Novel Methods for Vulnerability-Based Risk and Security Assessment in Cyber-Physical Systems and IoT

Ferhat Arat[1,*]

[1]Samsun University, Department of Software Engineering, Samsun, Türkiye

Abstract

Cyber-physical systems (CPS) and the Internet of Things (IoT), which are widely recognized for their facilitative and efficiency-enhancing role across various domains of daily life, have simultaneously become increasingly exposed to threats due to inherent characteristics, weaknesses, and deficiencies in the devices and networks they comprise. Identifying, modeling, and measuring the potential impact of risks, vulnerabilities, and threats on these systems constitutes the foundational step toward realizing a comprehensive security assessment. In this context, the adoption of a graph-based perspective, which consists of modeling, risk and vulnerability analysis, and security evaluation, offers efficient, practical, and realistic solutions for both structural and behavioral analysis. A review of the existing literature reveals that there are few studies that simultaneously address vulnerability modeling, quantitative risk measurement, and holistic security assessment within a unified, compact framework. In this work, we illustrate the research methodology and the literature gaps of the PhD thesis using an ontology-driven, method-based risk assessment model. We contribute to the identification and detection stages of security management through graph-based approaches and risk quantification. The proposed model aims to establish a novel methodological foundation that provides a systematic representation of vulnerability and risk assessment in specialized systems such as CPS and IoT.

Keywords

Risk and vulnerability analysis, threat modeling, Internet of Things security, cyber security, graph-based security

1. Introduction

As IoT environments grow in scale and complexity, the huge volume of interconnected devices has elevated security from a secondary concern to a fundamental design requirement [1]. The complex relationships among devices and the high volume of data exchange have made security a fundamental requirement. The first step in managing security based on vulnerabilities and risks is consistent modeling of system assets and their relationships. From this perspective, attack graphs, vulnerability graphs, and attack trees stand out as representative models of network structures that consider devices, their interactions, and potential paths established through compromised nodes [2, 3]. An attack graph models the devices and their connections within a system and enables the identification of possible attack paths across them. Widely adopted services provided by IoT and related domains are often accompanied by significant security vulnerabilities. Certain production-related issues have led to the neglect of security concerns, resulting in devices being deployed without adequate security mechanisms [4]. Most of the internet-connected devices and components have been reported to be vulnerable and susceptible to cyber risks.[5]. Several databases and organizations report and define these vulnerabilities and threats. Common Vulnerabilities and Exposures (CVE), National Vulnerability Database (NVD), and Common Weakness Enumeration (CWE) are examples of such organizations and repositories used to measure, analyze, and identify threats and vulnerabilities in devices and systems. However, even when some vulnerabilities are identified and defined, existing organizations do not comprehensively tackle all concerns, protection mechanisms, and evaluation methodologies [6].

In this context, the following fundamental research question will guide the evaluation of a significant part of this study: *Can an adaptable, efficient, and practical methodology be developed for vulnerability-*

Baltic DB&IS 2026 Conference Forum and Doctoral Consortium, 28 June - 1 July 2026, Tartu, Estonia

*Corresponding author.

ferhat.arat@samsun.edu.tr (F. Arat)

0000-0002-4347-0016 (F. Arat)

based risk assessment in cyber-physical systems? A graph theory-based reference model provides a foundational backbone for representing system assets, while hybrid mathematical risk assessment approaches enable the quantitative evaluation of potential impacts. Furthermore, leveraging vulnerability scores from established databases and organizations as real data inputs establishes a data-driven and verifiable framework for security and risk management.

This paper introduces the step-by-step process of conducting research, describes the research methodology, identifies literature gaps, and proposes contributions for the PhD thesis.

2. Research questions and objectives

The main goal of this PhD research is to develop an efficient, adaptable, and applicable risk assessment methodology for CPS and IoT systems composed of heterogeneous assets and components, accounting for network structure. The model will be designed by both modifying and improving existing graph-based approaches. In this context, a vulnerability dataset will be created by considering organizations that identify and share known vulnerabilities, a hybrid risk calculation infrastructure will be developed, and a holistic structure will be designed using graph approaches. In addition, attack vectors will be created by defining the behavior of each component in the system, both individually and across the network, from both the attacker and the security administrator perspectives. A generic risk assessment will be presented by demonstrating the system's stability using different scenarios. To achieve this goal, the study is conducted according to a defined systematic structure. In this context, five core research questions (RQs) are formulated to outline the general framework of the proposed methodology. The research questions are given below.

[RQ1]: What are the common graph-based approaches for the vulnerability-based risk assessment of IoT systems?

In RQ1, we aim to identify widely used applications, frameworks, methods, and algorithmic approaches that employ graph-based structures for CPS and IoT systems. The results obtained from the literature review are of critical importance for defining the boundaries of the core contributions of the PhD thesis and for making existing gaps apparent.

[RQ1.1]: Which graph-theoretic risk assessment approaches for system modeling and attack path detection provide the most efficient performance in terms of runtime, computational complexity, and resource utilization in CPS and IoT environments?

In RQ1.1, the graph-based approaches identified in RQ1 are systematically evaluated for relevance, considering their underlying methods, employed algorithms, and performance metrics. These approaches are filtered based on their suitability and applicability for the scope of the PhD work, ensuring the identification of the most appropriate methodological direction. Using a comparative analysis of the existing literature, the most applicable and efficient approaches are selected to form the methodological foundation of the thesis.

[RQ2]: Which commonly used algorithms can be customized and traditional graph-based methods employed to improve the efficiency and accuracy of detecting vulnerability-based attack paths in cyber-physical systems in risk assessment?

In RQ2, in addition to conventional graph traversal algorithms, we investigate the performance of greedy algorithms, such as Dijkstra, Bellman–Ford, and Floyd–Warshall, by adapting them to account for vulnerabilities in CPS and IoT environments. We model the potential progression of an attacker exploiting these vulnerabilities and, accordingly, consider the detectability of isolated nodes. The proposed approach is then evaluated against existing methods using specific performance metrics and computational complexity to obtain initial results for the work.

[RQ3]: How can quantitative risk calculation and threat assessment methods be developed for system assets and network-level vulnerabilities to enable measurable and structured risk evaluation?

In RQ3, we propose formal equations to quantify risk and threat for each individual asset, considering the network structure modeled by using graph-based representations. In this context, we develop

hybrid formulations that leverage metrics defined for device, connection, and attack-path variables, using widely adopted scoring mechanisms such as the Common Vulnerability Scoring System (CVSS) and existing scoring methods in the literature.

[RQ4]: Which sample case scenarios and data sets can be used to simulate and validate algorithmic approaches, schemes, and methods proposed throughout the PhD work?

In RQ4, we aim to simulate the sub-models and the holistic approach developed throughout the thesis, while measuring real-time execution performance, quantifying risk, and computing asymptotic complexity. The proposed models are validated by constructing real-world vulnerability datasets derived from sources such as CVE, NVD, and CWE. By designing CPS and IoT-specific scenarios and incorporating both static and dynamic data, we present a generic and environment-independent reference model for vulnerability and risk-based security assessment.

[RQ5]: How could vulnerability and risk assessment methods be improved and automated to ensure dynamic and real-time security evaluation by integrating continuously updated vulnerability data?

In RQ5, we aim to extend the methods presented in RQ2–RQ4 with dynamic risk analysis capabilities, considering the variability and mobility of network structure and vulnerabilities. Dynamic and automated methods are planned to be developed to automatically retrieve data from NVD, CVE, EPSS, and other widely adopted vulnerability sources based on the entities present in the network, and to periodically update this data to measure system-wide risk levels and perform security assessments. The significance of these changes for security experts and administrators would be determined through statistical methods.

3. Research method and proposed contributions

The PhD research is structured by four fundamental research phases, each aligned with the corresponding research questions. The progression of this work is illustrated in Figure 1.

1. **Phase 1 - Investigation:** To identify the state-of-the-art techniques, existing studies in the literature are examined and current methods are addressed to answer RQ1 and RQ1.1. In this phase, a systematic literature review (SLR) is conducted to identify and define the basic concepts, risks, vulnerabilities, and the graph-based approaches proposed to address security issues [1]. The SLR study is presented to investigate graph-based risk, vulnerability, and attack assessment methodologies for cyber-physical and IoT systems. Finally, following RQ1, the foundations for the PhD research are established, while the identified gaps are filtered to use in subsequent phases and the suitable methods for sub-approaches are reported.
2. **Phase 2 - Sub-model Development:** At this stage, examined and filtered methods in RQ1, are used to construct sub-models. Conventional and greedy algorithms, which are selected after literature comparisons and analysis, are customized to improve running time and computational complexity. To conduct RQ2 and progress PhD work, several studies are presented for preliminary results.
3. **Phase 3 - Risk Quantification:** In this phase, we extend the studies and intermediate results obtained in the first two phases by introducing risk quantification. Hybrid methods are developed by considering risk scoring approaches presented in widely used vulnerability databases and existing literature. Calculating individual and system-wide risk in complex heterogeneous systems such as CPS and IoT, and subsequently performing threat and security assessment, constitutes a significant process. In this regard, we address the research problem presented in RQ3 by developing novel intermediate models and proposing sub-methods.
4. **Phase 4 - Validation and Evaluation:** In this phase, various case scenarios are generated to simulate and validate the models developed across the first three phases. For each asset included in the scenarios, real vulnerability records are obtained from CVE and mapped accordingly. Then, simulations are conducted using different input parameters according to the generic structure of

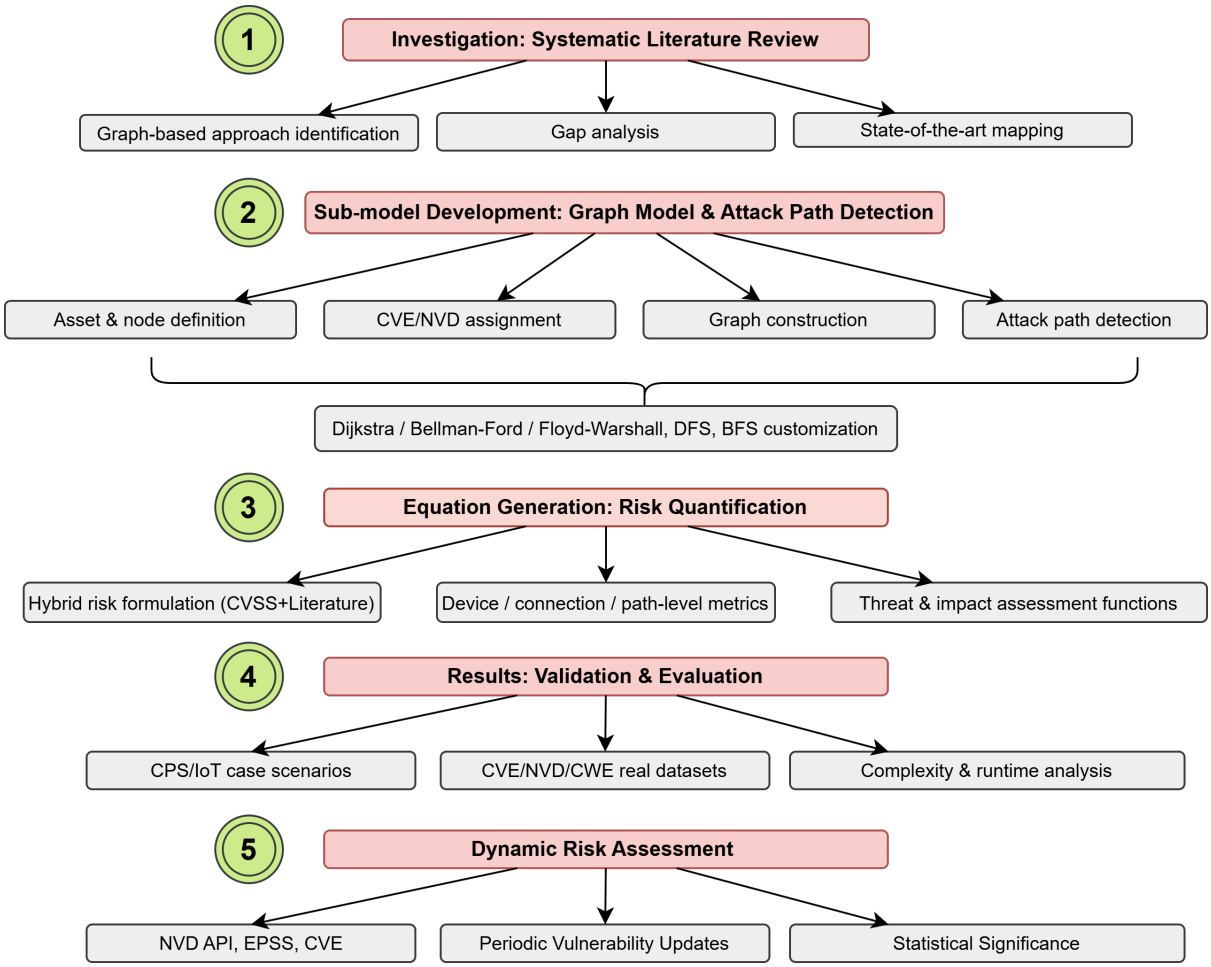

Figure 1: Overview of the proposed research workflow and contributions.

the developed vulnerability-based risk analysis and security assessment model. The results are compared against existing studies in the literature and reported comprehensively.

5. **Phase 5 - Dynamic Risk Assessment:** In this phase, we extend the vulnerability risk analysis methods developed in previous phases by automatically retrieving vulnerabilities periodically published via CVE and updated by NVD. This enables dynamic system network assessment at defined intervals. To facilitate the management of these changes, we present statistical significance testing for system administrators using statistical methods. Furthermore, our objective is to develop an automated approach by also focusing on quantitative risk changes.

Following the explained research methodology, the main contributions of the PhD thesis can be summarized as follows:

- **Development of Graph-Based Vulnerability and Threat Modeling for System Modeling:** This PhD research aims to represent existing risks and threats in the CPS and IoT domains using graph theory technologies. The primary goal is to provide a foundation for identifying potentially vulnerable assets and clearly visualizing their connections.
- **Developing Deterministic, Adaptive, and Intelligent Security Models:** The aim is to develop deterministic models by expanding existing approaches and methods in the literature. The goal is to present vulnerability-based risk analysis by developing generic approaches integrated with real-time data and efficient in terms of execution time and asymptotic complexity, and to compare them with state-of-the-art methods.
- **Defining Quantitative Risk Assessment Metrics with Hybrid Approaches:** Within the scope of this thesis, one of the main objectives is to provide hybrid standard risk calculation methods

with existing approaches in the literature, enabling the quantification of system vulnerability-based risk calculations.

- **Generic Model Testing and Optimization with Different Case Scenarios and Data Considering CPS and IoT Networks:** Finally, it is planned to test the presented algorithmic approaches and risk quantification methods in different case scenarios. Vulnerability matching will be performed using open data sources such as NVD, CVE, and CWE. The proposed models will offer improved solutions based on complexity, execution time, and efficiency for systems consisting of different assets such as defense, transportation, smart grid, and smart home.

4. Conducted studies and preliminary results

The first year of the PhD focused on state-of-the-art, concentrating on a general security definition for CPS and IoT technologies. In this context, fundamental concepts are addressed using a general-to-specific approach considering RQ1. First, a SLR study is performed [1].In the SLR study, 28 studies are examined with a focus on graph-based IoT security solutions and algorithmic approaches for deterministic security assessment. The main outcomes of this study are: 1) a comprehensive overview of repeatable, predictable, and deterministic graph-based structures, 2) a detailed comparative analysis of existing approaches encompassing design, algorithm, data, and simulation dimensions, 3) a structured comparison of the literature based on technique, complexity, case scenarios, and additional criteria, and 4) a systematic identification of graph-based solutions addressing attacks, vulnerabilities, and weaknesses in IoT environments.

Table 1 presents a summary of selected studies included in the SLR conducted within the scope of PhD research. This study, which addresses the core concepts and literature review emphasized in RQ1, defines fundamental security basics and proposed works, revealing varying gaps.

In the scope of RQ2, an attack tree-based graph model is introduced to accurately model attack paths and perform risk assessment for the entire system [25]. In this graph-based approach, IoT network devices are modeled as nodes, and inter-node interactions are structured based on physical parameters, such as transmission range. Attack paths are detected using Depth-First Search (DFS) and the Floyd-Warshall algorithm, providing individual and cumulative risk calculations at a fundamental level. The proposed approach is compared against existing methods and demonstrates improved asymptotic complexity.

Subsequently, a graph-based vulnerability model is proposed to represent devices, connections, and vulnerabilities in IoT-based networks [28]. A modified DFS algorithm is developed to identify possible attack paths across the system. Security assessment is performed at three levels: node level, attack path level, and network level, where risk scores are calculated based on each node's impact score, its CVSS value, and its degree of connectivity. Furthermore, the developed attack path filtering approach has reduced asymptotic complexity compared to existing ones.

In the final study, a novel graph-based approach is developed to model various threat types in IoT networks [29]. A customized DFS algorithm is integrated with graph-based analysis to optimize threat path detection in terms of runtime and efficiency. A unified algorithm combining risk threshold values, cumulative threat metrics, hop length, and critical node count is designed for threat path reduction. The proposed method is compared with the existing graph-based threat assessment model to demonstrate improvements in runtime and computational complexity.

Next, to address RQ3, two quantitative risk calculation sub-methods are proposed for CPS and IoT systems. First, a hybrid, quantitative risk assessment framework is constructed by incorporating the vulnerabilities of primary devices and their attack probabilities [30]. In this context, individual device-based risk and attack probability calculations from the literature are combined with path-level and graph-level risk modeling as a comprehensive risk computation method [28, 32].

Second, a risk-quantification-based study is proposed for low-power and lossy IoT networks, accounting for device and routing-path vulnerabilities and risks [31]. Incorporating real-time vulnerability data through device characteristics, network attributes, and CVSS scores, quantitative risk assessments are

Table 1
Summary of reviewed studies in [1]: approach, algorithm, data, and case scenario

Paper	Vuln./Attack Graph	Risk Computing	Algorithm	Focused Attack	Case Scenario
[7]	✓	✓	Greedy	General	Solar Array Mgmt.
[8]	✓	✓	Greedy	General	Network topology
[6]	✓	✓	Greedy, DFS	General	Custom graph
[9]	✓	✓	Greedy	General	Custom graph
[10]	✓	✓	Greedy, BFS	General	Custom graph
[11]	✓	✓	Greedy	General	Smart airport
[3]	✓	✗	Greedy	General	SCADA water treatment
[12]	✓	✓	Greedy	Malware infection	Smart home
[13]	✓	✗	Greedy	Sinkhole attack	EIoT smart home
[14]	✓	✓	Greedy	General	Network topology
[15]	✓	✓	Greedy	General	Maritime supply chain
[2]	✗	✓	Greedy	General	IoT healthcare
[16]	✓	✗	Greedy	General	Not given
[17]	✓	✓	Greedy, HMM	General	Network topology
[18]	✓	✗	Greedy, RPL	Ranking attack	Smart manufacturing
[19]	✓	✗	Greedy	Sinkhole attack	Edge-based IoT
[20]	✓	✓	Greedy	General	IoT hypothetical
[21]	✓	✓	Edmonds', DFS	General	Multi-cloud network
[22]	✓	✓	Greedy	General	Smart grid
[23]	✓	✓	MulVal, NLP, IOTA	General	Smart home
[24]	✓	✓	Greedy	General	Transportation network
[25]	✓	✓	Greedy, Floyd-Warshall, DFS	General	Smart logistics
[26]	✓	✓	SCC, MLC	General	SCADA water treatment
[27]	✓	✗	Greedy, RPL	Flooding attack	Custom graph
[28]	✓	✓	Greedy, DFS	General	Smart home
[29]	✓	✓	Greedy, DFS	General	Custom graph
[30]	✓	✓	Modified IOTA, RWB	General	Border surveillance
[31]	✓	✓	Modified RPL	General	Custom graph

performed at the device, path, and overall network levels.

Table 2 summarizes the proposed studies for the PhD work and highlights their core contributions.

Table 2
Summary of the studies conducted within the scope of the PhD research

Study	RQ	Approach	Algorithm	Key Contribution	Case Scenario
[25]	RQ2	Attack tree-based graph model	DFS, Floyd-Warshall	Attack path detection; individual and cumulative risk calculation	Smart logistics
[28]	RQ2	Graph-based vulnerability model	Modified DFS	Three-level security assessment (node, path, network); attack path filtering	Smart home
[29]	RQ2	Novel graph-based threat model	Customized DFS	Threat path reduction; unified algorithm with cumulative threat metrics	Custom graph
[30]	RQ3	Hybrid quantitative risk framework	Modified IOTA, RWB	Device-based risk and attack probability; path- and graph-level risk modeling	Border surveillance
[31]	RQ3	Risk quantification for lossy IoT	Modified RPL	Quantitative risk at device, path, and network levels using CVSS	Custom graph

5. Background and related works

Graph-based approaches offer the advantage of providing a strong mathematical framework for analysis and for assessing the system's overall security posture in heterogeneous ecosystems such as CPS and IoT. In this structure, interconnected devices and components are represented, and the network topology is clearly visible; threats and the non-isolated assets they affect can be handled with ease. Thus, complex attack paths can be detected, device vulnerabilities can be analyzed, and the overall security posture of the system can be assessed. In this context, well-known organizations and risk management standards such as ISO 27001 [33] and the NIST Cybersecurity Framework [34] serve as guidelines for evaluating and responding to cyber threats.

In addition to well-known organizations, the literature addresses vulnerabilities and security issues in CPS and IoT [1]. These existing works tackle vulnerability-based risk assessment from varying perspectives. In [26], a graph-based method was proposed that uses strongly connected components to detect minimum attack paths with linear complexity, addressing the NP-hard nature of the minimum cut problem via a min-label cut approach. Similarly, in [6], an attack graph-based system was presented for cyber attack path detection and dynamic risk management, employing a DFS-based approach with constraints to identify non-circular attack paths. In another study, [12], a graph-based threat analysis model was introduced that accounts for dynamic topology changes and malware propagation, addressing risk computation and mitigation across the entire network using greedy approaches. Finally, in [8], a vulnerability assessment model was developed to evaluate maximum attack path flows in IIoT environments, where node and edge relationships in the attack graph were analyzed to determine network-wide risk severity.

Given well-known organizations and existing literature, security assessment for CPS and IoT technologies is critical. In this context, modeling the network, defining assets, obtaining vulnerabilities, and measuring risk levels and threat severity constitute a significant research area. Therefore, for this PhD research, we focus on developing graph-based, efficient, generic, and adaptable solutions for vulnerability-based risk analysis and security assessment.

6. Work in progress

The studies presented in the previous phases address static vulnerability-based risk assessment and attack path detection. However, IoT environments are inherently dynamic, with vulnerabilities evolving, device configurations changing, and new CVE records continuously published. Existing approaches largely rely on static datasets, which limit their ability to reflect a system's current security posture. To address this limitation, a dynamic risk assessment (DRA) framework will be proposed as part of the ongoing PhD research. In Figure 2, the conceptual workflow is illustrated.

The proposed framework aims to integrate real-time CVE data retrieved via the NVD API with graph-based IoT network representations to enable continuous vulnerability monitoring. Attack paths are planned to be identified through topological analysis, and a hybrid statistical methodology is intended to detect devices with statistically significant risk changes over time. To validate the DRA framework, generating multiple domain-specific case scenarios, including smart grid and traffic, is planned, ensuring a comprehensive evaluation.

7. Concluding remarks

In this paper, we discussed the PhD thesis research to present a deterministic, quantitative, and compact methodology for novel vulnerability-based risk analysis and security assessment in cyber-physical systems. Progressing step by step through the formulated research questions, sub models are developed and the preliminary studies of the thesis are completed to obtain initial results adressing RQ1–RQ4. Graph-based methods are simulated on varying case scenarios using the developed quantitative computation metrics to provide reference models for researchers and professionals working on the security of

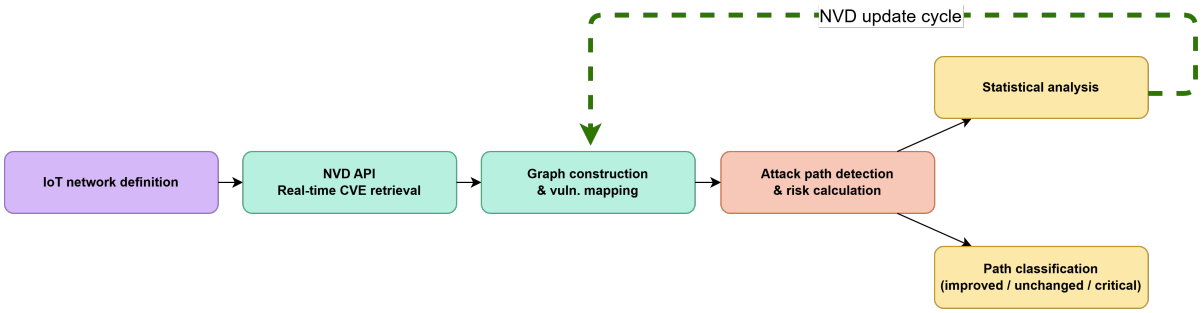

Figure 2: The abstract representation of the planned work for DRA.

CPS and IoT systems. In addition to initial contributions, we are currently working on a security assessment based on dynamic vulnerability management, considering the variability of network topology and up-to-date vulnerability definitions. Through RQ5, statistical methods are being developed alongside existing approaches to enable the automation of reference models and real-time vulnerability-aware security assessment. Finally, experts would be consulted to verify and validate the effectiveness of all sub-models and frameworks developed within the PhD thesis.

Acknowledgments

Ferhat Arat is a Ph.D student at the Department of Computational Sciences, Ondokuz Mayıs University, Türkiye, under the supervision of Sedat Akleylek. He has received a scholarship to perform his Ph.D. studies at University of Tartu under the supervision of Mubashar Iqbal. He is supported by the Scientific and Technological Research Council (TÜBİTAK) under the 2214-A International Research Fellowship for PhD Students.

Declaration on Generative AI

The author(s) have not used Generative AI tools to adjust the text's language and tone.

References

[1] F. Arat, A. Karakaya, S. Akleylek, A taxonomy of graph-based risk, vulnerability, and attack assessment methods in iot systems, Journal of Information Security and Applications 97 (2026) 104360.

[2] I. Stellios, P. Kotzanikolaou, C. Grigoriadis, Assessing iot enabled cyber-physical attack paths against critical systems, Computers & Security 107 (2021) 102316.

[3] A. T. Al Ghazo, M. Ibrahim, H. Ren, R. Kumar, A2g2v: Automatic attack graph generation and visualization and its applications to computer and scada networks, IEEE Transactions on Systems, Man, and Cybernetics: Systems 50 (2019) 3488–3498.

[4] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, N. Kumar, Iot vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges, IEEE access 8 (2020) 168825–168853.

[5] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, W. Ni, Anatomy of threats to the internet of things, IEEE communications surveys & tutorials 21 (2018) 1636–1675.

[6] N. Polatidis, M. Pavlidis, H. Mouratidis, Cyber-attack path discovery in a dynamic supply chain maritime risk management system, Computer Standards & Interfaces 56 (2018) 74–82.

[7] G. George, S. M. Thampi, A graph-based security framework for securing industrial iot networks from vulnerability exploitations, IEEE access 6 (2018) 43586–43601.

[8] H. Wang, Z. Chen, J. Zhao, X. Di, D. Liu, A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow, Ieee Access 6 (2018) 8599–8609.
[9] B. Yiğit, G. Gür, F. Alagöz, B. Tellenbach, Cost-aware securing of iot systems using attack graphs, Ad Hoc Networks 86 (2019) 23–35.
[10] M. Yi, X. Xu, L. Xu, An intelligent communication warning vulnerability detection algorithm based on iot technology, IEEE Access 7 (2019) 164803–164814.
[11] G. George, S. M. Thampi, Vulnerability-based risk assessment and mitigation strategies for edge devices in the internet of things, Pervasive and Mobile Computing 59 (2019) 101068.
[12] G. Kavallieratos, N. Chowdhury, S. Katsikas, V. Gkioulos, S. Wolthusen, Threat analysis for smart homes, Future Internet 11 (2019) 207.
[13] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. Rodrigues, Y. Park, Designing efficient sinkhole attack detection mechanism in edge-based iot deployment, Sensors 20 (2020) 1300.
[14] X. Liu, A network attack path prediction method using attack graph, Journal of Ambient Intelligence and Humanized Computing (2020) 1–8.
[15] N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, H. Mouratidis, From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks, Evolving Systems 11 (2020) 479–490.
[16] V. Shakhov, I. Koo, Graph-based technique for survivability assessment and optimization of iot applications: V. shakhov, i. koo, International Journal on Software Tools for Technology Transfer 23 (2021) 105–114.
[17] Y. Ma, Y. Wu, D. Yu, L. Ding, Y. Chen, Vulnerability association evaluation of internet of thing devices based on attack graph, International Journal of Distributed Sensor Networks 18 (2022).
[18] A. Seyfollahi, M. Moodi, A. Ghaffari, Mfo-rpl: A secure rpl-based routing protocol utilizing moth-flame optimizer for the iot applications, Computer Standards & Interfaces 82 (2022) 103622.
[19] A. Bilal, S. M. N. Hasany, A. H. Pitafi, Effective modelling of sinkhole detection algorithm for edge-based internet of things (iot) sensing devices, IET Communications 16 (2022) 845–855.
[20] M. A. Ramazanzadeh, B. Barzegar, H. Motameni, Automatic generation of threat paths in internet of things-based systems, IET Communications 16 (2022) 2394–2405.
[21] G. Stergiopoulos, P. Dedousis, D. Gritzalis, Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in industry 4.0: G. stergiopoulos et al., International Journal of Information Security 21 (2022) 37–59.
[22] T. D. Le, M. Ge, A. Anwar, S. W. Loke, R. Beuran, R. Doss, Y. Tan, Gridattackanalyzer: A cyber attack analysis framework for smart grids, Sensors 22 (2022) 4795.
[23] Z. Fang, H. Fu, T. Gu, P. Hu, J. Song, T. Jaeger, P. Mohapatra, Towards system-level security analysis of iot using attack graphs, IEEE Transactions on Mobile Computing 23 (2022) 1142–1155.
[24] K. Ntafloukas, L. Pasquale, B. Martinez-Pastor, D. P. McCrum, A vulnerability assessment approach for transportation networks subjected to cyber–physical attacks, Future Internet 15 (2023) 100.
[25] F. Arat, S. Akleylek, Attack path detection for iiot enabled cyber physical systems: Revisited, Computers & Security 128 (2023) 103174.
[26] A. T. Al Ghazo, R. Kumar, Critical attacks set identification in attack graphs for computer and scada/ics networks, IEEE Transactions on Systems, Man, and Cybernetics: Systems 53 (2023) 5604–5613.
[27] S. Ankam, N. S. Reddy, A mechanism to detecting flooding attacks in quantum enabled cloud-based lowpower and lossy networks, Theoretical Computer Science 941 (2023) 29–38.
[28] F. Arat, S. Akleylek, A new method for vulnerability and risk assessment of iot, Computer Networks 237 (2023) 110046.
[29] F. Arat, S. Akleylek, Modified graph-based algorithm to analyze security threats in iot, PeerJ Computer Science 9 (2023) e1743.
[30] F. Arat, S. Akleylek, Z. Y. Tok, A hybrid graph-based risk assessment and attack path detection model for iot systems, IEEE Access (2025).
[31] F. Arat, S. Akleylek, Security-aware rpl: Designing a novel objective function for risk-based routing with rank evaluation, Computer Networks (2025) 111122.

[32] H. Yang, H. Yuan, L. Zhang, Risk assessment method of iot host based on attack graph, Mobile Networks and Applications 29 (2024) 1504–1513.
[33] ISO, ISO/IEC 27001:2022 Information Security Management Systems, https://www.iso.org/standard/27001, 2022. Accessed: 2026-04-04.
[34] NIST, Cybersecurity Framework, https://www.nist.gov/cyberframework, 2018. Accessed: 2026-04-04.