PROVISIONAL PATENT APPLICATION

Title: Hybrid Quantum-Classical Threat Detection System with Adaptive Resource Allocation

Inventor(s): Brian James Rutherford

Application Type: Provisional Patent Application

Filing Date: August 28, 2025

Application Number: [To be assigned by USPTO]

Inventors: [TO BE COMPLETED WITH ACTUAL INVENTOR NAMES]

Assignee: MWRASP Quantum Defense Systems, Inc.

Attorney Docket No: MWRASP-001-PROV

Filing Basis: 35 U.S.C. § 111(b) Provisional Application

TECHNICAL FIELD

The present invention relates to cybersecurity systems and methods, and more particularly to hybrid quantum-classical computing architectures for real-time threat detection and response in enterprise cybersecurity environments.

BACKGROUND OF THE INVENTION

Current State of Cybersecurity

Traditional cybersecurity systems rely entirely on classical computing architectures to detect, analyze, and respond to cyber threats. These systems typically operate using predefined rules, signature-based detection, and statistical analysis methods that require significant computational resources and time to process complex threat patterns.

Current cybersecurity architectures suffer from several fundamental limitations:

1. Processing Speed Limitations: Classical systems require seconds to minutes to analyze complex threat patterns, during which sophisticated attacks can complete their objectives.

2. Pattern Recognition Constraints: Classical algorithms struggle with the exponential complexity of modern multi-vector cyber attacks that use advanced obfuscation and polymorphic techniques.

3. Resource Allocation Inefficiencies: Current systems cannot dynamically allocate computational resources based on threat complexity and urgency, leading to either over-provisioning (wasting resources) or under-provisioning (missing threats).

4. Scalability Issues: As cyber threats become more sophisticated and numerous, classical systems require exponentially more computational resources to maintain detection accuracy.

Emergence of Quantum Computing Threats

The advent of practical quantum computing presents both opportunities and challenges for cybersecurity:

Quantum Threats: Quantum computers can break current cryptographic standards (RSA-2048, ECC) in polynomial time using algorithms like Shor's algorithm, making current encryption methods obsolete.

Quantum Opportunities: Quantum computing offers exponential speedup for certain types of pattern recognition, optimization problems, and cryptographic operations that are fundamental to cybersecurity applications.

Limitations of Current Hybrid Approaches

While some attempts have been made to integrate quantum computing with classical cybersecurity systems, these approaches suffer from critical limitations:

1. Static Resource Allocation: Existing systems do not dynamically determine when quantum vs. classical processing is optimal for specific threat analysis tasks.

2. Lack of Real-Time Integration: Current hybrid systems operate in batch modes that are incompatible with real-time threat response requirements.

3. Limited Cybersecurity Focus: General-purpose quantum-classical hybrid systems are not optimized for the specific requirements of cybersecurity applications.

4. No Intelligent Routing: Existing systems lack intelligent algorithms to route different types of cybersecurity analysis to optimal computing resources.

SUMMARY OF THE INVENTION

The present invention provides a novel hybrid quantum-classical cybersecurity architecture that dynamically allocates computational resources between quantum and classical processors based on real-time threat analysis requirements, threat complexity, and available computational resources.

Primary Objectives

The hybrid quantum-classical cybersecurity system of the present invention addresses the limitations of prior art by providing:

1. Dynamic Resource Allocation: Intelligent algorithms that determine in real-time whether quantum or classical processing is optimal for specific cybersecurity analysis tasks.

2. Adaptive Threat Routing: Machine learning-based decision trees that route different types of cyber threats to the most appropriate computational resources.

3. Real-Time Integration: Seamless integration of quantum and classical processing with microsecond-level handoff capabilities.

4. Cybersecurity Optimization: System architecture specifically designed and optimized for cybersecurity threat detection and response workflows.

Key Technical Innovations

Hybrid Architecture Controller: A novel control system that coordinates between quantum and classical processors, making real-time decisions about resource allocation based on threat characteristics, system load, and computational requirements.

Quantum-Classical Decision Trees: Advanced decision algorithms that analyze incoming cyber threats and determine optimal processing pathways through quantum or classical computational resources.

Adaptive Resource Management: Dynamic resource allocation system that optimizes the use of both quantum and classical computing resources based on current system capacity, threat priority, and analysis complexity.

Real-Time Result Fusion: Novel algorithms for combining and correlating results from both quantum and classical analysis processes to provide enhanced threat detection accuracy.

DETAILED DESCRIPTION OF THE INVENTION

System Architecture Overview

The hybrid quantum-classical cybersecurity architecture comprises several interconnected components working in concert to provide enhanced threat detection and response capabilities:

1. Hybrid Architecture Controller (HAC)

The Hybrid Architecture Controller serves as the central coordination system that manages the interaction between quantum and classical computing resources. The HAC includes:

1.1 Threat Analysis Preprocessor

- Receives incoming network traffic, system logs, and threat intelligence data

- Performs initial analysis to characterize threat type, complexity, and urgency

- Generates threat classification metadata for routing decisions

1.2 Resource Allocation Decision Engine

- Analyzes current quantum and classical system capacity and availability

- Evaluates threat characteristics against processing capability requirements

- Makes real-time decisions about optimal resource allocation

- Implements machine learning algorithms that improve allocation efficiency over time

1.3 Quantum-Classical Interface Manager

- Manages communication protocols between quantum and classical processors

- Handles data serialization and deserialization for quantum processing

- Coordinates timing and synchronization between different processing paths

- Monitors and optimizes data transfer speeds and accuracy

2. Classical Processing Subsystem

The classical processing subsystem handles threat analysis tasks that are well-suited to traditional computing architectures:

2.1 High-Speed Preprocessing Pipeline

- Performs rapid initial analysis of high-volume network traffic

- Implements signature-based detection for known threat patterns

- Conducts statistical analysis and anomaly detection

- Filters and prioritizes threats for further analysis

2.2 Traditional Machine Learning Analytics

- Executes conventional ML algorithms for threat classification

- Performs behavioral analysis and pattern recognition

- Conducts historical analysis and trend identification

- Generates baseline security profiles and deviation alerts

2.3 Response Coordination System

- Coordinates incident response actions for classical-detected threats

- Manages integration with existing security infrastructure (SIEM, SOAR)

- Implements automated response protocols and escalation procedures

- Maintains audit logs and compliance reporting

3. Quantum Processing Subsystem

The quantum processing subsystem leverages quantum computing advantages for complex cybersecurity analysis tasks:

3.1 Quantum Threat Analysis Engine

- Implements quantum algorithms optimized for pattern recognition in encrypted or obfuscated data

- Uses quantum speedup for complex optimization problems in threat analysis

- Performs quantum-enhanced cryptographic analysis and key recovery

- Executes quantum machine learning algorithms for advanced threat detection

3.2 Quantum Cryptographic Analysis

- Analyzes quantum-resistant cryptographic implementations

- Detects quantum algorithm signatures in network traffic

- Performs post-quantum cryptographic validation and analysis

- Implements quantum key distribution (QKD) analysis and monitoring

3.3 Quantum Pattern Recognition

- Uses quantum algorithms for exponentially complex pattern matching

- Performs quantum-enhanced analysis of polymorphic malware

- Implements quantum superposition for parallel threat scenario analysis

- Executes quantum optimization for multi-vector attack correlation

4. Result Fusion and Correlation System

The result fusion system combines outputs from both quantum and classical processing to provide enhanced threat detection accuracy:

4.1 Confidence Scoring Algorithm

- Assigns confidence scores to results from both quantum and classical analysis

- Weighs results based on processing method reliability and threat type

- Implements dynamic confidence adjustment based on historical accuracy

- Provides uncertainty quantification for analysis results

4.2 Result Correlation Engine

- Correlates findings from quantum and classical processing paths

- Identifies complementary and contradictory analysis results

- Implements consensus algorithms for multi-path analysis validation

- Generates unified threat assessment reports

4.3 Adaptive Learning System

- Learns from the effectiveness of different processing approaches

- Adjusts routing algorithms based on historical success rates

- Improves fusion algorithms through continuous learning

- Optimizes system performance through reinforcement learning

Detailed Technical Implementation

Quantum-Classical Decision Tree Algorithm

The decision tree algorithm determines optimal routing of cybersecurity analysis tasks between quantum and classical processors:

```

Algorithm 1: Quantum-Classical Routing Decision

Input: Threat_Data T, System_State S, Historical_Performance H

Output: Processing_Route R (QUANTUM | CLASSICAL | HYBRID)

1. Extract threat characteristics: T_features = analyze(T)

2. Evaluate system capacity: Q_capacity = quantum_availability(S)

3. Evaluate system capacity: C_capacity = classical_availability(S)

4. Calculate processing requirements:

- Q_requirement = quantum_complexity_analysis(T_features)
- C_requirement = classical_complexity_analysis(T_features)
5. Historical performance lookup:
- Q_historical = lookup_quantum_performance(T_features, H)
- C_historical = lookup_classical_performance(T_features, H)
6. Compute optimization score:
- Q_score = (Q_historical Q_capacity) / Q_requirement
- C_score = (C_historical C_capacity) / C_requirement
7. Route decision:
If Q_score > C_score + threshold:
    R = QUANTUM
Else if C_score > Q_score + threshold:
    R = CLASSICAL
Else:
    R = HYBRID
8. Update historical performance data
9. Return R
```

Adaptive Resource Management System

The resource management system optimizes the allocation of quantum and classical computing resources:

Resource Monitoring Component:

- Continuously monitors quantum coherence time and error rates

- Tracks classical processor utilization and memory availability

- Monitors network bandwidth and latency for quantum-classical communication

- Maintains real-time system performance metrics

Dynamic Allocation Algorithm:

```
```

```
Algorithm 2: Dynamic Resource Allocation

Input: Active_Tasks A, Resource_State R, Performance_Targets P

Output: Resource_Allocation_Map M

1. Priority sorting: A_sorted = sort_by_priority(A)

2. For each task t in A_sorted:

    a. Determine resource requirements: req = calculate_requirements(t)

    b. Find optimal allocation: alloc = optimize_allocation(req, R, P)

    c. Reserve resources: R = update_resources(R, alloc)

    d. Add to allocation map: M[t] = alloc

3. Monitor allocation effectiveness

4. Trigger reallocation if performance targets not met

5. Return M
```

Real-Time Result Fusion Algorithm

The result fusion algorithm combines quantum and classical analysis results to provide enhanced accuracy:

```
Algorithm 3: Quantum-Classical Result Fusion

Input: Quantum_Results Q, Classical_Results C, Confidence_Scores S

Output: Fused_Result F, Combined_Confidence CC

1. Normalize result formats: Q_norm = normalize(Q), C_norm = normalize(C)

2. Calculate result correlation: correlation = compute_correlation(Q_norm, C_norm)

3. Determine fusion strategy:

    If correlation > high_threshold:

        fusion_method = REINFORCING

    Else if correlation < low_threshold:

        fusion_method = CONTRADICTORY
```

```
Else:
    fusion_method = COMPLEMENTARY
4. Apply fusion algorithm based on strategy:
    F = apply_fusion(Q_norm, C_norm, fusion_method)
5. Combine confidence scores:
    CC = combine_confidence(S.quantum, S.classical, correlation)
6. Validate fused result: validated = validate_result(F, CC)
7. Return F, CC
```

System Performance Optimizations

Latency Optimization

The system implements several techniques to minimize processing latency:

1. Predictive Resource Allocation: The system uses machine learning algorithms to predict future resource needs based on current threat patterns and historical data, pre-allocating resources before they are needed.

2. Parallel Processing Pipelines: Quantum and classical processing occur in parallel where possible, with intelligent synchronization to minimize total processing time.

3. Caching and Memoization: Frequently accessed analysis results and decision tree outcomes are cached to reduce computational overhead for similar threats.

Accuracy Optimization

The system maximizes threat detection accuracy through several mechanisms:

1. Multi-Path Validation: Critical threats are analyzed through both quantum and classical paths, with results correlated to improve accuracy.

2. Continuous Learning: The system continuously learns from both successful threat detections and false positives to improve its decision-making algorithms.

3. Adaptive Thresholds: Detection thresholds are dynamically adjusted based on current threat landscape and system performance metrics.

CLAIMS

Independent Claims

Claim 1: A hybrid quantum-classical cybersecurity system comprising:

a) a hybrid architecture controller configured to receive cybersecurity threat data and determine optimal processing allocation between quantum and classical computing resources;

b) a classical processing subsystem configured to perform traditional cybersecurity analysis including signature-based detection, statistical analysis, and conventional machine learning;

c) a quantum processing subsystem configured to perform quantum-enhanced cybersecurity analysis including quantum pattern recognition, quantum cryptographic analysis, and quantum optimization algorithms;

d) a result fusion system configured to combine and correlate results from both quantum and classical processing subsystems to generate enhanced threat detection results;

e) wherein the hybrid architecture controller implements adaptive decision algorithms that optimize resource allocation based on threat characteristics, system capacity, and historical performance data.

Claim 2: The hybrid quantum-classical cybersecurity system of Claim 1, wherein the hybrid architecture controller comprises:

a) a threat analysis preprocessor configured to characterize incoming threat data and generate threat classification metadata;

b) a resource allocation decision engine configured to evaluate system capacity and make real-time resource allocation decisions; and

c) a quantum-classical interface manager configured to coordinate communication and data transfer between quantum and classical processing subsystems.

Claim 3: The hybrid quantum-classical cybersecurity system of Claim 1, wherein the quantum processing subsystem comprises:

a) a quantum threat analysis engine configured to implement quantum algorithms optimized for cybersecurity pattern recognition;

b) a quantum cryptographic analysis module configured to analyze quantum-resistant cryptographic implementations and detect quantum algorithm signatures; and

c) a quantum pattern recognition system configured to perform quantum-enhanced analysis of complex and obfuscated cyber threats.

Dependent Claims

Claim 4: The hybrid quantum-classical cybersecurity system of Claim 1, wherein the adaptive decision algorithms implement machine learning models that improve resource allocation efficiency over time based on historical performance data.

Claim 5: The hybrid quantum-classical cybersecurity system of Claim 1, wherein the result fusion system implements confidence scoring algorithms that assign reliability metrics to quantum and classical analysis results.

Claim 6: The hybrid quantum-classical cybersecurity system of Claim 1, wherein the system operates with microsecond-level response times for threat detection and resource allocation decisions.

Claim 7: The hybrid quantum-classical cybersecurity system of Claim 2, wherein the resource allocation decision engine implements quantum-classical routing algorithms that select optimal processing paths based on threat complexity and system availability.

Claim 8: The hybrid quantum-classical cybersecurity system of Claim 3, wherein the quantum threat analysis engine implements quantum machine learning algorithms optimized for real-time cybersecurity applications.

Claim 9: A method for hybrid quantum-classical cybersecurity threat detection comprising:

a) receiving cybersecurity threat data at a hybrid architecture controller;

b) analyzing threat characteristics and system capacity to determine optimal processing allocation;

c) routing threat analysis tasks to quantum processing subsystem, classical processing subsystem, or both based on optimization algorithms;

d) performing quantum-enhanced analysis for complex pattern recognition and cryptographic analysis;

e) performing classical analysis for high-volume processing and traditional threat detection;

f) fusing results from quantum and classical analysis using correlation algorithms and confidence scoring;

g) generating enhanced threat detection results with improved accuracy and reduced processing time.

Claim 10: The method of Claim 9, wherein the step of determining optimal processing allocation implements adaptive decision trees that learn from historical performance data and continuously improve resource allocation efficiency.

INDUSTRIAL APPLICABILITY

The hybrid quantum-classical cybersecurity system described herein has significant industrial applicability across multiple sectors requiring advanced cybersecurity protection, particularly in environments where quantum computing threats pose existential risks to current security infrastructure.

Primary Industrial Applications

Enterprise Cybersecurity: Large corporations and government agencies can deploy this system to protect critical infrastructure against both current and emerging quantum-based cyber attacks. The system's adaptive resource allocation ensures optimal performance across varying threat landscapes while maintaining cost-effectiveness through intelligent quantum-classical resource management.

Financial Services: Banks, trading firms, and payment processors can utilize the quantum-enhanced pattern recognition capabilities to detect sophisticated financial fraud and cyber attacks that traditional systems cannot identify. The microsecond-level response times are particularly valuable for high-frequency trading environments and real-time transaction processing.

Critical Infrastructure Protection: Power grids, telecommunications networks, and transportation systems can implement this technology to protect against nation-state level cyber attacks that may employ quantum computing resources. The system's ability to detect quantum algorithm signatures provides early warning capabilities for quantum-based attacks.

Cloud Service Providers: Major cloud platforms can integrate this hybrid architecture to offer quantum-safe cybersecurity as a service, providing their customers with protection against both classical and quantum threats while optimizing computational costs through intelligent resource allocation.

Manufacturing and Commercial Deployment

The system is designed for practical manufacturing and deployment using commercially available quantum computing platforms from IBM, Google, Rigetti, and IonQ, combined with standard enterprise-grade classical computing infrastructure. This ensures immediate manufacturability and market deployment without requiring specialized or experimental hardware.

Scalable Implementation: The modular architecture allows for gradual deployment, starting with classical processing systems and adding quantum capabilities as quantum computing resources become more accessible and cost-effective.

Integration Compatibility: The system is designed to integrate with existing Security Information and Event Management (SIEM) systems, Security Orchestration, Automation and Response (SOAR) platforms, and other cybersecurity infrastructure, ensuring smooth adoption in enterprise environments.

Market Demand and Timing

The increasing threat of quantum computing to current cryptographic standards, combined with the rapid advancement of practical quantum computing systems, creates immediate market demand for quantum-safe cybersecurity solutions. The National Institute of Standards and Technology (NIST) post-quantum cryptography standards adoption timeline aligns with the commercial deployment potential of this technology.

Economic Impact: The system addresses a multi-billion dollar cybersecurity market while providing measurable return on investment through improved threat detection accuracy, reduced false positives, and optimized computational resource utilization.

This invention solves real-world cybersecurity challenges that cannot be addressed by purely classical or purely quantum approaches, making it immediately useful and commercially viable for industrial deployment across multiple high-value market sectors.

DRAWINGS DESCRIPTION

Figure 1: System Architecture Overview

- Overall system architecture showing hybrid architecture controller, quantum processing subsystem, classical processing subsystem, and result fusion system

- Data flow paths between components

- Interface connections and communication protocols

Figure 2: Hybrid Architecture Controller Detail

- Detailed view of threat analysis preprocessor, resource allocation decision engine, and quantum-classical interface manager

- Decision flow diagrams for resource allocation algorithms

- Control signals and data paths

Figure 3: Decision Tree Algorithm Flowchart

- Complete flowchart of quantum-classical routing decision algorithm

- Decision points and optimization criteria

- Feedback loops for continuous learning

Figure 4: Resource Allocation Timeline

- Temporal diagram showing dynamic resource allocation over time

- Quantum and classical processing capacity utilization

- Performance metrics and optimization results

Figure 5: Result Fusion Process

- Detailed view of result correlation and fusion algorithms

- Confidence scoring mechanisms

- Output validation and quality assurance processes

ABSTRACT

A hybrid quantum-classical cybersecurity system that dynamically allocates computational resources between quantum and classical processors based on real-time threat analysis requirements. The system comprises a hybrid architecture controller that analyzes incoming cyber threats and determines optimal processing allocation, a classical processing subsystem for traditional cybersecurity analysis, a quantum processing subsystem for quantum-enhanced pattern recognition and cryptographic analysis, and a result fusion system that combines outputs from both processing paths. The system implements adaptive decision algorithms that continuously optimize resource allocation based on threat characteristics, system capacity, and historical performance, achieving microsecond-level response times and enhanced threat detection accuracy compared to purely classical or quantum approaches.

INVENTOR DECLARATIONS

[TO BE COMPLETED WITH ACTUAL INVENTOR INFORMATION]

Primary Inventor: [Name]

- Title: [Title]

- Address: [Address]

- Contribution: System architecture design, quantum-classical integration algorithms

Co-Inventor: [Name]

- Title: [Title]

- Address: [Address]

- Contribution: Quantum processing subsystem design, quantum algorithm optimization

Co-Inventor: [Name]

- Title: [Title]

- Address: [Address]

- Contribution: Result fusion algorithms, performance optimization methods

ASSIGNEE INFORMATION

Assignee: MWRASP Quantum Defense Systems, Inc.

Address: [Company Address]

Country: United States

Assignment Date: [Date]

FILING INFORMATION

Application Type: Provisional Patent Application under 35 U.S.C. § 111(b)

Filing Date: August 25, 2025

Attorney Docket Number: MWRASP-001-PROV

Technology Center: 2100 (Computer Architecture and Software)

Art Unit: 2128 (Computer Security)

Priority Claim: This application claims priority benefit and is entitled to the filing date for the subject matter disclosed herein.

Related Applications: None at time of filing.

Foreign Priority: None claimed.

ATTORNEY INFORMATION

Attorney/Agent: [TO BE COMPLETED WITH ACTUAL ATTORNEY INFORMATION]

Registration Number: [Number]

Firm: [Law Firm Name]

Address: [Attorney Address]

Phone: [Phone Number]

Email: [Email Address]

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Provisional Patent Application has been served upon all interested parties in accordance with the applicable rules and regulations.

Date: August 25, 2025

Signature: [TO BE COMPLETED]

Name: [TO BE COMPLETED]

Title: [TO BE COMPLETED]

APPENDIX A: TECHNICAL SPECIFICATIONS

Design Performance Targets

- Threat Detection Response Time: System designed for microsecond-level response times

- Quantum-Classical Handoff Time: Architecture designed for minimal transition overhead

- System Throughput: Framework designed for high-volume event processing capability

- Detection Accuracy: System designed for high accuracy across multiple threat types

- False Positive Management: Architecture designed to minimize false positive occurrences

System Requirements

- Quantum Processor: Compatible with IBM, Google, Rigetti, IonQ quantum systems

- Classical Processors: 64-core CPU minimum, 256GB RAM

- Network: 10Gbps backbone connectivity

- Storage: 10TB NVMe SSD for high-speed data processing

This provisional patent application contains confidential and proprietary information of MWRASP Quantum Defense Systems, Inc. Any unauthorized use, reproduction, or distribution is strictly prohibited.

Document prepared: August 25, 2025

Filing deadline: August 27, 2025

Status: READY FOR IMMEDIATE FILING