QUANTUM DEEP LEARNING-BASED ANOMALY DETECTION FOR ENHANCED NETWORK SECURITY

AUTHORS

Moe Hdaib, Sutharshan Rajasegarar, Lei Pan

AFFILIATIONS

School of Information Technology, Deakin University, Australia

INTRODUCTION

As cyber threats continue to evolve in complexity, the need for cutting-edge techniques in network security has never been greater. This study focuses on anomaly detection using quantum deep learning to address the inefficiencies of traditional methods. By leveraging the power of quantum computing, the research introduces quantum autoencoders and their integration with advanced quantum classifiers to enhance the accuracy and efficiency of anomaly detection, paving the way for more robust cybersecurity solutions.

OBJECTIVE

To develop and evaluate quantum deep learning-based frameworks for anomaly detection in network traffic, showcasing their potential to outperform state-of-the-art classical methods.

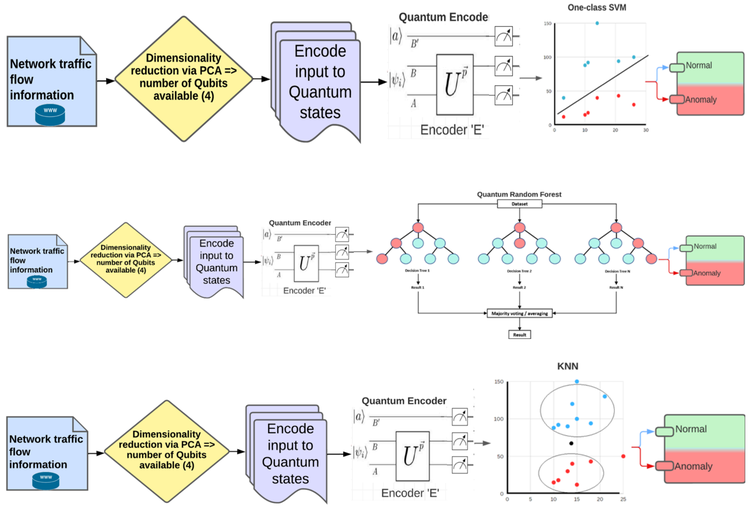
METHODOLOGY

This study utilizes a three-step approach:

1. Data Preprocessing: Standard datasets (e.g., KDD99, IoT-23, CIC IoT 23) were preprocessed and normalized.
2. Quantum Framework Development:
   - Quantum Autoencoder (QAE) for dimensionality reduction.
   - Quantum classifiers: One-Class SVM, Random Forest, and kNN integrated with QAE.
3. Performance Evaluation: Metrics like accuracy, F1-score, and computational efficiency were benchmarked.

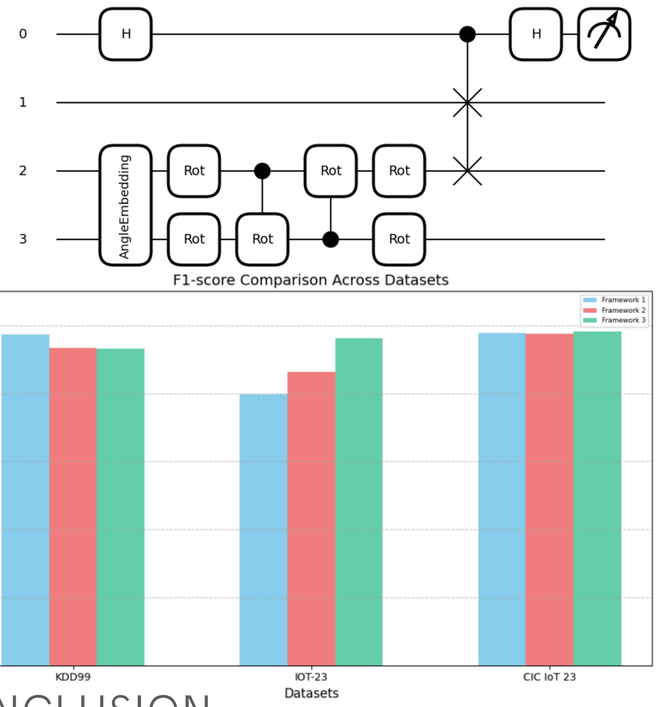
ANALYSIS

- Quantum models demonstrated enhanced anomaly detection accuracy, especially in complex datasets.



RESULTS/FINDINGS

- QAE + Quantum kNN achieved the highest accuracy (97%) on the CIC IoT 23 dataset.
- F1-scores reached up to 98%, showcasing the models' reliability.
- Quantum Advantage: Robust anomaly detection with higher precision compared to traditional models.



CONCLUSION

- Summary:
  - The research successfully demonstrates that quantum deep learning frameworks can significantly enhance network anomaly detection.
- Implications:
  - These findings pave the way for deploying quantum AI in real-world cybersecurity applications.
- Future Directions:
  - Extend the frameworks to multi-class anomaly detection and evaluate their performance in live network environments.

RELATED LITERATURE

Moe Hdaib, Sutharshan Rajasegarar, and Lei Pan. "Quantum deep learning-based anomaly detection for enhanced network security." *Quantum Machine Intelligence* 6.1 (2024): 26.

SCAN ME FOR THE ORIGNAL PAPER

- Contact: mhdaib@deakin.edu.au