IMPLEMENTASI *QUANTUM MACHINE LEARNING* DALAM MELAKUKAN DETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

Nauvan Dimas Saputra

09011181924001

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

IMPLEMENTASI *QUANTUM MACHINE LEARNING* DALAM MELAKUKAN DETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDoS)

TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh

Nauvan Dimas Saputra

09011181924001

Indralaya, 9 Januari 2024

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 24 November 2023

Tim Penguji :

1. **Ketua : Kemahyanto Exaudi, M.T.**
2. **Sekretaris : Rahmat Fadli Isnanto, M.Sc.**
3. **Penguji : Huda Ubaya, M.T.**
4. **Pembimbing : Ahmad Heryanto, M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Nauvan Dimas Saputra
NIM : 09011181924001
Judul : Implementasi *Quantum Machine Learning* dalam Melakukan Deteksi Serangan *Distributed Denial of Service* (DDoS)

Hasil Pengecekan Software Turnitin : 1%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyaataan ini saya buat dalam keadaan sadar dan tanpa pakasaan dari siapapun.

Indralaya, Januari 2024

Nauvan Dimas Saputra
NIM. 09011181924001

HALAMAN PERSEMBAHAN

Bismillahirrahmanirrahim

MOTTO

“ Setetes keringat orang tuaku seribu langkahku untuk maju”

Tiada lembar yang paling indah dalam laporan skripsi ini kecuali lembar persembahan. Alhamdulillahi Robbil 'Alamin dengan mengucap syukur atas rahmat Allah SWT dan sebagai ucapan terimakasih skripsi ini saya persembahkan untuk :

1. Pintu surgaku, Ibu Halimah. Perempuan hebat yang biasa saya sebut ibu, saya persembahkan skripsi untuk ibu. Terimakasih sudah melahirkan, merawat, dan membesarkan saya dengan penuh cinta, selalu berjuang untuk kehidupan saya, dan bekerja keras hingga akhirnya saya bisa tumbuh dewasa dan bisa berada di posisi saat ini.
2. Alm. Surono. Seseorang yang darahnya mengalir di dalam tubuh saya. Allhamdulillah kini saya berada di tahap ini. Beliau memang tidak dapat mendampingi secara langsung dari saya lahir sampai saat ini, tapi saya percaya bahwa beliau saat ini tersenyum dan bangga melihat saya sampai pada tahap ini.
3. Bapak Sunarko, seseorang yang biasa saya sebut bapak, terimakasih telah sabar merawat dan selalu bekerja keras dalam memenuhi kebutuhan saya sampai saat ini, saya persembahkan karya sederhana ini.
4. Kepada Naufal Al Furqon, saudara terbaik yang selalu mendukung dalam bentuk apapun itu, yang ingin saya selalu dikeadaan terbaik dan selalu membersamai dalam keadaan pahit. Terimakasih sudah menguatkan dan bekerja keras untuk membahagiakan saya. Saya persembahkan karya kecil ini untukmu.
5. Kepada seluruh anggota keluarga SUNARKO terimakasih atas kebahagiaan yang diberikan selama ini dan bantuan-bantuan sedari saya kecil sampai tahap ini. saya persembahkan karya ini untuk keluarga besar saya.

KATA PENGANTAR

Assalamu'alaikum Warrahmatullahi Wabarakatuh

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT yang telah memberikan karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini yang berjudul **"Implementasi *Quantum Machine Learning* dalam Melakukan Deteksi Serangan *Distributed Denial of Service* (DDoS)".**

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Tugas Akhir ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur dan terimakasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan Tugas Akhir ini dengan baik dan lancar.
2. Orang tua saya tercinta yang telah membesarkan saya dengan penuh kasih sayang dan selalu mengajarkan saya dalam berbuat hal yang baik. Terimakasih untuk segala doa, motivasi dan dukungannya baik moril, materil maupun spritual yang telah diberikan sampai saat ini .
3. Bapak Prof. Dr. Erwin, S.Si, M.Msi, selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, M.T., selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.
6. Bapak Dr. Ir. Bambang Tutuko, M.T., selaku dosen Pembimbing Akademik saya.
7. Mbak Renny dan kak Yopi selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.

8. Teman-teman CALMPONK, ada bayu, rahman, zainudin, habib, angga, agung, ochim, hendi, dan vano yang telah menemani selama perkuliahan, berkumpul bersama, bercerita bahagia ataupun susah. Terimakasih kawan atas kebahagian yang selama ini.
9. Teman laboratorium COMNETS, salah satunya reza mahesa terimakasih telah bersama-sama dari awal masuk perkuliahan sampai saat ini tak henti-henti memberi bantuan apapun itu.
10. Teman-teman kantin BUNDA ANJAS yang selalu menghibur dikala bosan dan bingung dalam pengerjaan tugas akhir ini.
11. Teman-teman SENJA terimakasih atas bantuan dan saling mengingatkan akan kelulusan sehingga menjadi acuan bagi penulis untuk selalu semangat.
12. Dan semua pihak yang telah membantu dalam menemani perjalanan saat pemberkasan ataupun memberi dukungan lewat apapun itu medianya untuk memberi semangat, terimakasih atas bantuan selama ini.

Penulis mengharapkan dan membuka diri untuk segala kritik dan saran yang membangun dari semua pihak sebagai acuan untuk penulisan penelitian yang lebih baik lagi. Akhir kata penulis ucapkan banyak terima kasih kepada semua pihak yang telah membantu. Semoga penelitian ini dapat bermanfaat bagi penulis dan pembaca sekalian.

Wassalamu'alaikum Wr. Wb.

Indralaya, Januari 2024

Penulis,

Nauvan Dimas Saputra

NIM. 09011181924001

Implementasi Quantum Machine Learning dalam Melakukan Deteksi Serangan Distributed Denial of Service (DDoS)

Nauvan Dimas Saputra (09011181924001)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : nauvandimas7201@gmail.com

ABSTRAK

Ancaman keamanan internet sangatlah rentan terhadap serangan dari pihak manapun, termasuk serangan *Distributed Denial-of-Services* (DDoS). Serangan DDoS mengirimkan paket secara terus menerus sehingga membanjiri jaringan, server, atapun situs web secara masif, mengakibatkan jaringan tidak bisa diakses oleh pengguna. Dalam mengidentifikasi serangan DDoS terdapat masalah yaitu input data yang sangat besar. Untuk mengatasi masalah pemrosesan dataset yang sangat besar ini, bidang *quantum computing* dapat mengatasinya. Upaya untuk menggabungkan dua bidang yaitu *quantum computing* dan *machine learning* menghasilkan *Quantum Machine Learning* (QML), bertujuan untuk mengatasi jumlah data yang sangat besar dan dapat meningkatkan kecepatan pemrosesan data yang dilakukan. Pada penelitian ini melakukan optimasi terhadap *wire quantum* dan melakukan skenario pengujian terhadap tiga jenis optimizer yaitu Adam, AdamW dan Sparse.Adam. Total skenario yang dilakukan dalam pengujian ada 36, dengan pembagian rasio data dan nilai parameter *learning rate* yang bervariasi. Dataset yang digunakan yaitu CIC-IDS 2017 yang memiliki dua label yaitu *benign* dan DDoS. Hasil pengujian terhadap *wire* quantum, dengan dua *wire* 58.2% dan empat *wire* 62.1%, performa yang terbaik dihasilkan pada optimizer AdamW dengan nilai *precision* 57.30%, *recall* 94.07%, *accuracy* 62.15%, F1-*score* 71.22%, *specificity* 30.47%, dan *false positive rate* 92.21%.

Kata Kunci : Serangan DDoS, Deteksi DDoS, Quantum Computing, Machine Learning, Quantum Machine Learning

Implementation of Quantum Machine Learning in Detecting Distributed Denial of Service (DDoS) Attacks

Nauvan Dimas Saputra (09011181924001)
Computer System Department, Computer Science Faculty, Sriwijaya University
Email : nauvandimas7201@gmail.com

ABSTRACT

Internet security is highly vulnerable to attacks from any source, including Distributed Denial-of-Service (DDoS) attacks. DDoS attacks involve the continuous transmission of packets, inundating networks, servers, or websites on a massive scale, rendering them inaccessible to users. Identifying DDoS attacks presents a challenge due to the substantial volume of input data. To address the processing challenges posed by extensive datasets, the field of quantum computing emerges as a viable solution. The integration of quantum computing and machine learning results in Quantum Machine Learning (QML), aimed at handling vast amounts of data and enhancing processing speed. This study optimizes quantum wire and conducts testing scenarios on three optimizer types: Adam, AdamW, and Sparse.Adam. The total number of scenarios in the testing phase is 36, with variations in data ratios and learning rate parameter values. The dataset used is CIC-IDS 2017, featuring two labels: benign and DDoS. Testing results on quantum wire, with two wires achieving 58.2%, and four wires reaching 62.1%, show the best performance with the AdamW optimizer, achieving a precision of 57.30%, recall of 94.07%, accuracy of 62.15%, F1-score of 71.22%, specificity of 30.47%, and a false positive rate of 92.21%."

Keywords : DDoS Attack, DDoS Detection, Quantum Computing, Machine Learning, Quantum Machine Learning

DAFTAR ISI

LEMBAR PENGESAHAN ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PERNYATAAN ..... **iv**
HALAMAN PERSEMBAHAN ..... **v**
KATA PENGANTAR ..... **vi**
ABSTRAK ..... **viii**
ABSTRACT ..... **ix**
DAFTAR ISI ..... **x**
DAFTAR GAMBAR ..... **viii**
DAFTAR TABEL ..... **xiv**
BAB I PENDAHULUAN **1**
1.1. Latar Belakang 1
1.2. Perumusan Masalah 4
1.3. Batasan Masalah 4
1.4. Tujuan 4
1.5. Manfaat 5
1.6. Sistematika Penulisan 5
BAB II TINJAUAN PUSTAKA **6**
2.1. Penelitian Terkait 6
2.2. Quantum Computing 13
2.2.1. Qubit 15
2.2.2. *Superposition* 16
2.2.3. *Entanglement* 17
2.2.4. *Uncertainty* 19
2.2.5. Dirac Notation 20
2.2.6. Bloch Sphere 20
2.2.7. Quantum Logic Gate 21
2.2.8. Quantum Circuit 22
2.3. Ditributed Denial-of-Service (DDoS) 23
2.4. Quantum Machine Learning 24

2.4.1. Quantum Support Vector Machine (QSVM) 28
BAB III METODOLOGI PENELITIAN 31
3.1. Kerangka Kerja 31
3.2. Studi Pustaka dan Literatur 32
3.3. Persiapan Data 32
3.4. Pra-pengolahan 34
3.4.1. *Feature Selection* 35
3.4.2. *Encoding* 36
3.4.3. Mereduksi Data dengan PCA 36
3.5. Pembagian Data Uji dan Data Latih 37
3.6. Pembuatan *Circuit Quantum* 37
3.7. Pengujian Model 39
3.7.1. *Jupyter Notebook* 40
3.7.2. *Python* 40
3.8. Evaluasi Model 40
3.9. Optimasi Model 42
3.10. Hasil Akurasi 43
3.11. Analisa dan Kesimpulan 43
3.11.1. Analisa 43
3.11.2. Kesimpulan 44
BAB IV HASIL DAN PEMBAHASAN 45
4.1. Pendahuluan 45
4.2. Dataset 45
4.3. Pra-pengolahan Data 45
4.4. Pengujian Model 47
4.5. Hasil Akurasi 48
4.5.1. Learning Rate 0.1 dengan Optimizer Adam 50
4.5.2. Learning Rate 0.01 dengan Optimizer Adam 56
4.5.3. Learning Rate 0.001 dengan Optimizer Adam 62
4.5.4. Learning Rate 0.1 dengan Optimizer AdamW 68
4.5.5. Learning Rate 0.01 dengan Optimizer AdamW 74
4.5.6. Learning Rate 0.001 dengan Optimizer AdamW 80

4.5.7. Learning Rate 0.1 dengan Optimizer Sparse.Adam 86
4.5.8. Learning Rate 0.01 dengan Optimizer Sparse.Adam 92
4.5.9. Learning Rate 0.001 dengan Optimizer Sparse.Adam 98
BAB V KESIMPULAN..... 107
DAFTAR PUSTAKA..... 108
LAMPIRAN..... 114

DAFTAR GAMBAR

Gambar 2.1 Metode Komputasi 14
Gambar 2.2 Roadmap Quantum Machine Learning 15
Gambar 2.3 Bit dan Qubit 16
Gambar 2.4 Keadaan Superposisi 17
Gambar 2.5 Keadaan Entanglement 18
Gambar 2.6 Keadaan Ketidakpastian 19
Gambar 2.7 Qubit 21
Gambar 2.8 Circuit 23
Gambar 2.9 Serangan DDoS 24
Gambar 2.10 Pemrosesan Conventional Machine Learning dan QML 26
Gambar 2.11 Kerangka kerja QML dengan PQC 27
Gambar 2.12 Quantum Support Vector Machine 30
Gambar 3.1 Kerangka Kerja Penelitian 31
Gambar 3.2 Arsitektur Quantum 32
Gambar 3.3 Diagram Tahap Pra-Pengolahan 35
Gambar 3.4 Proses Feature Selection 35
Gambar 3.5 Proses Encoding 36
Gambar 3.6 Proses PCA 37
Gambar 3.7 Circuit Quantum 38
Gambar 3.8 Kombinasi Gerbang RX,RY Dan RZ 38
Gambar 4.1 Proses PCA Pada Data 46
Gambar 4.2 Simulator Kuantum 47
Gambar 4.3 Model Quantum Machine Learning 48

Gambar 4.4 Optimizer Adam 49
Gambar 4.5 Optimizer AdamW 49
Gambar 4.6 Optimizer Sparse.Adam 49
Gambar 4.7 Perhitungan Data Train 50
Gambar 4.8 Perhitungan Data Tes 50
Gambar 4.9 Nilai Confusion Matrix 60:40 50
Gambar 4.10 Data Train 60:40 51
Gambar 4.11 Data Test 60:40 51
Gambar 4.12 Nilai Confusion Matrix 70:30 52
Gambar 4.13 Data Train 70:30 52
Gambar 4.14 Data Test 70:30 53
Gambar 4.15 Nilai Confusion Matrix 80:20 53
Gambar 4.16 Data Train 80:20 54
Gambar 4.17 Data Test 80:20 54
Gambar 4.18 Nilai Confusion Matrix 90:10 55
Gambar 4.19 Data Train 90:10 55
Gambar 4.20 Data Test 90:10 56
Gambar 4.21 Nilai Confusion Matrix 60:40 56
Gambar 4.22 Data Train 60:40 57
Gambar 4.23 Data Test 60:40 57
Gambar 4.24 Nilai Confusion Matrix 70:30 58
Gambar 4.25 Data Train 70:30 58
Gambar 4.26 Data Test 70:30 59
Gambar 4.27 Nilai Confusion Matrix 80:20 59

Gambar 4.28 Data Train 80:20 60
Gambar 4.29 Data Test 80:20 60
Gambar 4.30 Nilai Confusion Matrix 90:10 61
Gambar 4.31 Data Train 90:10 61
Gambar 4.32 Data Test 90:10 62
Gambar 4.33 Nilai Confusion Matrix 60:40 62
Gambar 4.34 Data Train 60:40 63
Gambar 4.35 Data Test 60:40 63
Gambar 4.36 Nilai Confusion Matrix 70:30 64
Gambar 4.37 Data Train 70:30 64
Gambar 4.38 Data Test 70:30 65
Gambar 4.39 Nilai Confusion Matrix 80:20 65
Gambar 4.40 Data Train 80:20 66
Gambar 4.41 Data Test 80:20 66
Gambar 4.42 Nilai Confusion Matrix 90:10 67
Gambar 4.43 Data Train 90:10 67
Gambar 4.44 Data Test 90:10 68
Gambar 4.45 Nilai Confusion Matrix 60:40 68
Gambar 4.46 Data Train 60:40 69
Gambar 4.47 Data Test 60:40 69
Gambar 4.48 Nilai Confusion Matrix 70:30 70
Gambar 4.49 Data Train 70:30 70
Gambar 4.50 Data Test 70:30 71
Gambar 4.51 Nilai Confusion Matrix 80:20 71

Gambar 4.52 Data Train 80:20 72
Gambar 4.53 Data Test 80:20 72
Gambar 4.54 Nilai Confusion Matrix 90:10 73
Gambar 4.55 Data Train 90:10 73
Gambar 4.56 Data Test 90:10 74
Gambar 4.57 Nilai Confusion Matrix 60:40 74
Gambar 4.58 Data Train 60:40 75
Gambar 4.59 Data Test 60:40 75
Gambar 4.60 Nilai Confusion Matrix 70:30 76
Gambar 4.61 Data Train 70:30 76
Gambar 4.62 Data Test 70:30 77
Gambar 4.63 Nilai Confusion Matrix 80:20 77
Gambar 4.64 Data Train 80:20 78
Gambar 4.65 Data Test 80:20 78
Gambar 4.66 Nilai Confusion Matrix 90:10 79
Gambar 4.67 Data Train 90:10 79
Gambar 4.68 Data Test 90:10 80
Gambar 4.69 Nilai Confusion Matrix 60:40 80
Gambar 4.70 Data Train 60:40 81
Gambar 4.71 Data Test 60:40 81
Gambar 4.72 Nilai Confusion Matrix 70:30 82
Gambar 4.73 Data Train 70:30 82
Gambar 4.74 Data Test 70:30 83
Gambar 4.75 Nilai Confusion Matrix 80:20 83

Gambar 4.76 Data Train 80:20 84
Gambar 4.77 Data Test 80:20 84
Gambar 4.78 Nilai Confusion Matrix 90:10 85
Gambar 4.79 Data Train 90:10 85
Gambar 4.80 Data Test 90:10 86
Gambar 4.81 Nilai Confusion Matrix 60:40 86
Gambar 4.82 Data Train 60:40 87
Gambar 4.83 Data Test 60:40 87
Gambar 4.84 Nilai Confusion Matrix 70:30 88
Gambar 4.85 Data Train 70:30 88
Gambar 4.86 Data Test 70:30 89
Gambar 4.87 Nilai Confusion Matrix 80:20 89
Gambar 4.88 Data Train 80:20 90
Gambar 4.89 Data Test 80:20 90
Gambar 4.90 Nilai Confusion Matrix 90:10 91
Gambar 4.91 Data Train 90:10 91
Gambar 4.92 Data Test 90:10 92
Gambar 4.93 Nilai Confusion Matrix 60:40 92
Gambar 4.94 Data Train 60:40 93
Gambar 4.95 Data Test 60:40 93
Gambar 4.96 Nilai Confusion Matrix 70:30 94
Gambar 4.97 Data Train 70:30 94
Gambar 4.98 Data Test 70:30 95
Gambar 4.99 Nilai Confusion Matrix 80:20 95

Gambar 4.100 Data Train 80:20.....96
Gambar 4.101 Data Test 80:20 96
Gambar 4.102 Nilai Confusion Matrix 90:10 97
Gambar 4.103 Data Train 90:10.....97
Gambar 4.104 Data Test 90:10 98
Gambar 4.105 Nilai Confusion Matrix 60:40 98
Gambar 4.106 Data Train 60:40.....99
Gambar 4.107 Data Test 60:40 99
Gambar 4.108 Nilai Confusion Matrix 70:30 100
Gambar 4.109 Data Train 70:30.....100
Gambar 4.110 Data Test 70:30.. 101
Gambar 4.111 Nilai Confusion Matrix 80:20.. 101
Gambar 4.112 Data Train 80:20.....102
Gambar 4.113 Data Test 80:20.. 102
Gambar 4.114 Nilai Confusion Matrix 90:10… 103
Gambar 4.115 Data Train 90:10.....103
Gambar 4.116 Data Test 90:10.. 104

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait 6

Tabel 2.2 Komputer Klasik dan QC 14

Tabel 2.1 Notasi Dirac 20

Tabel 2.1 Gerbang Logika Quantum 22

Tabel 3.1 Fitur Dataset 33

Tabel 3.2 Fitur Label 34

Tabel 3.3 Pembagian Rasio Data 42

Tabel 3.4 Optimizer 43

Tabel 3.5 Learning Rate 43

Tabel 4.1 Penjelasan Rasio Data 45

Tabel 4.2 Data Pengujian dan Parameter 46

Tabel 4.3 Optimizer 47

Tabel 4.4 Quantum Wire 47

Tabel 4.5 Hasil Quantum Wire 49

Tabel 4.6 Hasil Keseluruhan 104

BAB I
PENDAHULUAN

1.1. Latar Belakang

Ancaman keamanan internet sangatlah rentan terhadap serangan dari pihak manapun, termasuk *Denial of service* (DoS) yang merupakan serangan komputer telah menjadi masalah sejak pertama kali dikenal pada tahun 1980. Serangan tersebut merupakan tindakan illegal dimana penyerang mengganggu layanan sistem, sehingga mempengaruhi akses ke jaringan, email, dan sumber daya komputer[1]. Dalam beberapa tahun serangan DoS berkembang menjadi serangan *Distributed Denial-of-Services* (DDoS). Serangan DDoS merupakan serangan yang dilakukan dengan mengirim paket secara terus menerus sehingga membanjiri jaringan, server, atapun situs web secara masif. Sehingga mengakibatkan sumber daya mesin ataupun jaringan tidak bisa diakses oleh pengguna. Pada serangan DDoS biasanya dilakukan oleh beberapa mesin yang dioperasikan oleh pengguna ataupun bot[2].

Serangan DDoS merupakan ancaman serius bagi keamanan data karena mengakibatkan layanan menjadi tidak tersedia, sehingga berdampak kerugian yang signifikat. Menurut data F5 *Labs*[3] tren serangan DDoS pada tahun 2022 secara keseluruhan turun dari tahun sebelumnya. Pada laporan mencatat sedikit penurunan (-9,7%) dalam keseluruhan peristiwa di tahun 2021 dan penurunan serupa dalam keseluruhan peristiwa antara tahun 2020 dan 2021 (-3,5%). Serangan yang sering ditemui pada tahun 2020 dan 2021 adalah *multi*-vector ini merupakan istilah untuk serangan yang memanfaatkan lebih dari satu metode dalam satu waktu, lalu diikuti serangan volumetrik yaitu serangan yang menciptakan *traffic* dalam jumlah yang sangat besar sehingga limit dari *bandwidth* website akan mencapai batasnya, penggunaan botnet oleh pelaku yang menyebabkan server menjadi lumpuh. Tahun 2022 serangan vector aplikasi meningkat secara signifikan sebesar 165% bahkan pada saat jumlah keseluruhan serangannya menurun. Peristiwa ini menunjukan bahwa serangan vector aplikasi menjadi jauh lebih sering. Dan pada laporan tren menunjukkan bahwa puncak *bandwidth* kembali naik pada tahun 2022, serangan ini dalam rentang terabit per detik. Puncak maksimum *bandwidth* yang telah

diamati adalah 800mbps pada tahun 2022, turun dari 1,39 tbps pada tahun sebelumnya, penurunan sebesar 42,4%. Pada tahun 2020 laporan mencatat puncak *bandwidth* hanya 253mbps, dan tahun 2022 meningkat sebesar 216%.

Dampak serangan *Distributed Denial-of-Service (DDoS)* menyebabkan *crash* pada server dan sistem di jaringan akan dibanjiri paket ataupun permintaan di jaringan tersebut. Dengan berkembangnya sistem jaringan, jumlah pengguna yang didalamnya juga semakin banyak. Hal itu akan menyebabkan kesulitan dalam mengidentifikasi siapa pengguna legal dan siapa pereteas (*hacker*). Perkembangan teknologi saat ini sangat cepat sehingga membuat teknik serangan DDoS juga semakin meningkat. Dalam mengidentifikasi serangan DDoS menjadi masalah yang lebih kompleks karena terdapat berbagai jenis strategi serangan DDoS. Adapun beberapa jenis serangan DDoS yaitu ICMP flood, SYN flood, IP packet flood, dan lain-lain[4].

Pada tahun 2022 data *comparitech* melaporkan bahwa jumlah aktivitas serangan DDoS lebih tinggi dibandingkan tahun-tahun sebelumnya. Tidak hanya itu, serangan juga berlangsung lebih lama. Pada tahun 2021, rata-rata serangan DDoS berlangsung selama 30 menit, setahun kemudian meningkat dengan rata-rata 50 jam. Pada September 2022, Google mengumumkan berhasil menghentikan serangan DDoS yang mengirimkan 46 juta permintaan per detik[5].

Banyak metode yang dapat mendeteksi serangan DDoS, seperti *machine learning*. Namun, dalam kasus input data yang sangat besar banyak sekali hambatan yang terjadi. Akurasi *output* yang dihasilkan dapat dengan akurat tetapi membutuhkan waktu yang sangat lama, atau dengan cepat memproses pengujian dan pelatihan tetapi akurasi output buruk. Untuk mengatasi masalah pemrosesan dataset yang sangat besar ini. Bidang *quantum computing* dapat mengatasinya, *Quantum computing* yaitu mesin hipotetis yang menggunakan prinsip mekanika kuantum untuk operasi dasarnya, kuantum komputasi sendiri dapat meningkatkan pemrosesan data yang dilakukan. Beberapa tahun terakhir *quantum computing* dapat menyelasaikan masalah dengan tingkat efisiensi yang jauh lebih tinggi dari komputer klasik[6].

Penelitian sebelumnya menggabungkan *quantum* dengan bidang keamanan dalam mengimplementasikan protokol kriptografi, penelitian ini adalah Quantum

Key Distributed (QKD) yang merupakan teknologi maju dengan hukum fisika kuantum untuk mengamankan kerahasiaan kunci enkripsi melalui jaringan serat optic atau di ruang kosong. Semua upaya untuk mematai-matai jaringan akan terdeteksi dan mencegah intersepsi pasif. Penggunaan QKD sekarang memberikan perlindungan langsung untuk data terhadap serangan *brute force,* dan memberikan perlindungan data dengan usia simpan yang panjang serta terhindar dari serangan di masa komputasi pasca-kuantum[7].

Pada penelitian[8] *Quantum computing* juga menunjukkan keunggulan bekerja dalam melatih Jaringan Syaraf Tiruan (JST) dibandingkan dengan JST klasik. Pendekatan menggunakan *quantum computing* dalam melatih jaringan syaraf dianggap efisien dalam ruang komputasi karena hanya memerlukan qubit untuk mewakili nilai input dari data klasik.

Sejak awal tahun 1980-an, telah dimulai upaya untuk menggabungkan dua bidang yaitu *quantum computing dan machine learning*. Sebagian besar penelitian ini terinspirasi oleh prinsip biologis, hasil yang diharapkan agar dapat menemukan pemahaman tentang cara kerja otak dengan pendekatan *quantum* (hal yang masih diperdebatkan kontroversial). Awal tahun 2000-an, teori pembelajaran statistik dalam konteks kuantum mulai dibahas, tetapi hanya mendapat perhatian yang terbatas. Pada tahun 2013, penelitian dari Lloyd, Mohseni dan Rebentrost[9] memperkenalkan istilah "*Quantum Machine Learning*". *Quantum Machine Learning* (QML) adalah integrasi kuantum komputasi dengan solusi *machine learning*. Paling umum penggunaan QML mengacu pada algoritma *machine learning* untuk analisis data klasik yang dijalankan pada komputer kuantum. Metode ini bertujuan untuk menghitung jumlah data yang sangat besar. Pemrosesan data yang dilakukan sangat besar dan lama. Sistem kuantum yang digunakan dapat meningkatkan kecepatan dan pemrosesan data yang dilakukan. Teknologi komputasi kuantum sangatlah menjanjikan di area *machine learning* dikarenakan penyelesaian yang instan dan pengoptimalannya dari memproses *input* dataset yang sangat besar. Komputer kuantum memberikan percepatan kuadrat dan bahkan eksponensial terhadap *machine learning* konvensional seperti yang diusulkan. Komputasi kuantum telah diterapkan dan unggul dalam berbagai bidang keamanan informasi. Misalnya distribusi kuantum pada kunci kriptografi berhasil dalam

memecahkan masalah jaminan distribusi kunci antara pengguna. Selain itu ada beberapa karya penerapan QML untuk mendeteksi jenis serangan dunia maya yang konkret. Misalnya, *Quantum Support Vector Machine* (QSVM) yang dibuat untuk mendeteksi serangan DDoS[10].

Berdasarkan penjelasan – penjelasan tersebut, maka penulis akan melakukan penelitian untuk melakukan pendeteksian serangan DDoS menggunakan dataset CIC-IDS 2017, dan akan menggunakan metode *quantum machine learning*, sehingga penulis tertarik mengambil judul **"Implementasi *Quantum Machine Learning* dalam Melakukan Deteksi Serangan *Distributed Denial of Service* (DDoS)"**. Proses pendeteksian ini diharapkan dapat memberikan informasi dan mendapatkan hasil terbaik dalam mendeteksi suatu serangan.

1.2. Perumusan Masalah

Adapun beberapa masalah dalam penelitian ini adalah bagaimana cara kerja dari *quantum machine learning* dalam mengolah data serangan DDoS.

1.3. Batasan Masalah

Berikut adalah batasan masalah pada Tugas Akhir ini, yaitu :

1. Serangan yang digunakan pada penelitian ini adalah DDoS.
2. Metode yang dipakai pada penelitian ini adalah Quantum Machine Learning.
3. Dataset yang digunakan yaitu CIC-IDS 2017.

1.4. Tujuan

Tujuan dari penulisan Tugas Akhir ini adalah sebagai berikut :

1. Mengembangkan konsep komputasi *quantum computing* dan *machine learning*.
2. Mendeteksi serangan DDoS dengan proses *quantum*.
3. Menerapkan simulator kuantum dalam pengolahan data.
4. Menganalisa keefektifan penggunaan komputasi *quantum* dalam mendeteksi serangan DDoS.

1.5. Manfaat

Manfaat dari penulisan Tugas Akhir ini, yaitu:

1. Dapat menerapkan konsep *quantum machine learning* untuk mendeteksi serangan DDoS.
2. Dapat memperoleh *output* yang optimal dari proses konsep tersebut.
3. Mengetahui cara kerja simulator kuantum dalam mendeteksi serangan DDoS.
4. Dapat menganalisa performa dan kinerja hasil dari deteksi serangan DDoS berbasis *quantum*.

1.6. Sistematika Penulisan

Sistematika yang akan digunakan dalam penulisan tugas akhir adalah :

BAB I PENDAHULUAN

Bab pertama akan memaparkan sistematis mengenai latar belakang, tujuan penelitian, rumusan masalah, serta bentuk sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Bab kedua akan menjelaskan teori-teori dasar yang akan menjadi landasan dari penelitian ini. Dasar teori yang akan dibahas pada bab ini mengenai *Quantum Computing, serangan Distributed Denial of Service (DDoS),* dan *Quantum Machine Learning.*

BAB III METODOLOGI PENELITIAN

Bab ini berisi kerangka kerja atau tahapan dan metode yang akan dilakukan dalam penelitian ini.

BAB IV HASIL DAN ANALISA

Bab ini akan memaparkan hasil pengujian yang diperoleh dan menjelaskan analisa terhadap hasil penelitian yang telah dilakukan.

BAB V KESIMPULAN

Bab ini akan menampung simpulan yang dapat disimpulkan dari hasil keseluruhan penelitian dan analisa.

BAB II
TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Penelitian terkait merupakan hasil kegiatan eksplorasi terhadap penelitian-penelitian terdahulu, dengan tujuan penulis dapat menjadikan referensi dan dapat memperkaya teori dalam mempelajari penelitian yang dilakukan. Dari hasil eksplorasi penelitian terkait, penulis tidak menemukan penelitian yang judulnya sama dengan judul penulis. Penelitian ini sangatlah berbeda dengan penelitian terdahulu. Berikut ini adalah penelitian terdahulu yang terkait dengan penelitian penulis.

Tabel 2.1 Penelitian terkait

No.	Nama Penulis	Judul Penelitian	Tahun	Metode	Dataset	Hasil
1.	Maxim Kalinin, dan Vasiliy Krundyshev	Security Intrusion Detection Using Quantum Machine Learning Techniques[10]	2022	Quantum Machine Learning	IoT Network Intrusion Dataset	Pada penelitian ini hasil klasifikasi menggunakan QML menunjukkan keunggulan yang siginifikat dengan akurasi 98%
2.	Yuxuan Du, Yibo Yang, Dacheng Tao, dan Min-Hsiu Hsieh	Demystify Problem-Dependent Power of Quantum Neural Networks on Multi-Class Classification[11]	2022	Quantum neural networks	Data Fashion-MNIST	Hasil menunjukan bahwa QC tidak dapat mempelajari dataset Fashion-MNIST, dimana status fitur dari kelas yang sama tidak dapat diciutkan ke titik unik, selain itu ketidakmampuan mencapai training loss yang optimal

						menunjukkan keterbatasan kekuatan QC pada penelitian ini.
3.	Ricardo Daniel Monteiro Simões, Patrick Huber, Nicola Meier, Nikita Smailov, Rudolf M. Fuchslin, dan Kurt Stockinger	Experimental Evaluation of Quantum Machine Learning Algorithms[12]	2022	Quantum Machine Learning	Iris dataset, rain dataset, vlds dataset, custom dataset, dan adhoc dataset	Kinerja kombinasi terbaik dari sirkuit kuantum dan optimal per dataset, dengan rata-rata akurasi dari kelima set data adalah 85% pada simulator kuantum dan 84% pada computer kuantum. Hasil QNN unggul 5% lebih baik daripada hasil QSVM.
4.	Francesco Mercaldo, Giovanni Ciaramella, Giacomo Iadarola, Marco Storto, Fabio Martinelli dan Antonella Santone	Towards Explainable Quantum Machine Learning for Mobile Malware Detection and Classification[13]	2022	Quantum Machine Learning	Malicious Android applications (the Virustotal)	Hasil dari penelitian menunjukkan model yang terbaik adalah standard-CNN dengan presisi sebesar 0.972 dan nilai recall 0.970. performa yang baik juga diperoleh dengan menggunakan model MobileNet, VGG16, dan VGG19. Model Hybrid-QCNN menunjukkan presisi sebesar 0.905 dan recall 0.903, sedangkan model QNN memperoleh hasil yang

						lebih rendah dengan presisi 0.623 dan nilai recall 0.103. Jumlah sampel yang salah klasifikasi dalam model hybrid-QCNN jauh lebih besar daripada model standard-CNN.
5.	Mahabubul Alam, Satwik Kundu, Rasit Onur Topaloglu, dan Swaroop Ghosh	Quantum-Classical Hybrid Machine Learning for Image Classification[14]	2021	Quantum Neural Network	MNIST dataset	Pada penelitian ini menghasilkan 89% akurasi pelatihan dan 89% akurasi validasi untuk pendekatan model Convolutional Autoencoder + QNN sedangkan pendekatan Principal Components Analysis + QNN menghasilkan 78% akurasi pelatihan dan 71% akurasi validasi.
6.	Avinash Chalumuria, Raghavendra Kuneb, dan B. S. Manoj	Training an Artificial Neural Network Using Qubits as Artificial Neurons: A Quantum Computing Approach[8]	2020	Quantum Computing Artificial Neural Network (QC ANN)	Dataset Wisconsin Breast Cancer Diagnosis (WBCD)	Hasil menunjukkan bahwa QC ANN mengungguli ANN versi klasik untuk klasifikasi biner dengan akurasi 82,51% sedangkan ANN dengan akurasi 39,86%

7.	Saurabh Kumar, Siddharth Dangwal, dan Debanjan Bhowmiky	Supervised Learning Using a Dressed Quantum Network with Super Compressed Encoding": Algorithm and Quantum-Hardware-Based Implementation[15]	2020	Quantum Machine Learning	Fisher's Iris, Wisconsin's Breast Cancer (WBC), dan Abalone	Terdapat tiga hasil yang didapatkan pada penelitian ini, hasil dari komputer klasik, qiskit, dan IBM-Q. Dataset fisher's iris dengan akurasi 90% dari komputer klasik, 94% qiskit, 82% IBM-Q, selanjutnya data WBC 92.37% komputer klasik, 96.45% qiskit, 91.71% IBM-Q, dan data abalone 67.70% komputer klasik, 67.44% qiskit, dan 67.22% IBM-Q.
8.	Abir EL Azzaoui, dan Jong Hyuk Park	Post-Quantum Blockchain for a Scalable Smart City[16]	2020	Quantum Blockchain	Kerangka smart city	Hasil penelitian ini membuktikan komputer quantum mampu mempercepat secara eksponensial kecepatan pemecahan algoritma enkripsi klasik menggunakan algoritma Quantum seperti algoritma Shore dan algoritma Grover. Algoritme yang terkait dengan Blockchain, seperti skema berbasis

						SHA-1, SHA-2, SHA-256 dan Elliptic Curve seperti ECDSA dan BLS rentan terhadap serangan Quantum.
9.	Arnaldo Gouveia, dan Miguel Correia	Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection[17]	2020	Quantum Support Vector Machine (QSVM)	NSL-KDD	Penelitian ini menghasilkan nilai akurasi 92% untuk QSVM dan nilai akurasi 93% untuk SVM
10.	Teppei Suzuki dan Michio Katouda	Predicting Toxicity by Quantum Machine Learning[18]	2020	Quantum Machine Learning	Data 221 phenols	Hasil penelitian menunjukkkan QML berhasil dalam tugas regresi linier dengan pengingkatan 51% dan 12% untuk set pelatihan dan validasi. Model QML unggul dari model multiple linear regression (MLR) dan radial basis function neural networks (RBF-NNs).
11.	Alaa Tharwat, dan Aboul Ella Hassanien	Quantum-Behaved Particle Swarm Optimization for Parameter Optimization of	2019	Quantum-Behaved Particle Swarm Optimizatio-n (QPSO)	University of California at Irvin (UCI) Machine	Hasil dari yang diperoleh QSPO-SVM akan dibandingkan dengan PSO standar dan genetic algorithm (GA). Hasil percobaan

		Support Vector Machine[19]			Learning Repository	ini membuktikan QSPO-SVM mecapai hasil yang kompetitif dan unggul dari algoritma yang lain.
12.	Maxwell Henderson, Samriddhi Shakya, Shashindra Pradhan, dan Tristan Cook	Quanvolutional Neural Networks: Powering Image Recognition with Quantum Circuits[20]	2019	Quanvolutional Neural Networks	MNIST dataset	Penelitian ini menguji tiga model yaitu CNN, CNN dengan non linier dan QNN terhadap dataset MNIST. Hasil yang diperoleh model QNN memiliki akurasi set pengujian yang lebih tinggi serta pelatihan yang lebih cepat dibandingkan CNN murni klasik.
13.	Edward Farhi, dan Hartmut Neven	Classification with Quantum Neural Networks on Near Term Processors[21]	2018	Quantum Neural Networks	MNIST data	Pengujian pada penelitian ini menghasilkan jaringan kuantum dengan benar memberi label 97% status pengujian setelah menyajikan sekitar 1000 status pengujian. Dalam penelitian ini membuktikan QNN dapat membedakan dua set data dengan benar.

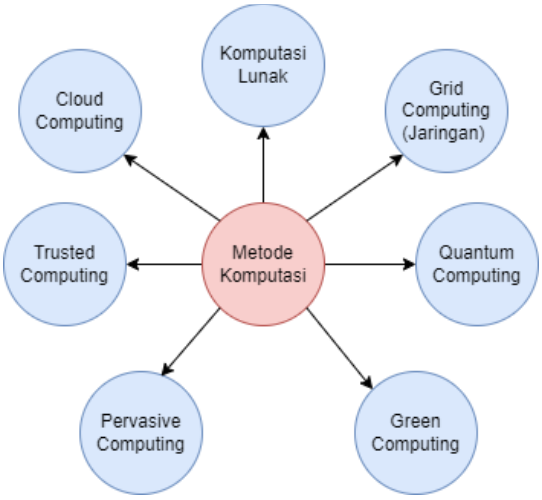
14.	Edward Grant, Marcello Benedetti, Shuxiang Cao, Andrew Hallam, Joshua Lockhart, Vid Stojevic, Andrew G. Green, dan Simone Severini	Hierarchical quantum classifiers[22]	2018	Quantum Computing	Iris dan MNIST	Dalam penelitian ini menunjukkan hirarki sirkuit kuantum dapat digunakan untuk mengklasifikasi data klasik dan kuantum. Sirkuit berdasarkan Multi-Scale Entanglement Renormalization Ansatz (MERA) dan Tree Tensor Networks (TTN). Hasil yang didapatkan pengklasifikasi MERA mencapai akurasi yang lebih tinggi daripada TTN. Sirkuit dapat dengan mudah diimplementasikan pada komputer kuantum.
15.	Zhaokai Li, Xiaome Lu, Nanyang Xu, dan Jiangfeng Du	Experimental Realization of Quantum Artificial Intelligence[23]	2014	Quantum Support Vector Machine	Standard font (Times New Roman) angka `6'serta`9' dan sample tulisan tangan	Penelitian ini menunjukan bahwa hasil yang dilalukan oleh mesin kuantum sangatlah efisien dari mesin klasik dalam melakukan pengujian terhadapat data yang besar. Sehingga model quantum dapat

						mempelajari font karakter standar kemudian mengenali karakter tulisan tangan dari satu set dengan dua pilihan. Dan ini adalah kecerdasam buatan pertama yang direalisasikan pada prosesor kuantum.

2.2. Quantum Computing

Komputasi merupakan bagian dari bidang matematika dan ilmu komputer, komputasi adalah sebuah metode untuk menemukan pemecahan masalah berdasarkan data *input* dengan menggunakan algoritma. Ribuan tahun yang lalu perhitugan dan komputasi dilakukan menggunakan kertas dan pena, atau kapur tulis dan batu. Namun seiring berjalannya zaman hal tersebut telah tergantikan dengan menggunakan komputer yang sering disebut dengan komputasi modern. Secara umum ilmu komputasi adalah bidang ilmu yang memperhatikan pengembangan model matematika, teknik penyelesaian numerik serta penerapan komputer dalam menganalisis dan memecahkan masalah.

Pada tahun 1903-1957 ilmuwan besar abad 21 Von Neumaan menciptakan sebuah konsep dimana suatu sistem yang dapat menerima intruksi-intruksi dan menyimpannya dalam memory, memory ini juga dari memory komputer dan disaat melakukan komputasi menggunakan komputer maka hal ini merupakan sebuah komputasi modern[24]. Dalam komputasi modern perhitungan yang dilakukan meliputi akurasi, kecepatan, problem volume besar, modeling, dan kompleksitas. Pada memory komputer digital menggunakan sistem binary (0 dan 1) yang dikenal sebagai BIT[25]. Gambar 2.1 dibawah ini merupakan gambar jenis-jenis metode komputasi.



Gambar 2.1 Metode komputasi

Pada tahun 1982, Richard Feynman seorang fisikawan mengusulkan simulasi sistem kuantum yang efisien. Secara umum komputer kuantum didefinisikan sebagai alat komputasi universal yang menyimpan informasi di dalam objek yang disebut bit kuantum (atau qubit) karena mampu berada di bermacam keadaan (*multiple states*) dan mengubah dengan mengeksploitasi sifat-sifat dari mekanika kuantum[26]. Pada tabel 2.2 menunjukkan perbedaan dari komputer klasik dan *quantum computing*.

Tabel 2.2 Komputer klasik dan *quantum computing*

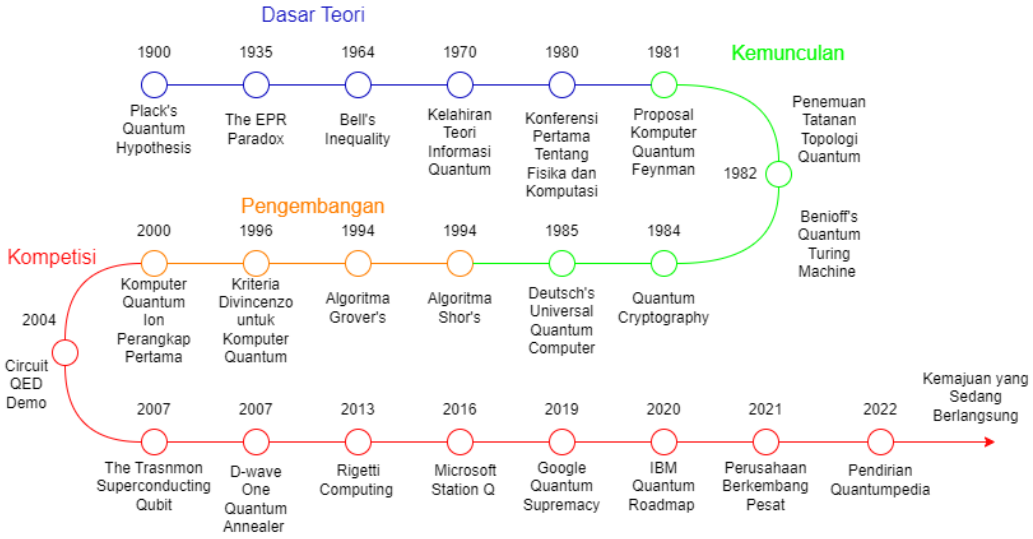
Komputer klasik	*Quantum computing*
Menghitung dengan transistor, yang dapat mewakili 0 dan 1.	Menghitung dengan qubit, dapat mewakili 0 dan 1 secara bersamaan.
Daya meningkat dalam hubungan 1:1 dengan jumlah transistor.	Daya meningkat secara eksponensial sesuai dengan jumlah qubit.
Komputer klasik memiliki tingkat kesalahan rendah.	Quantum computing memiliki tingkat kesalahan yang tinggi.
Sebagian besar pemrosesan sehari-hari paling baik dilakukan oleh komputer klasik.	Cocok untuk tugas dengan masalah optiasi, analisi data dan simulasi.

Quantum Computing adalah alat hitung yang menggunakan sebuah fenomena mekanika kuantum, misalnya superposisi dan keterkaitan untuk

melakukan operasi data. Dalam komputasi klasik, jumlah data dihitung dengan bit. Dalam komputer kuantum, hal ini dilakukan dengan qubit[27].

Quantum Computing ini berfokus pada mempelajari masalah penyimpanan, pemrosesan, dan transfer informasi yang dikodekan dalam sistem mekanika kuantum[28]. Prinsip dasar pada *quantum computing* yaitu sifat kuantum dari partikel dapat digunakan sebagai mewakili data dan struktur data, mekanika kuantum juga digunakan untuk melakukan operasi dengan data ini. Untuk mengembangkan komputer dengan sistem kuantum diperlukan logika baru yang tepat dengan prinsip kuantum[27].

Aplikasi kuantum banyak mencakup area yang berkaitan dengan sirkuit kuantum seperti pengkodean data, *compiler* atau juga deteksi keterikatan, identifikasi gerbang yang salah, dan juga pembelajaran mesin kuantum. Adapun subarea seperti sebagai pengurangan fitur atau pemrosesan Bahasa alami kuantum[29]. Gambar 2.2 dibawah ini merupakan *roadmap* dari *quantum computing.*

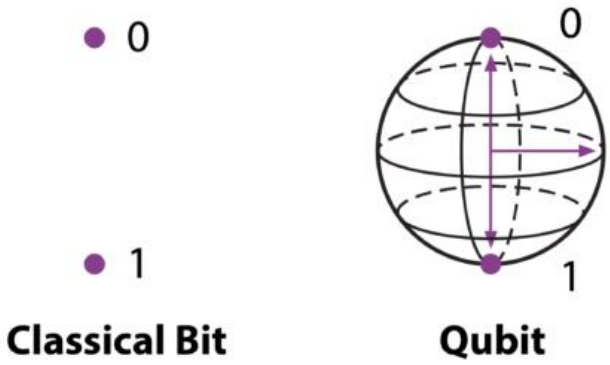


Gambar 2.2 *Roadmap quantum computing* [30]

2.2.1. Qubit

Qubit merupakan kuantum bit, mitra dalam komputasi kuantum dengan digit biner atau bit dari komputasi klasik. Sama seperti bit adalah unit dasar informasi dalam komputer klasik, qubit adalah unit dasar informasi dalam komputer kuantum. Dalam komputer kuantum, sejumlah

partikel elemental seperti elektron atau foton dapat digunakan (dalam Praktik, keberhasilan juga telah dicapai dengan ion), baik dengan biaya mereka atau polarisasi bertindak sebagai representasi dari 0 dan / atau 1. Setiap partikel-partikel ini dikenal sebagai qubit, sifat dan perilaku partikel-partikel ini (seperti yang diungkapkan dalam teori kuantum) membentuk dasar dari komputasi kuantum. Dua aspek yang paling relevan fisika kuantum adalah prinsip superposisi dan *Entanglement*[31]. Perbedaan Bit dan qubit terdapat pada gambar 2.3.



Gambar 2.3 Bit dan qubit

2.2.2. *Superposition*

Dalam kuantum computing, superposisi adalah konsep dasar yang memungkinkan qubit (quantum bit) untuk ada dalam dua atau lebih keadaan pada saat yang sama. Artinya, sebuah qubit dapat memiliki probabilitas untuk berada dalam keadaan 0 atau 1 secara simultan. Secara matematis, superposisi dapat dijelaskan dengan persamaan berikut:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1)$$

Keterangan :

$|\psi\rangle$ = Representasi vektor dari qubit

α dan β = Koefisien kompleks yang menentukan probabilitas dari masing-masing keadaaan qubit

$|0\rangle$ dan $|1\rangle$ = keadaan dasar qubit.

di mana α dan β adalah koefisien kompleks, dan $|0\rangle$ dan $|1\rangle$ adalah vektor dasar dalam ruang Hilbert 2-dimensi. Vektor $|\psi\rangle$ mewakili keadaan

qubit dalam superposisi, dan probabilitas untuk mengamati nilai 0 atau 1 dapat dihitung dengan menghitung kuadrat dari koefisien kompleksnya, yaitu |α|^2 dan |β|^2.

Superposisi adalah salah satu konsep dasar dalam kuantum computing yang memungkinkan qubit untuk melakukan operasi paralel pada beberapa nilai input sekaligus, yang sangat meningkatkan kecepatan komputasi dibandingkan dengan komputasi klasik[32].

Gambar 2.4 Keadaan superposisi

Pada gambar 2.4 diilustrasikan sebuah qubit dalam keadaan superposisi yang terdiri dari 50% |0⟩ dan 50% |1⟩[33].

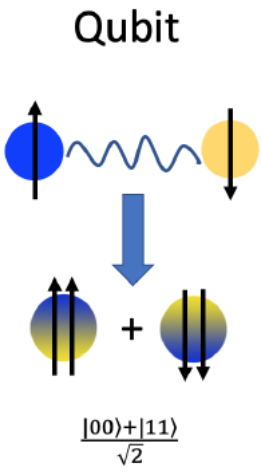
2.2.3. *Entanglement*

Entanglement adalah fenomena dalam ruang kuantum dan partikel dari setiap titik saling terkait dan tidak dapat dipisahkan. Jika suatu keadaan kuantum dari sistem gabungan tidak dapat direspresetasikan sebagai hasil langsung dari keadaan kuantum subsistem, maka sistem akan dapat berada dalam keadaan kuantum murni atau keadaan terikat. Teori ini juga dapat diterapkan pada keadaaan campuran, yang dapat dijelaskan bahwa keadaan seluruh system tidak dapat sepenuhnya ditentukan tetapi ada dalam keadaan kuantum yang sesuai dalam bentuk probabilitas tertentu, dan juga dapat dijelaskan menggunakan matriks densitas kuantum. Pada keadaan campuran yang tidak dapat dinyatakan secara akurat sebagai bentuk keadaan yang dapat diintegrasikan langsung dan tidak melibatkan keterikatan nonlinier

dianggap sebagai keadaan tidak terikat. Untuk kasus yang di mana subsistem komposit tidak dapat dibagi menjadi tiga atau lebih subsistem dan dua subsistem tidak dapat untuk dipresentasikan sebagai hasil langsung dari setiap subsistem, sebagai keadaan murni atau campuran dari sistem akan dianggap keadaan terikat[34].

Contoh sederhana dari *entanglement* adalah *Bell state*, di mana dua qubit dapat berada dalam superposisi *entangled*. Ketika dua qubit terikat dalam keadaan *Bell state*, keadaan kuantum dari satu qubit tidak dapat dijelaskan secara independen dari keadaan kuantum yang lain. Sebagai contoh, jika mengukur keadaan kuantum dari salah satu qubit akan secara instan mengetahui keadaan kuantum dari qubit yang lain tanpa melakukan pengukuran terhadap qubit yang lain.

Entanglement memainkan peran penting dalam banyak algoritma kuantum, termasuk algoritma pencarian *Grover* dan algoritma faktorisasi *Shor*. Pengembangan teknologi *entanglement* juga telah digunakan dalam pengembangan komunikasi kuantum yang aman dan memungkinkan pengiriman informasi secara efisien dan dengan keamanan yang lebih tinggi[35].



Gambar 2.5 Keadaan *entanglement*

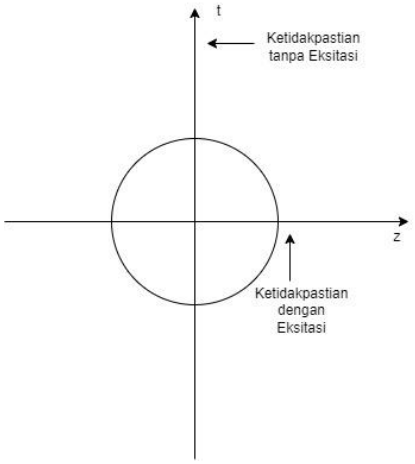
Gambar 2.5 merupakan ilustrasi sebuah qubit dalam keadaan terjerat (*entangled*). Sifat dari dua qubit pada keadaan terjerat satu sama lain akan mengukur salah satu dari mereka dan akan mengungkapkan qubit yang lain.

Bahkan ketika mereka berada dijarak yang sangat jauh[33].

2.2.4. *Uncertainty*

Dalam teori kuantum, *uncertainly* adalah hasil yang tak terhindarkan dari prinsip superposisi dan inkonsistensi dalam sifat yang dapat diobservasi. Karena konsep koherensi kuantum tergantung pada basis, penting untuk mengevaluasi apakah koherensi memperhatikan hubungan ketidakpastian untuk dua atau lebih basis yang tidak kompatibel[36].

Prinsip *Uncertainty* membuktikan bahwa tidak dapat secara bersamaan untuk menetapkan nilai pasangan posisi dan momentum, dengan presisi yang penuh. Konsekuensinya, untuk upaya mengukur posisi partikel hingga tingkat akurasi tertinggi akan mengarah pada peningkatan ketidakpastian dalam pengukuran momentum partikel, sehingga tingkat akurasi yang sama tingginya[37].



Gambar 2.6 Keadaan ketidakpastian (*uncertainly)*

Pada gambar 2.6 merupakan keadaan hubungan mekanika kuantum dengan ketidakpastian waktu dan energi. Bentuk kuantum ini dapat memungkinkan eksitasi di sepanjang arah ruang, sehingga tidak memungkinakn eksitasi di sepanjang arah waktu meskipun ada hubungan ketidakpastian antara variabel waktu dan energi. Eksitasi hanya terjadi pada energi dengan nilai tertentu. Keadaaan ini adalah naiknya energi pada sebuah sistem sehingga lebih tinggi dari keadaan awal[38].

2.2.5. Dirac Notation

Dirac Notation atau juga dikenal sebagai notasi bra-ket, merupakan sebuah notasi matematika yang digunakan dalam mekanika kuantum yang bertujuan untuk menggambarkan keadaan kauntum. Notasi ini Sebagian besar dipelopori oleh fisikawan inggris yang bernama Paul Dirac pada tahun 1939[39]. Pada *dirac notation* menggunakan simbol-simbol, pada bra simbolnya $\langle ... |$ dan pada ket simbolnya $| ... \rangle$ sebagai menggambarkan vector dalam ruang Hilbert kuantum. Ket menjelaskan keadaan kuantum dan untuk bra akan menjelaskan keadaa konjugat terbalik. Notasi bra-ket ini bertujuan memudahkan perhitungan dalam mekanika kuantum karena dapat memungkinkan operasi linear seperti penjumlahan, pengurangan, dan perkalian yang dilakukan secara mudah. Notasi ini akan membantu dalam hal menggambarkan *entanglement*, superposisi dan juga pengukuran dalam mekanika kuantum[40]. Pada tabel 2.3 dibawah ini adalah notasi dirac pada mekanika kuantum.

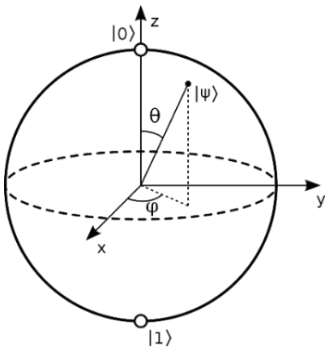
Tabel 2.3 Notasi dirac

Notasi	Keterangan
$\|\psi\rangle$	Dikenal sebagi ket
$\langle\psi\|$	Vektor ganda dari $\|\psi\rangle$ (bra)
$\langle\varphi\|\psi\rangle$	Hasil kali dalam antara $\|\varphi\rangle$ dan $\|\psi\rangle$
$\|\varphi\rangle\|\psi\rangle$	Produk tensor
$\langle\varphi\|A\|\psi\rangle$	Hasil kali dalam antara $\|\varphi\rangle$ dan $A\|\psi\rangle$

2.2.6. Bloch Sphere

Bloch Sphere adalah representasi geometris dari status qubit tunggal murni sebagai titik pada unit *sphere*. Operasi pada qubit tunggal yang biasa digunakan dalam pemrosesan informasi kuantum dapat direpresentasikan pada *Bloch sphere*. Kutub utara dan kutub selatan *Bloch sphere* didefinisikan sebagai dasar komputasi ortonormal menyatakan $|0\rangle$ dan $|1\rangle$, masing-masing, dan qubit tunggal arbitrer keadaan murni, hingga fase global, diwakili oleh sebuah titik pada bola satuan, dengan demikian menghubungkan superposisi keadaan dasar terhadap koordinat sudut titik.

Setiap operasi kesatuan, mengambil keadaan awal ke keadaan akhir qubit tunggal, setara dengan komposisi satu atau lebih rotasi sederhana pada *Bloch sphere*[41]. Gambar 2.7 merupakan representasi geometris dari ruang keadaan murni pada sistem mekanik kuantum dua tingkat, yaitu qubit.



Gambar 2.7 Qubit

2.2.7. Quantum Logic Gate

Komputer terdiri dari memori dan gerbang logika, tetapi komputer kuantum memiliki konten penyimpanan dan gerbang logika yang berbeda dibandingkan dengan komputer klasik. Sementara komputer klasik didasarkan pada mesin Turing serba guna, komputer kuantum didasarkan pada mesin Turing kuantum. Mesin Quantum Turing dapat setara dengan sirkuit logika kuantum, dan dengan menggabungkan berbagai gerbang logika kuantum, komputer kuantum dapat dibangun. Gerbang logika kuantum adalah blok bangunan dasar komputasi kuantum, dan mereka melakukan operasi pada bit kuantum. Tidak seperti gerbang logika klasik, gerbang logika kuantum harus dapat dibalik, dan semua operasi juga harus dapat dibalik. *With-gate, or-gate, hetero-or-gate, with-or-with gate,* dan *non-gate* adalah operasi ireversibel dan tidak dapat digunakan dalam komputasi kuantum. Namun, semua operasi reversibel dapat disusun menggunakan kontrol non-gerbang dan operasi rotasi satu bit. Gerbang logika kuantum diklasifikasikan berdasarkan jumlah bit input dan dapat berupa gerbang logika bit tunggal, dua bit, atau tiga bit. *Output* dari gerbang logika kuantum diperoleh melalui transformasi deterministik paling positif pada bit input. Deutsch menemukan bahwa hampir semua gerbang logika kuantum tiga-bit dapat digunakan dalam serangkaian atau rangkaian untuk

mendekati fungsi logika kompleks lainnya dengan presisi yang dapat diatur. Dalam konteks komputasi kuantum, serangkaian gerbang logika kuantum yang dihubungkan secara bersama-sama untuk membangun operasi yang lebih kompleks juga disebut dengan "*quantum circuit*"[42].

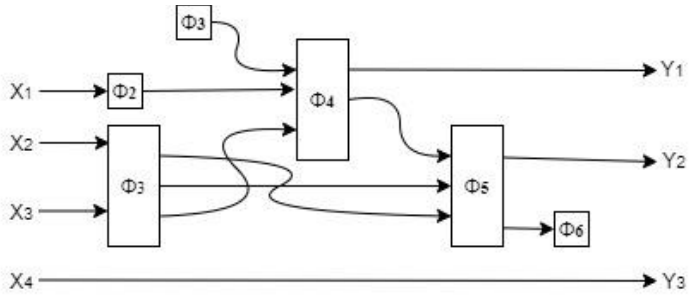
Gerbang kuantum adalah komponen yang sangat penting dalam komputasi kuantum yang dapat bekerja pada satu atau lebih qubit. Untuk menjalankan sebuah algoritma kuantum, perlu disusun sebuah sirkuit kuantum yang terdiri dari beberapa gerbang kuantum yang bekerja pada satu atau lebih qubit. Dalam sirkuit ini, gerbang kuantum dapat melakukan berbagai operasi matematis dan transformasi pada qubit[43].

Tabel 2.4 Gerbang Logika Quantum

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

2.2.8. Quantum Circuit

Quantum circuit merupakan beberapa gerbang kuantum yang telah dihubungkan dengan kabel. Gerbang kuantum mewakili operasi kuantum sedangkan kabel mewakili qubit tempat gerbang tersebut bekerja. Contoh gambar 2.8 merupakan rangkaian kuantum yang memiliki empat qubit masukkan dan tiga qubit sebagai keluaran.



Gambar 2.8 Circuit

Keterangan :

X1,..,X4 = Qubit *input*

Y1,…,Y3 = Qubit *output*

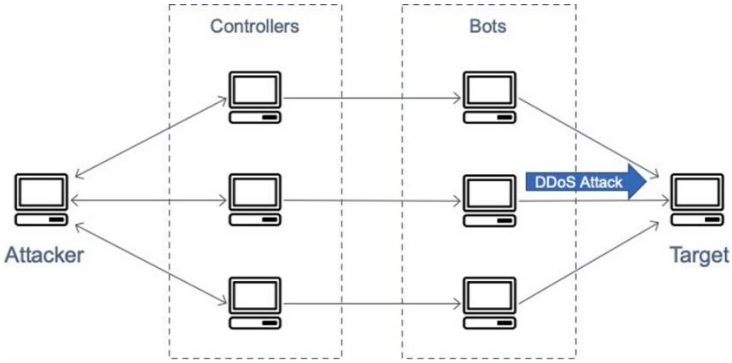
Φ1,…,Φ6 = Gerbang operasi kuantum

Secara umum gambar 2.2, dapat dijelaskan bahwa rangkaian kuantum dapat memiliki *n* qubit masukkan dan *m* qubit sebagai keluaran untuk setiap pilihan bilangan bulat $n, m \geq 0$. Rangkaian seperti ini menginduksi beberapa operasi kuantum dari *n* qubit ke *m* qubit, ditentukan dengan menyusun aksi masing-masing gerbang dengan cara yang sesuai. Ukuran sirkuit kuantum adalah jumlah total gerbang ditambah jumlah total kabel di sirkuit. Sirkuit kuantum kesatuan adalah sirkuit kuantum di mana semua gerbangnya sesuai dengan operasi kuantum kesatuan. Secara alami ini membutuhkan setiap gerbang, dan karenanya sirkuit itu sendiri, memiliki jumlah qubit masukkan dan keluaran yang sama. Hal umum dalam studi komputasi kuantum bahwa seseorang bekerja sepenuhnya dengan sirkuit kuantum kesatuan. Model kesatuan dan model umum terkait erat, seperti yang akan segera dijelaskan[44].

2.3. Ditributed Denial-of-Service (DDoS)

Serangan *Distributed Denial of Service* (DDoS) adalah salah satu kekhawatiran terbesar bagi para profesional keamanan. Serangan DDoS biasanya merupakan upaya eksplisit untuk mengganggu akses pengguna yang sah ke layanan. Penyerang biasanya mendapatkan akses ke sejumlah besar komputer dengan mengeksploitasi kerentanan mereka untuk menyiapkan pasukan penyerang Setelah pasukan penyerang telah disiapkan, penyerang dapat melakukan serangan skala besar yang terkoordinasi terhadap satu atau lebih

target[45].



Gambar 2.9 Serangan DDoS

Saat melakukan serangan sangat dibutuhkan banyak komputer yang dibutukan untuk meluncurkan serangan DDoS terkoordinasi kepada satu atau lebih target (pada gambar 2.9). Pelaku dapat melipat gandakan keefektifan DDoS secara signifikat menggunakan teknologi *client* atau *server* sehingga tanpa sadari menghabiskan sumber daya dari beberapa komputer yang berfungsi sebagai platform serangan. Serangan DDoS itu sendiri terdiri dari empat elemen, yaitu :

- Penyerang yang sebenarnya.
- Penangan atau *host* sebagai master, yang mampu mengontrol banyak agen.
- Agen daemon serangan atau *host zombie* sebagai yang bertanggung jawab untuk menghasilkan aliran paket kearah korban yang ditargetkan.
- Host target[46].

DDoS merupakan salah satu serangan yang sering terjadi didunia maya. Serangan DDoS susah dibedakan dari trafik normal, selain itu, dalam deteksi serangan tidak semua fitur dianalisa. Terlalu banyak fitur yang tidak relevan akan menghasilkan kategori kelas yang tidak berhubungan dan membebani waktu komputasi[47].

2.4. Quantum Machine Learning

Penerapan *quantum computing* ke *machine learning* adalah kemampuan mereka untuk melakukan aljabar linier cepat pada ruang keadaan yang tumbuh

secara eksponensial dengan jumlah qubit. Teknik berbasis aljabar linier yang dipercepat kuantum untuk *machine learning* ini dapat dianggap sebagai generasi pertama dari *quantum machine learning* (QML) yang menangani berbagai aplikasi dalam *supervised* dan *unsupervised learning*, termasuk *principal component analysis, support vector machine, kmeans clustering,* dan sistem rekomendasi. Algoritma ini sering menjadi solusi dikarenakan lebih cepat secara eksponensial dibandingkan dengan algoritma klasik pada jenis data kuantum tertentu[48].

Quantum Machine Learning (QML) menggunakan algoritma kuantum untuk penerapannya. Dengan cara menganalisis langkah-langkah yang ditentukan oleh algoritme kuantum. Potensi kuantum ini sangat unggul dalam masalah tertentu dengan mengurangi jumlah langkah yang diperlukan[49]. Kuantum dapat membantu pemrosesan input data besar yang menjadi solusi dalam masalah *machine learning* dalam mendeteksi serangan DDoS. Sistem kuantum bahkan berpotensi mampu mencapai akurasi prediksi yang lebih tinggi saat diberikan masalah yang sama dengan sistem klasik[50]. Untuk menggunakan algoritma QML, ada beberapa bagian yang perlu di perhatikan :

- Algoritma kuantum adalah blok bangunan QML dan berfungsi untuk melakukan perhitungan pada mekanika kuantum.
- *Varitional quantum circuit* adalah sirkuit kuantum berparameter yang dilatih dengan cara diawasi menggunakan data berlabel.
- *Classical deep neural networks,* ini digunakan sebagai bagian dari algoritma *hybrid classical quantum*[51].
- *Variational quantum algorithms,* algoritma ini berfungsi untuk memecahkan maslah optimasi.
- Keadaan kuantum, ini mengimplementasikan sistem kuantum dalam QML[52].
- Keterbatasan perangkat keras, sumber daya perangkat keras atau simulator kuantum pada saat ini belum optimal untuk pendekataan kuantum murni, sehingga pendekatan hibrida diusulkan untuk menyatukan komputasi klasik dan kuantum.
- Proses pelatihan, saat melakukan proses pelatihan algoritma QML

BAB V
KESIMPULAN

Berdasarkan pembahasan dan hasil pengujian komputasi quantum yang telah dilakukan, dapat disimpulkan sebagai berikut :

1. Penerapan *quantum machine learning* dapat membantu pemrosesan input data besar dalam mendeteksi serangan DDoS. Dengan cara menganalisis langkah yang ditentukan oleh algoritme kuantum.
2. Pada pengujian ini *confusion matrix* digunakan untuk mengevaluasi performa model dengan menunjukkan jumlah prediksi yang benar dan yang salah untuk setiap kelas atau label pada data yang diuji. Dari *confusion matrix*, beberapa nilai evaluasi performa model dapat dihitung, seperti *accuracy, precision, recall, F1-score, specificity,* dan *False Positive Rate.*
3. Percobaaan pengujian pada kabel (*wire*) kuantum dengan jumlah dua kabel dan empat kabel. Model ini menunjukkan bahwa dengan menggunakan empat kabel menghasilkan performa yang baik daripada dua kabel. Dengan nilai empat kabel 62.1% dan untuk dua kabel 58.2%. Ini menunjukkan bahwa dengan menambahkan kabel, model kuantum memiliki potensi dalam memodelkan masalah yang lebih kompleks dan menghasilkan solusi yang lebih akurat.
4. Perancangan model kuantum dengan menggunakan empat kabel (wire) untuk membangun dua sirkuit kuantum. Setiap sirkuit kuantum memiliki struktur berbeda-beda dengan serangkaian gerbang kuantum. Perancangan yang baik dalam penelitian ini dalam mendeteksi serangan DDoS.
5. Pada pengujian ini akan dilakukan beberapa skenario, yaitu dengan tiga *optimizer* Adam, AdamW, dan Sparse.Adam. Lalu melakukan pengujian dengan *learning rate* 0.1, 0.01, dan 0.001.
6. Berdasarkan pengujian yang dilakukan hasil performa yang terbaik diperoleh pada skenario pengujian dengan rasio data 80:20, *learning rate* 0.001 dan *optimizer* AdamW dengan nilai *precision* 57.30%, *recall* 94.07%, *accuracy* 62.15%, F1-score 71.22%, *specificity* 30.47%, dan *false positive rate* 92.21%.

DAFTAR PUSTAKA

[1] S. Bravo and D. Mauricio, “Systematic review of aspects of ddos attacks detection,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 14, no. 1, pp. 155–168, 2019, doi: 10.11591/ijeecs.v14.i1.pp155-168.

[2] D. Pratama, “Serangan Ddos Pada Software-Defined Network,” pp. 1–13, 2019.

[3] M. Heath, “2023 DDoS Attack Trends,” 2023. https://www.f5.com/labs/articles/threat-intelligence/2023-ddos-attack-trends

[4] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajković, “Distributed denial of service attacks,” *Proc. IEEE Int. Conf. Syst. Man Cybern.*, vol. 3, pp. 2275–2280, 2000, doi: 10.1109/ICSMC.2000.886455.

[5] S. Cook, “20+ DDoS attack statistics and facts for 2018-2023,” 2022. https://www.comparitech.com/blog/information-security/ddos-statistics-facts/#2018-2022_DDoS_stats_and_facts

[6] H. A. Bhat, F. A. Khanday, B. K. Kaushik, F. Bashir, and K. A. Shah, “Quantum Computing: Fundamentals, Implementations and Applications,” *IEEE Open J. Nanotechnol.*, vol. 3, no. May, pp. 61–77, 2022, doi: 10.1109/OJNANO.2022.3178545.

[7] J. E. Raya, A. S. Yahya, and E. K. Ahmad, “Protection from A Quantum Computer Cyber-Attack,” *Tech. Rom. J. Appl. Sci. Technol.*, vol. 5, pp. 1–12, 2023, doi: 10.47577/technium.v5i.8293.

[8] A. Chalumuri, R. Kune, and B. S. Manoj, “Training an Artificial Neural Network Using Qubits as Artificial Neurons: A Quantum Computing Approach,” *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 568–575, 2020, doi: 10.1016/j.procs.2020.04.061.

[9] S. Lloyd, M. Mohseni, and P. Rebentrost, “Quantum algorithms for supervised and unsupervised machine learning,” pp. 1–11, 2013, [Online]. Available: http://arxiv.org/abs/1307.0411

[10] M. Kalinin and V. Krundyshev, “Security intrusion detection using quantum machine learning techniques,” *J. Comput. Virol. Hacking Tech.*, vol. 19, no. 1, pp. 125–136, 2023, doi: 10.1007/s11416-022-00435-0.

[11] Y. Du, Y. Yang, D. Tao, and M.-H. Hsieh, “Demystify Problem-Dependent Power of Quantum Neural Networks on Multi-Class Classification,” vol. 1, pp. 1–23, 2022, [Online]. Available: https://arxiv.org/abs/2301.01597

[12] R. D. M. Simoes, P. Huber, N. Meier, N. Smailov, R. M. Fuchslin, and K. Stockinger, “Experimental Evaluation of Quantum Machine Learning Algorithms,” *IEEE Access*, vol. 11, pp. 6197–6208, 2023, doi: 10.1109/ACCESS.2023.3236409.

[13] F. Mercaldo, G. Ciaramella, G. Iadarola, M. Storto, F. Martinelli, and A. Santone, “Towards Explainable Quantum Machine Learning for Mobile Malware Detection and Classification †,” *Appl. Sci.*, vol. 12, no. 23, 2022, doi: 10.3390/app122312025.

[14] M. Alam, S. Kundu, R. O. Topaloglu, and S. Ghosh, “Quantum-Classical Hybrid Machine Learning for Image Classification (ICCAD Special Session Paper),” *IEEE/ACM Int. Conf. Comput. Des. Dig. Tech. Pap. ICCAD*, vol. 2021-Novem, 2021, doi: 10.1109/ICCAD51958.2021.9643516.

[15] S. Kumar, S. Dangwal, and D. Bhowmik, “Supervised Learning Using a Dressed Quantum Network with ‘Super Compressed Encoding’: Algorithm and Quantum-Hardware-Based Implementation,” pp. 1–17, 2020, [Online]. Available: http://arxiv.org/abs/2007.10242

[16] A. EL Azzaoui and J. H. Park, “Post-quantum blockchain for a scalable smart city,” *J. Internet Technol.*, vol. 21, no. 4, pp. 1171–1178, 2020, doi: 10.3966/160792642020072104025.

[17] A. Gouveia and M. Correia, “Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection,” *2020 IEEE 19th Int. Symp. Netw. Comput. Appl. NCA 2020*, 2020, doi: 10.1109/NCA51143.2020.9306691.

[18] T. Suzuki and M. Katouda, “Predicting toxicity by quantum machine learning,” *J. Phys. Commun.*, vol. 4, no. 12, 2020, doi: 10.1088/2399-6528/abd3d8.

[19] A. Tharwat and A. E. Hassanien, “Quantum-Behaved Particle Swarm Optimization for Parameter Optimization of Support Vector Machine,” *J.*

Classif., vol. 36, no. 3, pp. 576–598, 2019, doi: 10.1007/s00357-018-9299-1.

[20] M. Henderson, S. Shakya, S. Pradhan, and T. Cook, "Quanvolutional neural networks: powering image recognition with quantum circuits," *Quantum Mach. Intell.*, vol. 2, no. 1, 2020, doi: 10.1007/s42484-020-00012-y.

[21] E. Farhi and H. Neven, "Classification with Quantum Neural Networks on Near Term Processors," pp. 1–21, 2018, [Online]. Available: http://arxiv.org/abs/1802.06002

[22] E. Grant *et al.*, "Hierarchical quantum classifiers," *npj Quantum Inf.*, vol. 4, no. 1, pp. 1–16, 2018, doi: 10.1038/s41534-018-0116-9.

[23] L. Zhaokai, L. Xiaomei, X. Nanyang, and D. jiangfeng, "Experimental Realization of Quantum Artificial Intelligence," pp. 1–7, 2014, doi: 10.1103/PhysRevLett.114.140504.

[24] W. Aspray, "John von Neumann's Contributions to Computing and Computer Science," *Ann. Hist. Comput.*, vol. 11, no. 3, pp. 189–195, 1989, doi: 10.1109/MAHC.1989.10029.

[25] H. Saputra, "Kajian Tentang Komputer Kuantum Sebagai Pengganti Komputer Konvensional Di Masa Depan," *J. Generic*, vol. 4, no. 2, p. 79256, 2009.

[26] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, and J. M. Leimeister, "Quantum computing," *Electron. Mark.*, vol. 32, no. 4, pp. 2525–2536, 2022, doi: 10.1007/s12525-022-00570-y.

[27] A. Yogiyana, E. T. Hayuningtyas, F. Rifai, O. F. Metatama, and T. Raynaldi, "Teori Parallel Computation Kelas Dosen : Elyna Fazriyati Akhmad Yogiyana Ellana Tria Hayuningtyas Fadly Rifai Oka Fahlan Metatama Priantiko Nur Adi P".

[28] C. Ciliberto *et al.*, "Quantum machine learning: A classical perspective," *Proc. R. Soc. A Math. Phys. Eng. Sci.*, vol. 474, no. 2209, 2018, doi: 10.1098/rspa.2017.0551.

[29] D. P. García, J. Cruz-Benito, and F. J. García-Peñalvo, "Systematic Literature Review: Quantum Machine Learning and its applications," vol.

8329, pp. 0–3, 2022.

[30] L. Chen, “A Brief History of Quantum Computing,” 2023. https://quantumpedia.uk/a-brief-history-of-quantum-computing-e0bbd05893d0

[31] T. A. Napitupulu, “Quantum Computing Made Easy : Bits and Qubits,” pp. 1–4.

[32] M. Vogel, *Quantum Computation and Quantum Information, by M.A. Nielsen and I.L. Chuang*, vol. 52, no. 6. 2011. doi: 10.1080/00107514.2011.587535.

[33] S. S. Gill *et al.*, “Quantum computing: A taxonomy, systematic review and future directions,” *Softw. - Pract. Exp.*, vol. 52, no. 1, pp. 66–114, 2022, doi: 10.1002/spe.3039.

[34] N. Zou, “Quantum Entanglement and Its Application in Quantum Communication,” *J. Phys. Conf. Ser.*, vol. 1827, no. 1, 2021, doi: 10.1088/1742-6596/1827/1/012120.

[35] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement,” *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, 2009, doi: 10.1103/RevModPhys.81.865.

[36] U. Singh, A. K. Pati, and M. N. Bera, “Uncertainty relations for quantum coherence,” *Mathematics*, vol. 4, no. 3, 2016, doi: 10.3390/math4030047.

[37] S. Akama, *of Quantum AND ENGINEERING*. 2014.

[38] Y. S. Kim and M. E. Noz, “Is it possible to construct the proton structure function by lorentz-boosting the static quark-model wave function?,” *Int. J. Mod. Phys. A*, vol. 19, no. 31, pp. 5435–5442, 2004, doi: 10.1142/S0217751X04022682.

[39] M. B. Plenio, “Imperial Quantum Mechanics Course Notes,” p. 172, 2002.

[40] N. Dirac, T. Principles, and Q. Mechanics, “The inner product is the probability amplitude .,” pp. 1–2, 2014.

[41] C. R. Wie, “Two-Qubit Bloch Sphere,” *Phys.*, vol. 2, no. 3, pp. 383–396, 2020, doi: 10.3390/physics2030021.

[42] Frank K. Wilhelm, “Status of quantum computer development,” vol. 34, pp. 45–52, 2020.

[43] E. D. Dahl, “Quantum computing,” *Mach. Des.*, vol. 87, no. 1, pp. 36–41, 2015, doi: 10.1145/3402127.3402131.

[44] J. Watrous, “An introduction to quantum information and quantum circuits,” *ACM SIGACT News*, vol. 42, no. 2, pp. 52–67, 2011.

[45] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[46] C. Douligeris and A. Mitrokotsa, “DDoS attacks and defense mechanisms: A classification,” *Proc. 3rd IEEE Int. Symp. Signal Process. Inf. Technol. ISSPIT 2003*, pp. 190–193, 2003, doi: 10.1109/ISSPIT.2003.1341092.

[47] A. Harris and A. Rahim, “Seleksi Fitur dengan Information Gain untuk Meningkatkan Deteksi Serangan DDoS Menggunakan Random Forest An Information Gain Feature Selection to Improve DDoS Detection using Random Forest,” *Februari*, vol. 19, no. 1, pp. 56–66, 2020.

[48] M. Broughton *et al.*, “TensorFlow Quantum: A Software Framework for Quantum Machine Learning,” pp. 1–56, 2020.

[49] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning,” *Nature*, vol. 549, no. 7671, pp. 195–202, 2017, doi: 10.1038/nature23474.

[50] S. Dey, S. De, and S. Bhattacharyya, “Introduction to quantum machine learning,” *Quantum Mach. Learn.*, vol. 1, pp. 1–10, 2020, doi: 10.1515/9783110670707-001.

[51] P. Altmann, L. Sünkel, J. Stein, T. Müller, C. Roch, and C. Linnhoff-Popien, “SEQUENT: Towards Traceable Quantum Machine Learning Using Sequential Quantum Enhanced Training,” pp. 744–751, 2023, doi: 10.5220/0011772400003393.

[52] F. Vicentini *et al.*, “NetKet 3: Machine Learning Toolbox for Many-Body Quantum Systems,” *SciPost Phys. Codebases*, 2022, doi: 10.21468/scipostphyscodeb.7.

[53] M. Schuld, I. Sinayskiy, and F. Petruccione, “An introduction to quantum machine learning,” *Contemp. Phys.*, vol. 56, no. 2, pp. 172–185, 2015, doi:

10.1080/00107514.2014.964942.

[54] A. Zeguendry, Z. Jarir, and M. Quafafou, “Quantum Machine Learning: A Review and Case Studies,” *Entropy*, vol. 25, no. 2, pp. 1–41, 2023, doi: 10.3390/e25020287.

[55] O. Simeone, “An Introduction to Quantum Machine Learning for Engineers,” *Found. Trends Signal Process.*, vol. 16, no. 1–2, pp. 1–223, 2022, doi: 10.1561/2000000118.

[56] V. Havlíček *et al.*, “Supervised learning with quantum-enhanced feature spaces,” *Nature*, vol. 567, no. 7747, pp. 209–212, 2019, doi: 10.1038/s41586-019-0980-2.

[57] G. Singh, M. Kaur, M. Singh, and Y. Kumar, “Implementation of Quantum Support Vector Machine Algorithm Using a Benchmarking Dataset,” *Indian J. Pure Appl. Phys.*, vol. 60, no. 5, pp. 407–414, 2022, doi: 10.56042/ijpap.v60i5.60456.

[58] B. J. Chelliah, S. Shreyasi, A. Pandey, and K. Singh, “Experimental comparison of quantum and classical support vector machines,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 6, pp. 208–211, 2019.

[59] J. Jäger and R. V. Krems, “Universal expressiveness of variational quantum classifiers and quantum kernels for support vector machines,” *Nat. Commun.*, vol. 14, no. 1, pp. 1–8, 2023, doi: 10.1038/s41467-023-36144-5.

[60] L. Xu *et al.*, “Variational quantum support vector machine based on Hadamard test,” *Commun. Theor. Phys.*, vol. 74, no. 5, 2022, doi: 10.1088/1572-9494/ac6358.

[61] F. Yan and S. E. Venegas-Andraca, “Quantum image processing,” *Quantum Image Process.*, vol. 0, no. 2, pp. 1–171, 2020, doi: 10.1007/978-981-32-9331-1.

[62] D. Anguita, S. Ridella, F. Rivieccio, and R. Zunino, “Quantum optimization for training support vector machines,” *Neural Networks*, vol. 16, no. 5–6, pp. 763–770, 2003, doi: 10.1016/S0893-6080(03)00087-X.

[63] T. Nohara, S. Oyama, and I. Noda, “Pairwise classification using quantum support vector machine with Kronecker kernel,” *Quantum Mach. Intell.*, vol. 4, no. 2, 2022, doi: 10.1007/s42484-022-00082-0.