DOI: 10.5748/19CONTECSI/PSE/SEC/7088

QUANTUM MACHINE LEARNING FOR NETWORK INTRUSION DETECTION SYSTEMS, A SYSTEMATIC LITERATURE REVIEW

APRENDIZADO DE MÁQUINA QUÂNTICO PARA SISTEMAS DE REDE DE DETECÇÃO DE INTRUSÃO, UMA REVISÃO SISTEMÁTICA DA LITERATURA

Vagner Luiz Gava ; https://orcid.org/0000-0001-5965-957X
Instituto de Pesquisas Tecnológicas - IPT

Otavio Kiyatake Nicesio ; https://orcid.org/0000-0002-3975-1261
Instituto de Pesquisas Tecnológicas - IPT

Adriano Galindo Leal ; https://orcid.org/0000-0001-7114-6830
Instituto de Pesquisas Tecnológicas - IPT

QUANTUM MACHINE LEARNING FOR NETWORK INTRUSION DETECTION SYSTEMS, A SYSTEMATIC LITERATURE REVIEW

ABSTRACT

Quantum computing is a potential solution to several problems that classical computing faces such as computational time complexity. Quantum machine learning is therefore expected to have better runtime, capacity, and learning efficiency than classical methods offer. This article aims to present a systematic review of the state-of-the-art literature on quantum machine learning for cybersecurity in the specific application of network intrusion detection systems (IDS), identifying, analyzing, and correlating the different proposals for implementing quantum or hybrid algorithms. The methodology follows the Systematic Literature Review method, which, after its application, identified 5 articles that implemented quantum machine learning algorithms in the context of intrusion detection systems. The main algorithms were variational hybrid quantum-classical, with models based in quantum support vector machines and quantum neural networks. Benefits compared to purely classical models were observed and described, such as improved accuracy of attacking traffic data classification and reduced training time.

Keywords: Cybersecurity; Intrusion Detection System; Quantum Computing; Quantum Machine Learning; Systematic Literature Review.

APRENDIZADO DE MÁQUINA QUÂNTICO PARA SISTEMAS DE REDE DE DETECÇÃO DE INTRUSÃO, UMA REVISÃO SISTEMÁTICA DA LITERATURA

RESUMO

A computação quântica é uma solução potencial para diversos problemas que a computação clássica enfrenta como a complexidade de tempo computacional. Espera-se, portanto, que o aprendizado de máquina quântico apresente tempo de execução, capacidade e eficiência de aprendizado melhores do que os métodos clássicos oferecem. O presente artigo visa a apresentar uma revisão sistemática da literatura do estado da arte em aprendizado de máquina quântico para cibersegurança na aplicação específica de sistemas de detecção de intrusão em redes (IDS), identificando, analisando e correlacionando as diferentes propostas de implementação dos algoritmos quânticos ou híbridos. A metodologia utilizada segue o método de Revisão Sistemática de Literatura, o qual, após sua aplicação, identificou 5 artigos que implementaram algoritmos de aprendizado de máquina quântico no contexto de sistemas de detecção de intrusão. Os principais algoritmos foram clássico-quânticos híbridos variacionais, com um modelo baseado em máquinas de vetores de suporte quânticas e redes neurais quânticas. Os benefícios em comparação aos modelos puramente clássicos foram observados e descritos, como a melhoria na precisão da classificação dos dados de tráfego atacante e tempo de treinamento reduzido.

Palavras-chave: Cibersegurança; Sistema de Detecção de Intrusão; Computação Quântica; Aprendizado de Máquina Quântico; Revisão Sistemática da Literatura.

1. INTRODUÇÃO

Um ataque cibernético é uma tentativa de invadir um sistema computacional com o intuito de interromper, desativar ou obter acesso não autorizado ao computador ou rede de outra pessoa (UNISYS, 2022). De acordo com o relatório da IBM Security (2021), o custo de ataques cibernéticos cresceu nos últimos anos. Em 2018, o cibercrime custou à economia global cerca de 1 trilhão – 50% a mais do que o previsto no mesmo ano, enquanto o custo médio de uma violação de dados aumentou de US$ 3,86 milhões em 2020 para US$ 4,24 milhões em 2021. Segundo Morgan (2020), "espera-se que os custos globais de crimes cibernéticos cresçam 15% ao ano nos próximos cinco anos, chegando a US$ 10,5 trilhões anualmente até 2025".

Deste modo, há uma demanda crescente por soluções nas mais diversas áreas da cibersegurança para mitigar e detectar ataques, sendo a Inteligência Artificial uma possível ferramenta para este fim. Os algoritmos de Machine Learning são utilizados cada vez mais na implementação de Sistemas de Detecção de Intrusão (IDS), segurança de *endpoint* (proteção de dispositivos dos usuários finais, como desktops, laptops e telefones celulares contra a instalação de software malicioso e indesejado), aplicações e identificação de atividade suspeita de usuário (PARISI, 2019).

Um Sistema de Detecção de Intrusão (IDS) é um dispositivo ou aplicação de software que monitora uma rede em busca de atividades maliciosas ou violações de política (BARRACUDA NETWORKS, 2022). Pode ser baseado no hospedeiro, monitorando arquivos e aplicativos acessados ou baseado em rede, analisando o fluxo de informações de uma rede de computadores como pacotes, portas e requisições. Diferente dos Sistemas de Prevenção de Intrusão (IPS), que atuam respondendo às intrusões, o IDS relata a descoberta ao gerenciamento de eventos e informações de segurança (SIEM). O IDS pode ainda ser dividido em assinaturas ou em anomalias. Quando é baseado em anomalias, utiliza aprendizado de máquina para aprender e classificar o comportamento padrão de atividade, para em seguida classificar um novo comportamento (REBELLO et al., 2016).

Na busca por recursos tecnológicos cada vez melhores, a computação quântica aparece como potencial solução para problemas de modo mais rápido e eficiente do que a computação convencional (ou clássica). Um computador quântico utiliza a física quântica para realizar cálculos por meio do estudo do comportamento quântico de partículas como átomos, elétrons e fótons (GARCÍA et al., 2022). Suas vantagens em relação aos computadores clássicos são alcançadas por meio do uso de recursos quânticos como: emaranhamento e superposição de estados.

Enquanto um computador clássico utiliza bits para codificar dados, um computador quântico utiliza qubits. O estado de um bit convencional é determinístico e pode ser somente binário (0 ou 1), mas o estado de um qubit é uma sobreposição (de 0 e 1), o que significa que o qubit armazena uma combinação de dígitos binários, garantindo a um computador quântico uma velocidade de trabalho muito maior do que a de um computador convencional (NIELSEN, 2010). Atualmente, existe um desafio para criar um computador capaz de colocar em prática essas vantagens, tendo em vista que os dispositivos quânticos atualmente disponíveis têm menos de 100 qubits (ABHIJIT et al., 2022). Para que o computador quântico possa resolver problemas relevantes, serão necessários dispositivos com, aproximadamente, 1000 qubits, uma quantidade muito maior do que os computadores atual e os de 100 qubits, que são esperados num futuro próximo (MONROE, 2022).

Uma intersecção entre a computação quântica e a inteligência artificial, o aprendizado de máquina quântico coloca-se como uma das alternativas para a melhoria das ferramentas atuais utilizadas na computação clássica para a detecção e mitigação de ataques cibernéticos. Essa melhoria deve-se ao uso de algoritmos quânticos típicos como o algoritmo

de Shor, de Grover, *eigensolver* quântico variacional (VQE), estimativa de amplitude quântica (QAE), algoritmo quântico de otimização aproximada (QAOA), circuito quântico de profundidade variacional (vVQC), máquinas quânticas de Boltzmann (QBM) e algoritmos de regressão linear para computação quântica (BIAMONTE et al, 2017; PUSHPAK; JAIN, 2019).

As principais tendências para algoritmos de aprendizado de máquina quântico estão relacionadas às redes neurais quânticas como as ortogonais, convolucionais, *feed-forward* ou auto-supervisionadas (GARCÍA et al., 2022). Outras abordagens incluem simulação de cálculos de álgebra linear com amplitudes quânticas, algoritmos de aprendizado de máquina basedos em busca de Grover, recozimento quântico, aprendizado de máquina por reforço quântico-aprimorado, técnicas de amostragem quântica, modelos ocultos quânticos de Markov (HQMM) e os algoritmos puramente quânticos de aprendizado de máquina (PUSHPAK; JAIN, 2019; O'QUINN; MAO, 2020).

Reunindo essas ideias, este artigo tem como objetivo construir uma revisão sistemática de literatura que resuma o estado da arte dos algoritmos e métodos em aprendizado de máquina quântico para aplicações de sistemas de detecção de intrusão na mitigação de ataques cibernéticos. A metodologia utilizada segue o método de revisão sistemática de literatura proposto por Kitchenham e Charters (2007), o qual as etapas e diretrizes foram resumidas por Weidt e Silva (2016).

Desse modo, este estudo responderá à seguinte questão de pesquisa:

Como avaliar a evolução da aplicação dos algoritmos e métodos de aprendizado de máquina quântico para sistemas de mitigação e detecção de ataques cibernéticos aplicados a empresas e universidades relacionadas à área de computação quântica?

O artigo é organizado do seguinte modo: a seção 2 apresenta a fundamentação teórica em aprendizado de máquina quântico. A seção 3 apresenta o protocolo de revisão sistemática, indicando suas etapas. A seção 4 apresenta os resultados e a discussão da revisão sistemática de literatura separando-a por modelos de sistemas de detecção, e a seção 5 apresenta as conclusões.

2. FUNDAMENTAÇÃO TEÓRICA

Na computação clássica, o uso de inteligência artificial em sistemas de detecção de intrusão é baseado na detecção de anomalias em rede (representação na Figura 1), também chamado de sistema de rede de detecção de intrusão, ou NIDS (REBELLO et al., 2016).

Um NIDS desenvolvido usando aprendizado de máquina ou aprendizado profundo geralmente envolve três etapas de implementação:

- ✓ Fase de pré-processamento de dados;
- ✓ Fase de treinamento;
- ✓ Fase de teste.

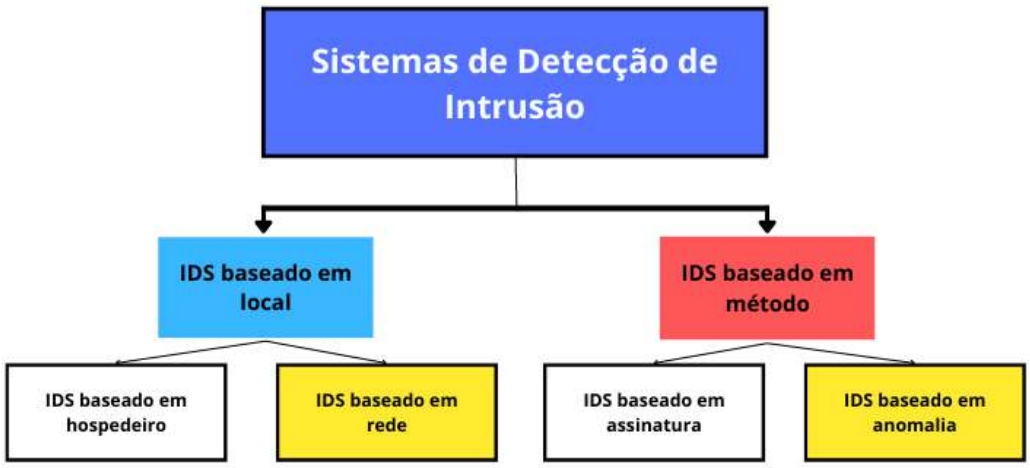

Figura 1 – Em amarelo, as categorias em que o aprendizado de máquina se encaixa na aplicação de sistemas de detecção de intrusão

Fonte: Adaptado de Ahmad et al. (2020)

Na primeira fase, o conjunto de dados é pré-processado para transformá-lo no formato adequado a ser utilizado pelo algoritmo, estágio que envolve codificação e normalização.

Os dados pré-processados são então divididos aleatoriamente em conjunto de dados de treinamento e conjunto de dados de teste numa proporção de 80% para 20% respectivamente (AHMAD et al, 2020).

Em seguida, na segunda fase, o algoritmo é treinado com os dados de treinamento, com tempo de aprendizado dependente do tamanho do conjunto e da complexidade do modelo. No entanto, definir o que é normal não é uma tarefa simples: se durante a fase de aprendizado a rede for vítima de um ataque não detectado, o IDS irá interpretar esse tráfego malicioso como padrão, não acionando nenhum alarme na próxima vez que um ataque similar acontecer (REBELLO et al., 2016).

Por fim, na última fase, o modelo é testado e avaliado com os dados de teste. O IDS deve classificar corretamente o tráfego de rede em classe padrão (normal) ou classe atacante (anômala).

Os algoritmos de aprendizado de máquina mais comuns usados para IDS são árvores de decisão, k-vizinhos mais próximos (KNN), rede neural artificial (ANN), máquinas de vetores de suporte (SVM), agrupamento k-means, redes neurais artificiais rápidas e métodos de ensemble (AHMAD et al., 2020).

A computação quântica utiliza propriedades da física quântica como interferência e sobreposição para realizar operações. Simplificadamente, para obter a solução de diversos problemas, o computador quântico realiza interferência construtiva nas respostas erradas e interferência construtiva na correta, de modo a aumentar a probabilidade de se observar e obter o conjunto solução do problema (NIELSEN, 2010).

Atualmente, a computação quântica está na era NISQ (quantum de escala intermediária com ruído). Ruído quântico ou decoerência quântica é a perda de informação dos estados quânticos por meio de fatores do ambiente como calor, defeitos de material, interferência indesejada de um qubit sobre o outro e flutuações de campo magnético ou elétrico (SAJID et al., 2021).

No Aprendizado de Máquina Quântico, as mesmas fases de implementação do IDS ocorrerão (ZICKERT, 2021). Contudo, os algoritmos adotarão variações, sendo capazes de realizar operações quânticas sobre qubits em um circuito quântico. Essas operações ocorrem

por meio de portas quânticas. Alguns exemplos de portas quânticas típicas são a porta C-NOT, as portas Pauli, a porta Hadamard, a porta de mudança de fase, as portas de rotação etc.

Como o estado de um qubit é um vetor bidimensional em um espaço vetorial complexo, as portas quânticas que atuam neste vetor podem ser representadas como matrizes (NIELSEN, 2010). Nesse caso, o circuito quântico torna-se um conjunto de operações especificas entre matrizes e vetores. Na Figura 2, observa-se o exemplo de algumas portas quânticas e a representação de um qubit na esfera de Bloch, que fornece uma maneira de descrever o estado quântico de um qubit (vetor complexo bidimensional) como um vetor tridimensional de valor real (SAJID et al., 2022).

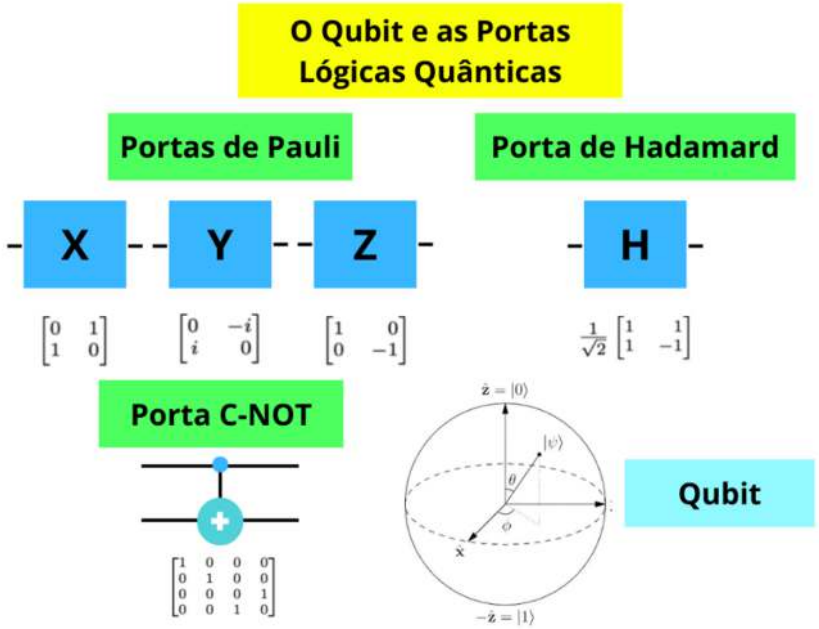

Figura 2 – Na imagem, o qubit é representado por um vetor na Esfera de Bloch, e alguns exemplos de portas lógicas são representadas por matrizes

Fonte: Elaborado pelos autores

Os qubits mantêm informações úteis por períodos muito curtos, já que são propensos a erros advindos do ruído. É possível mitigar essa instabilidade por meio da correção de erros, mas seria necessário atingir algo em torno de 1000 qubits "físicos" para isso. Os qubits físicos são implementações físicas que se comportam como um sistema quântico de dois estados, usados como componente do computador quântico. Normalmente é nesta categoria que se enquadra o número de qubits dos computadores divulgados pelos fabricantes. Ao atingir esse valor aproximado de 1000 qubits, a correção funcionaria de modo efetivo, criando um qubit "lógico". Um qubit lógico é um qubit físico ou abstrato que funciona conforme programado em um algoritmo ou circuito quântico (GREENGARD, 2021).

Em geral, a computação quântica difere-se da clássica pela diminuição da complexidade de tempo (ZICKERT, 2021) dos algoritmos. Tarefas com complexidade de tempo superpolinomial no computador clássico podem levar complexidade de tempo polinomial no computador quântico, vide algoritmo de Shor (SAJID et al., 2021). Essa melhoria é chamada de aceleração quântica e pode ser vista, por exemplo, nos algoritmos clássicos de aprendizado de máquina, que possuem operações básicas de álgebra linear (transformadas de Fourier, encontrar autovetores e autovalores, resolver equações lineares): a versão quântica dessas sub-rotinas apresentam aceleração quântica (BIAMONTE, 2017).

Existem quatro categorias de abordagem na junção de aprendizado de máquina e computação quântica:

- ✓ Dados Clássicos em Algoritmos Quânticos
- ✓ Dados Clássicos em Algoritmos Clássicos
- ✓ Dados Quânticos em Algoritmos Quânticos
- ✓ Dados Quânticos em Algoritmos Clássicos

Nesse contexto, dados quânticos são observações de um sistema quântico natural ou artificial, como medições das interações entre os qubits. Em outras palavras, são estados quânticos gerados por um processo quântico genérico, que pode ser outro circuito quântico, por exemplo. Dados clássicos consistem em observações de um sistema clássico como textos, imagens ou séries temporais (SAJID et al., 2021).

O foco de pesquisa mais recente para o aprendizado de máquina está na categoria de dados clássicos em algoritmos quânticos (SAJID et al., 2021). Uma abordagem que se enquadra nessa categoria é o Algoritmo Quântico-Clássico Híbrido Variacional. Este algoritmo é dividido em três fases: pré-processamento e pós-processamento em um computador clássico, e o processamento num circuito quântico. O pré-processamento consiste em codificar dados no domínio clássico em representações no domínio quântico (vetores de estados quânticos dos qubits). Em seguida, os dados são processados pelo circuito quântico e, no pós-processamento, são realizadas as medidas para as previsões do modelo de aprendizado (ZICKERT, 2021).

Um modelo de algoritmo quântico-clássico híbrido variacional pode ser visto na Figura 3.

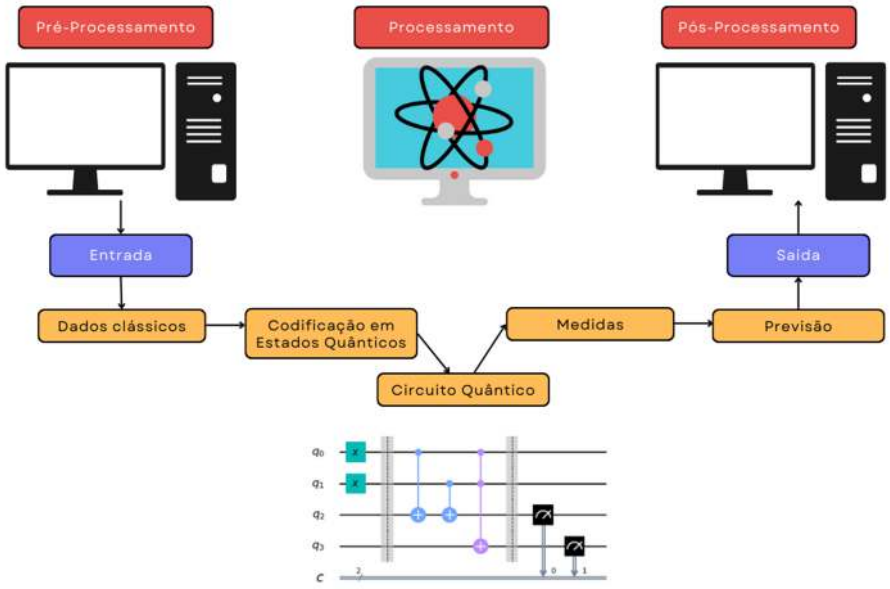

Figura 3 – O pré-processamento e o pós-processamento, ou seja, o tratamento dos dados e a previsão de classificação em si são realizadas num computador clássico, enquanto o processamento ocorre no circuito quântico-clássico variacional que contém o algoritmo.
Fonte: Elaborado pelos autores

3. MÉTODO

O estudo realizado neste artigo é baseado na metodologia de Revisão Sistemática da Literatura (SLR) apresentada no relatório técnico de Kitchenham e Charters (2007). Suas

principais diretrizes foram resumidas por Weidt e Silva (2016) e implementadas neste artigo. Essa metodologia divide o trabalho em três fases: fase de planejamento, fase de condução e, por último, fase de síntese.

O gerenciador de protocolo de revisão sistemática utilizado neste trabalho foi o Parsifal (https://parsif.al/), enquanto o gerenciador de referências bibliográficas foi o JabRef (https://www.jabref.org/). A geração de planilhas para documentação da revisão foi realizada pelo Microsoft Excel (https://www.microsoft.com/pt-br/microsoft-365/excel). E para a definição das strings finais de busca e de suas palavras-chaves, foi utilizado o software de bibliometria "VOSViewer" (https://www.vosviewer.com/), visando a melhorar os resultados da revisão sistemática por meio de co-ocorrência de palavras-chaves repetidas ao menos quatro vezes dentre todos os artigos obtidos na busca inicial.

3.1. Planejamento da Revisão Sistemática da Literatura

A fase de planejamento foi dividida em doze etapas, abrangendo desde o objetivo da pesquisa até as estratégias de análise utilizadas para publicação dos dados. As etapas estão descritas a seguir.

Objetivo da Pesquisa:

Construir uma revisão sistemática de literatura que resuma o estado da arte dos algoritmos e métodos em aprendizado de máquina quântico para aplicações de sistemas de detecção de intrusão na mitigação de ataques cibernéticos.

Questão de Pesquisa:

Como avaliar a evolução da aplicação dos algoritmos e métodos de aprendizado de máquina quântico para sistemas de mitigação e detecção de ataques cibernéticos aplicados a empresas e universidades relacionadas à área de computação quântica?

A questão de pesquisa foi decomposta utilizando a estratégia PICO de Petticrew e Roberts (2005). PICO representa um acrônimo para Population, Intervention, Comparison e Outcome.

População (P): empresas, universidades relacionadas à área de computação quântica em aplicações de sistemas de detecção de intrusão.

Intervenção (I): abordagens, técnicas e métodos para implementação de sistemas de detecção de intrusão que utilizem aprendizado de máquina quântico.

Controle (C): lista de referências obtida por meio de pesquisa exploratória do tema, servindo de base para a escolha das palavras chaves e fontes:

- ✓ Biamonte et al. (2017)
- ✓ García et al. (2022)
- ✓ Parisi (2019)

Resultados (O): uma avaliação do estado da arte dos sistemas de detecção de intrusão que utilizam aprendizado de máquina quântico.

Critérios de Seleção das Bases de Busca:

As bases utilizadas foram escolhidas devido ao seu reconhecimento mundial e por incluírem os principais artigos, revistas e eventos científicos em computação quântica e inteligência artificial (Quadro 1).

Lista das Bases de Busca:

Fonte de Busca	Endereço Online
ACM *Digital Library*	https://dl.acm.org/
IEEE *Xplore*	https://ieeexplore.ieee.org/
Scopus *Digital Library*	http://www.scopus.com/
ISI Web of Science	http://www.webofscience.com/

Quadro 1 – Bases de Busca utilizadas na Revisão Sistemática de Literatura
Fonte: Elaborado pelos autores

Strings de Busca:

A base Scopus e o VOSViewer foram utilizados nesta etapa para melhoria da string de busca. A busca nas bases durante esta etapa ocorreu em outubro de 2022. A única adaptação na string foi utilizada na base ACM, por não haver suporte às palavras-chaves com meta-caracteres introduzidas em aspas. Foi utilizado dois modos diferentes de escrita da palavra cibersegurança, das variantes de inglês americano e britânico. Visto que sistemas de detecção de intrusão para aplicação de inteligência artificial em cibersegurança e computação quântica é uma área que ainda está em fase embrionária de desenvolvimento, a string procurou abranger o maior número de artigos possíveis, sendo definida por:

IEEE, Web of Science e Scopus: (“cybersecurity” OR “cyber-security” OR “attack*” OR “intrusion detection”) AND (“quantum artificial intelligence” OR “quantum machine learning” OR “quantum neural network*” OR “quantum deep learning”)

ACM: (“cybersecurity” OR “cyber-security” OR “attack” OR “intrusion detection”) AND (“quantum artificial intelligence” OR “quantum machine learning” OR “quantum neural networks” OR “quantum deep learning”)

Critérios de Inclusão de Estudos:

A1) Estudos que apresentam exploração de sistemas para detecção ou mitigação de ataques cibernéticos utilizando aprendizado de máquina quântico;

A2) Estudos que apresentam as possíveis ameaças ou vulnerabilidades as quais estes métodos podem ser utilizados.

Critérios de Exclusão de Estudos:

E1) Estudos em outras línguas além de inglês;

E2) Estudos que não estão relacionados com Segurança da Informação;

E3) Estudos que não estão relacionados com Aprendizado de Máquina Quântico;

E4) Estudos não focados na implementação de um Sistemas de Detecção de Intrusão usando Aprendizado de Máquina Quântico;

E5) Estudos duplicados;

E6) Estudo não disponível na íntegra via CAFe (Comunidade Acadêmica Federada).

Estratégia de busca para a identificação dos artigos:

A aplicação da string nas bases de dados escolhidas ocorreu por método de pesquisa automático para todos os metadados (título, resumo e palavras-chaves). A única restrição utilizada foi o período de publicação: 2017-2022.

Estratégia para seleção dos trabalhos:

Os metadados (título, resumo e palavras-chaves) de todos os trabalhos obtidos foram importados para o JabRef, visando à organização e a documentação em planilhas específicas para cada fonte de busca na ferramenta Excel. Após a exportação dos metadados em arquivo de formato BibTeX, foram realizadas sucessivas avaliações de todos os trabalhos.

As avaliações foram realizadas em 3 fases com o uso das ferramentas Parsifal e Microsoft Excel.

1ª Fase: Leitura dos títulos, resumos e palavras-chaves dos artigos identificados pela busca inicial nas bases selecionadas. Nesta fase também foi feita a remoção automática dos artigos duplicados no Parsifal. Gerou-se uma planilha no Microsoft Excel indicando os critérios de inclusão e exclusão aplicados em cada estudo. Os artigos incluídos foram documentados numa nova planilha para a segunda fase de avaliação.

2ª Fase: Leitura da introdução e da conclusão dos artigos incluídos na 1ª Fase. Gerou-se uma nova planilha, e os artigos incluídos foram documentados para a terceira fase de avaliação.

3ª Fase: Leitura completa dos artigos incluídos na 2ª Fase. Após a aplicação dos critérios, uma planilha final foi gerada com os artigos incluídos na Síntese da Revisão Sistemática de Literatura.

Estratégia de extração e síntese dos dados:

a) Descrição do tipo de pré-processamento e codificação realizados nos dados clássicos;
b) Modelos de aprendizado de máquina quântico utilizados na implementação do sistema;
c) Descrição dos resultados e conclusões de cada modelo implementado.
d) Comparação do sistema de detecção de intrusão de modelo quântico com o modelo clássico;
e) Resumo dos estudos em função dos dados extraídos.

Estratégia de análise dos dados para publicação dos resultados:

a) Resumo comparativo entre os modelos de IDS utilizados nos estudos;
b) Como os dados obtidos ajudam a responder à pergunta de pesquisa.

4. RESULTADOS

4.1. Condução da Revisão Sistemática de Literatura

A revisão sistemática foi conduzida durante os meses de setembro e outubro de 2022. Na Figura 4, é apresentado o resumo da avaliação indicando cada fase.

No total, utilizando as bases escolhidas, foram encontrados e avaliados 239 trabalhos (152 da base IEEE, 39 da base Scopus, 20 da base ACM Library e 18 da base Web of Science). Em todas as fases, foram aplicados os critérios de inclusão e exclusão após a leitura das seções do artigo previamente indicadas.

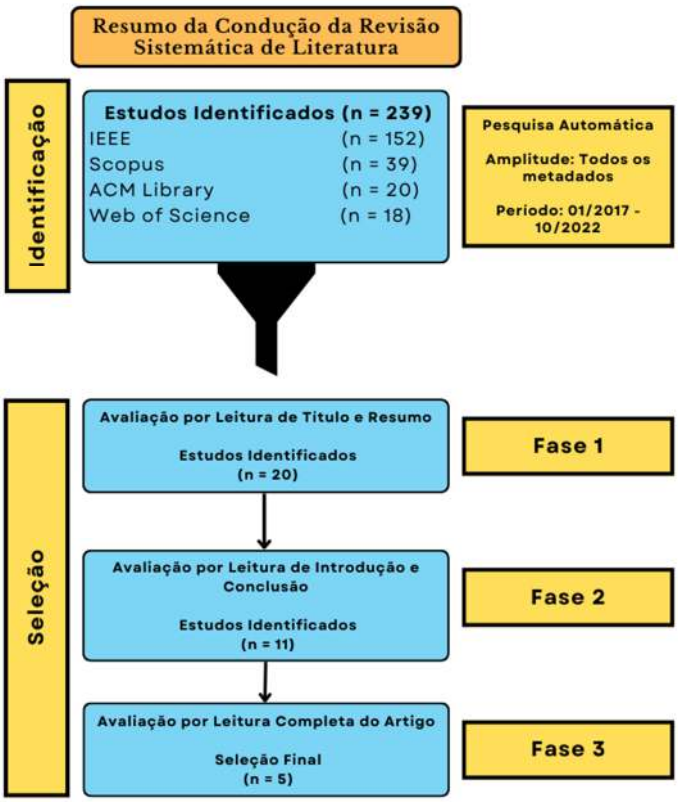

Figura 4 – Trabalhos Selecionados na Síntese da Revisão Sistemática
Fonte: Elaborado pelos autores

O resultado da Condução está representado na Quadro 2. A planilha completa com as informações dos artigos revisados e os critérios de inclusão e exclusão utilizados em cada fase foi disponibilizada na nuvem. Para acessar esse e outros dados referentes a este artigo, basta navegar pelo repositório disponível on-line via link (https://github.com/Kiyatake1/Quantum-Machine-Learning-for-Network-Intrusion-Detection-Systems-A-Systematic-Literature-Review).

#	Título	Autor	Ano	Critério de Seleção	Status
1	Quantum machine learning for intrusion detection of distributed denial of service attacks: A comparative overview	Payares, E.D. and Martinez-Santos, J.C.	2021	A1	Aceito
2	Security intrusion detection using quantum machine learning techniques	Kalinin, M. and Krundyshev, V.	2022	A1	Aceito
3	Network Attack Traffic Recognition Based on Quantum Neural Network	Zhang, M. and Lv, B. and Liu, Z.-S.	2022	A2	Aceito
4	Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection	Gouveia, Arnaldo and Correia, Miguel	2020	A1	Aceito
5	Network attack detection scheme based on variational quantum neural network	Gong, Changqing and Guan, Weiqi and Gani, Abdullah and Qi, Han	2022	A1	Aceito

Quadro 2 – Seleção Final de Artigos da Condução da Revisão Sistemática (a versão completa com fases anteriores está disponibilizada on-line)
Fonte: Elaborado pelos autores

4.2. Síntese da Revisão Sistemática de Literatura

Após a leitura minuciosa e completa dos trabalhos incluídos após a terceira avaliação, foi elaborado, na síntese da revisão sistemática, um resumo dos sistemas de detecção de intrusão implementados em cada estudo, conforme pode ser visto no Quadro 3. Como cada método se interrelaciona e como atuam comparativamente foi abordado na análise dos

resultados. Os dados reunidos neste estudo foram organizados para responder à questão de pesquisa.

Artigo	Síntese	Campos de Extração
Quantum machine learning for intrusion detection of distributed denial of service attacks: A comparative overview	Apresenta três modelos quânticos-clássicos para detectar ataques distribuídos de negação de serviço (DDoS).	**Codificção dos Dados Clássicos para o Modelo Quântico de IDS:** utilizou o método de incorporação de ângulos, que consiste em codificar um conjunto de N atributos nos ângulos de rotação de n qubits, onde N ≤ n, usando a Porta Rx que é um dos Operadores de Rotação.
		Modelo de Aprendizado de Máquina Quântico: máquinas de vetores de suporte quânticas, redes neurais clássicas-quânticas híbridas e um modelo ensemble que une dois circuitos em paralelo para duas unidades de processamento quântico.
		Conclusão e Resultados do Estudo: o modelo que mais usou recursos computacionais foi o de máquinas de vetores de suporte. O mais eficiente foi o de método ensemble. E o de melhor acurácia em proporção à eficiência foi o de redes neurais híbridas.
		Comparação com o modelo clássico de IDS: houve uma melhora significativa em relação aos estudos da abordagem clássica. Trabalhos futuros podem usar dados mais complexos e um conjunto de dados maior para aumentar a confiabilidade dos resultados.

Artigo	Síntese	Campos de Extração
Security intrusion detection using quantum machine learning techniques	Apresenta métodos de aprendizado de máquina quântica (QML) visando superar as barreiras da big data e das habilidades de computação de hardware comum para fins de detecção de intrusão de alto desempenho. Desenvolve uma solução de software que codifica os fluxos de tráfego de rede para computação quântica.	**Codificção dos Dados Clássicos para o Modelo Quântico de IDS:** usa uma solução própria que, primeiro, traduz um endereço IP num ângulo de rotação. Adiciona ao circuito uma porta Pauli com o ângulo de rotação encontrado. Por fim, adiciona este esquema resultante aos dados de treinamento.
		Modelo de Aprendizado de Máquina Quântico: máquinas de vetores de suporte quânticas (QSVM) e redes neurais quânticas convolucionais (QCNN).
		Conclusão e Resultados do Estudo: Comparando o IDS baseado em QSVM e QCNN, o QCNN é mais promissor, apesar do QSVM ser mais rápido, pois permite selecionar as atributos mais significativas com maior probabilidade, o que reduz a complexidade do método.
		Comparação com o modelo clássico de IDS: Em grandes conjuntos de dados de fluxo a abordagem quântica mostrou superioridade significativa (a precisão da classificação QSVM e QCNN é de 98%). O tempo de treinamento foi reduzido em mais de duas vezes.

Artigo	Síntese	Campos de Extração
Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection	Apresenta uma abordagem para aplicação de Aprendizado de Máquina Quântico não supervisionado no contexto de detecção de intrusão de rede.	**Codificção dos Dados Clássicos para o Modelo Quântico de IDS:** implementação baseada na função autoencode() fornecida pelo pacote Ruta do pacote de computação estatística R.
		Modelo de Aprendizado de Máquina Quântico: máquinas de vetores de suporte quânticas (QSVM).
		Conclusão e Resultados do Estudo: O modelo apresenta acurácia muito próxima da abordagem clássica, sendo necessário maior estudo para identificar aceleração quântica.
		Comparação com o modelo clássico de IDS: Os valores de desempenho mostram que a abordagem é viável e pode permitir que os NISDs se beneficiem do modelo. No entanto, há necessidade de similaridade estatística entre o conjunto de dados de teste e de treinamento.

Artigo	Síntese	Campos de Extração
Network Attack Traffic Recognition Based on Quantum Neural Network	Apresenta um método de reconhecimento de tráfego de ataque de rede baseado em rede neural quântica e cria seu próprio método de codificar dados clássicos em quânticos.	**Codificção dos Dados Clássicos para o Modelo Quântico de IDS:** primeiro, cada atributo clássico j é normalizado por decimais entre 0 e 1. Em seguida, cada atributo é definido por um conjunto de K qubits. O primeiro qubit é o valor inteiro do atributo, enquanto os outros K-1 qubits são os valores das casas decimais.
		Modelo de Aprendizado de Máquina Quântico: redes neurais quânticas (QNN).
		Conclusão e Resultados do Estudo: O modelo apresenta alta taxa de reconhecimento correto do tráfego benigno, mas taxa de 71% para o tráfego de ataque, devido a poucos qubits disponíveis, o que binarizou dados de atributos originais com perda de informações.
		Comparação com o modelo clássico de IDS: A vantagem da rede neural quântica é que sua função gradiente é limitada, evitando o problema de explosão de gradiente na rede neural de aprendizado profundo, tornando a rede otimizada mais estável e eficiente.

Artigo	Síntese	Campos de Extração
Network attack detection scheme based on variational quantum neural network	Propõe um esquema de detecção de intrusão baseado em VQNN, composto por um circuito quântico variacional (VQC) e uma estratégia clássica de aprendizado de máquina (ML). O sistema foi testado na plataforma em nuvem de computação quântica da IBM.	**Codificção dos Dados Clássicos para o Modelo Quântico de IDS:** utiliza uma codificação de estado quântico pelo método de amplitude e pelo método variacional.
		Modelo de Aprendizado de Máquina Quântico: redes neurais variacionais quânticas (VQNN).
		Conclusão e Resultados do Estudo: apesar da melhoria em relação à abordagem clássica, os resultados do VQNN em circuitos quânticos reais não são completamente satisfatórios. A principal razão é a falta de suporte à correção de erro nos equipamentos NISQ.
		Comparação com o modelo clássico de IDS: O modelo de IDS proposto tem uma precisão de 97,21%, superior a outros modelos clássicos de IDS.

Quadro 3 – Síntese dos artigos em função dos campos de extração
Fonte: Elaborado pelos autores

4.3. Análise dos Resultados

Nota-se, primeiramente, que o número de artigos encontrados nas bases, utilizando palavras-chaves gerais revela que o tema ainda está em fase inicial de desenvolvimento, apresentando assim escassez literária. Isso é visto também na lista de resultados, dado que todos os artigos foram publicados após 2020. Este resultado é esperado, visto que a computação quântica ainda está na era NISQ (quantum de escala intermediaria com ruído), com computadores ainda não disponíveis comercialmente e capaz de poucas aplicações práticas devido ao ruído (BIAMONTE, 2017).

Um tópico que engloba esta área com outras duas tão especificas como aprendizado de máquina e sistemas de detecção de intrusão apresentará uma produção literária ainda menor. A tendência é o tema evoluir com o crescimento em número de qubits e a diminuição no ruído dos dispositivos quânticos. Ainda neste âmbito, o estudo de Gong et al. (2022) indica que a atenuação do ruído é primordial para qualquer aplicação de IDS com respeito ao aprendizado de máquina quântico, pois qualquer melhoria prevista desses modelos, seja em complexidade de tempo, acurácia ou eficiência computacional só será concretizada num computador quântico dada essa condição.

Os cinco artigos encontrados apresentam, em geral, métodos semelhantes de implementação para o Sistema de Detecção de Intrusão, visto que utilizam a estrutura típica da construção de um modelo clássico-quântico híbrido variacional. O pré-processamento pode ser feito de maneiras distintas, mas todas abordam normalização e uma correção de erro nos conjuntos de dados de treinamento, seguida da codificação quântica. A codificação seguiu abordagens similares nos estudos de Payares e Martinez-Santos (2021), Kalinin e Krundyshev (2022) e Zhang et al. (2022).

A tendência dos algoritmos de aprendizado de máquina quântico implementados apresenta uma forte inclinação para máquinas de vetores de suporte quânticas (QSVM) e redes neurais quânticas em geral (QNN). Um resultado interessante pode ser visto em Payares e Martinez-Santos (2021), que utiliza método ensemble com duas unidades de

processamento quântico no circuito apresentando maior eficiência no uso de recursos computacionais, apesar de não ser o modelo mais acurado em seu estudo comparativo.

Além do ruído, outro problema da era NISQ é o número de qubits limitado, descrito em Zhang et al. (2020), que acaba por limitar também os atributos incorporados nos qubits. Tanto esse estudo, quanto Gong et al. (2022), se beneficiariam de um computador quântico com propriedades superiores aos da era atual.

Quanto à comparação com a abordagem clássica dos modelos de IDS que usam aprendizado de máquina, nos cinco estudos houve uma melhoria significativa, apresentando viabilidade, conforme Gouveia e Correia (2020), e até mesmo correção de alguns problemas dos algoritmos clássicos, como visto na explosão de gradiente das redes neurais em Zhang et al. (2020). Em geral, as redes neurais quânticas apresentam maior potencial por conta da proporção entre acurácia e demanda de recursos, enquanto as máquinas de vetores de suporte quânticas têm menor tempo de complexidade, porém demandam mais recursos.

5. CONCLUSÕES

A seguinte questão de pesquisa foi realizada:

Como avaliar a evolução da aplicação dos algoritmos e métodos de aprendizado de máquina quântico para sistemas de mitigação e detecção de ataques cibernéticos aplicados a empresas e universidades relacionadas à área de computação quântica?

Considerando o estudo desse artigo, é possível criar um método para avaliar a evolução das diferentes implementações de IDS com aprendizado de máquina quântico ao dividir suas metodologias em fases de pré-processamento, processamento e pós-processamento, indicando o modelo e os algoritmos aplicados, sejam híbridos ou não.

A codificação, a normalização e o trabalho de correção feito sobre os dados clássicos devem estar indicados nos estudos para a avaliação. Os resultados de cada estudo, tal como a comparação com os modelos clássicos de IDS entram na fase de pós-processamento. O processamento é composto por um circuito quântico indicado nas pesquisas. É possível então para uma empresa ou universidade observar essas avaliações de diferentes metodologias e resultados para, com facilidade, citá-las ou continuá-las em trabalhos futuros, sejam eles comerciais ou acadêmicos.

Além dessas informações, também é possível adicionar à avaliação o contexto temporal em que as metodologias ocorreram. No caso deste presente trabalho, na era NISQ, gerando assim discussão e correlação entre as técnicas de implementação do estado da arte e as possíveis melhorias das tecnologias quânticas futuras, pois uma evolução do hardware quântico também apoiará as melhorias das aplicações.

A revisão sistemática avaliou aplicações do aprendizado de máquina quântico em sistemas de detecção de intrusão na era NISQ. Espera-se, com estas avaliações, contribuir para futuras pesquisas no aprimoramento tanto das técnicas de aprendizado de máquina quântico, quanto das aplicações em cibersegurança nesta e em futuras gerações de computadores quânticos.

A pesquisa limitou-se a avaliar as características gerais das implementações dos modelos de IDS, como o tipo de pré-processamento, o algoritmo utilizado e a sua melhoria em relação à computação clássica, excluindo artigos que focavam em outras propriedades desses modelos já implementados ou que não necessariamente focassem na aplicação de IDS.

Para trabalhos futuros, sugere-se detalhar o processamento e os circuitos quânticos de cada modelo, evidenciando seu funcionamento e suas sub-rotinas quânticas nos sistemas de detecção de intrusão.

REFERÊNCIA BIBLIOGRÁFICA

AHMAD, Zeeshan et al. Network intrusion detection system: a systematic study of machine learning and deep learning approaches. **Transactions On Emerging Telecommunications Technologies**, [S.L.], v. 32, n. 1, p. 1-29, 16 out. 2020. Wiley. http://dx.doi.org/10.1002/ett.4150.

ABHIJIT, J. *et al*. Quantum Algorithm Implementations for Beginners. **ACM Transactions on Quantum Computing.** Nova York, p. 1-92. dez. 2022.

Barracuda Networks (USA) (ed.). **What is an Intrusion Detection System?** 2022. Disponível em: https://www.barracuda.com/glossary/intrusion-detection-system. Acesso em: 08 out. 2022.

BIAMONTE, Jacob *et al*. Quantum machine learning. **Nature**, [S.L.], v. 549, n. 7671, p. 195-202, set. 2017. Springer Science and Business Media LLC. http://dx.doi.org/10.1038/nature23474.

GARCÍA, David Peral; CRUZ-BENITO, Juan; GARCÍA-PEÑALVO, Francisco José. Systematic literature review: Quantum machine learning and its applications, **arXiv preprint arXiv:2201.04093** (2022).

GREENGARD, Samuel. Qubit devices inch toward reality. **Communications Of The ACM**, [S.L.], v. 64, n. 11, p. 11-13, nov. 2021. Association for Computing Machinery (ACM). http://dx.doi.org/10.1145/3484988.

GONG, Changqing et al. Network attack detection scheme based on variational quantum neural network. **The Journal of Supercomputing**, [S.L.], v. 78, n. 15, p. 16876-16897, 11 Maio 2022. Springer Science and Business Media LLC. http://dx.doi.org/10.1007/s11227-022-04542-z.

GOUVEIA, Arnaldo; CORREIA, Miguel. Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection. In: 2020 IEEE 19TH INTERNATIONAL SYMPOSIUM ON NETWORK COMPUTING AND APPLICATIONS (NCA), 19., 2020, Cambridge. **Conference Proceedings [...].** [S.L.]: IEEE, 2020. p. 1-8.

IBM Security (USA) (ed.). **Cyber Resilient Organization Study**. 2021. Disponível em: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/. Acesso em: 18 jul. 2022.

KALININ, Maxim; KRUNDYSHEV, Vasiliy. Security intrusion detection using quantum machine learning techniques. **Journal Of Computer Virology and Hacking Techniques.** [S.I], p. 1-12. 24 jun. 2022.

KITCHENHAM, Barbara; CHARTERS, Stuart. **Guidelines for performing Systematic Literature Reviews in Software Engineering (version 2.3)**. Keele, UK: Keele University, 2007.

MONROE, Don. Building a practical quantum computer. **Communications Of The ACM**, [S.L.], v. 65, n. 7, p. 15-17, Jul. 2022. Association for Computing Machinery (ACM). http://dx.doi.org/10.1145/3535191.

MORGAN, Steve (ed.). **Cybercrime to cost the world $10.5 Trillion annually by 2025**. 2020. Pesquisa elaborada por Cybersecurity Ventures. Disponível em: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/. Acesso em: 18 jul. 2022.

NIELSEN, Michael. **Quantum computation and quantum information**. 10. ed. Nova York: Cambridge University Press, 2010. 708 p.

O'QUINN, Wesley; MAO, Shiwen. Quantum Machine Learning: Recent Advances and Outlook. **IEEE Wireless Communications.** Piscataway, NJ, p. 126-131. jun. 2020.

PARISI, Alessandro *et al*. **Hands-On Artificial Intelligence for Cybersecurity**. Birmingham, UK: Packt Publishing Ltd., 2019.

PAYARES, Esteban; MARTINEZ-SANTOS, Juan Carlos. "Quantum machine learning for intrusion detection of distributed denial of service attacks: a comparative overview. In: QUANTUM COMPUTING, COMMUNICATION, AND SIMULATION, 1., 2021, California. **Proc. SPIE 11699.** [S.L.]: SPIE, 2021. p. 1-11.

PUSHPAK, Subodh Nath; JAIN, Sarika. An Introduction to Quantum Machine Learning Techniques. In: INTERNATIONAL CONFERENCE ON RELIABILITY, INFOCOM TECHNOLOGIES AND OPTIMIZATION (TRENDS AND FUTURE DIRECTIONS) (ICRITO), 9., 2021, Noida, India. **Proceedings of 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).** [S.L.]: IEEE, 2021. p. 1-6.

REBELLO, Gabriel *et al*. **Sistemas de Detecção de Intrusão**. 2016. Pesquisa elaborada pela Universidade Federal do Rio de Janeiro – UFRJ. Disponível em: https://www.gta.ufrj.br/grad/16_2/2016IDS/index.html. Acesso em: 08 out. 2022.

SAJID, Anis *et al*. **Qiskit: An Open-source Framework for Quantum Computing**. 2021. Disponível em: https://qiskit.org/. Acesso em: 28 set. 2022

Unisys Corporation (USA). **Cyber Attacks - What you need to know**. 2022. Disponível em: https://www.unisys.com/glossary/cyber-attack/. Acesso em: 18 jul. 2022

WEIDT, Frâncila; SILVA, Rodrigo Luis de Souza da. **Systematic Literature Review in Computer Science - A Practical Guide**. Juiz de Fora: Federal University Of Juiz de Fora, 2016.

ZICKERT, Frank. **Hands-on Quantum Machine Learning with Python**. 1. ed. [S.L]: PyQML, 2021. 435 p.

ZHANG, Meng *et al*. Network Attack Traffic Recognition Based on Quantum Neural Network. **7th International Conference on Computational Intelligence and Applications (ICCIA)**. Piscataway, NJ, p. 71-75. jun. 2022.