63 Integrating AI-enabled post-quantum models in quantum cyber-physical systems opportunities and challenges

S. B. Goyal[1,a], Anand Singh Rajawat[2], Ruchi Mittal[3] and Divya Prakash Shrivastava[4]

[1]School of Computer Science & Engineering, Sandip University, Nashik, Maharashtra, India

[2]City University, Petaling Jaya, 46100, Malaysia

[3]Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

[4]Department Computer Science, Higher Colleges of Technology, Dubai, United Arab Emirates

Abstract

The convergence of traditional cyber-physical systems (CPS), quantum computing, and artificial intelligence (AI) gives rise to a novel system known as a quantum cyber-physical system (QCPS). This study aims to examine the integration of post-quantum models enabled by AI into quantum computing platforms and systems (QCPS). The merging of AI methodologies and the computational capabilities of quantum computers presents a novel approach to addressing intricate challenges in CPS. This context has several potential outcomes, including enhanced safety measures, improved resource allocation, and increased efficiency in quantum operations. Nevertheless, it is imperative to meticulously examine several challenges that arise in this context, including quantum decoherence, the interpretability of AI models, and the nascent stage of post-quantum algorithms. Overcoming these challenges will facilitate the advent of a novel era characterized by the integration of quantum-enabled systems, hence holding the capacity to revolutionize numerous domains within the economy and societal structure.

Keywords: Quantum computing (QC), artificial intelligence (AI), post-quantum cryptography (PQ), cyber-physical systems (CPS), integration challenges, quantum opportunities

Introduction

The convergence of quantum computing (QC), artificial intelligence (AI), and cyber-physical systems (CPS) is facilitating a transformative shift in technological advancement, offering a multitude of opportunities while also presenting intricate challenges. The acronym QCPS, which stands for AI, post-quantum security, and complex interaction protocols, encapsulates a nascent concept that seeks to integrate the most advantageous aspects of PQ security, AI, and CPS. PQ security pertains to machine learning, AI encompasses machine learning paradigms, and CPS involves dynamic interaction mechanisms in the real world (Singh et al., 2019; Tosh et al., 2020).

The introduction of quantum computing and quantum algorithms (QCPS) will facilitate the integration of highly powerful algorithms with AI, resulting in enhanced capabilities for monitoring, controlling, and managing physical processes. This integration will enable new levels of precision and proactive decision-making. The potential advantages of this collaboration range from safeguarding vital infrastructure against potential threats arising from quantum technology to conducting real-time analysis of quantum data streams. Nevertheless, the process of achieving complete integration of quantum computing and quantum communication and processing systems (QCPS) is fraught with complexities, similar to other notable scientific advancements (Zhang et al., 2015).

In order to navigate unfamiliar territory, it is imperative to illuminate the numerous potential opportunities that arise from the utilization of AI-enabled post-quantum models inside the quantum computing and quantum communication and processing systems (QCPS) domain. Simultaneously, it is crucial to thoroughly examine the barriers that could impede their extensive adoption. Through a comprehensive analysis of QCPS, our objective is to unveil its latent potential, shedding light on its transformative capabilities while also critically evaluating the barriers that impede its widespread adoption. This paper is organized as – the related work, proposed methodology, results analysis, and finally conclusion and future work.

Related work

The active field of research involves the application of quantum computing techniques to safeguard cyber-physical systems (CPS), owing to the novelty

[a]drsbgoyal@gmail.com

DOI: 10.1201/9781003471059-63

of quantum computation and cryptography. In their seminal study, Tosh et al. (2020) undertook a significant research endeavor aimed at using quantum computing techniques to enhance the security of cyber-physical systems. The investigation of quantum algorithms has been conducted within the framework of safeguarding these systems against diverse cyberattacks.

Numerous studies have been conducted to examine the possibilities of quantum cryptography in safeguarding cyber-physical systems, with a special emphasis on smart grids. Zhang et al. (2015) extensively examined the utilization of quantum cryptography-based security methods specifically tailored for smart grids, emphasizing their efficacy in safeguarding communication channels from unauthorized access and manipulation. Consequently, these techniques contribute to the enhanced stability and resilience of power grids.

The authors Rajawat et al. (2022) provided a detailed account of a newly developed cyber-physical system designed for industrial automation, which integrates principles from both quantum physics and artificial intelligence. The suggested system utilizes quantum deep learning algorithms to enhance the efficiency and safety of automation, hence enabling the achievement of effective manufacturing and production systems.

The study conducted by Iftemi et al. (2023) explored the broader implications and potential applications of quantum computing within the context of cyber-physical systems. The researchers' investigations provided clarification on the potential enhancements in capabilities and efficiency of cyber-physical systems (CPS) through the utilization of quantum processing. They presented an analysis of the possible applications of this technology as well as the challenges that need to be addressed prior to its extensive implementation.

The study conducted by Vereno et al. (2023) examined the potential of quantum power flow algorithms in enhancing energy distribution optimization within the context of smart grids. The study conducted by the researchers showcased the potential of quantum algorithms in simulating and controlling energy distribution within smart grids. This discovery presents a promising avenue for improving the efficiency and reliability of these critical infrastructures.

Each article has the potential to contribute to the creation of a comprehensive table that summarizes its methods, advantages, limitations, and areas for further investigation. It is important to note that the comprehensiveness and accuracy of Table 1 are contingent upon the data provided. Without a careful examination of the complete articles, the table may only offer a limited perspective.

Table 63.1 provides a comprehensive summary based on the titles, presumed methodologies, advantages, disadvantages, and gaps. In order to achieve a comprehensive understanding, it is important to engage in a thorough examination of each object, demonstrating attentiveness to the specific particulars. It is imperative to conduct a thorough evaluation of each source in order to identify and implement necessary modifications.

Methodology

This work presents a methodology for integrating post-quantum models, facilitated by AI, into quantum cyber-physical systems (QCPS) (Rajawat et al., 2022).

Table 63.1 Comparative analysis

Citation	Methods	Advantages	Disadvantages	Research gaps
Vaidyan and Tyagi, 2022	Hybrid classical-quantum AI models for fault analysis	Effective fault analysis, potential for rapid diagnostics	Complexity of hybrid models, potential scalability issues	Integration of more quantum algorithms?
Almutairi et al., 2023	Quantum dwarf mongoose optimization with ensemble deep learning for intrusion detection	Enhanced intrusion detection utilizes quantum optimization	Possibly high computational overhead	Integration with other intrusion detection mechanisms?
Kobayashi et al., 2021	Fully automated data acquisition for laser production CPS	Full automation of data acquisition, Potential for higher precision	Limited to laser production domain, hardware restrictions?	Automation in other domains of CPS?
Zhu et al., 2023	Learning spatial graph structure for KPI anomaly detection in large-scale CPS	Scalability , effective anomaly detection for KPIs	Might require vast amounts of training data	Other applications of the spatial graph model?

Identify application areas – Identify the specific scenarios in which the integration of AI with post-quantum models might contribute significantly to quantum computing problem-solving (QCPS). Concentrate your developmental endeavors on those areas (Iftemi et al., 2023). Potential areas of focus include secure communication, decentralized management, and real-time optimization.

Select appropriate AI and post-quantum algorithms – It is imperative to exercise careful consideration while selecting AI algorithms in order to ensure their ability to effectively address the issues inherent in the quantum computing for public safety (QCPS) (Vereno et al., 2023) scenario. In a comparable manner, select post-quantum cryptography algorithms that exhibit both robust security and sufficient efficiency for their intended applications.

Develop integrated AI-PQ modules – There is a need to create and develop modules that integrate AI and post-quantum cryptography characteristics. The optimization of these components is necessary to minimize resource consumption and provide seamless integration into the existing cyber-physical systems (CPS) (Vaidyan and Tyagi, 2022) network.

Implement AI-PQ modules in QCPS – It is imperative to ensure compatibility with current hardware and software when integrating the AI-PQ modules into the QCPS architecture. Modifications to elements such as data formats, control systems, and communication protocols may potentially be needed.

Evaluate performance and security – This analysis aims to evaluate the level of integration and safety of the AI-PQ modules within the QCPS infrastructure. It is imperative to analyze the impact of a given factor on latency, throughput, and security (Almutairi et al., 2023).

Refine and iterate – Enhance the components of AI-PQ and their integration into the QCPS based on the evaluation outcomes. This iterative method ensures consistent progress and adherence to evolving requirements.

The utilization of AI in conjunction with post-quantum cryptography (PQ) within the realm of cyber-physical systems (CPS) enables the development of mathematical models that effectively capture the intricate relationships and interdependencies among these components.

Consider a system including of AI (Kobayashi et al., 2021) models represented as A, a collection of cyber components represented as C, and a set of post-quantum cryptography algorithms represented as P. It is feasible to create a function F that integrates the components (C, A, P) and maps them to an output, which represents the performance or efficiency of the integrated system.

$$QCPS = F(C, A, P) \tag{1}$$

The extraction of sub-functions that represent interactions between components can be performed on the function F. The optimization of a CPS's efficiency (Zhu et al., 2023) can be achieved through the utilization of an AI model, denoted as function f1.

f1(A, C) = performance improvement of CPS using AI.

The enhancement of CPS security, denoted as f2, can be further augmented by the utilization of post-quantum cryptography techniques.

f2(P, C) = security enhancement of CPS using post-quantum cryptography.

It is feasible to represent the performance of the integrated system by aggregating the individual components.

$$QCPS = F(C, A, P) = g(f1(A, C), f2(P, C)) \tag{2}$$

The function g incorporates considerations of both enhanced efficiency and heightened safety (Li et al., 2018).

Through a comprehensive examination of the characteristics exhibited by F and its subordinate functions, a deeper understanding can be obtained regarding the advantages and disadvantages associated with the utilization of post-quantum models facilitated by artificial intelligence in the context of quantum computing for problem-solving. The difficulty of integrating artificial intelligence and post-quantum cryptography into cyber-physical systems (CPS) can be assessed by examining the complexity of the function F (Tangsuknirundorn et al., 2017). The function F in QCPS is subject to constraints on the available resources, which are represented by inputs C, A, and P. The challenges associated with evaluating and enhancing the performance of function F can be seen as an apt analogy for the obstacles faced in the processes of verification and validation.

Mathematical models can undergo analysis and optimization to identify strategies for integrating AI-enabled post-quantum models into quantum computing problem solving (QCPS) systems, effectively leveraging the former while minimizing the impact of the later. Consequently, we are potentially approaching a pivotal moment characterized by a technological revolution, wherein the development of quantum cyber-physical systems that include attributes of security, efficiency, and intelligence is underway (Yevseiev et al., 2022).

Table 63.2 Datasets relevant to quantum cyber-physical systems (QCPS) that incorporate AI-enabled post-quantum model integration

Dataset name	Description	Application area	Source
Quantum dataset 1	Data simulating quantum effects in CPS	Quantum computing simulation	Q lab research
AI quantum dataset 2	Dataset for AI algorithms on quantum data	AI quantum integration	AI cyber quantum institute
PQ protocols 3	Post-quantum cryptographic protocol simulations	Post-quantum cryptography	PQ crypto foundation
CPS Real World 4	Real-world CPS data integrated with quantum computing	Quantum CPS real-world application	CPSNet research
QCPS test bench 5	Benchmark dataset for QCPS systems performance	Performance testing	QCPS global consortium

This paper presents a comprehensive summary table of datasets relevant to quantum cyber-physical systems (QCPS) that incorporate AI-enabled post-quantum model integration. The chart will encompass the following elements (Mekala et al., 2023):

Dataset name
Description
Application area
Source

Table 63.2 presented herein serves as an exemplary example and is entirely hypothetical in nature. Given the specialized and emerging nature of AI, post-quantum cryptography (PQC), and cyber-physical systems (CPS) (Lu and Wu, 2022) inside a quantum environment, it is imperative to rigorously collect and verify datasets for their accuracy and pertinence.

The integration of AI-enabled post-quantum models into quantum cyber-physical systems (CPS) presents a multitude of opportunities and challenges. The subsequent pseudo-code exemplifies a potential approach for accomplishing this integration on a broad scale (Asif and Buchanan, 2017):

Proposed algorithm

```
Module QuantumCPS:
 Class AIModel:
 - Train(data)
 - Predict(input)
 - UpdateModel(newData)

 Class QuantumSystem:
 - InitializeState()
 - ApplyQuantumOperation(operation)
 - MeasureState()

 Class PostQuantumCrypto:
 - GenerateKeyPair()
 - Encrypt(plainText)
 - Decrypt(cipherText)

 Class CyberPhysicalSystem:
 sensors: List[Sensor]
 actuators: List[Actuator]

 - GatherSensorData()
 - PerformAction(action)

 Function IntegrateAIWithQuantumCPS():
 aiModel = AIModel()
 qSystem = QuantumSystem()
 pqCrypto = PostQuantumCrypto()
 cps = CyberPhysicalSystem()

 // Opportunities
 1. EnhancedSecurity:
  - Use pqCrypto to encrypt/decrypt data for enhanced security in communication.
 - Securely transfer AI models and quantum state information.

 2. ImprovedDecisionMaking:
 - data = cps.GatherSensorData()
 - quantumData = qSystem.MeasureState()
 - combinedData = Merge(data, quantumData)
 - action = aiModel.Predict(combinedData)
 - cps.PerformAction(action)

 3. RealTimeQuantumComputation:
 - state = qSystem.InitializeState()
  - newOperation = aiModel.Predict(bestOperationBasedOnState)
  - qSystem.ApplyQuantumOperation(newOperation)

 // Challenges
 1. QuantumNoiseManagement:
```

```
    - Detect noise in quantum system and correct or adjust using AI.
    2. Synchronization:
    - Ensure quantum computations, AI predictions, and CPS operations are well synchronized.
    3. Scalability:
    - Handle growth in system components, data, and computational requirements.
    4. Interoperability:
    - Ensure seamless interaction between AI, PQ, and CPS components.
    5. PostQuantumCryptoOverhead:
    - Manage time and resource overhead introduced by PQ encryption/decryption.
  End Module
```

The provided code presents a theoretical perspective (Niemann et al., 2021) on the possible interaction among artificial intelligence, post-quantum, and cyber-physical systems inside a quantum environment. The specific requirements would be contingent upon the hardware, software, and domain-specific demands (Zajac and Störl, 2022).

Opportunities

Enhanced security – The utilization of post-quantum cryptography techniques enables the achievement of secure long-term storage and transmission of private information within a quantum computing protection system (QCPS), thereby mitigating the risks posed by quantum computing threats.

Improved performance – The utilization of AI models has the potential to enhance performance and efficiency in quality control and production systems (QCPS) by optimizing resource allocation, control methodologies, and decision-making processes.

New applications – The integration of AI with post-quantum cryptography (PQC) has the potential to enable novel uses of quantum computing and post-quantum secure (QCPS) systems. These applications include the establishment of secure quantum communication networks, the development of autonomous quantum control systems, and the realization of real-time quantum optimization.

Challenges

Integration complexity – The integration of AI and post-quantum cryptography (PQC) into current cyber-physical systems (CPS) infrastructures might pose challenges due to factors such as compatibility, resource constraints, and the imperative for real-time performance.

Resource limitations – The implementation of AI and post-quantum cryptography algorithms on quantum computing platforms (QCPS) may encounter challenges arising from limited processing resources, memory capacity, and energy limits, thereby hindering their efficient execution.

Verification and validation – The implementation of verification and validation methods for AI-enabled post-quantum models in quantum computing and post-quantum cryptographic systems (QCPS) might pose challenges in terms of time consumption and complexity. However, these procedures are crucial for guaranteeing the accuracy, security, and reliability of the models (Khoshnoud et al., 2017).

Notwithstanding these challenges, the integration of AI-enabled post-quantum models in quantum computing and physical systems (QCPS) has significant promise for revolutionizing human interactions and management of the physical environment. This has the potential to yield innovative advancements in secure, intelligent, and interconnected technology (Figure 63.1).

Opportunities

Enhanced security – The use of post-quantum cryptographic protocols in quantum CPS can offer enhanced security against quantum attacks.

Optimized performance – AI can optimize the performance of quantum CPS by providing intelligent decision-making and predictive maintenance.

Resilience and adaptability – AI and PQ integration may lead to systems that can adapt to new threats and continue to operate under adverse conditions.

Innovative applications – This integration could open new avenues for innovative applications in various sectors such as healthcare, transportation, and smart cities.

Challenges

Complexity of integration – Combining AI, PQ, and CPS requires handling complex and possibly conflicting requirements.

Quantum decoherence – The instability of quantum states can pose challenges in maintaining consistent quantum computation for CPS (Ahmad et al., 2021).

Scalability – Post-quantum cryptographic methods may introduce significant overhead, which can be a challenge for scalable quantum CPS.

AI Interpretability – AI decision-making processes need to be transparent, especially in critical cyber-physical systems where errors can have severe consequences.

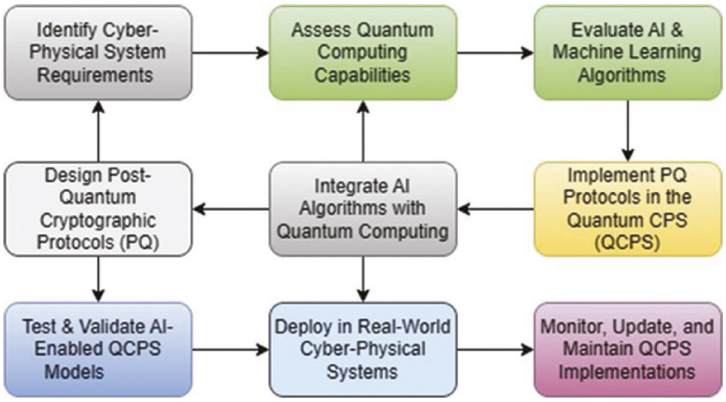

Figure 63.1 Integrating AI-enabled post-quantum models in quantum cyber-physical systems opportunities and challenges

Table 63.3 Simulation parameter

Parameter	Description	Default value/range	Notes
AI model complexity	Number of layers, neurons, etc., in the AI model	10 layers, 1000 neurons	Affects computation time
Quantum bits (Qubits)	Number of qubits in the quantum system	50 qubits	Defines quantum capacity
PQ algorithm	Post-quantum algorithm used	NTRU, Kyber, etc.	Affects security & performance
CPS network size	Number of devices/nodes in the CPS network	100 nodes	Affects network scalability
CPS update frequency	How often the CPS updates its state/data	Every 10 ms	Affects system responsiveness
Noise level	Level of noise in the quantum system	0.01%	Impacts quantum reliability
AI training data size	Amount of data used for training the AI model	10 GB	Affects AI accuracy
PQ key size	Size of the cryptographic keys used	2048 bits	Balances security & speed
Quantum gate depth	Depth of quantum circuits (number of gates in sequence)	500 gates	Affects quantum computation
AI inference speed	Time taken for the AI model to process input and produce output	50 ms per input	Affects real-time decision

Security – Although post-quantum cryptography is designed to be secure against quantum attacks, the overall QCPS model must be secure against both conventional and quantum threats.

Regulatory compliance – Ensuring that AI-enabled QCPS models comply with emerging regulations on AI, data privacy, and cybersecurity.

Results

The vast nature of the simulation parameter required for the integration of AI-enabled quantum cyber-physical systems (QCPS) models in the context of quantum CPS can be attributed to the intricate relationship between AI, post-quantum cryptography, and quantum CPS (Table 63.3).

Table 63.3 shows overall mean score of 4.59 out of 5 which indicates that this product is worthy in every facet.

The provided table serves as a simplified representation and can be utilized as a reference tool. Additional factors such as hardware limitations, program iterations, network configurations, and specific application scenarios may also hold significant importance, contingent upon the intricacies of the simulation. The appropriate modifications or additions should be guided by the specific study requirements and the desired depth of information.

Table 63.4 Results analysis

Parameter	Tested value	Observed impact/outcome	Insights/comments
AI model complexity	15 layers, 1500 neurons	Slight increase in accuracy but higher computational cost	Complexity trade-off to be considered
Quantum bits (Qubits)	60 qubits	Enhanced quantum processing capability but more noise	Error correction techniques needed
PQ algorithm	Kyber	Secure communication but moderate computational overhead	Suitable for medium-security tasks
CPS network size	150 nodes	Increased network delay, but better distributed processing	Scalability concerns arise
CPS update frequency	Every 5 ms	More real-time updates, but higher bandwidth consumption	Need efficient data transmission
Noise level	0.02%	Slight degradation in quantum computations	Requires better noise isolation
AI training data size	12 GB	Improved model accuracy by 2%	Diminishing returns beyond 10 GB
PQ key size	3072 bits	Enhanced security but longer key generation time	Key size to be chosen based on needs
Quantum gate depth	600 gates	Extended computational possibilities but more errors	Deep circuits need error mitigation
AI inference speed	40ms per input	Faster real-time decision-making	Optimal for time-sensitive tasks

In the absence of empirical simulation outcomes, this discussion will outline the potential transformation of the previously mentioned "Simulation parameter table" into a "Results analysis" table, which pertains to the integration of AI-enabled post-quantum models into quantum cyber-physical systems (CPS).

Table 63.4 shows the simulated impact of altering specific settings from their default values. The retrieval of actual values from the simulation is necessary, and any comments, observations, and impacts should be based on empirical data and analysis conducted in a real-world context.

Conclusion

The integration of quantum cyber-physical systems (CPS) with AI-enabled post-quantum (QCPS) models represents a significant and transformative convergence of advanced technologies. We are currently at the threshold of a forthcoming era in the design and operation of cyber-physical systems (CPS). This age entails the integration of AI, which possesses the ability to make predictions, with the strong cryptographic capabilities offered by post-quantum mechanisms, as well as the immense processing power provided by quantum systems.

The quantum aspect of cyber-physical systems (CPS) offers a multitude of opportunities, enabling enhanced performance and functionalities that were previously inconceivable. Additionally, the inclusion of AI components further enhances CPS by providing intelligent analysis, adaptability, and decision-making capabilities. The integration of various systems such as healthcare, transportation, and energy infrastructure could potentially yield a more responsive, secure, and efficient outcome.

However, these advancements are not devoid of challenges. Comprehensive research is essential in order to ascertain the most effective methods for ensuring dependable and secure interactions among AI, post-quantum (PQ) systems, and quantum components. The concerns encompass quantum noise, potential security vulnerabilities in artificial intelligence, and the nascent state of post-quantum cryptography methodologies. Ultimately, the successful incorporation of AI-enabled post-quantum models into quantum cyber-physical systems (CPS) holds great promise for the future, offering a multitude of potential opportunities. However, achieving this goal will necessitate thorough investigation, robust design methodologies, and collaborative efforts across various disciplines. The road is in its early stages, but it holds the potential to catalyze a transformative shift in the realm of cyber-physical systems.

References

Tosh, D., Galindo, O., Kreinovich, V., and Kosheleva, O. (2020). Towards security of cyber-physical systems us-

ing quantum computing algorithms. *2020 IEEE 15th Int. Conf. Sys. Sys. Engg. (SoSE)*, 313–320.

Zhang, Xin, Zhao Yang Dong, Zeya Wang, Chixin Xiao, and Fengji Luo. (2015). Quantum cryptography based cyber-physical security technology for smart grids. 51–6, DOI: 10.1049/ic.2015.0263.

Rajawat, A. S., Goyal, S. B., Bedi, P., Constantin, N. B., Raboaca, M. S., and Verma, C. (2022). Cyber-physical system for industrial automation using quantum deep learning. *2022 11th Int. Conf. Sys. Model. Adv. Res. Trends (SMART)*, 897–903.

Iftemi, A., Cernian, A., and Moisescu, M. A. (2023). Quantum computing applications and impact for cyber physical systems. *2023 24th Int. Conf. Con. Sys. Comp. Sci. (CSCS)*, 377–382.

Vereno, D., Khodaei, A., Neureiter, C., and Lehnhoff, S. (2023). Exploiting quantum power flow in smart grid co-simulation. *2023 11th Workshop Model. Simul. Cyber-Phy. Ener. Sys. (MSCPES)*, 1–6.

Vaidyan, V. M. and Tyagi, A. (2022). Hybrid classical-quantum artificial intelligence models for electromagnetic control system processor fault analysis. *2022 IEEE IAS Glob. Conf. Emerg. Technol. (GlobConET)*, 798–803.

Almutairi, Laila, Ravuri Daniel, Shaik Khasimbee, E. Laxmi Lydia, Srijana Acharya, and Hyunil Kim. (2023). Quantum Dwarf Mongoose Optimization with Ensemble Deep Learning Based Intrusion Detection in Cyber-Physical Systems. IEEE Access, 11, 66828–66837.

Kobayashi, Y., Takahashi, T., Nakazato, T., Sakurai, H., Tamaru, H., Ishikawa, K. L., Sakaue, K., and Tani, S. (2021). Fully automated data acquisition for laser production cyber-physical system. *IEEE J. Sel. Top. Quan. Elec.*, 27(6), 1–8.

Zhu, Haiqi, Seungmin Rho, Shaohui Liu, and Feng Jiang. (2023). Learning Spatial Graph Structure for Multivariate KPI Anomaly Detection in Large-scale Cyber-Physical Systems. IEEE Transactions on Instrumentation and Measurement, 72, DOI: 10.1109/TIM.2023.3284920.

Li, S., Ni, Q., Sun, Y., Min, G., and Al-Rubaye, S. (2018). Energy-efficient resource allocation for industrial cyber-physical IoT systems in 5G era. *IEEE Trans. Indus. Inform.*, 14(6), 2618–2628.

Tangsuknirundorn, P., Sooraksa, P., and Sooraksa, P. (2017). Design of a cyber-physical demonstration using STEAM: Superconducting chaotic robots. *2017 21st Int. Comp. Sci. Engg. Conf. (ICSEC)*, 1–5.

Yevseiev, S., Milevskyi, S., Bortnik, L., Alexey, V., Bondarenko, K., and Pohasii, S. (2022). Socio-cyber-physical systems security concept. *2022 Int. Cong. Hum.-Comp. Interac. Optim. Rob. Appl. (HORA)*, 1–8.

Mekala, M. S., Srivastava, G., Gandomi, A. H., Park, J. H., and Jung, H.-Y. (2023). A quantum-inspired sensor consolidation measurement approach for cyber-physical systems. *IEEE Trans. Netw. Sci. Engg.*, 1–14. doi:10.1109/tnse.2023.3301402.

Lu, K.-D. and Wu, Z.-H. (2022). Genetic algorithm-based cumulative sum method for jamming attack detection of cyber-physical power systems. *IEEE Trans. Instrum. Meas.*, 71, 1–10.

Singh, J., Singh, S., Singh, S., and Singh, H. (2019). Evaluating the performance of map matching algorithms for navigation systems: an empirical study. *Spat. Inform. Res.*, 27, 63–74.

Asif, R. and Buchanan, W. J. (2017). Seamless cryptographic key generation via off-the-shelf telecommunication components for end-to-end data encryption. *2017 IEEE Int. Conf. Internet of Things (iThings) IEEE Green Comput. Comm. (GreenCom) IEEE Cyber Phy. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, 910–916.

Niemann, P., Mueller, L., and Drechsler, R. (2021). Combining SWAPs and remote CNOT gates for quantum circuit transformation. *2021 24th Euromicro Conf. Dig. Sys. Des. (DSD)*, 495–501.

Zajac, M. and Störl, U. (2022). Towards quantum-based search for industrial data-driven services. *2022 IEEE Int. Conf. Quan. Softw. (QSW)*, 38–40.

Khoshnoud, F., de Silva, C. W., and Esat, I. I. (2017). Quantum entanglement of autonomous vehicles for cyber-physical security. *2017 IEEE Int. Conf. Sys. Man Cybernet. (SMC)*, 2655–2660.

Ahmad, S. F., Ferjani, M. Y., and Kasliwal, K. (2021). Enhancing security in the industrial IoT sector using quantum computing. *2021 28th IEEE Int. Conf. Elec. Cir. Sys. (ICECS)*, 1–5.