Detecção de Ransomware: Uma abordagem por Aprendizado de Máquina Quântico

Diego Abreu, Alan Veloso, Antônio Abelém

***Resumo*—Os ataques ransomware representam uma ameaça significativa a indivíduos e organizações ao criptografar dados e exigir um resgate para sua liberação. Detectar esses ataques de forma rápida é fundamental para mitigar seu impacto e evitar perdas de dados ou prejuízos financeiros. Abordagens tradicionais de detecção de ransomware frequentemente dependem de sistemas baseados em regras ou análise estatística, que podem ter dificuldades em acompanhar a natureza em constante evolução dos ataques ransomware. Neste artigo, propomos uma abordagem para a detecção de ransomware utilizando Aprendizado de Máquina Quântico. Ao aproveitar as propriedades únicas da computação quântica, buscamos aprimorar a precisão e eficiência na detecção de ransomware em comparação com abordagens clássicas de Aprendizado de Máquina. Nossos resultados experimentais demonstram que o modelo de Aprendizado de Máquina Quântico alcança uma precisão e acurácia superiores quando comparado com classificadores clássicos na detecção de ataques ransomware.**

***Index Terms*—Ransomware, Quantum Machine Learning**

I. Introdução

No campo do Aprendizado de Máquina (*Machine Learning* - ML), técnicas tradicionais têm sido amplamente utilizadas para a detecção de ataques de rede [1], [2]. No entanto, com a crescente complexidade e sofisticação de ataques ransomware, surge a necessidade de abordagens mais avançadas que possam lidar com os desafios impostos pela natureza em constante evolução dessas ameaças. Nesse contexto, o Aprendizado de Máquina Quântico (*Quantum Machine Learning* - QML) surge como uma promissora alternativa [3], explorando as propriedades únicas da computação quântica para melhorar a precisão e eficiência na detecção de ransomware.

O objetivo deste trabalho é investigar e explorar o potencial do QML para a detecção de ataques ransomware. Nossa abordagem proposta envolve a utilização de algoritmos de QML e a comparação de seu desempenho com classificadores clássicos (não quânticos) amplamente utilizados. Ao superar as limitações das abordagens clássicas, espera-se alcançar resultados superiores em termos de acurácia, precisão e eficácia geral na detecção de ransomware.

II. Estudo de Caso

A QML combina princípios da Computação Quântica (*Quantum Computing* - QC) e ML para desenvolver algoritmos e técnicas inovadoras para análise de dados e reconhecimento de padrões [3]. Na QC, a superposição permite que os qubits (bits quânticos) estejam em múltiplos estados simultaneamente, ampliando as possibilidades computacionais. O emaranhamento quântico, por sua vez, conecta os estados de múltiplos qubits, possibilitando correlações entre os estados. Aproveitando a superposição e o emaranhamento, a QML aprimora algoritmos de Aprendizagem de Máquina clássicos (não quânticos), abordando problemas computacionais complexos de maneira mais eficiente.

O Classificador Quântico Variacional (*Variational Quantum Classifer* - VQC) [4] é um algoritmo de QML que combina circuitos quânticos com técnicas clássicas de otimização para realizar tarefas de classificação. O VQC explora e compara diferenças entre estados quânticos, que dependem de um conjunto de parâmetros. Esses estados podem ser preparados usando um circuito quântico parametrizado, onde portas quânticas são definidas com parâmetros ajustáveis. O VQC utiliza um circuito quântico, que pode ser otimizado com base nos dados de treinamento para aprender o limite de decisão ótimo entre diferentes classes.

No VQC, primeiramente, os dados de entrada são codificados em estados quânticos usando um mapa de características quânticas. O circuito variacional age então nesses estados codificados, realizando computações e transformações que dependem dos parâmetros ajustáveis. Essas computações envolvem a aplicação de portas quânticas, como operações de rotação e emaranhamento, para manipular o estado quântico e extrair informações relevantes. O otimizador clássico modifica os parâmetros ajustáveis do circuito variacional iterativamente, buscando minimizar uma função de custo ou perda predefinida. Esse processo de otimização visa encontrar a configuração ideal do circuito variacional que melhor corresponda ao objetivo de classificação desejado [4].

A Fig. 1 apresenta as 5 primeiras linhas do circuito quântico utilizado, que consiste em uma série de portas lógicas quânticas aplicadas aos qubits para realizar cálculos [5]. Essas portas, análogas às portas lógicas clássicas, são responsáveis por realizar operações nos qubits, como superposição, emaranhamento e medida [5]. No QML, algoritmos e circuitos quânticos são projetados para processar e manipular estados quânticos, representando dados e realizando cálculos de forma quântica. Esses circuitos quânticos podem oferecer vantagens em relação às abordagens clássicas em termos de velocidade computacional, paralelismo e capacidade de lidar com conjuntos de dados em larga escala e alta dimensionalidade.

D. Abreu faz parte do Programa de Pós-graduação em Ciência da Computação da Universidade Federal do Pará, Belém, Pará (e-mail: diego.abreu@itec.ufpa.br)

A. Veloso faz parte do Programa de Pós-graduação em Ciência da Computação da Universidade Federal do Pará, Belém, Pará (e-mail: aveloso@ufpa.br)

A. Abelém. faz parte da Faculdade de Computação da Universidade Federal do Pará, Belém, Pará (e-mail: abelem@ufpa.br)

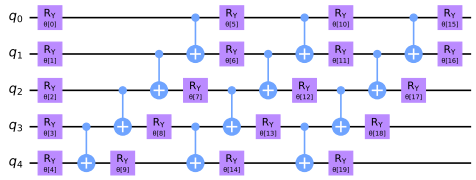

Figura 1. Parte do Circuito Quântico utilizado no Variational Quantum Classifer.

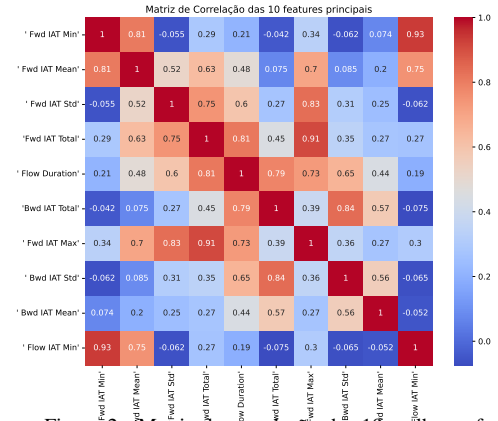

Figura 2. Matriz de correlação das 10 melhores features.

Para realizar o experimento foi utilizado o *dataset* CIC-MAL-17 [6], filtrando as famílias de ransomware existentes. No total, a base contém 81 características (*features*) de fluxo de rede de dados considerados benignos (43.091instâncias) e de ataques ransomware (313.634 instâncias). Entre os ataques ransomware 10 famílias de ataques estão presentes na base de dados: Charger, Jisut, Koler, Lockerpin, Pletor, Porndroid, RansomBo, Svpeng, Simplocjer, Wannalocker.

III. Resultados

Para realizar a detecção e classificação dos ataques ransomware o primeiro passo foi identificar as principais *features* que influenciam a distinção entre os ataques e a classe normal. A Fig. 2 apresenta a matriz de correlação destacando as 10 melhores *features*. Essas *features* serão utilizadas para realizar classificação, tanto binária quanto multiclasse dos ataques.

A Tabela I apresenta o resultado para a classificação binária (ataque vs normal) em termos das métricas: precisão (Prec.), *Recall* e F1 score. A Tabela II apresenta os resultados por família de ransomware, destacando os resultados de TPR (*True Positive Rate*) e FAR (*False Alarm Rate*) além do número de instâncias presentes por tipo de ataque. No cenário de classificação binária (Tabela I), o VQC se destaca com um desempenho superior em termos de precisão, recall e F1-score. O VQC alcança precisão de 92%, recall e F1-score de 98% e 95%, respectivamente, mostrando sua capacidade de recuperar a maioria das amostras positivas corretamente e equilibrar precisão e recall de forma eficaz. Em contraste, os classificadores clássicos RF (*Random Forest*) e kNN (*k-Nearest Neighbours)* obtêm resultados inferiores em todas as métricas, com o RF sendo mais robusto que o kNN. Por outro lado, na classificação multiclasse (Tabela II), observa-se que embora o VQC obtenha resultados superiores ao RF em algumas classes (por exemplo, Pletor com TPR de 43% e Benign com TPR de 42%), seu desempenho é menos consistente em outras classes, como Lockerpin e SVpeng, com TPRs baixos de 15% e 24%, respectivamente. Em comparação, o RF exibe um desempenho mais equilibrado entre as classes, em termos de TPR e FAR em várias delas. O cenário multiclasse é geralmente mais desafiador do que o binário, e isso pode explicar o desempenho inferior ao cenário binário.

Tabela I
Resultados da Classificação Binária.

Dataset	Prec%	Recall%	F1score%
VQC	92%	98%	95%
RF	89%	90%	89%
kNN	82%	86%	83%

Tabela II
Resultados da Classificação Multiclasse.

Classificador		VQC		RF	
Classe	**Instâncias**	**TPR**	**FAR**	**TPR**	**FAR**
Normal	43.091	42%	7%	26%	11%
Charger	39.551	26%	8%	16%	9%
Jisut	25.672	19%	5%	22%	5%
Koler	44.555	38%	9%	29%	8%
Lockerpin	25.307	15%	4%	15%	4%
Pletor	4.715	43%	0%	0%	0%
PornDroid	46.082	33%	9%	29%	12%
RansomBO	39.859	29%	8%	22%	9%
Simplocker	36.340	47%	10%	31%	11%
SVpeng	54.161	24%	7%	30%	9%
WannaLocker	32.701	25%	6%	25%	7%

IV. Conclusão e Trabalhos Futuros

Esse trabalho propões a utilização de QML para a detecção de ataques ransomware, comparando-o com os algoritmos clássicos. Como trabalhos futuros, pretendemos investigar e aprimorar o desempenho do VQC em cenários de classificação multiclasse para a detecção de ransomware, com estratégias de pré-processamento e otimização de hiperparâmetros. Além de explorar outras técnicas de QML para melhorar a eficiência da proposta e sua capacidade de lidar com grandes conjuntos de dados.

Agradecimentos

Agradecemos ao apoio da Fundação de Amparo a Pesquisa do Estado de São Paulo (FAPESP), por meio do processo no 2020/04031-1.

Referências

[1] D. Abreu and A. Abelém, "Ominacs: Online ml-based iot network attack detection and classification system," in *2022 IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE, 2022, pp. 1–6.

[2] ——, "Sistema híbrido e on-line de detecção e classificação de tráfego malicioso," in *Anais do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. SBC, 2022, pp. 322–335.

[3] 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.

[4] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, "Supervised learning with quantum-enhanced feature spaces," *Nature*, vol. 567, no. 7747, pp. 209–212, 2019.

[5] A. Abelem, D. Towsley, and G. Vardoyan, "Quantum internet: The future of internetworking," *arXiv preprint arXiv:2305.00598*, 2023.

[6] A. H. Lashkari, A. F. A. Kadir, L. Taheri, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark android malware datasets and classification," in *2018 International Carnahan conference on security technology (ICCST)*. IEEE, 2018, pp. 1–7.