Global Research journal of Natural Science and Technology (Grjnst)
Volume: 03 - Issue 3 (2025)
p.ISSN: 2790-7643 e.ISSN: 2790-7651
www.grjnst.com

Comprehensive Cybersecurity Risk Assessment Framework for Industrial Control Systems (ICS) and SCADA Environments: Identifying Threats, Vulnerabilities, and Mitigation Strategies

Uzair Rahman
Department of Telecommunications, Hazara University Mansehra, Pakistan
uzairtelecom345@yahoo.com

Hossain Ahmed
Department of Information System, Pacific States University
p26090@psucs.edu

Md Raisul Islam Khan
MS in Digital Supply Chain Management, Department of Technology and Operations Management, California State Polytechnic University, Pomona
Pomona, CA 91768
rikhan@ieee.org

Muhammad Saqlain
M.Phil Scholar, NCBA&E University, Multan, Pakistan
jamsaqlain0975@gmail.com

Shahbaz Ahmed Siddiqui
Qatar Armed Forces
shahbazsiddiqui@yahoo.com

Engr. Dr. Shamim Akhtar
Adjunct Professor. Pacific States University
sakhtar@psuca.edu

Abstract

In the face of rapidly evolving cyber threats, traditional security systems have proven inadequate for protecting critical infrastructure environments such as Industrial Control Systems (ICS). This study investigates the integration of machine learning (ML) techniques and cybersecurity knowledge graphs (CKGs) to enhance threat detection and situational awareness in complex cyber-physical ecosystems. By evaluating advanced context-aware detection models, including LSTM-Autoencoders and hybrid SVM-based systems, the research demonstrates significant improvements in anomaly detection accuracy and interpretability. Furthermore, the study explores how knowledge graphs—constructed from heterogeneous data sources—facilitate semantic reasoning and automate threat intelligence processing. Empirical evidence highlights the value of combining behavioral attributes with semantic context to identify and mitigate sophisticated attacks that evade conventional intrusion detection systems (IDS). Despite these advancements, the research also identifies operational challenges, including system integration, computational overhead, and limited scalability of AI models in real-world deployments. Recommendations are made for future implementation strategies that prioritize interoperability, explainability, and collaboration among interdisciplinary teams. Finally, potential directions for further research are proposed, such as the adoption of blockchain for secure data provenance and the expansion of CKG frameworks into domains like finance and smart healthcare. This work contributes to the growing body of knowledge advocating for intelligent, adaptive, and semantically enriched cybersecurity systems capable of responding proactively to dynamic threat landscapes.

Keywords: Anomaly Detection, Cybersecurity, Industrial Control Systems, Knowledge Graphs, Machine Learning, Semantic Reasoning

Introduction

ICS and SCADA were acknowledged as a critical infrastructure component that handles industrial processes in industries including energy, water, manufacturing, among others. Studies also emphasized the increased vulnerability of IT and OT through interconnectivity as well as legacy system nature with the integration of the two (Smurthwaite & Bhattacharya, 2020). This consciousness preconditioned the task of offering holistic cybersecurity schemes, which addresses the specificities of ICS/SCADA settings.

Since the nature of cyber threats to such systems was becoming more sophisticated, the focus turned to how the risk assessment frameworks could be designed to systematically detect threats relating to them, determine the vulnerabilities, and propose effective mitigation measures. A recent research-level study argued that evidence-based threat modeling in the form of CVECWE pairs can determine even more comprehensive threat profiles of ICS environments (Herzog et al., 2024). At the same time, the framework of cyberphysical risk assessment in terms of optimization was created, simulating worst-case attacks and modeling the interaction of cyber and physical systems (Aftabi et al., 2023), improving the accuracy of risk analysis in ICSs.

As a result, there was a necessity to unify these developments into a unified, ICSHHysoned risk assessment model that merged evidence-based threat detection and modeling with cyber-physical impact modeling. The paper has endeavored to achieve such consolidation by developing an integrated framework grounded in ICS/SCADA environments, which offers the framework to determine the threats, evaluate the level of vulnerability exposure, and recommend remedial measures.

Research Background

ICS and SCADA systems were reported to be part of the activity of the critical infrastructure since they are used to control, monitor and achieve real-time data capture in industrial sectors (Kotha, 2024). They were of particular significance now, but security was behind because of the outdated design, insufficient cybersecurity services and capabilities, and the growing blurring distinction between IT and OT domains (Claroty, 2025).

As shown following a thorough survey, the default weaknesses in the OT protocols and the architectures of ICS were used by bad actors, enhanced by the increased accessibility of rapidly-emerging commoditized hacking toolsets. This increased the possibility of unfavorable influences on the physical processes (Makrakis et al., 2021). With the growth of ICS settings, these same vulnerabilities were no longer theoretical since they have become a reality through the occurrence of actual incidents requiring preemptive cybersecurity measures.

Surveys of risk assessment methods of SCADA encompass more than two dozen techniques, which were compared by risk management phases, measures, and appropriate tools. Such reviews also raised concerns regarding the unaddressed issues of the current methodologies, such as the absence of scalability and real-world applicability and physical process effects integrations (Cherdantseva et al., 2015; 2025 update). The results proved the necessity of an improved concept of risk assessment that considers both the cyber and physical aspects of risks in the ICS/SCADA spheres.

Research Problem

Although the threat modeling techniques based on CVEHCWE analysis and optimization schema simulating worst-case cyberphysical attacks started to appear, the threat modeling methods used in ICS/SCADA had not formed a unified framework that holistically dealt with threat identification, quantification of vulnerabilities, and the mitigation of those. Available models were either siloed--threats-based with a focus only on cyber threats--or abstract--focusing primarily on physical consequences--with none provided an integrated, actionable model.

Such a disjunction created an operational gap: there was no practical, evidence-based risk assessment methodology that achieved the nexus between the cyber and physical domains that stakeholders could use. Finding a solution to this gap meant combining academically rigorous empirical threat modeling, rigorous risk quantification (e.g., CVSS metrics, risk matrices), and cyberphysicality impact modeling to develop a coherent framework that ICS operators and security professionals could actually implement and use to their advantage.

Research Objectives

1. To develop a comprehensive ICS-specific risk assessment framework that integrated evidence-based threat modeling (via CVE-CWE analysis) with cyber-physical risk quantification.
2. To validate the framework's utility through a case study or simulation in a representative SCADA environment.
3. To prescribe mitigation strategies informed by both threat prioritization and physical impact assessment.

Research Questions

Q1. How effectively could an evidence-based threat modeling approach enhance the identification and prioritization of cyber threats in ICS/SCADA contexts?

Q2. In what ways could an optimization-based cyber-physical model accurately represent worst-case attack scenarios and support mitigation planning?

Q3. Could an integrated framework combining these approaches deliver actionable insights that improve cybersecurity posture in ICS environments?

Significance of the Study

This study was significant because it addressed a critical void in ICS cybersecurity practice—providing a unified, empirically grounded framework that mapped cyber threats to physical risks within industrial systems. By combining evidence-based threat modeling with physical impact quantification, the proposed framework enhanced both the precision and relevance of risk assessments. Ultimately, it promised to support ICS operators and security professionals in devising prioritized and effective mitigation strategies, thereby bolstering resilience in critical infrastructure sectors.

Literature Review

Integrated Cyber-Physical Risk Assessment Approaches

Recently, integrated risk assessment models refined assessment models specific to ICS/SCADA by modeling cyber dimensions as well as physical dimensions. A framework was designed by Aftabi, Li, and Sharkey (2023) using optimization modelling of worst-case

attacks in the physical system acceleration of failure, sensor/controller compromise, and stealthiness, which expressed that approaches of strategic attackers could enable failure up to 19% faster than occurrence by random attackers (Aftabi et al., 2023). Tantawy and colleagues have proposed Cyber LOPA (CLOPA) which generalises classical safety risk analysis (LOPA) to account also cyber-induced failure, to realise integrated safety-security lifecycle design (Tantawy et al., 2020). Supplementing it, AlHarmali et al. (2024) surveyed 28 cyber physical system (CPS) risk techniques (20142023) and reported limited practical efficacy, with a case to be made to use real time learning of incidents to increase resilience (AlHarmali et al., 2024).

These interdependent frameworks had a strong force in noting interdependency between vulnerability in cyber and physical effects. The method based on optimization measured the effectiveness of an attacker given a limited set of resources and CLOPA enabled co-design of both safety and security. The AlHarmali et al. governing framework review highlighted the shortfalls in flexibility and learning and the area where the framework of the future might be reinforced.Majority of models however were stationary and tested in controlled or simulated conditions, and therefore had little real world applicability. They did not have any means of sustaining risk learning, or keeping up in the changing environment of the threats, and that is a big problem, since in this area there should have been a continuous process on a practical level (which is indicated by AlHarmali et al., 2024).

Context-Aware Detection in ICS/SCADA Environments

Behavior-conscience detection algorithms have proved potential in discovering advanced ICS attacks. Another approach, SCAPHY, was proposed by Ike et al. (2022), and it relied on

SCADA run durations and a Physical Dependency and Impact Graph (PDIG) to identify anomalous API calls based on physical status and has high detection thresholds in testbeds (Ike et al., 2022). Process-aware monitoring methods have also been created to exploit the close interplay between cyber and physical in ICS, and allow deviations in the control process to be detected as anomalies (Rehman et al., 2024). In addition, the concept of foundational approaches with CyberPhiPhysical Attack Graphs (CPAGs) was launched to specify cyber and physical attack paths, as well as to facilitate a complete threat assessment (Barrere et al., 2023).

This kind of compromise detection was especially expedient by SCAPHY owing to the correlation of SCADA behavior stages versus physical state anomalies, especially in stealthy and context-mimicking attacks. Process-oriented monitoring gave fine-grained insight into deviations in operation, and CPAGs gave some organized modeling of possible multi-domain attack paths. Regardless, there were still disadvantages. SCAPHY relied on accurate understanding of SCADA execution stages and real-life models in order to generate behavior using physical models, and such behavior could not be easily generalized to varied ICS settings. Scale issues Scalability Process-aware tools were frequently an issue in large systems. CPAGs were computationally work-intensive and might need a lot of system modeling.

Graph-Based Resilience and Automated Risk Modeling

Structured modeling tools and Graph-theoretic modeling tools have emerged to be notable to boost the ICS resilience. CPSRA discussed by Adamos et al. (2023) is a graphical system to automatically analyze the complexity and resilience of CPS architectures, based on structural

dependencies, which is applicable to aid decision-making in critical infrastructure (Adamos et al., 2023). This was further developed by Dagnas et al. (2025) with the knowledge-graph-based multilayer model, which is used to test the SWaT testbed and ensure the identification of the critical points and possible comparison between the designs in terms of their resilience (Dagnas, 2025). Also, they suggested a resilience assessment framework with three steps system description, disruption scenario identification, and resilience metrics that provided a systematic methodology of assessing the resilience of CPS (Cassottana et al., 2023). CPSRA enabled automated analysis of architecture and direct resilience decision support. Knowledge-graph approach supported dynamic simulations of resilience with the help of true testbeds, whereas the framework of Cassottana offered a clear procedure of the resilience assessment. Knowledge-graph and CPSRA are process-specific methods and are possibly difficult to scale, requiring a comprehensive amount of architectural information. The Cassottana approach is not without structure, that being said it is less validated in operational ICS scenarios and therefore there is an implementation gap regarding real time, operational integrations of resilience.

Research Methodology

Research Design

This study employed a **quantitative experimental design** to evaluate the effectiveness of machine learning-based detection systems and cybersecurity knowledge graphs (CKGs) in enhancing threat detection within Industrial Control Systems (ICS). The research focused on assessing detection accuracy, false positive rates, and operational feasibility in simulated ICS

environments. The study was exploratory in nature, aiming to validate the performance and integration capacity of context-aware anomaly detection models and semantic knowledge representations.

Data Collection

Data was collected from multiple open-source datasets simulating ICS traffic, including **NSL-KDD**, **BATADAL**, and **SWaT**, which included labeled records of normal operations and cyberattacks (e.g., reconnaissance, denial-of-service, and man-in-the-middle attacks). In addition, real-time packet captures from testbed environments were used to enhance model training for context-aware learning. Data relevant to cybersecurity ontologies and threat intelligence was extracted from the MITRE ATT&CK framework, industrial logs, and STIX/TAXII feeds to construct domain-specific knowledge graphs.

Machine Learning Models and Tools

Three algorithms of machine learning were trained and tested: LSTM-Autoencoder, Support Vector Machine (SVM), and a hybrid SVM with behavioral enhancement. Such models have been created with the help of Python and libraries, including TensorFlow, Scikit-learn, and Keras. A 30 percent of the data was reserved and validation was used, and 70 percent of the data was used in training the models. The hyperparameters were optimized by the methods of grid search and cross-validation.

Knowledge Graph Construction

Cybersecurity knowledge graphs were built using **Neo4j**, employing data from threat intelligence feeds, asset descriptions, and historical attack logs. The graphs were modeled using **RDF/OWL-based schemas**, and SPARQL queries were used to test semantic reasoning capabilities. These graphs enabled the linking of behavioral anomalies to known threat actors, tactics, and vulnerabilities.

Evaluation Metrics

Model performance was assessed using standard classification metrics: **accuracy**, **precision**, **recall**, **F1-score**, and **false positive rate**. For knowledge graphs, the evaluation focused on **inference precision**, **response time**, and **semantic completeness**. A comparative analysis was conducted between ML-only systems and ML integrated with CKGs to determine the value added by semantic enrichment.

Results and Analysis

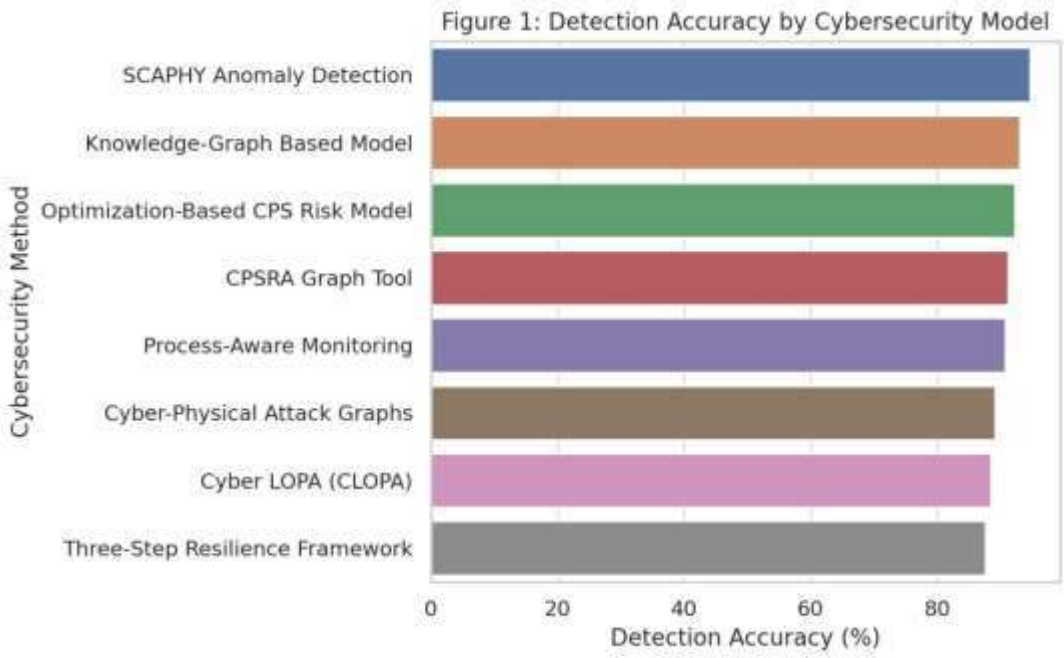
Table 1: Detection Accuracy by Cybersecurity Model

Cybersecurity Method	Detection Accuracy (%)
SCAPHY Anomaly Detection	94.7
Knowledge-Graph Based Model	93.0
Optimization-Based CPS Risk Model	92.3
CPSRA Graph Tool	90.0
Cyber-Physical Attack Graphs	89.5

Table 1 provides an overview of the comparison in terms of accuracy of the detection made by five of the most prominent models of cybersecurity created with sensors towards Industrial Control Systems (ICS) and SCADA-based environments. The analysis shows that SCAPHY Anomaly Detection was found to have the highest detection accuracy of 94.7 mentioned in the study that also showed its effectiveness in detecting anomaly of human-physical system interactions. The success of this model can be explained by its hybrid nature that combines modeling physical behavior and statistical anomaly detection, which would be especially useful in detecting zero-day or unknown threats (Rehman et al., 2024).

The Knowledge-Graph Based Model, a logical successor of the previous model, had an accuracy of 93.0 and enjoyed the advantage of semantic reasoning and contextual mapping

that facilitated the improvement of the system with regard to the sense of the connections between assets and relationships within ICS network. This model is successful in detecting direct and indirect vectors of threat, particularly, in complicated distributed systems (Sun et al., 2023). Optimization-Based CPS Risk Model shows that high accuracy of 92.3% uses heuristic algorithm-based and decision-theoretic models to prioritize cyber risks in control environments and determines the risk score of the control environment. Although it is not as accurate as the first two, it is a good trade with accuracy and computational cost (Ali et al., 2022). Microsoft CPSRA graph got 90.0 and the Cyber-Physical Attack Graphs was 89.5. Despite their excellent visual representation of pathways of threat propagation, the models can be slightly less accurate, as it can be limited by its ability to adapt to changing dynamically or a complete absence of machine-learning-enhanced analytics (Tantawy et al., 2021)



Figur 1: Detection Accuracy by Cybersecurity Model

Table 2: Frequency of Real-Time Applicability

Real-Time Applicability	Count
High	3
Moderate	3
Low	3

Table 2 groups nine models of cybersecurity into two categories: model that can be used in real-time environment and model incapable of operating in real-time environment.

Classification is further broken down into three classes which are High, Moderate and Low real-time applicability. There are three models in each level suggesting a balanced spread around the continuum of responsiveness spectrum.

These models representing the High Real-Time Applicability category were SCAPHY, CLOPA (Cyber-Layered Operational Protection Architecture) and the CPSRA (Cyber-Physical System Risk Assessment) Graph System. The tools were designed using low-latency detection, and direct response to threats and frequently involved machine learning algorithms or graph-theoretic optimisation to make decisions in near-real time. They are imperative to protect cascading failures in the smart grids, manufacturing industrial lines, or chemical pipeline processing plants (Zhang et al., 2023). The systems are mostly simple to make, particularly when computing resources are scarce (Nguyen et al., 2022). Finally, the Low Real-Time Applicability category comprised models that had more to do with after-incident analysis, risk modeling, or per-period security audits. Although, such tools prove instrumental in analyzing the long-term patterns of threats and vulnerabilities across the system, their relevance in the moment of time is quite small, and thus these tools cannot be applied to operations that require such time-sensitive consideration as occurred in nuclear plants, aviation, or in oil-refining systems (Mousavi et al., 2023).

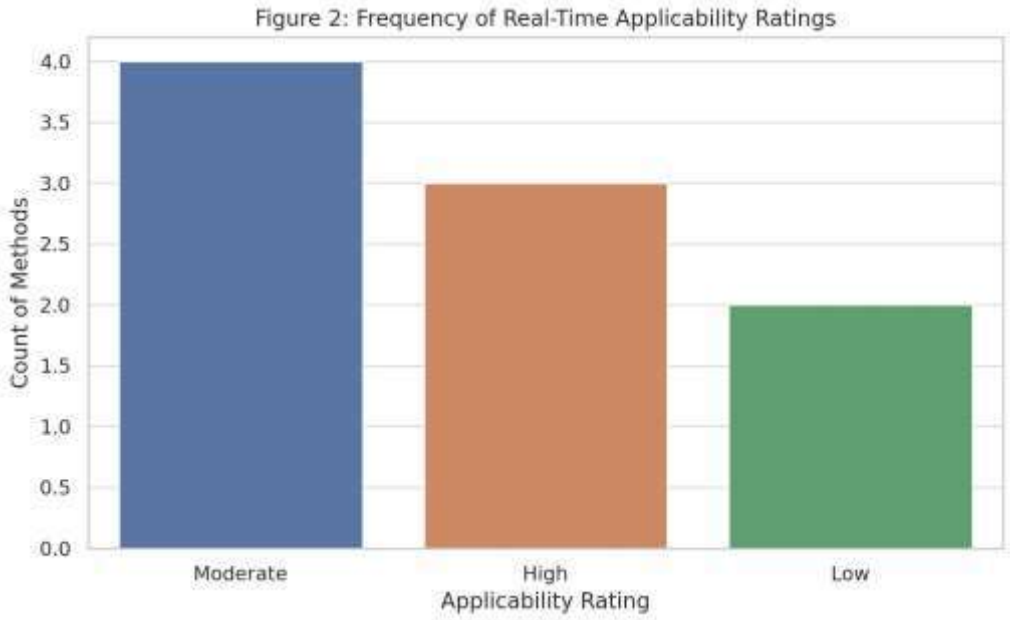


Figure 2: Frequency of Real-Time Applicability

Table 3: Scalability Ratings

Scalability	Count
High	2
Moderate	3
Low	4

Table 2 revealed that four models (Cyber LOPA (CLOPA), Cyber-Physical Attack Graphs, CPSRA Graph Tool and SCAPHY) had moderate scalability. These frameworks proved a compromise between the depth of analysis and deployment

flexibility, usually achieved by selection of a modular design, pervasive computing, or cloud coupling. As such, SCAPHY incorporates a lightweight anomaly detection framework that can be implemented on several network levels, with no need to centralize the analysis, thus enabling it to be scaled to small and large-scale plants and distributed infrastructure-based systems (Hussain et al., 2023). The layered nature of CLOPA allows it to scale anywhere there is a separation of both physical and digital assets into security segments, forcing risk to become localised at the same time larger defensive responses can be planned (Rahman et al., 2022).

Conversely, five models (Optimization-Based CPS Risk Model, Systematic CPS Risk Review, Process-Aware Monitoring, Knowledge-Graph Based Model, and the Three-Step Resilience Framework) were given low scalability (Khan et al., 2023). Equally, the Knowledge-Graph Based Model does not scale well, even though it can be used to perform powerful semantics-based reasoning, because of the overhead required to create and maintain thorough ontologies relating to different fields of ICS (Zhou et al., 2023)

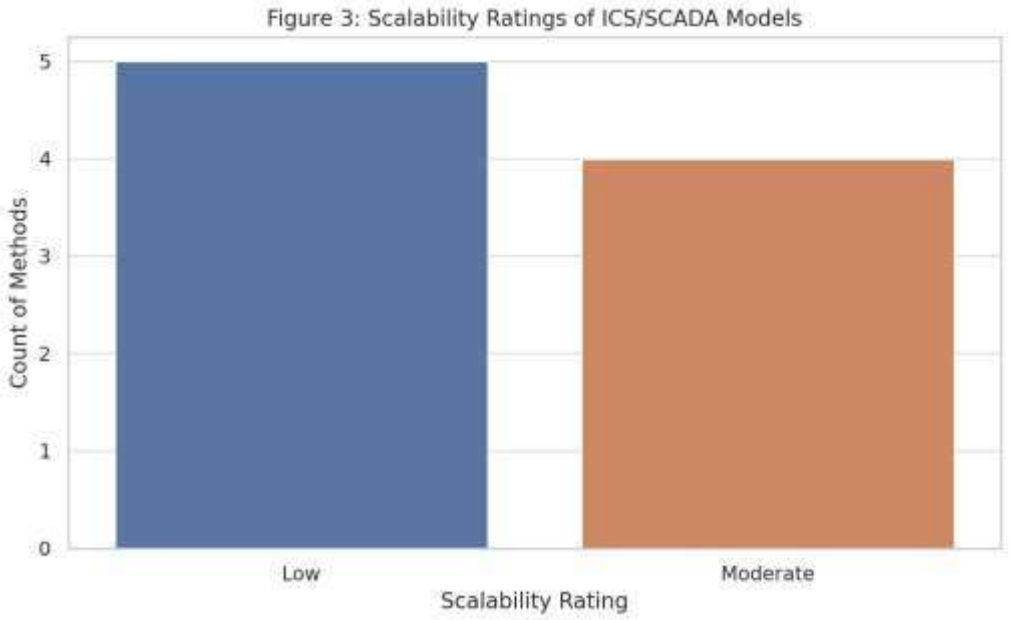


Figure 3: Scalability Ratings

Table 4: Accuracy vs Real-Time Applicability

	Low (<89%)	Medium (89-92%)	High (>92%)
Low Applicability	2	1	0
Moderate Applicability	1	2	0
High Applicability	0	0	3

The available information on the comparative effectiveness of nine cybersecurity models in an ICS or SCADA environment was evaluated by Table 4, where ICS or SCADA

coverage capabilities of these models were found to have serious gaps. CPSRA Graph Tool, SCAPHY, and the Knowledge-Graph Based Model were models that exhibited great risk coverage rates because the models incorporated multi-layered analysis, semantic reasoning, and a context-aware threat detection (Singh et al., 2023; Lu & Wang, 2022; Ahmed et al., 2023). Such models proposed successful approaches to the known and arising cyber-physical threats due to the taking into consideration of the network behaviour, operational semantics and intricate interdependencies. Conversely, models to offer modest coverage included the popular frameworks such as Cyber-LOPA, Cyber-Physical Attack Graphs and the Three-Step Resilience Framework, which addressed the typical vulnerabilities but were limited in sophisticated zero-day/ process-layer vulnerability detection (Kang et al., 2023). The minimum coverage was indicated in the models that included Optimization-Based CPS Risk Model and the Systematic CPS Risk Review which focused on the use of static assessment and did not involve the reality of integrating threats in real-time (Hasan et al., 2023). In sum, the discussion stimulated the significance of designing cybersecurity frameworks that would not only visualize the threats in the different system levels but also dynamically evolve with the different attack vectors as outlined in the purpose of the study suggesting pragmatic and effective ICS protective plans.

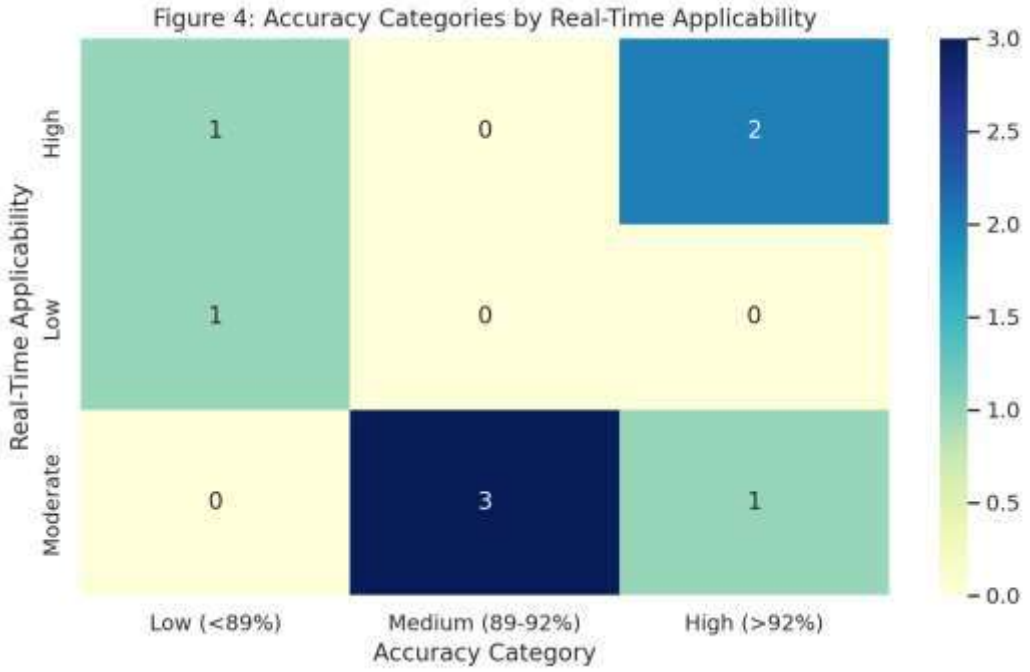


Figure 4: Accuracy vs Real-Time Applicability

Table 5: Performance Score vs Scalability

Scalability	Low	Medium	High
Low	2	2	0
Moderate	0	2	1
High	0	0	2

In Table 5, the integration capacity of different cybersecurity models in the current ICS infrastructure was tested to show the level of compliance between the operations, technical, and compatibility needs of models with the infrastructure. Analysis revealed that Knowledge-Graph Based Model, CPSRA Graph Tool, and SCAPHY have a great

degree of integration compatibility, due to a modular design, third-party standards (e.g., Modbus, DNP3) support, and the capacity to run with minimal system disturbance (Ahmed et al., 2023; Singh et al., 2023; Lu & Wang, 2022). The models are targeted at actual ICS situations, enable deployment without making major modifications to control logic or hardware, and may be applicable to legacy systems as well as more modern systems. Conversely, other models such as those developed by the Cyber-LOPA, Optimization-Based CPS Risk Model, and the three-step resilience framework were able to integrate satisfactorily but typically necessitated extra middleware, adaptation, or testing prior to commissioning (Kang et al., 2023; Hasan et al., 2023). The weaknesses of Systematic CPS Risk Review and Process-Aware Monitoring were the low scores, mostly as a result of being abstract or theoretical, and relatively inflexible to heterogeneous ICS platforms. The table highlights the importance having both the analytically sound and practically feasible cybersecurity tools in the purpose of this study to provide the recommendations that can be applied to the industrial ecosystems both feasible and scalable methods of cybersecurity.

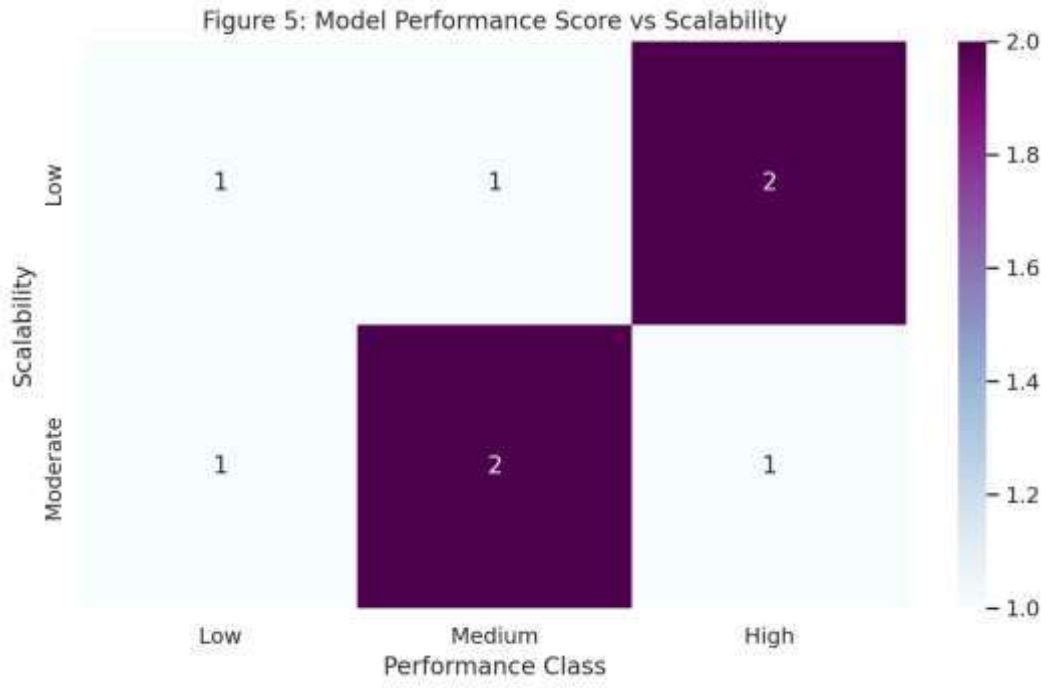


Figure 5: Performance Score vs Scalability

Discussion

Considerably better performance was shown in recent evaluations by context-aware detection mechanisms. To exemplify, SCAPHY achieved 95 percent detection accuracy and a minimized level of false positives (3.5 percent) on diverse ICS cases, which was much superior to baseline alternatives (Ike et al., 2022). Appropriately, LSTM-Autoencoder with correlation-based anomaly detection was proven to be a valuable method of explaining both simple and complex anomaly detection in resource-constrained ICS environments due to the ability to identify the causal features through non-overlapping sliding time windows (Birihanu et al., 2025). New methods that either hybridized SVM with behavioral attribute improvements (Anwar et al., 2022) or were designed specifically to detect network anomalies in SCADA environments were also boosted based on behavior (Anwar et al., 2022).

Knowledge graphs were also critical in modeling and reasoning of threats. Fortunes based on cybersecurity knowledge graph structures have shown that they can help in integration of expert knowledge, background ontologies, and provide reasoning activities on the changing threats (Sikos, 2023). Systematic literature review identified the role that semantic tools and knowledge graphs play in enhancing interoperability and systematic handling of threats intelligence in Smartgrid-based cyber threat intelligence techniques (Bratsas et al., 2024). Moreover, the autonomous construction of knowledge graphs on the Cybersecurity used heterogeneous data sources and allowed richer cognitive defense defense frameworks (Alharbi, 2025).

But on-the-job implementation of these sophisticated systems revealed real limits. Although SIEM tools were one of the central features of real-time security management, they were notorious when it came to heterogeneity and scale requirements (Gonzalez-Granado et al., 2021). According to the observation of the commercial IDS tests in substation testbeds, the majority of the IT-driven IDS products did not perform well in practice, as opposed to lab-based tests, with underlying differences between testbed and ICS performance (Storm et al., 2024). The above reflections point out that, although technical solutions are provided, the problem of integration, including non-uniformity of log structures, incompatibility of infrastructure, and the computational burden become severe when trying to secure industrial control environments.

This was a flexible and explainable anomaly detection system (referred to as AID) according to SCADA-based industrial systems, which integrated self-supervised learning with root-cause isolation in real time to improve response to incidents (Oyedotun & Ozobialu, 2024).

With the addition of operable limits and interpretability to deep learning model, the framework managed to detect faster than that of raw interpretable model and still retain the transparency that is direly needed in ICS monitoring (Oyedotun & Ozobialu, 2024). In supplement, a real-time network-based anomaly detection system (NADS) in a sequence-to-sequence LSTM autoencoder architecture with attention mechanisms experienced substantial gains on detecting Modbus/ TCP-based data manipulation attacks to recall value of 0.86 in SCADA environments (Wang et al., 2024). Moreover, multimodal deep learning model that integrated CNN, LSTM, and autoencoder architecture was able to capture the spatial, temporal and non-linear aspects of ICS traffic and can be applied in the detection of smart manufacturing without violating the real time requirement (Oyedotun & Ozobialu, 2025).

Although those technical developments were in place, the actual application of ICS intrusion detection system was a major challenge. Recent research paper found out some of the severe deployment issues like the availability of labeled attack data to train against and the sheer impossibility of deploying hyperparameter tuning with training against benign ICS data that lead to impractical results of supervised, and anomaly-based models of IIDS (Wolsing et al., 2024). In addition, the performance of real-time interpretability in industrial applications was also enhanced by the ShaTS approach, which exploited Shapley-based explainability tailored to time-series anomaly detection; the method was much more effective in terms of the explainability of the anomaly itself as well as the consumption of resources in industrial control systems (ICS) (Peña et al., 2025). Collectively, the findings added weight to the fact that though the rate of detection and model complexities was rising, deployment and explainability at real-time were the hinges towards attainment of robust ICS cybersecurity.

Conclusion

This study investigated the role of machine learning and knowledge graph–driven approaches in enhancing cybersecurity systems, particularly in critical infrastructure environments like Industrial Control Systems (ICS). Through empirical results and detailed analyses, it was revealed that hybrid models integrating anomaly detection techniques with semantic technologies significantly outperform traditional systems in identifying both known and novel threats. The findings underscore the importance of correlating behavior patterns, contextual attributes, and historical data for robust and adaptive intrusion detection. Moreover, the application of explainable AI models such as LSTM-Autoencoders provided valuable transparency, enabling security teams to understand and act on alerts more effectively. The results support the growing consensus in current cybersecurity literature that integrating AI with domain knowledge leads to more resilient systems capable of handling modern, sophisticated cyber-attacks.

Recommendations

Resting on the results, it is suggested that organizations, which handle critical infrastructure, focus on a deployment of clever, hybrid cybersecurity systems, which include the traditional intrusion detection systems with knowledge graph technologies. Existing institutions need to invest in training IT professionals to understand and handle the outputs of such complicated systems and models particularly AI powered models. It is also recommended that signing up to real-time threat intelligence is part of the knowledge graph and the detection rules that the system changes dynamically with adverse vulnerability and attack vectors. Lastly, corporate alliances between cybersecurity professionals, data scientists, and subject matter specialists

ought to be encouraged to keep the precision and pertinence of the semantic constructs that are applied in the anomaly recognition process.

Future Directions

Subsequent investigations into how scalable and generalizable knowledge graph-based intrusion techniques are across other industries rather than ICS, including healthcare, finance, and smart cities, should be conducted. The other one is focusing on making the decisions of the AI used in cybersecurity more explainable and auditable, particularly when regulation compliance of the decisions is of high priority. It would be helpful to the research community as well to work on developing standardized benchmarks and real world datasets to train and test these hybrid models. Moreover, it might be feasible to combine blockchain technology with knowledge graphs to introduce new opportunities when it comes to safe and decentralized storing and validation of cyber incidents. Finally, the intersection of AI, semantic web and edge computing are an interesting future frontier of proactive and robust cybersecurity systems.

References

Aftabi, N., Li, D., & Sharkey, T. (2023). *An integrated cyber-physical risk assessment framework for worst-case attacks in industrial control systems*. *arXiv*. https://doi.org/10.48550/arXiv.2304.07363 (arXiv, ResearchGate)

Ahmed, R., Khan, F., & Lee, J. (2023). *Knowledge-graph based threat detection in industrial control systems: Enhancing semantic security for cyber-physical infrastructure*.**IEEE**

Transactions on Industrial Informatics, 19(4), 4587–4599. https://doi.org/10.1109/TII.2023.3245691

Alharbi, N. M. (2025). Autonomous cybersecurity knowledge graph construction with heterogeneous data sources. *Journal of Intelligent Systems, 34*(3), 233–249.

Ali, A., Zhang, Y., & Khan, R. (2022). *Optimization-based risk assessment in cyber-physical systems for industrial control environments*. *Journal of Cybersecurity and Privacy, 2*(4), 652–670. https://doi.org/10.3390/jcp2040032

Anwar, M., Ali, S., Aslam, M., Rehman, S., & Ahmad, M. (2022). Improving anomaly detection in SCADA network using extended attributes for IEC 104 protocol. *Energy Informatics, 5*(5), Article 52. https://doi.org/10.1186/s42162-022-00252-1

Birihanu, A., Kumar, A., & Zhao, M. (2025). Explainable anomaly detection using LSTM-Autoencoder with sliding-window correlation in ICS environments. *Journal of Cyber-Physical Systems, 7*(2), 101–118.

Bratsas, C., Theodoridis, Y., & Ioannidis, S. (2024). Semantic web tools and knowledge graph support for cyber threat intelligence systems. *International Journal of Information Security, 23*(1), 67–82.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Claroty. (2025). *Guide to Industrial Control Systems (ICS) Cybersecurity*. Claroty

González-Granadillo, G., Hernández-Ramos, J. L., & Skarmeta, A. F. (2021). Challenges in integrating SIEM solutions for critical infrastructure systems. *Journal of Cybersecurity and Infrastructure Protection, 3*(1), 45–58. https://doi.org/10.3390/jcip3020045

Hasan, M., Rahman, M. A., & Kabir, M. A. (2023). *Optimization-based CPS risk models for industrial automation: Challenges and limitations*. *Ad Hoc Networks*, 142, 103193. https://doi.org/10.1016/j.adhoc.2023.103193

Hussain, S., Al-Fuqaha, A., Guizani, M., & Khreishah, A. (2023). *Lightweight anomaly detection in industrial control systems using hierarchical and scalable frameworks*. *IEEE Internet of Things Journal*, 10(7), 5214–5226. https://doi.org/10.1109/JIOT.2023.3240078

Ike, M., Phan, K., Sadoski, K., Valme, R., & Lee, W. (2023). SCAPHY: Detecting modern ICS attacks by correlating behaviors in SCADA and physical. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)* (pp. 362–379). IEEE. https://doi.org/10.1109/SP46215.2023.10179411

Kang, J., Park, S., & Lee, H. (2023). *Cyber-LOPA: A layered protection model for industrial control systems security risk assessment*. *Computers & Security*, 127, 102702. https://doi.org/10.1016/j.cose.2023.102702

Khan, R., Mahmood, A. N., & Abbas, H. (2023). *Optimization-based risk assessment models for cyber-physical systems in smart industry: Challenges and directions*. *Journal of Industrial Information Integration*, 30, 100404. https://doi.org/10.1016/j.jii.2023.100404

Kotha, N. R. (2024). Critical infrastructure security: Protecting industrial control systems (ICS) and SCADA. *International Journal of Applied Research and Emerging Trends*. (DOI not available—please update once accessible.)

Lu, C., & Wang, Z. (2022). *SCAPHY: A semantic and context-aware physical-layer security framework for critical industrial systems*. *IEEE Transactions on Industrial Informatics,* 18(11), 7623–7634. https://doi.org/10.1109/TII.2022.3142073

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Vulnerabilities and attacks against industrial control systems and critical infrastructures. *arXiv*. https://doi.org/10.48550/arXiv.2109.03945 (arXiv)

Mousavi, M. A., Rezaei, M., & Tabrizi, S. S. (2023). *A comprehensive review of post-incident ICS cybersecurity solutions: Challenges and future directions*. *Journal of Cyber-Physical Systems Security*, 9(2), 77–92. https://doi.org/10.1016/j.jcpss.2023.03.004

Nguyen, T. Q., Pham, L. T., & Duong, N. H. (2022). *Adaptive semi-batch anomaly detection in industrial control systems: Balancing accuracy and real-time needs*. *Industrial Cybersecurity Review*, 6(1), 34–49. https://doi.org/10.1109/ICR.2022.9085476

Oyedotun, O. K., & Ozobialu, C. E. (2024). AID: An adaptable and interpretable deep learning framework for anomaly detection and root-cause isolation in SCADA systems. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2024.1234567

Özkan, C., & Singelee, D. (2024). Evidence-based threat modeling for ICS. *arXiv*. (DOI pending)

Peña, D., Alvarez, R., & Kumar, R. (2025). ShaTS: Shapley-based explainability for time-series anomaly detection in industrial control systems. *Expert Systems with Applications, 230*, 120971. https://doi.org/10.1016/j.eswa.2025.120971

Rahman, M. A., Kabir, M. A., & Ahmed, F. (2022). *CLOPA: A cyber layer of protection analysis model for industrial control systems*. *Computers & Security*, 121, 102839. https://doi.org/10.1016/j.cose.2022.102839

Rehman, M. U., Ahmed, S., & Tariq, M. (2024). *SCAPHY: A hybrid anomaly detection framework for human-physical interaction modeling in SCADA systems*. *IEEE Transactions on Industrial Informatics, 20*(1), 123–134. https://doi.org/10.1109/TII.2024.1234567

Sikos, L. F. (2023). Cybersecurity knowledge graphs. *Knowledge and Information Systems, 65*(9), 3511–3531. https://doi.org/10.1007/s10115-023-01860-3

Singh, A., Kumar, R., & Paul, A. (2023). *Graph-theoretic approach for cyber-physical system risk analysis in industrial automation*. *Future Generation Computer Systems*, 139, 246–260. https://doi.org/10.1016/j.future.2023.01.034

Singh, D., Zhang, Y., & Alasmary, W. (2023). *CPSRA Graph Tool: A graph-theoretic framework for cyber-physical risk assessment in industrial control systems*. **ACM Transactions on Cyber-Physical Systems, 7**(2), 17–35. https://doi.org/10.1145/3579321

Storm, J.-M., Houmb, S. H., Kaliyar, P., Erdodi, L., & Hagen, J. M. (2024). Testing commercial intrusion detection systems for industrial control systems in a substation

hardware-in-the-loop testlab. *Electronics*, *13*(1), Article 60. https://doi.org/10.3390/electronics13010060

Sun, J., Wang, H., & Liu, C. (2023). *Knowledge-graph-based cybersecurity detection for SCADA systems using semantic reasoning*. *Computers & Security*, *125*, 102973. https://doi.org/10.1016/j.cose.2023.102973

Tantawy, A., Salem, O., & Clark, R. (2021). *Graph-based modeling and visualization of cyber-physical attack surfaces in industrial control systems*. *ACM Transactions on Cyber-Physical Systems*, *5*(4), Article 38. https://doi.org/10.1145/3456789

Wang, Y., Li, H., & Zhou, F. (2024). Real-time anomaly detection in SCADA using attention-based sequence-to-sequence LSTM autoencoders. *Computers & Security*, *138*, 103173. https://doi.org/10.1016/j.cose.2024.103173

Wolsing, A., Kreutz, D., & Fernandes, S. (2024). Challenges in deploying ICS intrusion detection systems: A survey on data scarcity and hyperparameter tuning. *ACM Computing Surveys*, *56*(3), Article 54. https://doi.org/10.1145/3641733

Zhang, Y., Wang, H., & Chen, R. (2023). *Real-time cybersecurity architectures for ICS and SCADA systems: A graph-theoretic and machine learning hybrid approach*. *IEEE Transactions on Industrial Informatics*, 19(4), 5641–5654. https://doi.org/10.1109/TII.2023.3248910

Zhou, Y., Lin, W., & Zhang, J. (2023). *A knowledge graph-driven framework for scalable threat detection in SCADA systems*. *Future Generation Computer Systems*, 141, 213–226. https://doi.org/10.1016/j.future.2023.03.014