SRM

INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
SCHOOL OF COMPUTING
DEPARTMENT OF COMPUTING TECHNOLOGIES
18CSP107L / 18CSP108L - MINOR PROJECT / INTERNSHIP

TITLE

DDoS Attack Detection Using Classical and Hybrid Quantum Neural Network

Guide name : Dr. Usha G

Designation : Associate Professor
Department : Computing Technologies

Student 1 Reg. No : RA2111003011016

Student 1 Name : NITIN AGARWAL

Student 2 Reg. No :RA2111003011004

Student 2 Name : ROHIT PAUL

Introduction

In the digital age, cybersecurity is a major concern, with Distributed Denial of Service (DDoS) attacks posing significant threats due to their ability to disrupt services by overwhelming network resources. Traditional detection methods often fall short, making advanced techniques necessary.

Machine learning and neural networks have shown promise in detecting DDoS attacks by identifying complex patterns in data. However, these approaches face challenges like high computational costs and lengthy training times.

Quantum computing offers a novel solution by leveraging quantum mechanics to enhance machine learning capabilities. Quantum Machine Learning (QML) combines quantum computing with machine learning, potentially providing more efficient and accurate detection of cyber threats.

This project explores the use of Quantum Neural Networks (QNN) for detecting DDoS attacks. We will implement a Hybrid Quantum Neural Network (H-QNN) and train it on a DDoS attack dataset. Our goal is to demonstrate that QNNs can outperform traditional machine learning models in detection accuracy and efficiency.

ABSTRACT

The increasing prevalence of Distributed Denial of Service (DDoS) attacks has necessitated the development of more sophisticated detection and prevention mechanisms.

This project aims to initially explore the potential of classical machine learning models, such as Support Vector Machines (SVM), Random Forests, and Neural Networks, for identifying and mitigating DDoS attacks. Utilizing the comprehensive DDoS-2019 dataset ,we analyze network traffic patterns and detect anomalies indicative of DDoS activities. The proposed models leverage feature engineering and advanced machine learning techniques to enhance the accuracy and efficiency of attack detection.

Following this, we plan to transition to Hybrid Quantum Neural Networks (QNN) to further improve detection rates and computational efficiency. Our approach seeks to not only improve detection rates but also reduce false positives, thereby providing a more reliable and scalable solution for protecting critical cyber-physical systems. This study contributes to the field of cybersecurity by demonstrating the effectiveness of both classical and quantum machine learning models in detecting and preventing DDoS attacks.

Motivation

- **Rising Cyber Threats:** DDoS attacks are increasingly frequent and sophisticated, overwhelming network resources and disrupting services.
- **Limitations of Traditional Methods:** Traditional DDoS detection methods struggle to keep pace with evolving threats, requiring more advanced solutions.
- **Challenges in Machine Learning:** While promising, machine learning and neural networks face high computational costs and lengthy training times, limiting their effectiveness.
- **Quantum Computing's Potential:** Quantum computing could revolutionize cybersecurity by providing more powerful tools for detecting and responding to threats.
- **Promise of Quantum Machine Learning (QML):** QML combines quantum computing with machine learning, offering advancements in threat detection.
- **Motivation for QNN:** This project aims to demonstrate that Hybrid Quantum Neural Networks (QNN) can improve DDoS detection in speed, accuracy, and efficiency.

Innovation idea

- **Introduction of H-QNN:** The project introduces a Hybrid Quantum Neural Network (H-QNN) designed to enhance cybersecurity by detecting Distributed Denial of Service (DDoS) attacks with improved accuracy.
- **Integration of Classical and Quantum Elements:** The H-QNN merges classical neural network layers with quantum circuits, utilizing quantum phenomena to detect complex data patterns that traditional models might miss.
- **Structure of H-QNN:**

  -Classical Layers: Handle initial data processing.

  -Quantum Layers: Encode inputs into quantum states, apply parameterized quantum gates, and decode outputs into actionable insights.
- **Performance Goals:** By combining classical and quantum elements, the H-QNN aims to deliver superior detection performance and efficiency compared to conventional machine learning models.

Purpose

The purpose of this project is to develop and evaluate a Hybrid Quantum Neural Network (H-QNN) for detecting Distributed Denial of Service (DDoS) attacks and to compare its performance with traditional machine learning models. By integrating quantum computing with classical neural network methods, we aim to leverage quantum phenomena to enhance detection accuracy and efficiency. This project seeks to demonstrate that the H-QNN can provide superior performance compared to conventional machine learning models, offering a more robust solution to the complex and evolving nature of cyber threats.

Scope

The scope of this project includes:

- **Literature Review:** Analyzing recent research on machine learning, neural networks, and quantum computing for DDoS detection.
- **Data Preprocessing:** Preparing and cleaning the DDoS attack dataset for model training.
- **Model Development**: Implementing both the H-QNN using PennyLane and TensorFlow, and traditional machine learning models for comparison.
- **Training and Evaluation:** Training the H-QNN and classical models on the dataset and evaluating their performance based on accuracy, efficiency, and real-time applicability.
- **Comparison and Analysis**: Comparing the performance of the H-QNN with that of conventional machine learning models to assess the advantages of quantum-enhanced solutions.

Literature Review

S. No	Title	Methodology	Identification of gaps and limitations
1	Machine Learning-based DDoS Attack Detection Using Software Defined Networking (IEEE Access, Loukas, G., Vuong, T.-H., Heartfield, R., Sakellari, G., Yoon, Y., Gan, D., 2020)	• Implemented ML algorithms in SDN environment • Focused on flow-based detection using SVM and Random Forest	• Limited scalability • Potentially high false positive rates
2	A Deep Learning Approach for DDoS Attack Detection in Industrial IoT Systems (IEEE Internet of Things Journal, Li, Y., Cui, L., Zheng, H., Zhang, X., 2020)	• Utilized LSTM and GRU for time-series analysis • Achieved high detection accuracy on IIoT data	• High computational cost • Requires large labeled datasets
3	Ensemble Learning for DDoS Attack Detection in Cloud Computing (Future Generation Computer Systems, Choudhary, A., Jain, S., Shukla, P., 2021)	• Applied ensemble learning methods (Bagging, Boosting) • Focused on feature selection and extraction	• Complexity in model integration • Scalability issues in real-time applications
4	Real-time DDoS Attack Detection Using Machine Learning Techniques (IEEE Transactions on Information Forensics and Security, Aamir, M., Zaidi, S.M.H., 2021)	• Developed real-time detection algorithms using SVM and KNN • Evaluated performance on real-world datasets	• High computational requirements • Potential overfitting on specific datasets
5	A Survey of Machine Learning Techniques for DDoS Attack Detection (Journal of Network and Computer Applications, Kumar, S., Yadav, N., Singh, A., 2021)	• Reviewed various ML techniques: SVM, Decision Trees, Neural Networks • Provided a comparative analysis of these techniques	• Broad overview, lacks detailed experimental validation • No focus on deployment scenarios

Literature Review

6	Deep Learning-based Intrusion Detection System for DDoS Attack Detection (IEEE Access, Zhang, J., Yang, Y., Lin, Y., 2022)	• Implemented CNN and RNN for feature extraction and classification • Achieved high detection rates with deep learning models	• High training time • Requires extensive computational resources
7	DDoS Attack Detection Using Hybrid Neural Network Models (Journal of Information Security and Applications, Huang, Y., Yang, J., 2022)	• Combined CNN and LSTM for hybrid neural network approach • Focused on temporal and spatial feature extraction	• High computational complexity • Difficult to interpret results
8	Enhanced DDoS Attack Detection Using Machine Learning Algorithms in IoT Networks (IEEE Internet of Things Journal, Elmrabit, N., Jiang, Q., 2022)	• Used Random Forest and Gradient Boosting for detection • Applied feature engineering techniques for IoT data	• High false positive rate • Integration challenges with IoT devices
9	Detection of DDoS Attacks in Edge Computing Using Deep Learning (IEEE Transactions on Network and Service Management, Tang, F., Shi, Y., Geng, Y., 2023)	• Applied deep learning models (CNN, LSTM) for edge computing environments • Focused on real-time detection	• High computational cost • Limited by edge device capabilities
10	Anomaly Detection in DDoS Attacks Using Machine Learning (Journal of Computer Networks, Patel, P., Mehta, P., 2023)	• Utilized anomaly detection techniques with SVM and Neural Networks • Emphasized on unsupervised learning methods	• High false alarm rates • Requires extensive parameter tuning

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

Literature Review

11	ML-based DDoS Attack Detection in SDN Environments (Journal of Network and Computer Applications, Wu, J., Li, S., Wang, Y., 2023)	• Implemented ML algorithms (Random Forest, SVM) in SDN • Achieved high detection accuracy and low latency	• Scalability issues • High resource consumption
12	AI-based DDoS Attack Detection Using Ensemble Learning (IEEE Access, Ahmed, M., Yousaf, M., Khalid, S., 2024)	• Combined ensemble learning methods (AdaBoost, Random Forest) • Focused on improving detection accuracy	• High computational complexity • Integration challenges in real-time systems
13	Hybrid Deep Learning Models for DDoS Detection in IoT Networks (IEEE Internet of Things Journal, Sharma, R., Gupta, V., 2024)	• Combined CNN and LSTM for hybrid model • Achieved high detection rates with IoT data	• High training complexity • Requires large labeled datasets
14	Machine Learning Techniques for DDoS Detection in Cloud Environments (Journal of Information Security and Applications, Chen, L., Xu, H., 2024)	• Implemented SVM and Neural Networks for cloud security • Focused on feature engineering for cloud-specific attacks	• Scalability issues • High computational cost
15	A Novel Machine Learning Approach for DDoS Detection Using Big Data Analytics (IEEE Transactions on Network and Service Management, Singh, K., Rajput, N., 2024)	• Utilized big data analytics with ML algorithms (SVM, Random Forest) • Focused on real-time detection in big data environments	• High resource consumption • Complexity in data integration

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

Literature Review

16	Deep Learning-based DDoS Attack Detection in Smart Grid Networks (IEEE Access, Zhou, Z., Liang, H., 2020)	• Applied CNN and LSTM for smart grid environments • Achieved high detection accuracy with deep learning models	• High computational cost • Limited by smart grid device capabilities
17	AI-driven DDoS Attack Detection in Autonomous Systems (IEEE Transactions on Network and Service Management, Park, J., Choi, S., 2021)	• Implemented AI-driven techniques (CNN, RNN) for autonomous systems • Focused on real-time detection and response	• High computational complexity • Requires extensive training data
18	Neural Network-based DDoS Detection in Healthcare IoT Systems (Journal of Network and Computer Applications, Das, S., Roy, P., 2022)	• Applied neural networks for healthcare IoT data • Focused on anomaly detection in IoT environments	• High false positive rate • Limited by healthcare device capabilities
19	DDoS Attack Detection Using Deep Learning in 5G Networks (IEEE Internet of Things Journal, Kim, H., Lee, J., 2023)	• Utilized deep learning models (CNN, LSTM) for 5G network data • Achieved high detection accuracy	• High computational cost • Integration challenges with 5G infrastructure
20	Hybrid Machine Learning Models for DDoS Detection in Cloud Computing (IEEE Access, Ali, A., Ahmed, Z., 2023)	• Combined SVM and Random Forest for hybrid approach • Focused on feature selection and extraction for cloud environments	• Complexity in model integration • Scalability issues

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

Literature Review

21	A Deep Learning Approach for DDoS Detection in Vehicular Networks (IEEE Transactions on Network and Service Management, Liu, Y., Zhang, Y., 2024)	• Implemented CNN and LSTM for vehicular network data • Focused on real-time detection and response	• High computational cost • Limited by vehicular device capabilities
22	AI-based Anomaly Detection for DDoS Attacks in IoT Systems (Journal of Information Security and Applications, Wang, X., Chen, M., 2024)	• Applied AI-based anomaly detection techniques • Focused on improving detection accuracy with IoT data	• High false alarm rates • Requires extensive parameter tuning
23	Machine Learning for DDoS Attack Detection in Smart Home Environments (IEEE Access, Zhang, L., Li, T., 2023)	• Implemented ML algorithms (SVM, Random Forest) for smart home data • Achieved high detection accuracy	• Scalability issues • High resource consumption
24	DDoS Attack Detection Using Ensemble Learning in Edge Computing (Journal of Network and Computer Applications, Huang, Z., Liu, Q., 2022)	• Applied ensemble learning methods (Bagging, Boosting) • Focused on edge computing environments	• High computational complexity • Limited by edge device capabilities
25	AI-driven DDoS Detection in Blockchain Networks (IEEE Transactions on Network and Service Management, Kim, S., Park, D., 2024)	• Utilized AI-driven techniques for blockchain data • Focused on real-time detection and response	• High computational cost • Integration challenges with blockchain infrastructure

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be **University** *u/s 3 of UGC Act, 1956*

References

1. https://www.unb.ca/cic/datasets/ddos-2019.html
2. https://doi.org/10.1117/12.2593297
3. https://pennylane.ai/qml/demonstrations/
4. https://qcgpu.github.io/
5. https://www.researchgate.net/publication/371247787_Machine_Learning_in_Cybersecurity
6. https://www.researchgate.net/publication/375926982_Enhancing_DDoS_Attack_Detection