Major Project Synopsis Report

Quantum-Enhanced Anomaly Detection for QoS Degradation in Microservices Applications Project Category: Research / Deep-tech Department: Computer Science and Engineering

Projexa Team Id- FB534B

Submitted in partial fulfilment of the requirement of the degree of

BACHELORS OF COMPUTER APPLICATIONS

in

Specialization with AI & DS (Section-B)

to

K.R Mangalam University

by

Raghvendra
(2301201125)

Chirag

(2301201089)

Under the supervision of

Ms. Jyoti Yadav

Department of Computer Science and Engineering

School of Engineering and Technology

INDEX

ABSTRACT

Modern software systems are increasingly built using microservices architectures to ensure scalability and resilience. However, maintaining Quality of Service (QoS) in these distributed environments is challenging due to the high volume and complexity of telemetry data. Traditional anomaly detection methods often suffer from high false-positive rates and latency when dealing with high-dimensional data. This project proposes a **Quantum-Enhanced Anomaly Detection** framework that leverages Quantum Machine Learning (QML) to identify subtle performance degradations—such as latency spikes or resource exhaustion—more accurately than classical approaches. By utilizing quantum feature maps and Variational Quantum Circuits (VQC), the system can detect "silent" anomalies that signal impending QoS failures, allowing for proactive system mitigation.

KEYWORDS: Quantum Machine Learning, Microservices, QoS Degradation, Anomaly Detection, AIOps.

1. INTRODUCTION

The rapid shift toward cloud-native applications has led to the adoption of microservices, where complex applications are broken down into hundreds of interconnected services. While this increases agility, it creates significant overhead for monitoring systems. Urbanization and the global reliance on digital infrastructure have made the uptime of these services critical for modern life. Current monitoring solutions struggle to distinguish between normal operational noise and genuine anomalies in high-velocity data streams. This project introduces a quantum-classical hybrid approach to enhance the sensitivity of surveillance over digital micro2services environments.

2. MOTIVATION

The motivation for this project stems from the limitations of classical monitoring tools which require massive storage and manual intervention to identify service interruptions. As microservices grow, the "curse of dimensionality" makes it difficult for standard algorithms to process all telemetry metrics in real-time. Quantum computing offers a new paradigm to handle this complexity by mapping data into high-dimensional Hilbert spaces, providing superior pattern recognition capabilities. Developing a system that can self-identify QoS drops before they impact the end-user is essential for maintaining the reliability of critical digital services.

3. LITERATURE REVIEW

☐ **Investigative Tools in Monitoring:** Research shows that while data is often available (up to 45% of cases), it is only useful if effectively processed by investigators or automated tools.

☐ **IoT and Real-time Alerts:** Previous smart surveillance models highlight the need for immediate notifications and reduced storage by only recording significant anomalies.

☐ **Machine Learning in Security:** Existing studies demonstrate that platforms like TensorFlow and OpenCV can detect physical threats (e.g., ATM robbery) using deep learning, establishing a precedent for automated threat detection.

☐ **Dynamic Database Creation:** Recent work in facial recognition suggests that smart systems should be able to create their own "feature collections" and track future occurrences without predefined labels, 4a **c4oncept** we adapt for system metric profiles.

4. GAP ANALYSIS

Most current research focuses on physical security measures, traffic management, or border safety. There is a significant lack of specialized research applying high-order algorithms like Quantum Machine Learning to the internal health and QoS of microservices applications. While existing AIOps tools provide basic monitoring, they do not offer the refined subset of requirements needed for high-sensitivity anomaly detection in highly distributed, "noisy" **cloud** environments.

5. PROBLEM STATEMENT

Traditional CCTV-style monitoring for digital services requires huge volumes of storage and manual checks to identify intruders or unusual events. In microservices, "intruders" are performance anomalies that degrade QoS. Current systems do not adequately notify users of these subtle motions in data, creating a need for a smarter, automated detection system that can mitigate risks before a **system**-wide failure occurs.

6. OBJECTIVES

☐ To design a scalable monitoring system providing 24/7 surveillance of microservices metrics.

☐ To integrate **Quantum Feature Mapping** to identify potential QoS threats and reduce false alarms.

☐ To implement a centralized dashboard for real-time visualization of live telemetry feeds and alerts.

☐ To evaluate system performance in various "environmental" conditions, such as high traffic and low-resource availability.

☐ To develop a Python-based GUI (using Tkinter) to make quantum insights accessible to system administrators.

.

7. Tools/Technologies Used

☐ **Programming Language: Python** (chosen for its extensive libraries in ML, AI, and GUI development).

☐ **Quantum Framework:** Qiskit or PennyLane (for implementing Variational Quantum Circuits).

☐ **Monitoring Tools:** Prometheus and Grafana (for data ingestion).

☐ **Orchestration:** Kubernetes (to host the microservices testbed).

☐ **GUI Library:** Tkinter (for the management interface).

8.METHODOLOGY

The project utilizes a **Hybrid Quantum-Classical pipeline**. Telemetry data is first pre-processed using classical techniques before being encoded into a quantum state.

- **Structural Similarity for Metrics:** Similar to the **SSIM** metric used in image processing, our system will compare "current state" frames of system metrics against "stable state" frames to find differences in Luminance (Mean), Contrast (Variance), and Structure (Correlation).

- **Quantum Comparison:** The system calculates a similarity index between states; a value near +1 indicates stability, while a shift toward -1 indicates a significant QoS anomaly.

REFERENCES

1. The project utilizes a **Hybrid Quantum-Classical pipeline**. Telemetry data is first pre-processed using classical techniques before being encoded into a quantum state.
2. **Structural Similarity for Metrics:** Similar to the **SSIM** metric used in image processing, our system will compare "current state" frames of system metrics against "stable state" frames to find differences in Luminance (Mean), Contrast (Variance), and Structure (Correlation).
3. **Quantum Comparison:** The system calculates a similarity index between states; a value near +1 indicates stability, while a shift toward -1 indicates a significant QoS anomaly.
4.