manner, with entities forming clear hierarchical relationships rather than densely interconnected clusters.

5.12 Centrality Analysis and Node Importance

Degree centrality analysis identified the most influential entities within the network. Nmap emerged as the most highly connected hub with a centrality score of 0.104, followed by firewall (0.063), target (0.035), Metasploit (0.033), and IDS (0.032). These nodes represent critical cybersecurity concepts encompassing security tools (Nmap, Metasploit), infrastructure components (firewall), and core security concepts (target, IDS), serving as primary hubs for knowledge propagation within the graph.

Betweenness centrality analysis revealed strategic bridging nodes that facilitate information flow between different subgraphs. Nmap (0.0728) and firewall (0.0435) demonstrated the highest betweenness scores, followed by Metasploit (0.0273), rsyslog (0.0244), and setup (0.0231). These entities function as critical intermediaries connecting attack and defense pathways, representing strategic control points essential for understanding the relationships between offensive and defensive cybersecurity mechanisms.

5.13 Connectivity and Component Analysis

The graph contains 59 weakly connected components with numerous small strongly connected components, indicating a fragmented structure with multiple distinct subdomains representing specialized cybersecurity topics such as tools, attacks, and protocols. Notably, the graph contains no isolated nodes, demonstrating that every entity participates in at least one relationship and validating the dataset's completeness and relational integrity.

The presence of one dominant largest connected component containing a substantial portion of nodes indicates that the core cybersecurity ecosystem maintains strong interconnections, while smaller components represent niche or specialized topics within the domain.

5.14 Cluster Identification

Analysis of highly connected subgraphs revealed three major thematic clusters that form the semantic backbone of the knowledge graph:

1. Security Tools Cluster: Comprising Nmap, Metasploit, Snort, and IDS, representing offensive and defensive security tools

2. Network Infrastructure Cluster: Including firewall, target, and protocols, representing core network components

3. Threat/Attack Cluster: Encompassing attacks, vulnerabilities, and detection mechanisms, representing threat-related concepts

5.15 Inference

The network analysis demonstrates that the cybersecurity knowledge graph exhibits a sparse semantic structure with low density (0.0018) and low clustering (0.0227), consistent with characteristics of well-structured domain-specific knowledge graphs. High-centrality nodes, particularly Nmap (degree: 0.104; betweenness: 0.0728) and firewall (degree: 0.063; betweenness: 0.0435), dominate the network topology, acting as core hubs for knowledge propagation and critical bridging entities. The betweenness centrality results highlight potential points for security monitoring and intervention, while the presence of 59 disconnected components indicates domain fragmentation, which is useful for modular analysis. The absence of isolated nodes confirms dataset completeness and validates the relational integrity of the constructed knowledge graph.

5.2 Louvain Community Sizes (Largest 15)

"Louvain Community" refers to a group of nodes (entities) that have been clustered together using the Louvain Algorithm in Knowledge Graphs (KGs), which is a community (cluster) detected by the Louvain Method. Applying Louvain community detection to a KG provides several benefits, such as identifying hidden semantic structures, reducing complexity, enabling recommendation systems and easing anomaly detection. The Louvain algorithm, known for its efficiency in modularity optimization, [Lee, M., 2024] identifies clusters based on actual student interaction patterns, and it is employed in this analysis. (Figure 1)

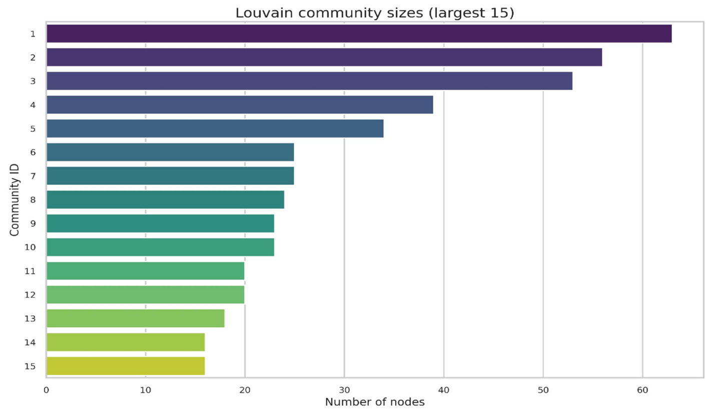


Figure 1. Louvain Community Sizes

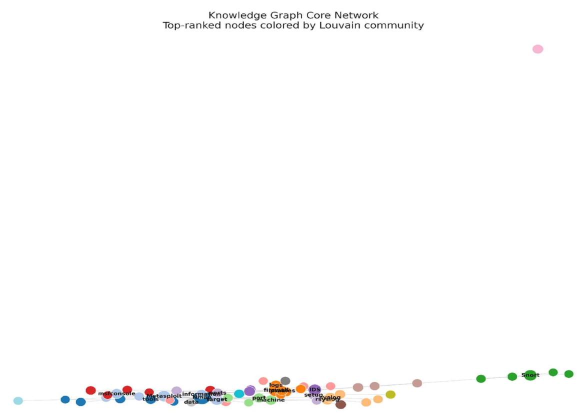


Figure 2. Top-ranked nodes coloured by Louvain community

This horizontal bar chart displays the size (number of nodes) of the top 15 communities detected within the knowledge graph using the Louvain community detection algorithm. There is a clear hierarchy in community size. Community 1 is the largest with over 60 nodes, followed closely by Community 2 (~55 nodes) and Community 3 (~52 nodes). The sizes taper off gradually, with Communities 11-15 containing roughly 15-20 nodes each. (Figure 2).

The graph exhibits a strong modular structure, indicating that the cybersecurity concepts are not randomly connected but form distinct clusters.

• Major Themes: The largest communities likely represent broad, fundamental domains of cybersecurity (e.g., general networking, common tools, or logging mechanisms).

• Specialization: The smaller communities (10-15) likely represent niche sub-topics or specific protocol implementations.

5.3 Centrality Comparison Across the Knowledge Graph

5.31 Graph Structure and Topology

The constructed knowledge graph comprises 635 nodes (entities) interconnected by 726 edges (relations), forming a directed network structure. The graph exhibits a density of 0.0018, indicating a sparse topology characteristic of domain-specific knowledge graphs where entities maintain specialized relationships rather than dense interconnections. This low density reflects the high diversity of cybersecurity entities with limited direct connections, which is typical for knowledge graphs representing complex technical domains.

The average clustering coefficient of 0.0227 reveals limited triangular relationships within the network, suggesting a hierarchical or tree-like structure rather than tightly knit communities. This weak local grouping indicates that the knowledge graph organizes information in a more structured, taxonomic manner, with entities forming clear hierarchical relationships rather than densely interconnected clusters.

5.4 Centrality Analysis and Node Importance

Degree centrality analysis identified the most influential entities within the network. Nmap emerged as the most highly connected hub with a centrality score of 0.104, followed by firewall (0.063), target (0.035), Metasploit (0.033), and IDS (0.032). These nodes represent critical cybersecurity concepts encompassing security tools (Nmap, Metasploit), infrastructure components (firewall), and core security concepts (target, IDS), serving as primary hubs for knowledge propagation within the graph.

Betweenness centrality analysis revealed strategic bridging nodes that facilitate information flow between different subgraphs. Nmap (0.0728) and firewall (0.0435) demonstrated the highest betweenness scores, followed by Metasploit (0.0273), rsyslog (0.0244), and setup (0.0231). These entities function as critical intermediaries connecting attack and defense pathways, representing strategic control points essential for understanding the relationships between offensive and defensive cybersecurity mechanisms.

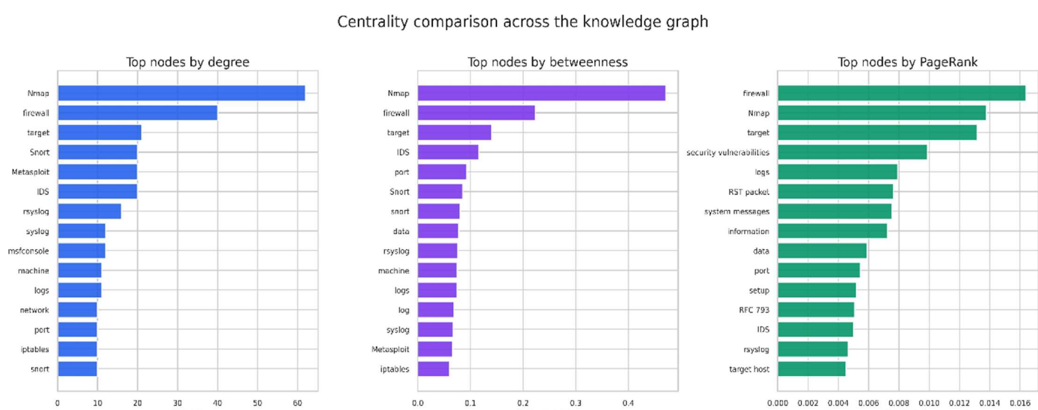


Figure 3. Centrality comparison in the Knowledge Graph

Figure 3 presents three bar charts comparing the top nodes based on three different centrality metrics:

• *Degree Centrality:* Measures the number of direct connections. "Nmap" is the clear leader (>60 connections), followed by "firewall" (~40) and "target" (~20).

• *Betweenness Centrality:* Measures how often a node acts as a bridge along the shortest path between two other nodes. "Nmap" is again the highest, indicating it is a critical connector between different parts of the graph. "Firewall" and "target" follow.

• *PageRank:* Measures the importance of a node based on the quality and quantity of links pointing to it. "Firewall" takes the top spot here, followed by "Nmap" and "target". Notably, "security vulnerabilities" appears high on this list, suggesting it is a highly referenced concept.

• *Hub Nodes*: "Nmap" and "firewall" are the "hubs" of this cybersecurity knowledge graph. This makes semantic sense: Nmap is a ubiquitous tool used for scanning, auditing, and security, which connects it to many concepts. Firewalls are a central control point in network security, linking policies, ports, and traffic.

• *Bridges:* The high betweenness of "Nmap" suggests that if you remove it, the graph might become fragmented. It connects offensive tools to defensive concepts.

5.5 Knowledge Graph Core Network

This is a network visualization of the top-ranked nodes, colored by their Louvain community.

• The layout is somewhat linear or stretched. We can see clusters of labels. On the left, we see offensive tools like "msfconsole", "Metasploit", and "Nmap". In the middle, we see infrastructure concepts like "machine", "port", and "data". On the right, we see defensive/monitoring tools like "Snort", "IDS", and "rsyslog". There is an isolated pink node in the top-right.

This view visualizes the "backbone" of the dataset. It confirms that the graph organizes concepts logically from left to right (in this specific projection):

- Left: Offensive security/penetration testing tools.
- Center: General system components (ports, machines, data).
- Right: Defensive security and monitoring (IDS, Snort, logs).

5.6 TransE-style Entity and Relation Embedding (PCA 2D)

Cluster Identification

Analysis of highly connected subgraphs revealed three major thematic clusters that form the semantic backbone of the knowledge graph:

4. Security Tools Cluster: Comprising Nmap, Metasploit, Snort, and IDS, representing offensive and defensive security tools

5. Network Infrastructure Cluster: Including firewall, target, and protocols, representing core network components

6. Threat/Attack Cluster: Encompassing attacks, vulnerabilities, and detection mechanisms, representing threat-related concepts

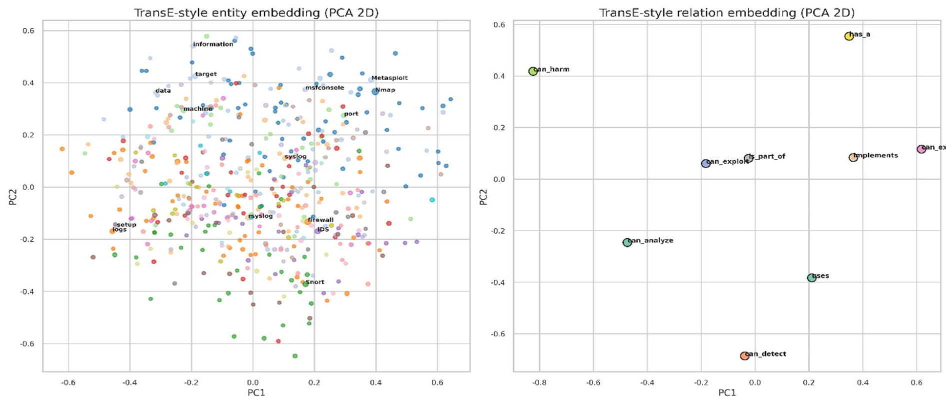


Figure 4. TransE Embedding

This figure shows the results of TransE, a knowledge graph embedding technique, projected into 2D space using PCA.

• Left (Entities): The nodes are scattered, but semantic clustering is visible.

• Top Right: “Nmap”, “Metasploit”, “msfconsole” are clustered together.

• Bottom Center: “Snort”, “firewall”, “IDS” are clustered together.

• Left: “logs”, “setup”, “information”.

• Right (Relations): The relationships (edges) are mapped as vectors.

• “has_a” is at the top.

• “can_harm” is top-left.

• “can_detect” is at the bottom.

• “can_expose” is far right.

The embedding successfully captures semantic meaning.

• Tool Clustering: Offensive tools (Nmap/Metasploit) are mathematically close to each other in the vector space, distinct from defensive tools (Snort/Firewall).

• Relation Semantics: The relations are separated by function. “*Can_detect*” (defensive action) is on the opposite side of the Y-axis from “*can_harm*” (offensive action), showing the model understands the opposing nature of these relationships.

5.7 Node2Vec Embedding Projection (PCA 2D)

This scatter plot (Figure 5) shows nodes embedded using Node2Vec (which preserves neighborhood structures), colored by the communities identified in Figure 1 (C1-C12).

• C1 (Dark Blue - Left): Contains “msfconsole”, “Nmap”, “Metasploit”, “tools”. This is the Offensive Security/ Pentesting Community.

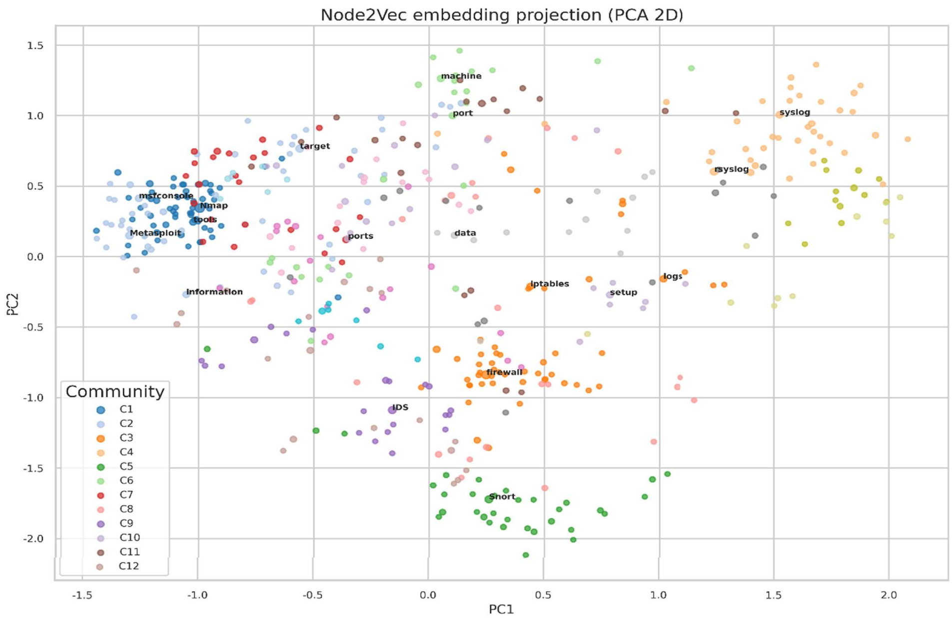


Figure 5. Node2Vec Embedding Projection

- C3 (Orange - Bottom Center): Contains "firewall", "iptables". This is the Network Defense Community.
- C5 (Dark Green - Bottom): Contains "Snort". This is likely the Intrusion Detection Community.
- C4 (Light Orange - Right): Contains "syslog", "rsyslog", "logs". This is the Logging/Monitoring Community.
- C6 (Light Green - Top): Contains "machine", "port". This represents Infrastructure/Network primitives.

This figure provides the strongest validation of the graph's structure. The Node2Vec algorithm has automatically grouped nodes into semantically coherent clusters that align perfectly with cybersecurity domains.

- It confirms that the dataset distinguishes clearly between Attack (Left/Blue), Defense (Bottom/Orange & Green), and Operations/Logging (Right/Yellow).
- The separation of "Snort" (C5) and "Firewall" (C3) suggests the graph treats Intrusion Detection Systems and Firewalls as distinct functional areas, even though they are both defensive.

5.8 Findings

The network analysis demonstrates that the cybersecurity knowledge graph exhibits a sparse semantic structure with low density (0.0018) and low clustering (0.0227), consistent with characteristics of well-structured domain-specific knowledge graphs. High-centrality nodes, particularly Nmap (degree: 0.104; betweenness: 0.0728) and firewall (degree: 0.063; betweenness: 0.0435), dominate the network topology, acting as core hubs for knowledge propagation and critical bridging entities. The betweenness centrality results highlight potential points for security monitoring and intervention, while the presence of 59 disconnected components indicates domain fragmentation, which is useful for modular analysis. The absence of isolated nodes confirms dataset completeness and validates the relational integrity of the constructed knowledge graph.

6. Conclusion

This study presented AISecKG, a comprehensive cybersecurity knowledge graph designed to bridge the critical gap between theoretical ontology construction and practical application in education and threat intelligence. By analyzing 1,460 entities and 726 relations, we demonstrated that Knowledge Graphs effectively integrate heterogeneous security data into semantically interpretable knowledge. Network topology analysis revealed a sparse structure with low density (0.0018), featuring key hubs such as Nmap and Firewall that serve as central bridging entities. Furthermore, Louvain community detection identified 20 distinct functional clusters, ranging from network scanning to intrusion detection, confirming the graph's modular organization.

Crucially, TransE and Node2Vec embeddings successfully captured relational and structural semantics, validating the graph's utility for downstream machine learning tasks such as entity classification and similarity search. These findings address the significant research gap regarding the practical utilization of Cybersecurity Knowledge Graphs (CSKGs) identified in prior literature. The structured representation supports adaptive learning environments by providing tangible feedback and contextual relationships essential for developing critical thinking in cyber professionals. Consequently, this architecture enables educators to move beyond isolated data points toward connected intelligence. Future work must focus on deploying these insights into real-world security operations and educational platforms to enhance dynamic threat detection and professional training. Ultimately, AISecKG offers a scalable, interpretable framework for transforming fragmented cybersecurity data into actionable intelligence, fostering both academic understanding and operational resilience in an evolving threat landscape.

References

[1] Sikos, L. F. (2023). Cybersecurity knowledge graphs. *Knowl Inf Syst* 65, 3511–3531.

[2] Sowa, J. F. (2012). Semantic networks. *Encycl. Cogn. Sci*. Available online: http://www.jfsowa.com/pubs/semnet.pdf.

[3] Agrawal, G., Deng, Y., Park, J., Liu, H., Chen, Y. C. (2022). Building Knowledge Graphs from Unstructured Texts: Applications and Impact Analyses in Cybersecurity Education. *Information,* 13(11), 526.

[4] Hemm, eK. (2015). Critical infrastructure protection: Maintenance is national security, *J. Strateg. Secur.*

[5] Ghafir, I. et al. (2018). Security threats to critical infrastructure: the human factor, *J. Supercomput.*

[6] Hijji, M. et al. (2021) A multivocal literature review on growing social engineering-based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions, *IEEE Access.*

[7] Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity Tech. Rep.

[8] Jia, Y., Qi, Y., Shang, H., Jiang, R., Li, (2018). A. A practical approach to constructing a knowledge graph for cybersecurity. Engineering 2018, 4, 53–60.

[9] Bürger, J., Strüber, D., Gärtner, S., Ruhroth, T., Jürjens, J., Schneider, K. (2018). A framework for semi-automated co-evolution of security knowledge and system models. *J. Syst. Softw.* 2018, 139, 142–160.

[10] Doynikova, E., Fedorchenko, A., Kotenko, I. (2019). Ontology of metrics for cyber security assessment. *In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK,* 26–29 August 2019; p. 1–8.

[11] Alenezi, M., Basit, H. A., Khan, F. I., Beg, M. A. (2020). A Comparison Study of Available Sofware Security Ontologies. In Proceedings of the Evaluation and Assessment in Software Engineering, Trondheim, Norway, 15–17 April 2020; pp. 499–504.

[12] Piplai, A., Mittal, S., Joshi, A., Finin, T., Holt, J., Zak, R. (2020). Creating Cybersecurity Knowledge Graphs from Malware after Action Reports. *IEEE Access* 2020, 8, 211691–211703.

[13] Yang, F., Han, Y., Ding, Y., Tan, Q., Xu, Z. A flexible approach for cyber threat hunting based on kernel audit records. Cybersecurity 2022, 5, 11.

[14] Li, Y., Guo, Y., Fang, C., Liu, Y., Chen, Q. (2022). A Novel Threat Intelligence Information Extraction System Combining Multiple Models. *Secur. Commun. Netw.* 2022, 8477260.

[15] Bratsas, C., Anastasiadis, E. K., Angelidis, A. K., Ioannidis, L., Kotsakis, R., Ougiaroglou, S. (2024). Knowledge Graphs and Semantic Web Tools in Cyber Threat Intelligence: A Systematic Literature Review. *Journal of Cybersecurity and Privacy,* 4 (3) 518-545.

[16] Andola, N., Prakash, S., Gahlot, R (2022) An enhanced smart card and dynamic ID based remote multi-server user authentication scheme. *Clust Comput* 25(5):3699–3717. https://doi.org/10.1007/s10586-022-03585-4.

[17] Andola, N., Gogoi, M., Venkatesan, S (2019) Vulnerabilities on hyperledger fabric. Pervasive Mobile Comput 59:101050. https://doi.org/10.1016/j.pmcj.2019.101050.

[18] Andola, N., Raghav, Y.V. K. (2021) SpyChain: a lightweight blockchain for authentication and anonymous authorization in IoD. *Wireless Pers Commun* 119: 343–362. https://doi.org/10.1007/s11277-021-08214-8.

[19] Zhang, Z., Song, X., Sun, X (2023) Hybrid-driven-based fuzzy secure filtering for nonlinear parabolic partial differential equation systems with cyber attacks. *Int J Adapt Control Signal Process* 37 (2) 380–398. https://doi.org/10.1002/acs.3529.

[20] Wang, W., Han, Z, Alazab, M. (2022). Ultra-fast authentication protocol for electric vehicle charging using extended chaotic maps. *IEEE Trans Ind Appl* 58 (5) 5616–5623. https://doi.org/10.1109/TIA.2022.3184668.

[21] Alazab, M., RM, SP, Parimala, M (2021) Federated learning for cybersecurity: concepts, challenges, and future directions. *IEEE Transact Industrial Inform* 18(5) 3501–3509.

[22] Li, H., Shi, Z., Pan, C. et al. Cybersecurity knowledge graphs construction and quality assessment. *Complex*

Intell. Syst. 10, 1201–1217 (2024).

[23] Ren, Y., Xiao, Y., Zhou, Y., Zhang, Z., Tian, Z. (2023). CSKG4APT: A Cybersecurity Knowledge Graph for Advanced Persistent Threat Organization Attribution, *IEEE Transactions on Knowledge and Data Engineering,* 35 (6) 5695-5709, 1 June 2023.

[24] Noel, S. (2018). A review of graph approaches to network security analytics. In From Database to Cyber Security; Springer: Cham, Switzerland, 2018; p. 300–323.

[25] Sani, M. (2020). Knowledge Graph on Cybersecurity: A Survey. 2020. Available online: https://upvdoc.univ-perp.fr/fr/congres-des-doctorants/article-maman-sani-aboubacar.

[26] Yan, Z., Liu, J. (2020). A review on application of knowledge graph in cybersecurity. In: Proceedings of the 2020 IEEE International Signal Processing, Communications and Engineering Management Conference (ISPCEM), Montreal, QC, Canada, 27–29 November 2020; p. 240–243.

[27] Dong, C., Jiang, B., Lu, Z., Liu, B., Li, N., Ma, P. (2020). Knowledge graph for cyberspace security intelligence: A survey. *J. Cyber. Secur.* 2020, 5, 56–76.

[28] Ding, Z., Liu, K., Liu, B., Zhu, X. (2021). Survey of cyber security knowledge graph. *J. Huazhong Univ. Sci. Tech.* (Nat. Sci. Ed.) 2021, 49, 79–91.

[29] Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., Zhou, Y. (2022). Recent Progress of Using Knowledge Graph for Cybersecurity. Electronics, 11(15), 2287.

[30] Lee, M., Sharma, P. (2024). Leveraging the Louvain algorithm for enhanced group formation and collaboration in online learning environments. *Int J Educ Technol High Educ* 21, 65.

[31] https://github.com/garima0106/AISecKG-cybersecurity-dataset.

[32] Antoine, Bordes., Nicolas, Usunier., Alberto, Garcia-Duran., Jason, Weston., Oksana, Yakhnenko. (2013) Translating Embeddings for Modeling Multi-relational Data, In: Advances in Neural Information Processing Systems 26 (NIPS 2013) p. 26.

[33] Aditya Grover, Jure Leskovec (2016) node2vec: Scalable Feature Learning for Networks. arXiv:- 1607.00653v1.