NONPROVISIONAL UTILITY PATENT APPLICATION

TITLE OF INVENTION

Quantum Cybersecurity Framework for Policy Assessment and Maturity Evaluation

INVENTORS

Andrew Vance, PhD
Taylor Rodriguez Vance, PhD
5 Union Square West, Suite 1124
New York, NY 10003

ASSIGNEE

Cyber Institute
5 Union Square West, Suite 1124
New York, NY 10003

CROSS-REFERENCE TO RELATED APPLICATIONS

Not Applicable

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not Applicable

BACKGROUND OF THE INVENTION

1. Quantum computing threatens traditional encryption protocols, creating vulnerabilities in cybersecurity systems. This framework addresses the gap in assessing and enhancing cybersecurity readiness in the quantum era. Many entities fail to accurately evaluate their

preparedness, leading to ineffective policies and resource misallocation. Current fragmented approaches hinder collective progress in quantum cybersecurity. This invention aims to provide a centralized, systematic method for evaluation and policy optimization to tackle these challenges effectively.

SUMMARY OF THE INVENTION

2. The invention provides a structured tiered model for assessing quantum cybersecurity maturity. Utilizing AI-driven algorithms, it delivers dynamic evaluations, policy optimization, and tailored recommendations. The system incorporates a centralized repository for policy aggregation, enabling adaptive responses to emerging threats and a sustainable approach to long-term cybersecurity resilience.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1: Illustrative view of the Quantum Cybersecurity Maturity Framework.

FIG. 2: Dynamic Bayesian Inference Evaluation.

FIG. 3: Reinforcement Learning Policy.

DETAILED DESCRIPTION OF THE INVENTION

3. The present invention provides entities, including industry organizations and government bodies, with a capability to assess their quantum cybersecurity maturity and generate tailored policy recommendations to facilitate the secure adoption of emerging quantum technologies. Unlike existing tools, which focus primarily on isolated aspects of quantum-safe cryptography or general cybersecurity measures, the present invention is the first to systematically address quantum cybersecurity maturity assessments and

provide actionable policy frameworks tailored to an entity's specific geographic, sectoral, and operational requirements. By addressing the unique risks posed by quantum computing, this invention equips entities with the tools necessary to evaluate their preparedness, identify vulnerabilities, and implement strategies aligned with their operational needs, regulatory environments, and technical capabilities. At the core of the invention lies the Quantum Cybersecurity Maturity Evaluation Algorithm (QCMEA), a novel framework that systematically evaluates maturity levels, identifies systemic gaps, and optimizes policy recommendations through advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques.

QCMEA Framework and Maturity Levels

4. The QCMEA framework employs a structured, tiered model encompassing five maturity levels, each representing a stage of quantum cybersecurity readiness:
5. Initial Maturity: Entities at this level exhibit basic awareness of quantum computing risks but lack structured mitigation strategies. Recommended actions include initiating awareness campaigns and assessing data vulnerability to quantum threats.
6. Basic Maturity: Organizations begin adopting foundational quantum-resistant measures, such as hybrid cryptographic methods and governance frameworks. These efforts lay the groundwork for more advanced quantum-safe implementations.
7. Intermediate Maturity: At this stage, entities deploy scalable quantum-safe solutions and conduct regular risk assessments, including transitioning critical systems to lattice-based encryption protocols and auditing cybersecurity defenses.
8. Advanced Maturity: This level reflects comprehensive integration of quantum-safe technologies and governance policies across all operational domains. Organizations at this level align their strategies with international standards, such as the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standards.
9. Dynamic Maturity: The highest level of maturity represents continuous adaptability to emerging quantum threats. Entities leverage machine learning to refine policies iteratively, enabling preemptive risk mitigation and sustainable resilience.

10. The QCMEA framework provides a systematic evaluation of these maturity levels and also dynamically adapts its recommendations based on evolving threats and organizational changes.

Core Components Supporting QCMEA

11. The QCMEA framework is supported by several advanced AI/ML-driven components that enable it to perform dynamic evaluations, identify gaps, and optimize policies. Bayesian Inference: Bayesian Inference dynamically updates maturity evaluations as new data becomes available. This probabilistic approach allows the framework to accommodate uncertainty and refine assessments incrementally without requiring full recalibration. For example, as an organization adopts quantum-safe cryptographic methods, Bayesian Inference immediately adjusts the maturity score to reflect the enhanced readiness. Graph Neural Networks (GNNs): GNNs analyze interdependencies among policies, technologies, and vulnerabilities, identifying systemic risks and potential cascading failures. This capability enables organizations to address gaps that could compromise quantum cybersecurity resilience, offering a holistic view of interconnected risks. Reinforcement Learning (RL): Reinforcement Learning refines policy recommendations through iterative simulations. The RL module learns optimal strategies by simulating quantum risk scenarios, balancing multiple objectives such as compliance, cost-efficiency, and risk mitigation. Simulation and Validation: The framework tests policies under simulated quantum risk scenarios to evaluate their effectiveness and scalability. For example, it can simulate a quantum brute-force attack to compare the resilience of Advanced Encryption Standard (AES-256) encryption versus post-quantum algorithms like CRYSTALS-Kyber.

Centralized Policy Repository

12. An integral component of the invention is a centralized repository that proactively aggregates cybersecurity policies relevant to quantum initiatives and risks from global sources. This repository allows entities to consistently benchmark their strategies against evolving and established standards to adopt best practices effectively. Policies from frameworks such as the NIST Post-Quantum Cryptography Standards and the General

Data Protection Regulation (GDPR), and the European Union Quantum Technologies Flagship Initiative are continuously updated using Python-based web crawling technologies. By providing up-to-date, actionable guidance, the repository ensures that policy recommendations remain relevant and aligned with the latest standards.

Advanced Data Aggregation and Policy Recommendations

13. The framework employs advanced data aggregation techniques to collect and analyze information from diverse sources, including public policy repositories, user inputs, and probabilistic risk models. Automated tools, such as web scraping, Application Programming Interfaces (APIs), and optical character recognition (OCR) systems, extract structured and unstructured data from policy documents, databases, and PDFs. This data is preprocessed using natural language processing (NLP) techniques and metadata extraction tools, ensuring efficient storage and retrieval in scalable databases like MongoDB and PostgreSQL. Policy recommendations are dynamically generated through a Policy Recommendation Dashboard, which aligns insights with an entity’s maturity level, geographic location, sector-specific requirements, and the entities’ technical capabilities. The dashboard visualizes critical metrics such as risk reduction percentages and the outcomes of implemented recommendations. For instance, a healthcare organization may receive a policy framework that incorporates HIPAA compliance, regional encryption standards, and international quantum-safe protocols.

Visualization and Reporting Tools

14. The invention incorporates advanced visualization and reporting tools to facilitate informed decision-making. Dashboards present key insights, including maturity level progress, policy alignment metrics, and outcomes of implemented strategies. For example, after deploying updated encryption protocols, an entity may observe a 30% reduction in vulnerability scores, demonstrating the tangible impact of the adopted measures, and facilitate the move from Intermediate Maturity to Advanced Maturity. These visualizations enable users to prioritize improvements and monitor the effectiveness of their cybersecurity posture.

Technical Infrastructure

15. The technical infrastructure supporting the QCMEA framework is flexible and scalable, incorporating cloud-based and AI/ML technologies to facilitate deployment across diverse environments. Data is processed and stored in distributed systems such as object storage platforms and relational or NoSQL databases. The framework leverages serverless computing for real-time operations and containerized applications for scalable simulations. By utilizing these technologies, the invention ensures adaptability and efficiency in addressing quantum cybersecurity challenges.

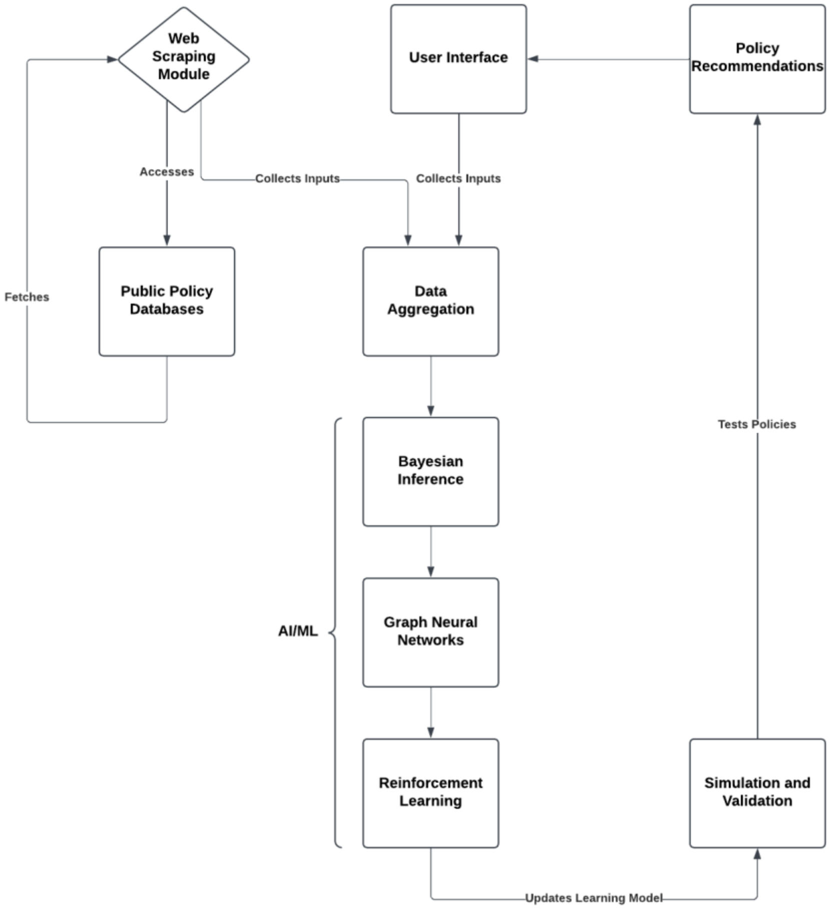


Figure 1

Workflow of the Quantum Cybersecurity Maturity Evaluation Algorithm (QCMEA), illustrating data aggregation, Bayesian inference, graph neural networks, reinforcement learning, and simulation-based validation, culminating in tailored policy recommendations.

Enablement

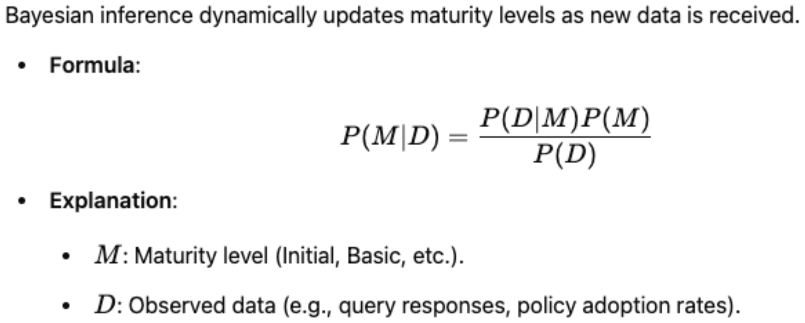
16. The Quantum Cybersecurity Maturity Evaluation Algorithm (QCMEA) is designed to address the dynamic challenges of quantum cybersecurity by employing advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques. The system integrates Bayesian Inference, Graph Neural Networks (GNNs), Reinforcement Learning (RL), and simulation-based validation, collectively forming a unified framework capable of continuous learning, real-time adaptation, and intelligent policy optimization.
17. The system begins with a robust data aggregation pipeline, which collects inputs from various sources, including public policy repositories, user-provided data, and probabilistic risk scores. These inputs are processed using natural language processing (NLP) tools to categorize data, identify relevant metadata, and refine the information for analysis. The data is subsequently structured and stored in scalable database systems such as MongoDB or PostgreSQL to support efficient retrieval and ongoing computation.
18. Bayesian Inference dynamically updates cybersecurity maturity evaluations by incorporating real-time inputs, such as organizational feedback and external risk models. This method enables the system to refine its predictions incrementally without requiring a full recalculation of prior assessments. GNNs analyze the interdependencies among policies, technologies, and vulnerabilities, identifying cascading risks that might otherwise be overlooked. The RL module, by contrast, optimizes policy recommendations through iterative simulations, prioritizing cost-effective and compliant strategies. This approach ensures that recommended policies are both practical and effective, even in novel or rapidly evolving threat landscapes.
19. Simulation and validation capabilities are integrated to rigorously test proposed policies under quantum-specific threat scenarios. For example, the system can simulate the comparative performance of AES-256 encryption against post-quantum cryptographic methods, such as CRYSTALS-Kyber, in a hypothetical quantum brute-force attack. These simulations evaluate resilience, scalability, and compliance, ensuring that the recommended policies are not only theoretically sound but also operationally viable.
20. The QCMEA process flow begins with the web scraping module, which dynamically collects data from public policy repositories and user inputs. Bayesian models process

this data to generate real-time maturity scores, while GNNs perform a comprehensive gap analysis to identify systemic vulnerabilities. RL algorithms refine policy recommendations through trial-and-error simulations, and validated recommendations are presented through a user-friendly interface. The system leverages cloud-based infrastructure, such as AWS Lambda, Azure Cosmos, or Google Cloud Functions, to support these computationally intensive processes.

Best Mode Disclosure

21. The optimal implementation of QCMEA involves a synergistic use of innovative AI/ML techniques and cloud-based infrastructures. The Bayesian Inference component utilizes the formula (Figure 2) to compute posterior probabilities dynamically, incorporating new data streams to refine predictions. This approach allows the system to quantify confidence levels and adapt to incomplete or uncertain data, enabling robust maturity evaluations tailored to specific organizational risks.

22.



Bayesian inference dynamically updates maturity levels as new data is received.

- **Formula:**

$$P(M|D) = \frac{P(D|M)P(M)}{P(D)}$$

- **Explanation:**
  - M: Maturity level (Initial, Basic, etc.).
  - D: Observed data (e.g., query responses, policy adoption rates).

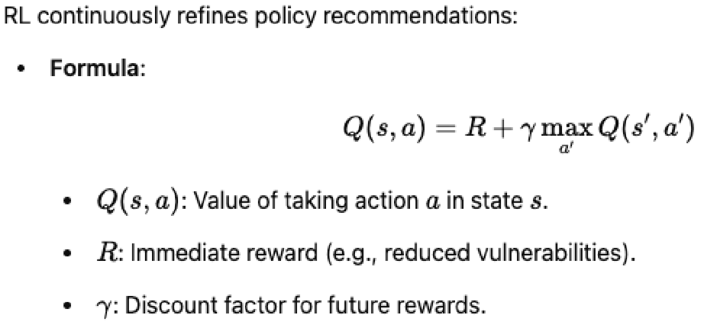
23. Figure 2.

24. GNNs are trained on graph-based datasets representing interconnections between policies and vulnerabilities. By analyzing these dependencies, the system identifies systemic risks that could cascade through an organization’s cybersecurity infrastructure. This analysis is critical for sectors such as healthcare and finance, where policy interdependencies can amplify vulnerabilities.

25. The RL module employs a reward-driven optimization framework, where the effectiveness of policies is measured by a reward function defined as Risk Reduction Percentage (Figure 3). This enables the system to prioritize high-impact, cost-efficient policies. Simulations within the RL environment tests the applicability of various

strategies under hypothetical quantum threat conditions, ensuring that recommendations align with international standards, such as NIST Post-Quantum Cryptography Guidelines.

26.



RL continuously refines policy recommendations:

- **Formula**:

$$Q(s,a) = R + \gamma \max_{a'} Q(s',a')$$

  - $Q(s,a)$: Value of taking action a in state s.
  - R: Immediate reward (e.g., reduced vulnerabilities).
  - γ: Discount factor for future rewards.

27. Figure 3.

28. The user interface is designed to simplify interactions with the system. Built using modern JavaScript frameworks, the system provides an intuitive dashboard that visualizes risk scores, maturity levels, and policy recommendations. High-contrast themes ensure accessibility, while responsive design principles allow the system to function seamlessly across devices. Data security is prioritized through Transport Layer Security (TLS 1.3) encryption for all communications and AES-256 encryption for data storage.

Clarity of Novel Features

29. The Quantum Cybersecurity Maturity Evaluation Algorithm (QCMEA) introduces groundbreaking innovations by combining probabilistic reasoning, systemic analysis, and adaptive learning to address quantum cybersecurity challenges. Unlike static maturity models, which rely on fixed rules or pre-trained algorithms, QCMEA dynamically updates maturity evaluations in real time. This ensures that assessments reflect the most current data, risks, and evolving threat landscapes. The Bayesian Inference methodology enables the system to quantify uncertainty, accommodate incomplete data, and make incremental adjustments, offering responsiveness and adaptability absent in traditional approaches.
30. Graph Neural Networks (GNNs) provide a unique capability to model and analyze the interdependencies between cybersecurity policies, technologies, and vulnerabilities. By simulating these complex interconnections, the system uncovers cascading risks and systemic weaknesses that would typically remain undetected through conventional

assessment methods. This feature ensures a more accurate and actionable evaluation of an organization’s quantum cybersecurity readiness.

31. The Reinforcement Learning (RL) module further sets QCMEA apart by treating cybersecurity policies as dynamic actions within a simulated environment. Through iterative trial-and-error simulations, the system learns to prioritize policy strategies that balance cost-effectiveness, compliance, and risk mitigation. This adaptive approach enables the system to respond dynamically to novel quantum threats and regulatory changes, extending beyond the capabilities of static rule-based systems.

32. Additionally, QCMEA is distinct in its ability to provide tailored, quantum-specific policy recommendations. Unlike existing tools that offer generalized guidelines or assessments, QCMEA generates recommendations specific to quantum risks and organizational contexts. These recommendations may address issues such as transitioning to post-quantum cryptographic methods, implementing hybrid encryption protocols, or adopting sector-specific compliance standards. The system’s centralized policy repository aggregates and analyzes global quantum cybersecurity policies, allowing organizations to benchmark against industry standards and adopt best practices in real time.

33. To date, no existing invention assesses quantum cybersecurity maturity while simultaneously generating partial or complete quantum-specific policy recommendations for entities. This absence underscores QCMEA’s novelty and its value as a transformative solution for addressing emerging quantum computing threats. By integrating real-time data processing, AI-driven evaluation models, and simulation-based validation, QCMEA delivers an unparalleled framework for organizations to achieve comprehensive quantum cybersecurity resilience. The system reliably tests proposed policies under quantum-specific threat scenarios, such as quantum brute-force attacks, ensuring their theoretical soundness and practical viability. This empirical validation provides decision-makers with confidence in the effectiveness of their cybersecurity strategies prior to deployment. The unified integration of advanced AI/ML components and centralized repositories ensures that QCMEA is not only reliable and scalable but also intentionally adaptive to a range of industries and organizational needs. These features collectively establish QCMEA as a novel and transformative tool in the field of quantum cybersecurity.

ABSTRACT OF THE DISCLOSURE

This invention introduces the Quantum Cybersecurity Maturity Evaluation Algorithm (QCMEA), a comprehensive framework for assessing and optimizing quantum cybersecurity readiness. The QCMEA utilizes advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques, including Bayesian Inference, Graph Neural Networks, and Reinforcement Learning, to dynamically evaluate maturity levels and provide tailored policy recommendations. The framework comprises a five-tiered maturity model; Initial, Basic, Intermediate, Advanced, and Dynamic, enabling entities to identify vulnerabilities, assess their preparedness, and implement quantum-safe policies. A centralized repository aggregates global cybersecurity standards and updates, ensuring alignment with international protocols, such as NIST Post-Quantum Cryptography Standards. By incorporating simulation-based validation, the QCMEA reliably tests policy effectiveness under quantum threat scenarios, providing actionable insights for sustainable resilience. This invention enables organizations to adapt to the evolving quantum cybersecurity field and achieve reliable, scalable defenses against emerging risks.

CLAIMS

Claim 1: A quantum cybersecurity maturity model comprising five distinct tiers, Initial, Basic, Intermediate, Advanced, and Dynamic Maturity, each defined by specific readiness levels, policies, and technologies for addressing quantum cybersecurity threats.

Claim 2: A system integrating Artificial Intelligence and Machine Learning for real-time aggregation of cybersecurity policies, dynamic evaluation of quantum threat preparedness, and optimization of risk mitigation strategies.

Claim 3: A Quantum Cybersecurity Maturity Evaluation Algorithm (QCMEA) leveraging Bayesian inference for dynamic maturity assessments, Graph Neural Networks (GNNs) for systemic risk analysis, and Reinforcement Learning (RL) for iterative policy optimization in quantum threat scenarios.

Claim 4: Simulation tools configured to validate policy effectiveness under quantum-specific threat scenarios, including quantum brute-force attacks, by comparing the resilience of cryptographic methods and assessing scalability and compliance.

Claim 5: A system for generating adaptive policy recommendations tailored to sector-specific requirements, geographic regulations, and organizational risk profiles, leveraging real-time data analysis and quantum threat simulations.