Final PROJECT TITLE: DDoS Attack Detection and Prevention Using Classical and Hybrid Quantum Neural Network

Guide Name	Panel Head
Dr. Usha G	Dr. Usha G

Faculty Advisor	Project Domain
Dr. Iniyan S	Quantum Machine Learning

Student(s) Details: Name

1. Nitin Agarwal
2. Rohit Paul

Passport size photo(s)

Registration Number(s)

1. RA211100301016
2. RA2111003011004

Email ID(s)&Mobile Number(s)

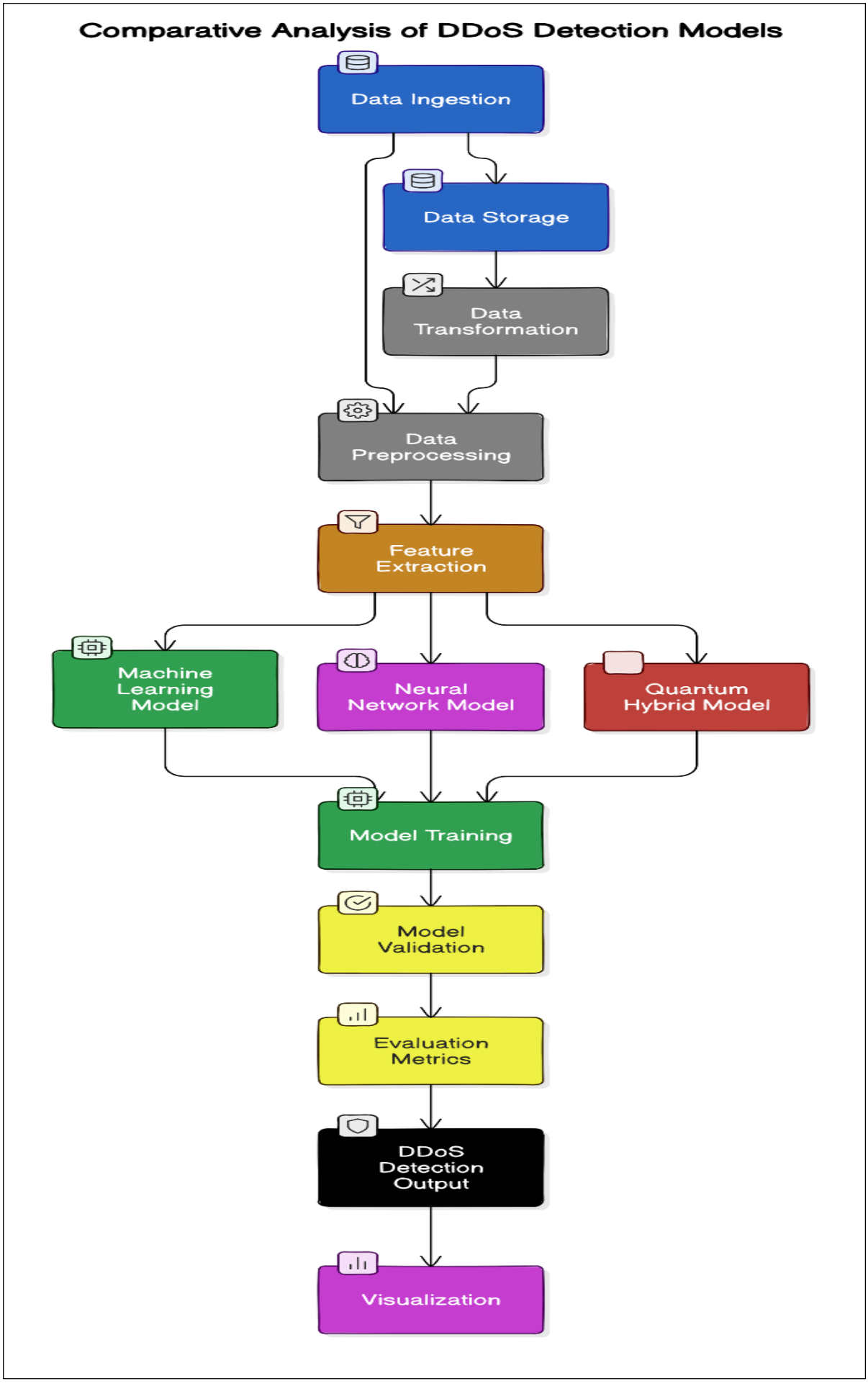
1: nb6743@srmist.edu.in 9907992264	2: rj1609@srmist.edu.in 8250397308

Abstract

The rising threat of Distributed Denial of Service (DDoS) attacks demands advanced detection and prevention strategies. This project explores the use of classical machine learning models, such as Support Vector Machines (SVM), Random Forests, and Neural Networks, to identify DDoS attacks by analyzing network traffic patterns using the DDoS-2019 dataset. By applying feature engineering and advanced machine learning techniques, we aim to improve detection accuracy and reduce false positives. Subsequently, we plan to utilize Hybrid Quantum Neural Networks (QNN) to enhance detection rates and computational efficiency, providing a scalable solution for securing cyber-physical systems. This research demonstrates the potential of both classical and quantum approaches in cybersecurity.

Final PROJECT TITLE: DDoS Attack Detection and Prevention Using Classical and Hybrid Quantum Neural Network

Architecture Diagram



Final PROJECT TITLE: DDoS Attack Detection and Prevention Using Classical and Hybrid Quantum Neural Network

Significance of the Project

- Enhances DDoS attack detection accuracy and reduces false positives.
- Utilizes both classical machine learning and quantum neural networks for improved performance.
- Improves computational efficiency in cybersecurity applications.
- Provides a scalable and reliable solution for safeguarding critical cyber-physical systems.

Conclusion

This project demonstrates that combining classical machine learning models with quantum neural networks can effectively enhance DDoS attack detection and mitigation. By improving detection accuracy, reducing false positives, and increasing computational efficiency, our approach offers a robust and scalable solution for protecting critical cyber-physical systems against evolving cyber threats.

Conference/Journal Publication Details (Mandatory)

Md.A. Hossain and Md.S. Islam Measurement: Sensors 32 (2024) 101037