JURNAL EMACS e-ISSN: 2686-2573
[Engineering, MAthematics and Computer Science] Vol.7 No.3 September 2025: 327-335 DOI: 10.21512/emacsjournal.v7i3.14325

Optimizing Enterprise Risk Management for Decision Making Using Knowledge Graph

Aan Albone

Data Science Program, Computer Science Department,
School of Computer Science,
Bina Nusantara University,
Jakarta, Indonesia 11480
aan.albone@binus.ac.id

Correspondence: aan.albone@binus.ac.id

Abstract – *The challenge in current enterprise risk management is that hundreds of risks are eventually recorded without knowing how hazards relate to one another or cascade. The distinction between peripheral and critical hazards is unknown to decision-makers. Organizations can depict the interconnectedness of risk in a structured, adaptable, and understandable way by showing these components as nodes and their interactions as edges. This knowledge graph makes it possible to store and query risk data in ways that are not entirely supported by conventional relational models. This method's ability to execute graph queries that uncover links and patterns that would otherwise be obscured in siloed datasets is one of its main advantages. Such inquiries can reveal how a single threat can lead to many vulnerabilities across multiple assets, or how flaws in shared systems can directly and indirectly raise exposure to interconnected hazards. These revelations draw attention to structural flaws that linear or isolated investigations frequently ignore. Organizations can improve situational awareness and long-term risk governance by using such a knowledge graph to find hidden trends, pinpoint important risk spots, and more efficiently prioritize mitigation efforts. The knowledge graph also helps to optimize enterprise risk management goals like resource allocation, control prioritization, and prompt reaction planning. Enterprise risk management can effectively represent the intricate relationships between risks, vulnerabilities, threats, and assets by incorporating a knowledge graph. Businesses can concentrate mitigation efforts where they will have the biggest impact by determining which nodes and edges are the most important and highest impact. This focused strategy increases overall resilience and decreases inefficiencies.*

Keywords*: Enterprise Risk Management; Assets; Threat; Vulnerability; Knowledge Graph*

I. INTRODUCTION

Enterprise Risk management facilitates risk analysis, monitoring, and control. This necessitates the creation of a risk management system that can deliver the data necessary for decision making. The term enterprise risk management (ERM) describes the process by which businesses employ a variety of scientific techniques to investigate and pinpoint risk sources, assess and alert to unknown risk sources, and manage risk incidents to meet operational goals (Fanga, et al., 2023).

If we have a list of risk data on our systems, maybe we're not aware of the relationships between components of the risks, so it is difficult to analyze and get the insight from the data. Information silos and data barriers are currently a problem for business risk analysis and management (Li, et al., 2024). Current risk assessment techniques frequently have laborious and time-consuming procedures, which make it difficult to have a thorough awareness of potential security threats (Unger, et al., 2024).

The business plan should be supported with risk management. However, risks are not linked to important goals in siloed approaches. Executives find it more difficult to understand

how risks affect long-term business objectives and value as a result. Since risk management is a decision-oriented system, it should promptly alert management to prospective crises (risk management as an early warning system) and give information on risk exposure to help with decision-making by enabling the comparison of risks (Gleiner & Berger, 2024).

Operational, cyber, compliance, financial, and strategic risks, for instance, are frequently handled by separate divisions. When there is no integration, each team concentrates on its own domain. Some systemic risks are undetected until they manifest, and this results in blind spots and duplication. Organizations can identify hidden relationships by using a knowledge graph, which provides substantial benefits in decision-making by representing complex, interrelated data in an organized yet adaptable manner. Having this talent is especially helpful in risk management, where making judgments requires an awareness of complex dependencies (Hogan, 2022).

Knowledge graph (KG) is linked to datasets enhanced with semantics that allow us to confidently use the underlying data for complex decision-making. The collection of real-world elements (data) linked by semantic relations is represented by KG in order words. This allows for sophisticated reasoning to uncover hidden conceptual linkages that aid in well-informed decision-making (Isah & Kim, 2023).

By transforming risk management from a flat list into an interconnected network, a knowledge graph offers a solution in this area. A knowledge graph, the flexible structure that results, enables rapid adaptation of complex data and linkages through interconnections. Because of its innate connection, graph algorithms can be used to uncover hidden patterns and draw novel conclusions. Additionally, as demonstrated by social network analysis, knowledge graphs scale to extremely high sizes and are computationally efficient (Albagli-Kim & Beimel, 2022).

Knowledge graphs are frequently used to reason over related data for tasks like question answering and recommendation (Shi, et al., 2022). Risk management assesses and ranks different risks according to their significance, impact, and probability. To lessen the impact of risk occurrence and to handle potential losses, risk prevention entails creating plans and preventive procedures that are appropriate for different risks (Ma, et al., 2024).

This paper proposes developing a knowledge graph to optimize enterprise risk management by shifting the view from isolated lists of risks into an interconnected network of enterprise vulnerabilities, threats, and assets as a holistic view for decision-making.

II. METHODS

This section explains the detailed method to develop Knowledge Graph to optimize Enterprise Risk Management.

2.1 Risk Identification and Analysis

The first step is, we need to identify three essential elements in risk management: assets, threats, and vulnerabilities. After those components have been precisely defined, we will do risk analysis.

Assets are anything of value to an organization that needs protection. They can include physical assets (servers, buildings), digital assets (data, software, intellectual property), human assets (employees, knowledge), and reputational assets (brand image, customer trust). By identifying assets, we will understand that the value and criticality of each asset help prioritize which areas require stronger protection or controls.

A threat is any event, actor, or condition that has the potential to cause harm to an asset. Threats can be intentional (e.g., cyberattacks, insider misuse, fraud) or unintentional (e.g., human error, natural disasters, system failures).

Recognizing threats is essential to understanding what could go wrong and who or what might cause it. Without identifying threats, it is impossible to evaluate how an organization's assets may be exposed to damage or disruption.

Vulnerabilities are the weaknesses or gaps in systems, processes, or controls that can be exploited by threats to harm assets. Examples include outdated software, poor access control, lack of employee training, or weak encryption. In risk assessment, analyzing vulnerabilities helps determine how easily a threat can succeed. Reducing vulnerabilities directly lowers the likelihood of risk occurrence.

Risk analysis is the process of systematically identifying, evaluating, and

understanding potential risks that could negatively affect an organization's objectives, assets, operations, or reputation. It involves determining what could go wrong, how likely it is to happen, and what the possible consequences would be. Risk analysis helps decision-makers assess the likelihood and impact of different risk events and prioritize which ones need attention. It often includes identifying assets (what need protection), threats (what could cause harm), and vulnerabilities (weaknesses that could be exploited). By analyzing these factors together, organizations can calculate the level of risk and decide on appropriate controls or mitigation strategies to reduce potential harm.

Risk analysis can be performed for assets in critical scenarios by identifying their vulnerabilities for decision-making about how to mitigate them (García Pérez, et al., 2023).

There is a need for organizations to do risk analysis on their assets so that it can be analyzed and any gaps in their protection can be found (Fathullah & Subbarao, 2022).

By analyzing the relationships between those three elements, we can calculate the level of risk (Risk = Likelihood × Impact on Asset) and design appropriate mitigation strategies. This triad ensures that risk management efforts are focused, measurable, and aligned with the organization's most critical values and objectives.

2.2 Graph Data Model

In the graph data model, we show assets, threats, vulnerabilities, and risks as nodes, and the connections between them are shown as edges. The graphical model makes it possible to assess the effects of hazards that have been identified as well as their possible future influence. The relationship allows us to see how many things are from a holistic point of view, which helps with semantic understanding, information retrieval, and other uses.

Because attackers often combine and exploit multiple vulnerabilities when launching attacks, determining how to analyze the relationship between vulnerabilities and combining it with the impact relationship by linking the knowledge graph to achieve attack objectives through holes is important. The risks brought by vulnerability exploitation to the system have become very important (Jiao et al., 2024).

Data-driven architectures in graph data model can represent the network to find ways to prevent attacks by pinpointing the most vulnerable services via examining the firewall as an asset. Using knowledge graphs, exposed vulnerabilities can be listed for mitigation by providing correlation data between threat, assets, and vulnerability (Sikos et al., 2023).

After we have graph data model, we need to prepare the data before loading data process. The objective of data preparation is to ensure that every node and edge is precisely mapped and aligns with overall data that contains threats, assets, vulnerability and risk.

A knowledge graph is a technical means for iteratively extracting structured knowledge from a large amount of data of various structure types (Qin, et al., 2020).

The next step is to load the data into the graph database's entities and edges and create a fully functional knowledge graph. Using a knowledge graph, we can record the intricate relationships between these components, facilitating more thorough analysis, improved prioritization, and ultimately more successful risk management tactics. After the load data process, we will have the ability to visualize the interconnection of threats, assets, vulnerabilities, and risk data that we load, analyze intricate dependencies, and extract actionable insights.

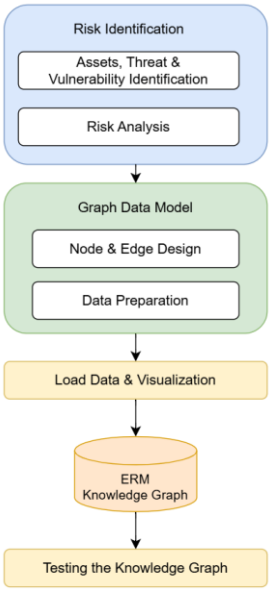

Figure 1. ERM Knowledge Graph Method

2.3 Testing Knowledge Graph

Knowledge graphs must be tested using a straightforward query. We will check the response to our queries based on the use case requirements.

Graphs of threats and attacks are a tool for analyzing vulnerabilities that capture different and prospective attacks on a system. It shows possible paths that an attacker can exploit on our assets (Pekaric et al., 2023).

By testing the knowledge graph, we may pinpoint areas that need work and adjust to optimize the result. Through this testing, we can check that our knowledge graph supports the use cases and runs efficiently. The objective of this test is to see if the knowledge graph can address our business inquiries. The inquiries should confirm that the graph offers useful information and achieves the objective of establishing this knowledge graph as a useful instrument for aiding in enterprise risk management decision-making.

III. RESULTS AND DISCUSSION

As the foundation of an effective risk analysis process, we must conduct assets, vulnerabilities, and threats. Identifying assets allows us to understand what needs protection and to prioritize resources based on their value and criticality. Analyzing vulnerabilities reveals weaknesses in systems, processes, or controls that could be exploited, while recognizing threats helps us understand the potential sources or events that might cause harm.

The result of this identification process is a comprehensive view of the organization's risk landscape, showing how threats can exploit vulnerabilities to impact critical assets. This structured understanding enables more accurate risk assessment, prioritization, and the development of targeted mitigation strategies to strengthen overall security and resilience.

Events or people who might exploit their weaknesses are considered potential threats. We identified some threats, vulnerabilities, and assets in Table 1. A vulnerability may go unnoticed if no threat takes advantage of it, but when they come together, they expose a serious risk to the asset.

Table 1. Assets, Vulnerability, and Threat Identification

Assests: Software, Server, Network, Information, Hardware, Employe.
Vulnerability: Bugs, Outdated versions, Misconfiguration, Hidden backdoors, Phishing, Weak passwords, Incompatibility, Human error, Power failure, Low awareness, Poor training, Unencrypted communication, Insider threats, Poor access control, Weak authentication, Physical damage, Lack of physical security, Unencrypted storage, Lost/stolen device, Outdated firmware, Unencrypted data, Missing backups, Ransomware, Data integrity not assured, Malware, Outdated patches, Outdated OS/software, Lack of monitoring, Poor IDS/IPS, Weak segmentation, Unencrypted comms, Open Wi-Fi, Unpatched devices, Poor segmentation, Weak IDS.
Threats: Exploitation buffer overflow, Privilege escalation, Service crash, Malware infections, Ransomware, Remote code execution, Unauthorized access, Persistent threats, Data exfiltration, Brute-force attacks, Privilege misuse, Application crashes, Denial of service, Service disruption, Accidental data, leakage, Downtime, Falling victim to scams, Mishandling data, Credential theft, Malware infection, Data theft, Sabotage, Insider abuse, Credential compromise, System failure, Data loss, Device theft, Hardware manipulation, Data breach if device stolen, Rootkits, Device takeover, Infiltration, Hardware damage, Corruption, Data leakage, Unauthorized modification, Permanent data loss, No recovery, Data manipulation, Fraud, Misinformation, Remote exploitation, DoS, Identity theft, Delayed detection, Undetected breaches, Unauthorized entry, Intrusions, Eavesdropping, MITM attack, Malware spreading, Lateral movement by attackers

Because risks arise from complex interactions, a single risk can be associated with multiple threats, vulnerabilities, and assets. Different threats may take advantage of different weaknesses in different assets, and a particular vulnerability may expose multiple assets to multiple threats at the same time. One systemic risk, for instance, frequently results from a cascade in critical infrastructure, where several vulnerabilities in interconnected assets. We can analyze the connection between threats, vulnerabilities, assets, and risks in Table 2.

In contemporary risk modeling frameworks, the many-to-many link between threats, vulnerabilities, assets, and risk is fundamental (Ekstedt, et al., 2023).

A single vulnerability can expose numerous assets to distinct attacks, while a single threat can exploit multiple vulnerabilities across diverse assets. This structure helps organizations visualize and analyze these scenarios. By utilizing graph database technology, risk managers can comprehend interdependencies more dynamically and clearly, which facilitates more precise risk assessment and more successful mitigation techniques.

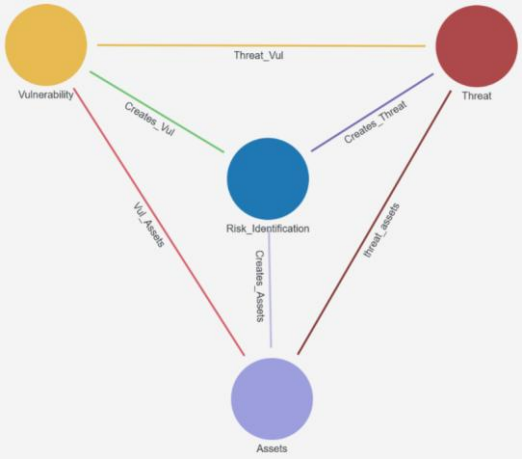

Figure 2. Graph Data Model

Table 2. Risk Analysis

Potential Threat	Related Vulnerabilities	Asset(s)	Risk (Description)	Impact	Likelihood	Risk Level
Exploitation (buffer overflow, privilege escalation, service)	Bugs, Outdated versions, Misconfiguration	Softwar, Server	Attackers exploit flaws to gain higher privileges or crash services.	High	Medium	High
Malware infections, ransomware, remote code execution	Outdated versions, Hidden backdoors, Phishing, Outdated firmware	Softwar, Server, Network	Malware spreads, encrypts systems, causes ransom and downtime.	High	High	Critical
Unauthorized access, persistent threats, data exfiltration	Hidden backdoors, Weak passwords, Misconfiguration	Softwar, Server, Network, Information	Attackers steal data or maintain long-term system control.	High	High	Critical
Brute-force attacks, privilege misuse, unauthorized access	Weak passwords, Misconfiguration	Server, Network	Accounts taken over, privilege abuse on systems.	High	Medium	High
Application crashes, denial of service	Incompatibility, Human error	Softwar, Server	Critical apps unavailable, disrupts operations.	Medium	Medium	Medium
Service disruption, accidental data leakage, downtime	Human error, Power failure	Softwar, Server, Hardware	Operations halted, accidental exposure of sensitive data.	Medium	Medium	Medium
Falling victim to scams, mishandling data	Low awareness, Poor training	Employee, Information	Employees mishandle sensitive data, weak incident response.	High	High	High
Credential theft, malware infection	Phishing, Weak passwords, Unencrypted communication	Employee, Softwar, Information	Compromised accounts allow unauthorized entry.	High	High	Critical
Data theft, sabotage, insider abuse	Insider threats, Poor access control	Employee, Server, Information	Employees steal or leak sensitive company info.	High	Medium	High

Credential compromise, unauthorized access	Weak passwords, Weak authentication	Employee, Server, Network	Attackers bypass authentication controls.	High	High	Critical
System failure, downtime, data loss	Physical damage, Power failure	Hardware, Server	IT systems unavailable due to hardware/software breakdown.	High	Medium	High
Device theft, hardware manipulation	Lack of physical security, Insider threats	Hardware, Employee	Stolen devices used for data theft or sabotage.	High	Medium	High
Data breach if device stolen	Unencrypted storage, Lost/stolen device	Hardware, Information	Confidential data leaked from lost hardware.	High	High	Critical
Rootkits, device takeover, infiltration	Outdated firmware, Hidden backdoors	Hardware, Server, Network	Attackers gain persistent stealthy control of systems.	High	High	Critical
Downtime, hardware damage, corruption	Power failure, Physical damage	Hardware, Server	Permanent data loss and business disruption.	High	High	High
Data leakage, unauthorized access	Unencrypted data, Human error	Information , Software	Sensitive data exposed without protection.	High	Medium	High
Unauthorized modification, insider abuse	Insider threats, Poor access control	Employee, Information	Fraud or sabotage from malicious insiders.	High	Medium	High

Following the graph database design with nodes and edges, the next step is to load data for each node (e.g., assets, threats, and vulnerabilities) and their edges. When data population is complete, the graph structure can be displayed, providing consumers with a clear network image of the interrelated connections. Visualization can help improve risk management decision-making. In the context of optimizing the enterprise risk management process, it is crucial to verify the knowledge graph using straightforward queries that represent the anticipated results of its evolution. These queries are used as validation to make sure the knowledge graph can efficiently obtain pertinent insights, it can show how assets, threats, vulnerabilities, and risks are related to one another, and ultimately facilitate more precise analysis and decision-making within the framework of enterprise risk management.

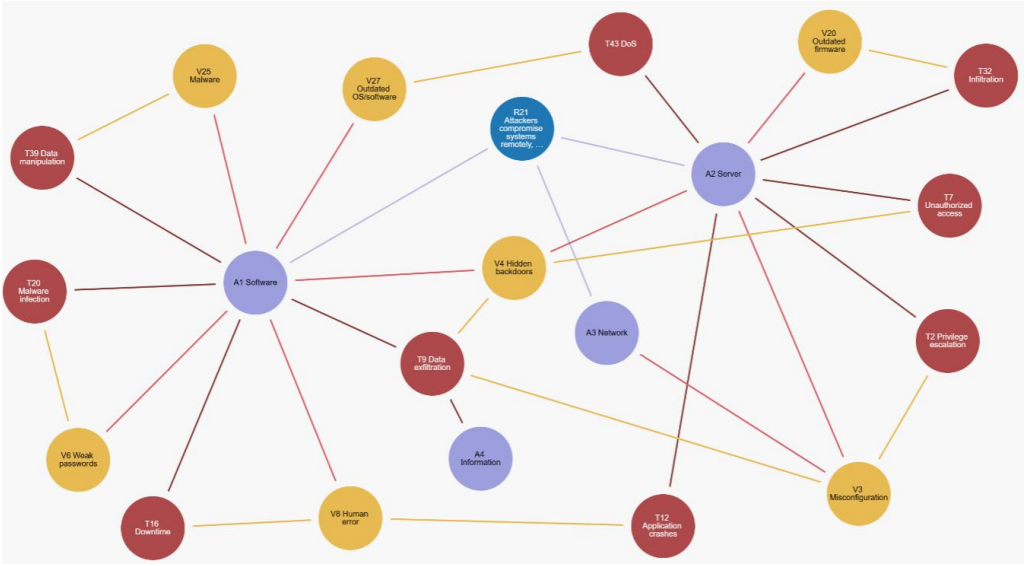

Figure 3. Knowledge Graph Result: Query 1

3.1 Test Query 1:

In the first query, we have done a deep impact analysis to determine which vulnerabilities can lead to direct and indirect impact that cause a high level of risk. Recognizing how vulnerabilities are linked helps organizations anticipate chain reactions rather than treating each weakness in isolation. This understanding supports a more proactive and holistic risk management approach—where fixing one vulnerability also prevents others from emerging. By mapping these relationships, security teams can identify root causes and strengthen defenses more effectively, reducing both direct and indirect risks to critical assets.

The query results show that the vulnerability "V3-Misconfiguration" can occur directly on 2 assets (Server and Network) and 2 assets (Software and Information) indirectly. This raises the risk level high because the impact will be multiple if not properly controlled.

Misconfiguration on a server (e.g., open administrative ports or default passwords) can allow unauthorized users to gain access, modify system settings, or install malware. This directly compromises the integrity and availability of the server. Misconfigured networks like routers, firewalls, or switches can expose internal network segments to the public or allow unintended traffic flow. This increases the attack surface and can lead to unauthorized network intrusion or denial-of-service attacks.

Once a server or network is compromised, attackers can exploit their control to alter application configurations, inject malicious code, or disrupt service operations. This affects the functionality and reliability of critical software. It can also lead to data breaches, information leakage, or unauthorized modification of sensitive data.

The loss of confidentiality, integrity, and availability of information can cause regulatory violations, financial loss, and reputational damage.

This analysis is what we get when conducting a risk assessment using a knowledge graph. This will optimize the early warning process or provide faster and more comprehensive decision-making for the company to implement better mitigation.

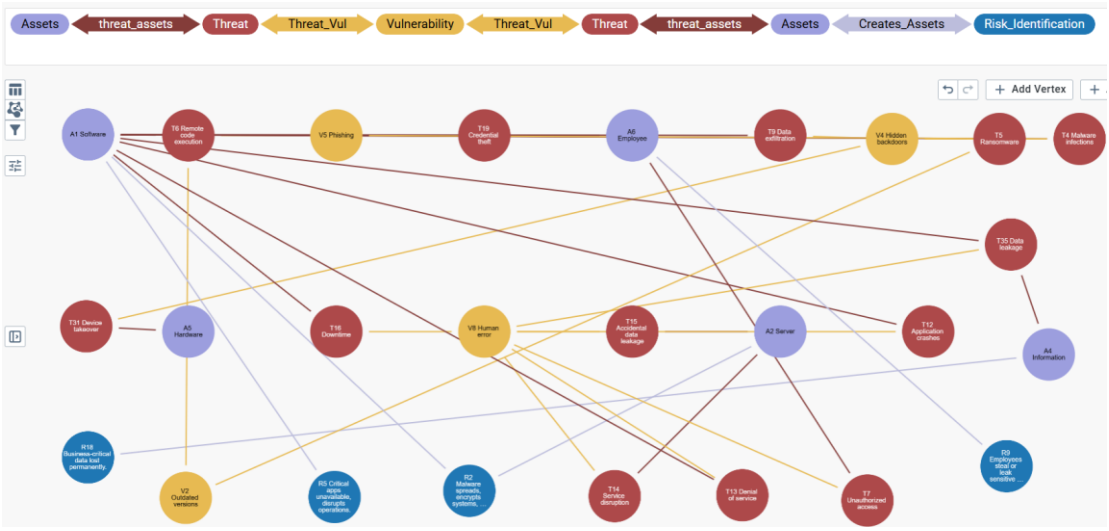

Figure 4. Knowledge Graph Result: Query 2

3.2 Test Query 2:

The 2nd query is to analyze from a threat perspective. We want to know which treat that the threats that can trigger other threats, either directly or indirectly, and thereby create additional risks and vulnerabilities.

From the query result, we know that the Remote Code Execution (RCE) has a direct impact on two assets (Software and Hardware). RCE primarily exploits software vulnerabilities; its consequences can extend to hardware assets because software acts as the control layer for hardware components.

When an attacker gains remote execution capability, they effectively obtain the same level of access as the compromised software

including control over the hardware it manages, such as running high CPU/GPU workloads, overloading storage or memory resources. And there're 2 risks that connected with remote execution treats:

- R1: Critical apps unavailable, disrupts operations,
- R2: Malware spreads, encrypts systems, causes ransom and downtime.

The level of risk will be high if we aren't aware of those risks and don't implement any controls to mitigate the impact. Through the knowledge graph, we can visualize and analyze risks from multiple interconnected perspectives — threats, vulnerabilities, and assets. We allow searching for relationships between nodes, so that there is no hidden information for the analysis and decision-making process. Organizations can improve situational awareness and long-term risk governance by using such a knowledge graph to find hidden trends, pinpoint important risk spots, and more efficiently prioritize mitigation efforts.

Organizations can improve situational awareness and long-term risk governance by using such a knowledge graph to find hidden trends, pinpoint important risk spots, and more efficiently prioritize mitigation efforts.

IV. CONCLUSION

ERM Knowledge Graph can effectively represent the intricate relationships between risks, vulnerabilities, threats, and assets by incorporating a knowledge graph. Organizations can depict the interconnectedness of risk in a structured, adaptable, and understandable way by showing these components as nodes and their interactions as edges. This graph-based method makes it possible to find the connection between those components in Risk Management.

This approach's ability to execute graph queries that uncover patterns and relationships that would otherwise be obscured in siloed datasets is one of its main advantages. For instance, in queries 1 and 2, the inquiries can reveal how a single threat or other component can lead to numerous vulnerabilities across several assets, or how shared system flaws can raise exposure to related hazards.

The knowledge graph's depiction improves comprehension even more by making risk interdependence clear and understandable. By tracking possible routes of threat dissemination, decision-makers can reenact "what-if" scenarios in addition to monitoring the current level of hazards. And the visualization and analytical capabilities enhance situational awareness about risk. (Figure 2, 3 and 4).

Additionally, the knowledge graph aids in the optimization of enterprise risk management objectives such as control prioritization, resource allocation, and quick response planning. By identifying the most critical nodes and edges, those with the most centrality or influence, businesses may focus mitigation efforts where they will have the greatest impact.

REFERENCES

Albagli-Kim, S., & Beimel, D. (2022). Knowledge graph-based framework for decision-making process with limited interaction. Multidisciplinary Digital Publishing Institute (MDPI).

Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., & Lagerstrom, R. (2023). Yet another cybersecurity risk assessment framework. International Journal of Information Security.

Fanga, R., Liaoa, H., Xua, Z., & Herrera-Viedma, E. (2023). Risk assessment in project management by a graph-theory-based group decision-making method with comprehensive linguistic preference information. Economic Research – Ekonomska Istraživanja, 36(1).

Fathullah, M. A., & Subbarao, A. (2022). Security risk analysis for information asset. Journal of System and Management Sciences, 12. https://doi.org/10.33168/JSMS.2022.0412

García Pérez, A., López Martínez, A., & Gil Pérez, M. (2023). Adaptive vulnerability-based risk identification software with virtualization functions for dynamic management. Journal of Network and Computer Applications. https://doi.org/10.1016/j.jnca.2023.103728

Gleiner, W., & Berger, T. B. (2024). Enterprise risk management: Improving embedded risk management and risk governance. Journal of Multidisciplinary Digital Publishing Institute (MDPI).

Hogan, A. (2022). Knowledge graphs: A guided tour. International Research School in Artificial Intelligence in Bergen.

Isah, M. A., & Kim, B.-S. (2023). Development of knowledge graph based on risk register to support risk management of construction projects. KSCE Journal of Civil Engineering.

Jiao, J., Li, W., & Guo, D. (2024). The vulnerability relationship prediction research for network risk assessment. Electronics, 13.

Li, P., Zhao, Q., Liu, Y., Zhong, C., Wang, J., & Lyu, Z. (2024). Survey and prospect for applying knowledge graph in enterprise risk management. Computers, Materials and Continua, 78(3), 3825–3865. https://doi.org/10.32604/cmc.2024.07803

Ma, J., Li, Y., She, L., Qin, Z., Meng, J., & Hu, Y. (2024). Design and research of enterprise risk management avoidance system based on KGN-LLM algorithm. Proceedings of the 2nd International Conference on Mathematical Physics and Computational Simulation.

Pekaric, I., Frick, M., Adigun, J. G., Groner, R., Witte, T., Raschke, A., Felderer, M., & Tichy, M. (2024). Streamlining attack tree generation: A fragment-based approach. Proceedings of the Hawaii International Conference on Social Systems (HICSS-57).

Qin, Y., Cao, H., & Xue, L. (2020). Research and application of knowledge graph in teaching: Take the database course as an example. Journal of Physics: Conference Series.

Shi, Z., Matyunin, N., Graffi, K., & Starobinski, D. (2022). Uncovering product vulnerabilities with threat knowledge graphs. IEEE Secure Development Conference (SecDev) (pp. 84–90). IEEE.

Sikos, L. F. (2023). Cybersecurity knowledge graphs. Knowledge & Information Systems, 65, 3511-3531. https://doi.org/10.1007/s10115-023-01860-3

Unger, S., Arzoglou, E., Heinrich, M., Scheuermann, D., & Katzenbeisser, S. (2024). Risk assessment graphs: Utilizing attack graphs for risk assessment. International Journal of Information Security.