Quantum Artificial Intelligence for Cyber Security Education in Software Engineering

Maria Teresa Baldassarre[1], Mirko De Vincentiis[1], Anibrata Pal[1] and Michele Scalera[1]

[1]University of Bari Aldo Moro, Department of Computer Science, Via Edoardo Orabona 4, Bari, Italy

Abstract

The impact of Cyber Security is global, requiring immediate attention for protecting, conserving, and maintaining the integrity of any data. The need for cyber security is of utmost importance in Industry or Academics. To address this, all stakeholders should have substantial knowledge about cyber security and how to implement it. The use of published generic standards and guidelines does not describe the technologies or solutions that can be used. Currently, machine learning-based applications, serious games, or remote training can be used to bridge this gap. This paper proposes a vision model based on Quantum Artificial Intelligence (QAI) that generates secure software development (SSD) rules to educate and train developers and testers during different phases of the Software Development Life Cycle (SDLC). The proposed model trains QAI algorithms on data from industry standards, vulnerability information, and proprietary and historical data to create security rules that developers and testers can quickly adapt. Consequently, a case study about the automotive industry SSD discusses the application of the vision model.

Keywords

Cyber Security Education, Industry Education, Quantum Artificial Intelligence,

1. Introduction

The ever-growing capabilities of modern computers have empowered researchers to achieve astounding feats. The problem of Cyber Security (CS) also has become more sophisticated and, therefore, should be managed with more caution and urgency [1]. The protection of personal as well as public data and its integrity is indispensable for any software solution [2].

Due to advanced research, Artificial Intelligence (AI) techniques are used in a wide range of CS applications [3]. For example, in the automotive field, AI is used to detect attacks that exploit vulnerabilities of standard in-vehicle network protocols [4]. To create robust components that prevent attacks, automotive standards require the introduction of cybersecurity in their development strategies [5]. Machine Learning (ML) approaches have been extensively used to develop Intrusion Detection Systems for many devices [6, 7].

Emerging technologies have forayed into Quantum Computing (QC) as a viable and faster alternative to ML, and it has been proven to solve complex problems in a reasonable amount of time [8, 9]. However, commercial and broader usage of Quantum Technologies is still under consideration because of the inherent instability of quantum computers.

IS-EUD 2023: 9th International Symposium on End-User Development, 6-8 June 2023, Cagliari, Italy

teresa.baldassarre@uniba.it (M. T. Baldassarre); mirko.devincentiis@uniba.it (M. De Vincentiis); anibrata.pal@uniba.it (A. Pal); michele.scalera@uniba.it (M. Scalera)

Developing secure software is extremely challenging, even though there are different standards for secure software development, as it requires advanced skills, knowledge, and considerable time. Developers and testers in the industry cannot gain such skills overnight and, thus, need a framework and strategic training to support development and decision-making during the Software Development Life Cycle (SDLC).

This paper presents a vision model involving Quantum Artificial Intelligence (QAI) to propose a CS education and training framework for Developers and Testers, and empower the resources to make better and informed decisions during the SDLC. The model can be tailored and implemented across industries or academia. We present the related works in Section 2 and the vision model in Section 3, followed by the conclusion in Section 4, stating the potential principal gains from using the model.

2. Related Work

Implementing cyber security in diverse systems requires high skills in CS, coding efforts, and time, which calls for directed CS education and training of resources [9]. The European Union (EU) stresses the member states to increase their cybersecurity capacity by propagating CS education in their academic curriculum [10]. Also, the lack of cybersecurity skills in the European labour force should be addressed seriously by addressing and reshaping the latest educational content [11].

Alahmari et al.[12] proposed that CS Education and training can be imparted through serious games to deliver security training based on the Transactive Memory System Theory (TMS). Tioh et al. [13] also justified using serious games for CS training as it combines the benefits of both traditional and hands-on training. As per Dominguez et al. [14], remote CS training is also a viable option in the industry using cabinets with elements for automation, control, administration, and communication elements. Furthermore, industrial CS training activities can also be carried out using augmented reality-based tools as per Skorenkyy et al. [15].

In a different study [16], to attend to the expanding need for security specialists, the authors suggested a wide variety of education and training curricula based on the Cyber Security Body of Knowledge (CyBOK). Pirta-Dreiman et al. [17] adopted the Intervention Mapping paradigm to propose a cyber security educational framework incorporating validated theoretical and evidence-based approaches. Rajamäki et al. [18] proposed a framework for the education and training of healthcare workers based on the principle of interactivity, guidance, and relevancy to users' operational environment.

Cyber Security also applies to the automotive sector, where modern vehicles use the latest technologies, making them prone to remote CS attacks[19, 20]. CS education in the automotive industry renders standards like ISO/SAE 21434 [21] and Automotive SPICE (ASPICE) mandatory. Moreover, there are taxonomies to analyze and classify automotive attacks to support the development process [22]. Rahmani et al. [23] proposed a Quantum Secure Multiparty Computation (QSMC) that uses quantum features to allow secure communication between vehicles, preserving their confidential data privacy.

To date, several QAI algorithms have been published that could be used in a wide range of industries, including but not limited to transport, healthcare, pharmaceutical, etc. For instance,

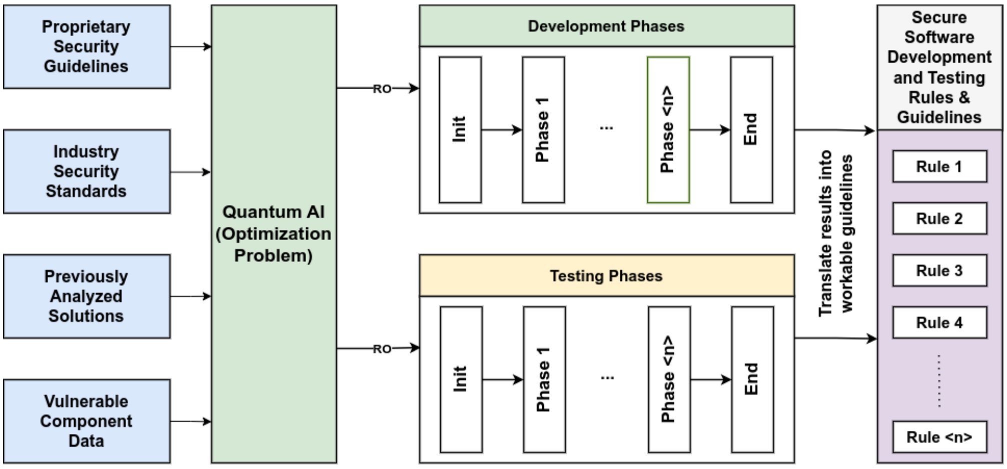
Proprietary Security Guidelines
Industry Security Standards
Previously Analyzed Solutions
Vulnerable Component Data
Quantum AI (Optimization Problem)
RO
RO
Development Phases
Init
Phase 1
...
Phase <n>
End
Testing Phases
Init
Phase 1
...
Phase <n>
End
Translate results into workable guidelines
Secure Software Development and Testing Rules & Guidelines
Rule 1
Rule 2
Rule 3
Rule 4
Rule <n>

Figure 1: ICSEQAI Vision Model to support Developers and Testers during SDLC

Quantum ML was successfully implemented to detect cyber attacks on vehicles [24]. Most QML algorithms adapt traditional ML algorithms to implement their quantum counterparts [25, 26, 27].

For these reasons, QML could emerge as a future key element of the cyber security training process in software engineering and also improve the developer's and organizations' education in SDLC.

3. Methodology

We present a vision model that we call Industrial Cyber Security Education with Quantum Artificial Intelligence (ICSEQAI), a high-level abstraction of a learning framework to support developers and testers during the SDLC (Figure:1).

As per the ICSEQAI (Figure:1) vision model, artefacts including but not limited to Company Proprietary Security Guidelines, Industry Security Standards, previously analyzed solutions or reports, and vulnerable component data can be processed and repurposed to support decision-making by the developers and testers during the SDLC. These artefacts can be translated into specific rules necessary for secure software development [28]. The rules can be mapped using industry standards, for example, automotive industry standards or global application standards like OWASP Application Security Verification Standard[1] to generate a robust model for decision-making. Quantum Artificial Intelligence (QAI) can be trained for such a constrained model to provide an optimal solution, which can be used to update existing security guidelines or standards and educate the developers and testers regarding CS during SDLC.

To understand the model, we present, as a case study, a secure software development process to fix a vulnerable automobile component. The Industry Standard for Road vehicles — Cybersecurity engineering, ISO/SAE 21434:2021 [29], a high-level guideline for security solutions in the automotive domain, does not provide concrete design ideas, making assimilation into SDLC

[1] https://owasp.org/www-project-application-security-verification-standard/

difficult. Therefore, the guide can be split into multiple rules for SDLC support. Vulnerable Electronic Control Units (ECU), building blocks of a car's internal network, can provide invaluable information about specific attacks and details about the vulnerabilities. Historical security analyses, solutions, and fixes for previous ECU attacks and vulnerabilities are equally important as they contain precious information about specific drawbacks and implemented fixes.

A constrained optimization problem can be formulated from the dataset of similar rules, standards, data, and constraints based on ISO/SAE 21434:2021, OWASP, and SDLC, which can be trained on QAI algorithms to perform Rule Optimization (RO in Figure:1), generating optimal secure development rules for vulnerability fixes. For example, ICSQAI would suggest the best K strategies among N different actions suited to a specific developmental phase, where K is the constraint (rules to fix vulnerability). These rules can be translated to update company security guidelines, propose updated standards, and educate and train Developers and Testers to adjust to newer security requirements and standards during SDLC.

The proposed ICSQAI model can be efficiently used to continuously train and educate the company resources, like architects, developers, and testers, on CS skills. The model can educate the developers by displaying automated messages providing details about secure coding rules applicable to a specific module during coding/unit testing. Whereas the testers would receive onscreen comprehensive testing guidance for newly incorporated fixes.

Finally, different QAI algorithms can be trained in different contexts to achieve the proposed goal. Quantum classification algorithms can be used to help the system in the classification of vulnerable components, whereas the optimization algorithms like constrained quadratic models (CQM) or discrete quadratic models (DQM) can generate the rules for training and education. Concurrently, reinforcement learning using variational quantum circuits can also help adapting new development guidelines to update the existing ones [30].

4. Conclusion

The likelihood of cyber-attacks is amplified by the magnitude and intricacy of the SDLC. However, only broad standards are available, and their implementation is challenging due to the dearth of necessary expertise and knowledge. Nevertheless, this gap could be overcome by adopting new solutions based on Quantum Artificial Intelligence algorithms and processes that could support Cyber Security Education in the industry. A vision model, ICSEQAI, was presented in this paper, where industry rules, standards, and information about existing vulnerable software components can be formulated as optimization problems and trained on QAI models to support the development and testing phase in the organization. To support our claim, we presented a brief case study showing the impact of the proposed learning framework in cyber security education in the automotive industry. The development of serious games can be an interesting future approach to address the issue of cyber security education in industry and academics.

Acknowledgments

This study has been partially supported by the following projects: SSA (Secure Safe Apulia – Regional Security Center, Codice Progetto 6ESURE5) and KEIRETSU (Codice Progetto V9UFIL5) funded by ”Regolamento regionale della Puglia per gli aiuti in esenzione n. 17 del 30/09/2014 (BURP n. 139 suppl. del 06/10/2014) TITOLO II CAPO 1 DEL REGOLAMENTO GENERALE ”Avviso per la presentazione dei progetti promossi da Grandi Imprese ai sensi dell'articolo 17 del Regolamento”; and SERICS (Security and Rights In the CyberSpace - PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

[1] V. S. Barletta, F. Cassano, A. Pagano, A. Piccinno, New perspectives for cyber security in software development: when end-user development meets artificial intelligence, in: 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2022, pp. 531–534. doi:10.1109/3ICT56508.2022.9990622.

[2] M. T. Baldassarre, V. S. Barletta, D. Caivano, A. Piccinno, A visual tool for supporting decision-making in privacy oriented software development, in: Proceedings of the International Conference on Advanced Visual Interfaces, AVI '20, Association for Computing Machinery, New York, NY, USA, 2020. URL: https://doi.org/10.1145/3399715.3399818. doi:10.1145/3399715.3399818.

[3] C. Catalano, A. Chezzi, M. Angelelli, F. Tommasi, Deceiving ai-based malware detection through polymorphic attacks, Computers in Industry 143 (2022) 103751.

[4] V. S. Barletta, D. Caivano, M. D. Vincentiis, A. Ragone, M. Scalera, M. A. S. Martin, V-soc4as: A vehicle-soc for improving automotive security, Algorithms 16 (2023). doi:10.3390/a16020112.

[5] J. Dobaj, G. Macher, D. Ekert, A. Riel, R. Messnarz, Towards a security-driven automotive development lifecycle, Journal of Software: Evolution and Process n/a (2021) e2407. doi:https://doi.org/10.1002/smr.2407.

[6] L. Haripriya, M. Jabbar, Role of machine learning in intrusion detection system: Review, in: 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2018, pp. 925–929. doi:10.1109/ICECA.2018.8474576.

[7] V. S. Barletta, D. Caivano, C. Catalano, M. De Vincentiis, A. Pal, Machine learning for automotive security in technology transfer, in: Information Systems and Technologies - WorldCIST 2023 Volume 1, 2023.

[8] Jose D. Martın-Guerrero, Lucas Lamata, Quantum machine learning, in: ESANN 2020 Proceedings, i6doc.com, 2020, pp. 257–266. URL: http://www.i6doc.com/en/.

[9] V. S. Barletta, D. Caivano, M. De Vincentiis, A. Magrì, A. Piccinno, Quantum optimization for iot security detection, in: V. Julián, J. Carneiro, R. S. Alonso, P. Chamoso, P. Novais (Eds.), Ambient Intelligence—Software and Applications—13th International Symposium on Ambient Intelligence, Springer International Publishing, Cham, 2023, pp. 187–196.

[10] European Union Agency for Cybersecurity., Cybersecurity education initiatives in the EU

Member States: December 2022., Publications Office, 2023. URL: https://data.europa.eu/doi/10.2824/486119.

[11] B. J. Blažič, Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?, Education and Information Technologies 27 (2022) 3011–3036. URL: https://link.springer.com/10.1007/s10639-021-10704-y. doi:10.1007/s10639-021-10704-y.

[12] S. Alahmari, K. Renaud, I. Omoronyia, Moving beyond cyber security awareness and training to engendering security knowledge sharing, Information Systems and e-Business Management 21 (2023) 123–158. URL: https://link.springer.com/10.1007/s10257-022-00575-2. doi:10.1007/s10257-022-00575-2.

[13] J.-N. Tioh, M. Mina, D. W. Jacobson, Cyber security training a survey of serious games in cyber security, in: 2017 IEEE Frontiers in Education Conference (FIE), 2017, pp. 1–5. doi:10.1109/FIE.2017.8190712.

[14] M. Domínguez, D. Pérez, A. Morán, S. Alonso, M. A. Prada, J. J. Fuertes, Remote training in cybersecurity for industrial control systems, IFAC-PapersOnLine 55 (2022) 320–325. URL: https://linkinghub.elsevier.com/retrieve/pii/S2405896322015427. doi:10.1016/j.ifacol.2022.09.299.

[15] Y. Skorenkyy, R. Kozak, N. Zagorodna, O. Kramar, I. Baran, Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education, Journal of Physics: Conference Series 1840 (2021) 012026. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1840/1/012026. doi:10.1088/1742-6596/1840/1/012026.

[16] C. Catal, A. Ozcan, E. Donmez, A. Kasif, Analysis of cyber security knowledge gaps based on cyber security body of knowledge, Education and Information Technologies 28 (2023) 1809–1831. URL: https://link.springer.com/10.1007/s10639-022-11261-8. doi:10.1007/s10639-022-11261-8.

[17] R. Pirta-Dreimane, A. Brilingaitė, G. Majore, B. J. Knox, K. Lapin, K. Parish, S. Sütterlin, R. G. Lugo, Application of intervention mapping in cybersecurity education design, Frontiers in Education 7 (2022) 998335. URL: https://www.frontiersin.org/articles/10.3389/feduc.2022.998335/full. doi:10.3389/feduc.2022.998335.

[18] J. Rajamäki, J. Nevmerzhitskaya, C. Virág, Cybersecurity education and training in hospitals: Proactive resilience educational framework (prosilience ef), in: 2018 IEEE Global Engineering Education Conference (EDUCON), 2018, pp. 2042–2046. doi:10.1109/EDUCON.2018.8363488.

[19] C. Miller, C. Valasek, Adventures in automotive networks and control units, Def Con 21 (2013) 15–31.

[20] C. Miller, C. Valasek, Remote exploitation of an unaltered passenger vehicle, Black Hat USA 2015 (2015) 1–91.

[21] I. I. S. Organisation, ISO/SAE DIS 21434 Road vehicles—cybersecurity engineering, 2021.

[22] F. Sommer, J. Dürrwang, R. Kriesten, Survey and classification of automotive security attacks, Information 10 (2019) 148. doi:10.3390/info10040148.

[23] Z. Rahmani, L. Barbosa, A. Pinto, Collision warning in vehicular networks based on quantum secure multiparty computation, in: Anais do II Workshop de Comunicação e Computação Quântica, SBC, Porto Alegre, RS, Brasil, 2022, pp. 19–24. URL: https://sol.sbc.org.br/index.php/wquantum/article/view/21496. doi:10.5753/wquantum.2022.223569.

[24] D. Caivano, M. De Vincentiis, F. Nitti, A. Pal, Quantum optimization for fast can bus intrusion detection, in: Proc. 1st Int. Workshop on Quantum Programming for SE, QP4SE 2022, ACM, 2022, p. 15–18. doi:10.1145/3549036.3562058.

[25] S. L. Wu, S. Sun, W. Guan, C. Zhou, J. Chan, C. L. Cheng, T. Pham, Y. Qian, A. Z. Wang, R. Zhang, et al., Application of quantum machine learning using the quantum kernel algorithm on high energy physics analysis at the lhc, Physical Review Research 3 (2021) 033221.

[26] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, J. M. Gambetta, Supervised learning with quantum-enhanced feature spaces, Nature 567 (2019) 209–212.

[27] D. P. García, J. Cruz-Benito, F. J. García-Peñalvo, Systematic literature review: Quantum machine learning and its applications, arXiv preprint arXiv:2201.04093 (2022).

[28] M. T. Baldassarre, V. S. Barletta, D. Caivano, A. Piccinno, M. Scalera, Privacy knowledge base for supporting decision-making in software development, in: C. Ardito, R. Lanzilotti, A. Malizia, M. Larusdottir, L. D. Spano, J. Campos, M. Hertzum, T. Mentler, J. Abdelnour Nocera, L. Piccolo, S. Sauer, G. van der Veer (Eds.), Sense, Feel, Design, Springer International Publishing, Cham, 2022, pp. 147–157.

[29] ISO, ISO/SAE 21434:2021 - road vehicles — cybersecurity engineering, 2021. URL: https://www.iso.org/standard/70918.html.

[30] A. Sequeira, L. P. Santos, L. S. Barbosa, Policy gradients using variational quantum circuits, Quantum Mach. Intell. 5 (2023) 1–15. doi:10.1007/s42484-023-00101-8.