In proceedings of IEEE International conference on Intelligence and Security Informatics (ISI 2023)

An Overview of Cybersecurity Knowledge Graphs Mapped to the MITRE ATT&CK Framework Domains

Joshua Bolton
Dept. of Information Systems
University of Maryland, Baltimore County
Baltimore, USA
jbolton1@umbc.edu

Lavanya Elluri
Dept. of Computer Information Systems
Texas A&M University - Central Texas
Killeen, USA
elluri@tamuct.edu

Karuna Pande Joshi
Dept. of Information Systems
University of Maryland, Baltimore County
Baltimore, USA
karuna.joshi@umbc.edu

***Abstract*—A large volume of cybersecurity-related data sets are generated daily from systems following disparate protocols and standards. It is humanly impossible for cybersecurity experts to manually sieve through these large data sets, with different schema and metadata, to determine potential attacks or issues. A myriad of applications and tool sets are offered to automate the analysis of large cyber data sets. Semantic Web's community has been studying the field of cybersecurity for over a decade and produced numerous knowledge graphs and frameworks. The Unified Cybersecurity Ontology (UCO) connected many of the leading knowledge representation frameworks, providing a holistic mapping of cyber data, beginning in 2016. MITRE ATT&CK is used by a wide variety of practitioners to understand how their current data and tooling prepare them to defend against both Advanced Persistent Threats (APTs) and less formal threat actors. The UCO and MITRE ATT&CK have provided researchers and practitioners, respectively, with tools to standardize data collection, correlation, and analysis. However, it is not apparent how current knowledge graphs and their applications in the cybersecurity domain utilize ATT&CK. In this paper, we present the results of our study on whether current cybersecurity knowledge graphs have mapped the main MITRE ATT&CK matrices.**

***Index Terms*—MITRE ATT&CK, knowledge graphs, semantic web, cybersecurity**

I. Introduction

Cybersecurity, one of the fastest growing fields globally, is generating large volumes of data that is difficult to analyze and reason over in real time. Recent major cybersecurity incidents have catalyzed the world into action. SolarWinds [1], Industrial Control Systems (ICS) take downs in Ukraine [2], and Log4Shell [3] are just a few of the many cyber attacks in recent years. In response, companies throughout the world have ramped up their cyber defense. Microsoft has promised a 20 billion dollar investment in cyber services, and other big tech companies have joined [4]. Why are such drastic changes needed to our digital security? To find the answer to this question we must consider the size and scale of the cyber landscape. The challenges of big data are being faced by cyber practitioners. In October of 2021, Microsoft reported over 24 trillion security signals per day [5]. In one year, they blocked nine billion endpoint threats, thirty-one billion identity threats, and thirty-two billion email threats [5]. The ever increasing scale of big cyber data compounds traditional issues, but the scope of threat feeds continues to increase. Cloud infrastructure, IoT devices, ICS devices, and smart hospitals are just a few of the many digitized sensors providing data over the internet. Deep subject matter expertise is often required to join dispirit data and understand the complexity behind the fields of a data frame. It is challenging to correlate data, much less protect them intelligently.

Approximately one third of all cybersecurity jobs are unoccupied. There are almost a million filled jobs, and an additional approximately 600,000 yet to be filled [6]. Cybersecurity is an increasing complex field, with widespread consumer adoption of cloud, and ever-increasing complex dependencies on software supply chains and hardware configurations. The learning curve is steep, and tech burnout is at an all time high. Fueled by the great resignation, following the COVID-19 pandemic, highly skilled labor is leaving old jobs for more lucrative and flexible working conditions. The complexity of the software interface with physical systems through compilers provides a natural obfuscation for those new to the field or those who have not gotten their hands "close to the metal". This lack of familiarity combined with a steep learning curve to understand the software, network, and hardware, including possible vulnerabilities creates a vacuum. Knowledge transfer is essential to creating successful employees, however highly non-linear value curves for experienced and knowledgeable employees make training new employees a non-trivial task. There is a need for centralized and transferable information on common types of attacks, defenses, and log naming conventions. MITRE ATT&CK and D3FEND play critical mirrored roles in defining the Tactics, Techniques, and Procedures used by both attackers and defenders of cyber physical systems [7].

Semantic Web technologies like knowledge graphs, also referred to as ontologies, are used to develop knowledge representation across industries. Knowledge graphs are

used for intelligently showing distributed knowledge with a logical visible architecture. Knowledge graphs also serve as query-able data sources with the ability to add via manual or machine learning methods, and can be integrated into bigger systems. For these reasons, we have decided to explore how Cyber Knowledge Graphs (CKGs), when combined with MITRE ATT&CK, can be used to perpetuate best practices, understand common areas of study, and identify gaps in application.

The remainder of the paper is organized as follows. Section II discusses the background and related work. Section III describes the methodology of our study. Experimental results are presented in Section IV and Section V summarizes our conclusions and ongoing work.

II. Background and Related Work

A. Cybersecurity

Activity logs are generated by software running on an operating system; some software is designed in and some added on afterwards. There are four broad categories of logs: Operating System (OS), network, cloud, and ICS. There are dozens to hundreds of logging tools for these categories. Each logging tool has fields to describe system, user, operation, etc. Each kind of operating system, network, sensor, account, or Cloud Service Provider (CSP) will have logs with different fields. Fields may be similar among categories of hardware/software, but strict inter-tool naming conventions are not enforced on the field. Knowing what types of events or series of events indicate malicious activity comes from experience and education.

1) Cybersecurity Domains: One of the most common frameworks for understanding attacker tactics, techniques, and procedures (TTPs), is the MITRE ATT&CK framework. MITRE ATT&CK is used by practitioners to understand the attack landscape, as well as how their organization is positioned to defend given the tools at their disposal. ATT&CK is divided into three topical domains, each with a corresponding matrix: Enterprise, Mobile, and ICS. Enterprise is the best known, and broadest, of the domains. Network, OS (Windows, macOS, Linux), Cloud (Azure AD, Office 365, AND Google workspace), and PRE are the four primary areas of research within an enterprise [7]. PRE, meaning before active campaign begins, focuses on the activities leading up to exploitation and are applicable to any information system. These areas of cybersecurity make natural breakpoints in the knowledge mapping of data.

B. Semantic Web

In cyber environments, users need to be able to exchange information, queries, and requests with some assurance that they share a common meaning. Discussions collate the experiences and interests of participants into coherent hypotheses. These hypotheses are tested through increasingly wider dissemination with conflicting hypotheses being weighed and discussed. The result of deconfliction is communal sense of truth as perceived by the participants. Consistencies in definitions allow for common ground to be established – a widely acknowledged need for progression among seemingly disparate entities. How this information is defined and labelled is the field of semantic reasoning, part of semantic analysis. The official birth of the Semantic web is a matter of some debate, but the basis for modern semantic web research is not. In May 2001, Berners-Lee et al. published their article entitled "The Semantic Web", kicking off a cascade of research to define ontologies, construct knowledge graphs, and build The Semantic Web [10]. Since then, several researchers have employed Semantic Web techniques for modeling and reasoning about cybersecurity information [11]- [50]. In 2016, Syed et al. developed the Unified Cybersecurity Ontology (UCO) as a way of integrating previously developed ontologies and providing a starting point for cybersecurity researchers to understand their big datasets from a semantic perspective [51].

Semantic Web technologies allow data to be annotated with machine-understandable meta-data, permitting the automation of their retrieval and their usage in correct contexts [54]- [60]. Semantic Web technologies contain languages such as Resource Description Framework (RDF) [52] [53] and Web Ontology Language (OWL) [54] [55] for defining ontologies and illustrating meta-data using these ontologies, as well as tools for reasoning over these descriptions. These technologies can be used to deliver semantics of cybersecurity standards enabling all cyber practitioners who understand fundamental Semantic Web technologies to communicate and use each others' data and services effectively.

Schema is built using W3C standardized languages to maintain design requirements including: sound semantics, interoperability, and the availability of system components and tools. It is possible to model the classes of data and relationships between these using semantic web technologies. As a result, the information is stored in a machine-understandable format, allowing machines to identify the correct context of data usage or retrieval. RDF [56] and OWL [57] are popular languages used to design the knowledge graphs.

The most fundamental requirement of practitioners is a representation supporting interoperability at both the syntactic and semantic levels to facilitate easy data exchange. A second design requirement is for a language designed to integrate well with cybersecurity standards and big data. These technologies can be used to provide standard semantics of service information and policies enabling all agents who understand essential Semantic Web technologies to communicate and use each others' data and services effectively.

Knowledge graphs are visual and query-able data structures describing relationships between objects, typically constructed in the form of triples. As the name implies, triples are a three-piece format defining the relationship, or edge, between two

nodes [51]. The nodes, subject and object, are joined by the predicate to indicate relationship. For example, Karen teaches Susan. Karen is the subject and inferred teacher, while Susan is the student. Triples can be used in pairs to specify bi-directional relationships.

III. Methodology

The purpose of this paper is to benchmark the application of knowledge graphs in the field of cybersecurity, exploring potential linkage to the MITRE ATT&CK framework. The methodology of this study was designed to follow the procedures of Kurniawan, et al [61]. We followed three steps: planning, literature searching, and analyzing the results [61]. A systematic literature review was chosen to ensure all manuscripts or other published works, relevant to the topics, were selected.

A. Planning

We have defined four research questions (RQs) to guide the review. RQ1 was chosen to understand prevalence of onotologies and knowledge graphs in cybersecurity research. RQ2 was chosen to understand how the current body of literature maps to the needs of practitioners through MITRE ATT&CK. We hypothesize there may be gaps between research and application. Of note, we did not map to the tactics or techniques levels of ATT&CK as most research surveyed did not reference ATT&CK or provide a sufficient level of detail to be certain of the tactics and techniques modelled. RQ3 was chosen to understand if and how researchers have adapted to the relatively new field of cloud security. RQ4 was chosen to understand how, and to what extent, knowledge graphs are used as a diagnostic for categorization of defensive systems. Systems is broadly applied to mean data, infrastructure, and tools. IEEE Xplore was selected to facilitate the literature searching phase, as it is a prominent search engine for information systems and semantic analysis peer-reviewed research.

- RQ1: What knowledge graph is most prevalent in cybersecurity applications?
- RQ2: What is the prevalence of knowledge graph applications in enterprise, Mobile, and ICS?
- RQ3: What are the state of the art of knowledge graphs for cyber defense of cloud computing?
- RQ4: What are the state of the art of knowledge graphs for cyber defense system scanning?

Each of the research questions is broken down into two or more reviewer questions to be asked by the reviewer of the selected manuscripts. Table I shows the mapping of research questions to reviewer questions: RQ1 has two associated questions, RQ2 has three, RQ3 has two, and RQ4 has two.

B. Literature Search

To keep the search simple and avoid unintentional exclusions, we limited our search to two sets of words for each topic: "Semantic Analysis" or "Knowledge Graphs" combined with "Cyber" or "Cybersecurity". All meta data was included in the search, and results were gathered as of July 17th, 2022. A total of 719 entries were found across all four phrase combinations, including 94 duplicates and two erroneous entries.

TABLE I
Research Question Mapping

Research Question	Reviewer Question Number	Reviewer Question
RQ1: CKG	1	Name of Ontology
	2	Constructed Knowledge Graph (Yes/No)
RQ2: MITRE ATT&CK	3	Used Knowledge Graphs for Enterprise Security (Yes/No)
	4	Used Knowledge Graphs for Mobile Security (Yes/No)
	5	Used Knowledge Graphs for ICS Security (Yes/No)
RQ3: Cloud Security	6	Does the paper use knowledge graphs primarily for defense or investigation of cloud infrastructure and data (Yes/No)
	7	If question 6 is true: What is the role of the knowledge graph?
RQ4: Cyber Defense Systems	8	Does the paper use knowledge graphs for scanning of cyber defense systems (Tooling, infrastructure, and/or data) (Yes/No)
	9	If question 8 is true: What type of cyber defense system (Tooling, infrastructure, and/or data)?

1) Exclusion Criteria: The exclusion criteria for data set creation comes in three distinct stages: search, title review, and abstract review. For the search phase, any non-English titles were disallowed from review. The four possible combinations of these phrases yielded 623 deduplicated and cleaned results when restricted to the last 10 years, 2012-2022. Deduplication was performed by comparing exact matches in title and author list. All research published after July 17th, 2022, are considered out of scope.

Titles not demonstrating applicability to both semantic and cybersecurity domains were excluded. Title review reduced the field by 84 percent, to 97 manuscripts. After the reduction, the authors looked at the abstracts of each of the 97 manuscripts to determine if the manuscript focused on semantic analysis of cybersecurity domains. Manuscript abstracts demonstrating both relevance to knowledge graphs and cybersecurity were selected for full manuscript review. A total of 48 manuscripts were selected for full review, with eight of these manuscripts being later discarded during

the full manuscript review because of lack of focus on cybersecurity (n=7) or lack of use of knowledge graphs or ontologies (n=1).

C. Analyzing Results

The final 40 manuscripts [11]- [50] were reviewed for answers to each of the reviewer questions. Most reviewer questions have simple defined acceptance criteria and results. Reviewer question seven examines the purpose of using the knowledge graph for cloud applications. The author reviewing the paper made the determination, based on the reviewed literature (N=4), of the implied or explicit primary reason for the use of knowledge graphs. Overall the trend of manuscripts per year for the last ten years, has been positive, with 2021 being the current maximum at 11 manuscripts published. We further analyzed the discarded manuscripts from the abstract review portion, and the general positive trend persisted shallowly. In the last 5 years, the were more papers accepted for this study than rejected at the abstract phase. We believe this is due to the convergence of semantic web and cybersecurity research.

IV. Results

While none of the 40 selected manuscripts explicitly focused on ATT&CK, we used reasonable extension to explore whether the topics covered could be mapped to the ATT&CK matrices. This research was reviewed against the four research questions and the nine reviewer questions, yielding a clean data set for analysis.

Interestingly, forty percent of the research did not use a specific reference knowledge graph when determining a method for knowledge representation. Three manuscripts did not construct a knowledge graph. Table II shows the prevalence of the utilized knowledge graphs. Of the CKGs used (n=24), the most common were the Unified Cybersecurity Ontology (UCO) and the UCO 2.0.

TABLE II
Cybersecurity Knowledge Graph Prevalence

Name of Reference Knowledge Graph	Number of Manuscripts
Unified Cybersecurity Ontology (UCO)	7
Unified Cybersecurity Ontology (UCO) 2.0	5
Created Ontology	3
Network Security Knowledge Ontology	1
Security Protocol Implementation Ontology	1
Cyber Policy Ontology	1
STUCC Ontology	1
CSOC Analysis Process Ontology	1
Other Ontology	5
Not Applicable	16

TABLE III
Mapping of the Reviewed CKG Research to MITRE ATT&CK Domains

Used Knowledge Graphs for MITRE ATT&CK Domain:	Manuscript Covering (Yes)	Manuscript Not Covering (No)
Enterprise Security	24	16
Mobile Security	1	39
ICS Security	4	36

Table III shows the mapping of reviewed manuscripts to ATT&CK high level domains. For the purposes of this study, manuscripts are not required to mention ATT&CK to be categorized into a domain. RQ2, focuses on how the current body of literature applies to best practices for cyber practitioners. MITRE ATT&CK is used extensively by defenders of information systems. Relating research to the stages of ATT&CK, and its broader domains will ease in adoption of new methods by cyber practitioners. The vast majority of research reviewed did not directly correlate the methods and tooling created to the ATT&CK framework, and will result in a knowledge or translation gap between researchers and practitioners. This gap can limit the effectiveness of the novel methods and tooling developed by researchers.

Sixty percent of manuscripts reviewed provided data, methods, or knowledge representation frameworks to practitioners in the broader enterprise security domain. Far fewer focused on mobile applications or ICS. As evidenced by attacks on the Colonial Pipeline attack and critical infrastructure in Ukraine, ICS defense is an important area for researchers to cover.

Several manuscripts took the concepts from a knowledge graph and created a new Cyber Knowledge Graph (CKG). These CKGs are good examples of practical usage of standardized knowledge graphs, like UCO and UCO 2.0. However, they will be specific to the tooling, infrastructure, and data used to create them. Reviewer question 8, gets at the heart of the applicability. 31 (77.5 percent) manuscripts applied knowledge graphs to scanning of systems (Tooling, Infrastructure, and/or data). The majority of research scanned data (n=20) and nearly half scanned tooling. Two manuscripts used CKGs for all three system types, and eight additional manuscripts scanned two system types. With nearly one-third of the manuscripts scanning multiple system types, current research provides a good variety of applicability to multi-system solutions.

In October of 2019, MITRE added cloud specific techniques to ATT&CK [62]. In almost three years, only three manuscripts have been published focusing on defense and scanning of clouds using knowledge graphs. One additional paper was published in 2018, and focused on

TABLE IV
APPLICABILITY OF CURRENT CKG RESEARCH TO CLOUD

Role of the Knowledge Graph in Cloud:	Manuscript Count
Correlation of Cybersecurity Data Sources	2
Word Generation	1
Defined Security Context Rules	1

general forensic analysis. Table IV shows a summary of the usage of CKGs for cloud applications. Of the four manuscripts, two focused on using CKGs for correlating data sets in the cloud. One focused on semantic word generation to extend semantic queries. The fourth manuscript used its CKG for defining context rules to be used for alerting. Knowledge representation for cloud services, attack paths, log analysis, and cloud specific tooling represent a few of the gaps in current analysis of cloud security.

V. CONCLUSION AND FUTURE WORK

With an expanding required knowledge base, cyber defense practitioners need of a variety of semantic tools. Knowledge graphs have been a tool increasingly utilized for enterprise security modeling, as well as extracting insights from Malware. The build out of CKGs to include cloud monitoring and hosting of traditional services in the cloud will be critical for continued information system defense. There has been little work on expanding the enterprise to Mobile or ICS monitoring. Blended networks, where an organization has both mobile and enterprise, or enterprise and ICS systems, are growing in prevalence. All three domains require additional research to link knowledge graphs to the tactics and techniques listed by the ATT&CK framework.

ACKNOWLEDGMENT

This research was partially supported by the NSF award 1747724, Phase I IUCRC UMBC: Center for Accelerated Real time Analytics (CARTA). The authors would like to thank Jessica Bolton for expertise in professional writing for this manuscript.

REFERENCES

[1] Jibilian, Isabella and Katie Canales. The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. 15 April 2021. Web.

[2] Park, Donghui and Michael Walstrom. Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. 2017 October 2017. Web.

[3] Berger, Andreas. What is Log4Shell? The Log4j vulnerability explained. 2021 December 2021. Web.

[4] Rosenbaum, Eric. Microsoft has a $20 billion hacking plan, but cybersecurity has a big spending problem. 8 September 2021. Web.

[5] Microsoft. "Microsoft Digital Defense Report." Annual Report. 2021. Document.

[6] Rockerman, Olivia. Bloomberg Technology — Cybersecurity. 30 March 2022. 23 August 2022.

[7] The MITRE Corporation. MITRE ATT&CK — Matrices. 1 April 2022. 23 August 2022.

[8] McQuillan, John, Ira Richer, and Eric Rosen. "The new routing algorithm for the ARPANET." IEEE transactions on communications 28.5 (1980): 711-719.

[9] M. Powell, J. Brule, M. Pease, K. Stouffer, C. Tang, T. Zimmerman, C. Deane, J. Hoyt, M. Raguso, A. Sherule, K. Zheng and M. Zopf, "Protecting Information and System Integrity in Industrial Control Systems Environments: Cybersecurity for the Manufacturing Sector," NIST NCCoE, Gaithersburg, 2022.

[10] Berners-Lee, Tim, James Hendler and Ora Lassila. "The Semantic Web." Scientific American (2001).

[11] Li, R., Dai, W., He, S., Chen, X., & Yang, G. (2019, October). A knowledge graph framework for software-defined industrial cyber-physical systems. In IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society (Vol. 1, pp. 2877-2882). IEEE.

[12] Yan, Zhihao, and Jingju Liu. "A Review on Application of Knowledge Graph in Cybersecurity." 2020 International Signal Processing, Communications and Engineering Management Conference (ISPCEM). IEEE, 2020.

[13] He, Xudong, et al. "A security analysis method of security protocol implementation based on unpurified security protocol trace and security protocol implementation ontology." IEEE Access 7 (2019): 131050-131067.

[14] Joshi, Ketki, Karuna Pande Joshi, and Sudip Mittal. "A semantic approach for automating knowledge in policies of cyber insurance services." 2019 IEEE International Conference on Web Services (ICWS). IEEE, 2019.

[15] Amato, Flora, et al. "An application of semantic techniques for forensic analysis." 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2018.

[16] Qi, Yulu, et al. "An APT Attack Analysis Framework Based on Self-define Rules and Mapreduce." 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC). IEEE, 2020.

[17] Kang, Ji, et al. "Analysis System for Security Situation in Cyberspace Based on Knowledge Graph." 2021 7th International Conference on Big Data and Information Analytics (BigDIA). IEEE, 2021.

[18] Qi, Yulu, et al. "Association analysis algorithm based on knowledge graph for space-ground integrated network." 2018 IEEE 18th International Conference on Communication Technology (ICCT). IEEE, 2018.

[19] Chen, Lanxiang, et al. "CASE-SSE: Context-aware Semantically Extensible Searchable Symmetric Encryption for Encrypted Cloud Data." IEEE Transactions on Services Computing (2022).

[20] Onwubiko, Cyril. "Cocoa: An ontology for cybersecurity operations centre analysis process." 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, 2018.

[21] Mitra, Shaswata, et al. "Combating Fake Cyber Threat Intelligence using Provenance in Cybersecurity Knowledge Graphs." 2021 IEEE International Conference on Big Data (Big Data). IEEE, 2021.

[22] Piplai, Aritran, et al. "Creating cybersecurity knowledge graphs from malware after action reports." IEEE Access 8 (2020): 211691-211703.

[23] Zhu, Zheng, et al. "Cyber security knowledge graph based cyber attack attribution framework for space-ground integration information network." 2018 IEEE 18th International Conference on Communication Technology (ICCT). IEEE, 2018.

[24] Yeboah-Ofori, Abel, et al. "Cyber threat ontology and adversarial machine learning attacks: analysis and prediction perturbance." 2021 International Conference on Computing, Computational Modelling and Applications (ICCMA). IEEE, 2021.

[25] Chukkapalli, Sai Sree Laya, et al. "Cyber-physical system security surveillance using knowledge graph based digital twins-a smart farming usecase." 2021 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, 2021.

[26] Dasgupta, Soham, et al. "Cybersecurity Knowledge Graph Improvement with Graph Neural Networks." 2021 IEEE International Conference on Big Data (Big Data). IEEE, 2021.

[27] Mittal, Sudip, et al. "Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities." 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). IEEE, 2016.

[28] Narayanan, Sandeep Nair, et al. "Early detection of cybersecurity threats using collaborative cognition." 2018 IEEE 4th international conference on collaboration and internet computing (CIC). IEEE, 2018.

[29] Joshi, Arnav, et al. "Extracting cybersecurity related linked data from text." 2013 IEEE Seventh International Conference on Semantic Computing. IEEE, 2013.

[30] Satyapanich, Taneeya, Tim Finin, and Francis Ferraro. "Extracting rich semantic information about cybersecurity events." 2019 IEEE International Conference on Big Data (Big Data). IEEE, 2019.

[31] Li, Yongfei, et al. "Intelligent Answer System Based on Vulnerability Knowledge Graph." 2021 7th International Conference on Computer and Communications (ICCC). IEEE, 2021.

[32] Carvalho, Rodrigo, Michael Goldsmith, and Sadie Creese. "Investigating Malware Campaigns With Semantic Technologies." IEEE Security & Privacy 17.1 (2019): 43-54.

[33] Piplai, Aritran, et al. "Knowledge enrichment by fusing representations for malware threat intelligence and behavior." 2020 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, 2020.

[34] Garrido, Josep Soler, Dominik Dold, and Johannes Frank. "Machine learning on knowledge graphs for context-aware security monitoring." 2021 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2021.

[35] Choi, Chang, and Junho Choi. "Ontology-based security context reasoning for power IoT-cloud security service." IEEE Access 7 (2019): 110510-110517.

[36] Lundquist, Doug, Kunpeng Zhang, and Aris Ouksel. "Ontology-driven cyber-security threat assessment based on sentiment analysis of network activity data." 2014 International Conference on Cloud and Autonomic Computing. IEEE, 2014.

[37] Bandi, Charan, et al. "Ontology-driven framework for trend analysis of vulnerabilities and impacts in IOT hardware." 2021 IEEE 15th International Conference on Semantic Computing (ICSC). IEEE, 2021.

[38] Asamoah, Claude, et al. "Powering filtration process of cyber security ecosystem using knowledge graph." 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE, 2016.

[39] Merah, Yazid, and Tayeb Kenaza. "Proactive Ontology-based Cyber Threat Intelligence Analytic." 2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI). IEEE, 2021.

[40] Mendsaikhan, Otgonpurev, et al. "Quantifying the significance and relevance of cyber-security text through textual similarity and cyber-security knowledge graph." IEEE Access 8 (2020): 177041-177052.

[41] Ou, Yunjia, Tianyang Zhou, and Junhu Zhu. "Recommendation of cyber attack method based o n knowledge graph." 2020 International Conference on Computer Engineering and Intelligent Control (ICCEIC). IEEE, 2020.

[42] Pingle, Aditya, et al. "Relext: Relation extraction using deep learning approaches for cybersecurity knowledge graph improvement." Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. 2019.

[43] Zhengqiu, He, et al. "Research of Secure Service Composition Based on Semantic Security Policy." 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2016.

[44] Zhong, Xiaofeng, et al. "Research on Automated Cyber Asset Scanning Tools based on Cybersecurity Knowledge Graph." 2021 7th International Conference on Computer and Communications (ICCC). IEEE, 2021.

[45] Kriaa, Siwar, and Yahia Chaabane. "SecKG: Leveraging attack detection and prediction using knowledge graphs." 2021 12th International Conference on Information and Communication Systems (ICICS). IEEE, 2021.

[46] Wu, Songyang, Yong Zhang, and Xiao Chen. "Security assessment of dynamic networks with an approach of integrating semantic reasoning and attack graphs." 2018 IEEE 4th International Conference on Computer and Communications (ICCC). IEEE, 2018.

[47] Nimbalkar, Piyush, et al. "Semantic interpretation of structured log files." 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI). IEEE, 2016.

[48] Sleeman, Jennifer, Tim Finin, and Milton Halem. "Temporal Understanding of Cybersecurity Threats." 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). IEEE, 2020.

[49] Yang, Jing, et al. "Tensor-Based Knowledge Fusion and Reasoning for Cyberphysical-Social Systems: Theory and Framework." IEEE Systems, Man, and Cybernetics Magazine 8.2 (2022): 31-38.

[50] Piplai, Aritran, et al. "Using knowledge graphs and reinforcement learning for malware analysis." 2020 IEEE International Conference on Big Data (Big Data). IEEE, 2020.

[51] Syed, Zareen, et al. "UCO: A Unified Cybersecurity Ontology." 2016.

[52] O. Lassila, R. Swick and others, Resource Description Framework (RDF) Model and Syntax Specification, WWW Consortium, 1999.

[53] D. McGuinness, F. Van Harmelen, et al., OWL web ontology language overview, W3C recommendation, World Wide Web Consortium, 2004.

[54] Elluri, Lavanya, et al. "A BERT Based Approach to Measure Web Services Policies Compliance With GDPR." IEEE Access 9 (2021): 148004-148016.

[55] Elluri, Lavanya, Ankur Nagar, and Karuna Pande Joshi. "An integrated knowledge graph to automate gdpr and pci dss compliance." 2018 IEEE International Conference on Big Data (Big Data). IEEE, 2018.

[56] Joshi, Karuna Pande, Lavanya Elluri, and Ankur Nagar. "An integrated knowledge graph to automate cloud data compliance." IEEE Access 8 (2020): 148541-148555.

[57] Elluri, Lavanya, et al. "A policy-driven approach to secure extraction of covid-19 data from research papers." Frontiers in big Data 4 (2021).

[58] Kim, Dae-young, Lavanya Elluri, and Karuna P. Joshi. "Trusted Compliance Enforcement Framework for Sharing Health Big Data." 2021 IEEE International Conference on Big Data (Big Data). IEEE, 2021.

[59] Elluri, Lavanya, Karuna Pande Joshi, and Anantaa Kotal. "Measuring semantic similarity across eu gdpr regulation and cloud privacy policies." 2020 IEEE International Conference on Big Data (Big Data). IEEE, 2020.

[60] Elluri, Lavanya, and Karuna Pande Joshi. "A knowledge representation of cloud data controls for EU GDPR compliance." 2018 IEEE World Congress on Services (SERVICES). IEEE, 2018.

[61] Kurniawan, Kabul, Fajar J Ekaputra and Peb R Aryan. "Semantic Services Description and Compositions: A Systematic Literature Review." 2nd International Conference on Informatics and Computational Sciences. 2018.

[62] The MITRE Corportation. MITRE ATT&CK Updates - October 2019. 7 July 2020. 23 August 2022.