|  |  |
| --- | --- |
|  | |
| Book Name: | **Post-Quantum AI: Building Secure Machine Learning Systems in the Quantum Era** |
| Manuscript Number: | **Ms\_BPR\_6323** |
| Title of the Manuscript: | **Post-Quantum AI: Building Secure Machine Learning Systems in the Quantum Era** |
| Type of the Article | **Complete Book** |

|  |  |  |
| --- | --- | --- |
| PART 1: Comments | | |
|  | Reviewer’s comment **Artificial Intelligence (AI) generated or assisted review comments are strictly prohibited during peer review.** | Author’s Feedback *(Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)* |
| **Please write a few sentences regarding the importance of this manuscript for the scientific community. A minimum of 3-4 sentences may be required for this part.** | This paper is highly relevant to the scientific community since it explores the budding intersection between artificial intelligence, machine learning, and quantum computing. By identifying classical cryptographic system weaknesses and suggesting post-quantum strategies for securing AI, it presents enlightening points about a field that is only beginning systematic research. By enriching both the technical comprehension of quantum-resistant algorithms and secure machine learning and identifying the ethical, legal, and regulatory implications upon which responsible deployment of these technologies depends, this work is especially relevant to researchers, policy-makers, and practitioners who seek to ensure that AI systems remain resilient, transparent, and liable against the background of advancing into a new era of quantum. |  |
| **Is the title of the article suitable?**  **(If not please suggest an alternative title)** | The existing title is unequivocal, precise, and pertinent, directly encapsulating the manuscript's emphasis on artificial intelligence security within the context of the quantum era. |  |
| Is the abstract of the article comprehensive? Do you suggest the addition (or deletion) of some points in this section? Please write your suggestions here. | The abstract provides a strong overview of the motivation (quantum threats to AI security), scope (AI, PQC, ethics, regulatory aspects), and methods (discussion of frameworks and case studies) |  |
| **Is the manuscript scientifically, correct? Please write here.** | The paper exhibits scientific validity and conceptual strength. It integrates data from artificial intelligence, quantum computing, post-quantum cryptography, and ethical implications and hence presents a logically sound argument. Its use of diagrams, case studies, and references makes it highly creditable. |  |
| **Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.**  **-** | References are sufficient and quite up to date (2020–2023) and include major fields of PQC, AI, and ethics. |  |
| Is the language/English quality of the article suitable for scholarly communications? | English within this document reads easily and does a great job relaying advanced concepts but does have some instances whereby it dips into informal or chatty style ("super important," "mess with AI systems," "cool frameworks"). It will be completely publication-ready after a quick run of copy editing. |  |
| Optional/General comments | I recommend the manuscript for publication after minor revisions to improve clarity, strengthen the abstract, and refine the language. |  |

|  |  |  |
| --- | --- | --- |
| **PART 2:** | | |
|  | Reviewer’s comment | Author’s comment *(if agreed with the reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)* |
| **Are there ethical issues in this manuscript?** | *No* |  |

**Reviewer details:**

**Iryna Mihus, Estonia**