Projet Pack Quantique

Région îledeFrance

AQACYB

Avantage Quantique pour l'Analyse de CYBermenaces

Quantum Advantage for Cyber Threats Analysis

Proposé par

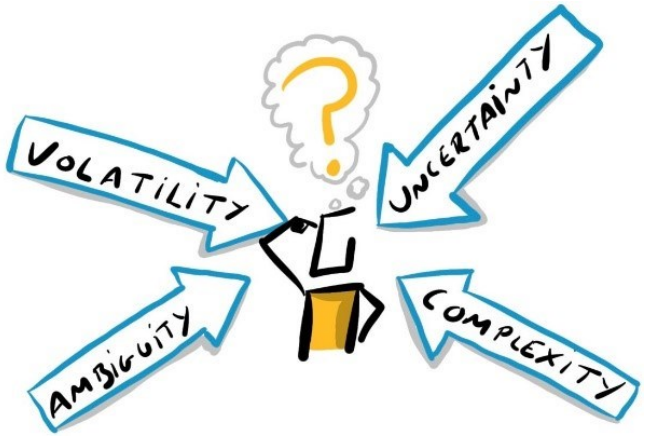
Allianz IQM MULTIVERSE COMPUTING

Avec l'accompagnement du

GENCI
Le calcul intensif au service de la connaissance

CYBERSECURITY

In today's VUCA world (Volatility, Uncertainty, Complexity, Ambiguity), cybersecurity is essential for states, citizens, and companies.



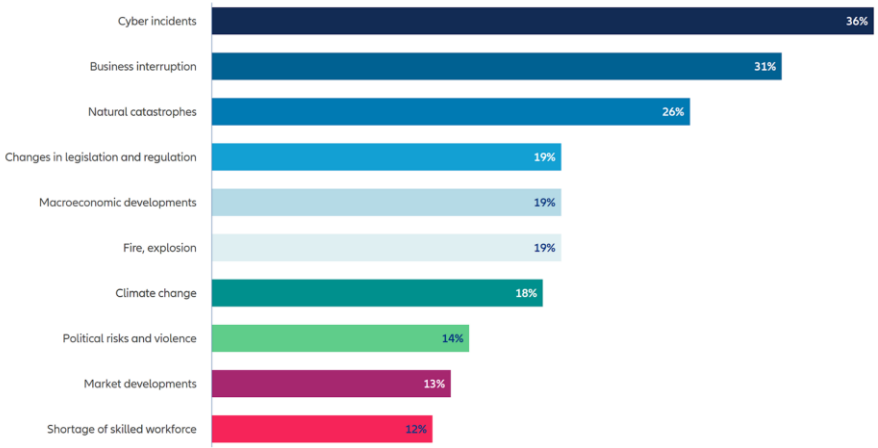
CYBERSECURITY – The Most Important Business risk

Allianz

The most important business risks in 2024: global

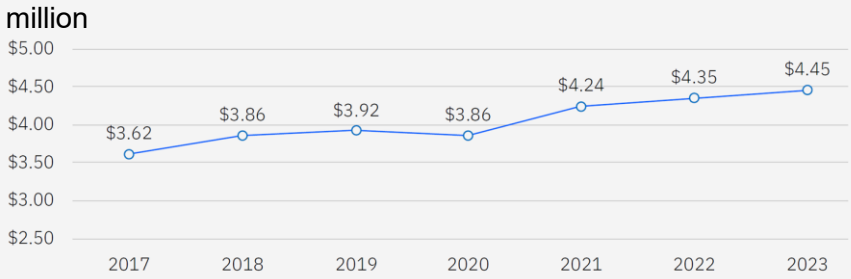
Allianz Risk Barometer 2024

Figures represent how often a risk was selected as a percentage of all survey responses from 3,069 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.



Source : Allianz Risk Barometer 2024

Total cost of a data breach



Investing now can save millions

USD 4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

51%

51% of organizations are planning to increase security investments as a result of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools.

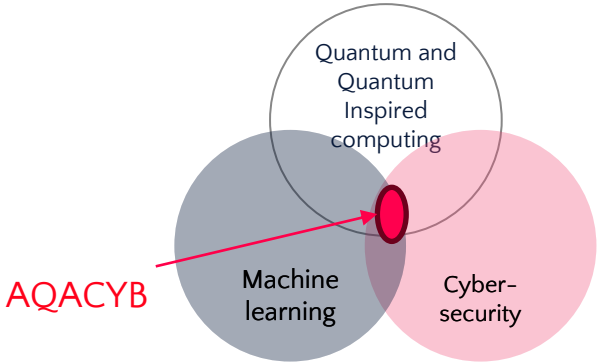
USD 1.76 million

The average savings for organizations that use security AI and automation extensively is USD 1.76 million compared to organizations that don't.

Source : IBM Security Report 2023

PROJECT OBJECTIVE

Allianz, an insurance company, recognizes the importance of cybersecurity and is leveraging AI to prevent cyber threats. As part of this effort, they are exploring the potential benefits of quantum algorithms in improving cybersecurity threat detection.



Develop a product for threats detection in cybersecurity. Based on an AI model leveraging quantum and MULTIVERSE quantum-inspired algorithms applied in IQM QPU.

AQACYB 3 PARTNERS – 1 AIM

A

Allianz

Global player and European leader in insurance

I

IQM *France*

Pan-European leader in the construction of quantum computers

M

MULTIVERSE

European leader in the development of quantum and quantum-inspired software

RELATED WORKS

Despite project time lag, AQACYB partners have been involved in other cyber projects e.g. Allianz and LMU explored unsupervised anomaly detection with *quantum Boltzmann machines*.

Exploring Unsupervised Anomaly Detection with Quantum Boltzmann Machines in Fraud Detection

Jonas Stein[1], Daniëlle Schuman[1], Magdalena Benkard[2], Thomas Holper[2], Wanja Sajko[1], Michael Kölle[1], Jonas Nüßlein[1], Leo Sünkel[1], Olivier Salomon[2] and Claudia Linnhoff-Popien[1]

[1]*LMU Munich, Germany*
[2]*Allianz France*
jonas.stein@ifi.lmu.de

Keywords: Quantum Boltzmann Machine, Quantum Annealing, Anomaly Detection

Abstract: Anomaly detection in Endpoint Detection and Response (EDR) is a critical task in cybersecurity programs of large companies. With rapidly growing amounts of data and the omnipresence of zero-day attacks, manual and rule-based detection techniques are no longer eligible in practice. While classical machine learning approaches to this problem exist, they frequently show unsatisfactory performance in differentiating malicious from benign anomalies. A promising approach to attain superior generalization than currently employed machine learning techniques are quantum generative models. Allowing for the largest representation of data on available quantum hardware, we investigate Quantum Annealing based Quantum Boltzmann Machines (QBMs) for the given problem. We contribute the first fully unsupervised approach for the problem of anomaly detection using QBMs and evaluate its performance on an EDR inspired synthetic dataset. Our results indicate that QBMs can outperform their classical analog (i.e., Restricted Boltzmann Machines) in terms of result quality and training steps in special cases. When employing Quantum Annealers from D-Wave Systems, we conclude that either more accurate classical simulators or substantially more QPU time is needed to conduct the necessary hyperparameter optimization allowing to replicate our simulation results on quantum hardware.

1 INTRODUCTION

Anomaly detection is the identification of abnormal behavior in data, which manifests in individual data points that differ significantly from the majority of the data (Chandola et al., 2009). This task frequently appears in many domains including finance, medicine and telecommunications (Aleskerov et al., 1997; Spence et al., 2001; Kumar, 2005). A particularly challenging application of Anomaly Detection can be found in Endpoint Detection and Response (EDR), which aims at detecting and investigating suspicious activities on endpoints such as mobile phones or workstations in cybersecurity (Chuvakin, 2022). In practice, the respective networks can be comprised of billions of nodes, generating an immense amount of data, in which the search for extremely scarce, malicious anomalies can be very tedious.

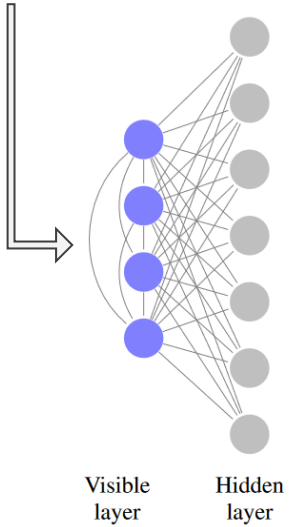
This vast number of typically high-dimensional data points and additional impediments such as zero-day attacks raise a demand for suitable anomaly detection techniques deviating from the still widely-used manual and rule-based approaches. While many classical machine learning approaches to this mostly unsupervised learning problem exist, (e.g., clustering (Munawar et al., 2012), autoencoders (Fiske et al., 2021) or Bayesian networks (Moscato et al., 2014)), the distinction between malicious and benign anomalies frequently remains intractable due to insufficient generalization (Kerani, 2018). This problem substantiates in a trade-off between detecting an unacceptably high number of false positives (i.e., benign data) and failing to reliably detect all true positives (i.e., the malicious anomalies).

In search for alternative approaches that can cope with the encountered real world data better, we investigate the application of Quantum Computing (QC) to this problem, as QC has shown promising performance in generative data modelling, which is a popular technique used in unsupervised anomaly detection (Otter et al., 2022). The general motivation behind using generative models for unsupervised anomaly detection is that their core functionality of replicating a given data distribution yields a data model that closely represents the input dataset with the exclusion of all anomalies, as they are too scarce to be learned

- EDR inspired synthetic dataset.
- Quantum Annealing based implementation.

Results: QBMs can outperform classical models (training steps and result quality).

Still not achieved with current QPUs.

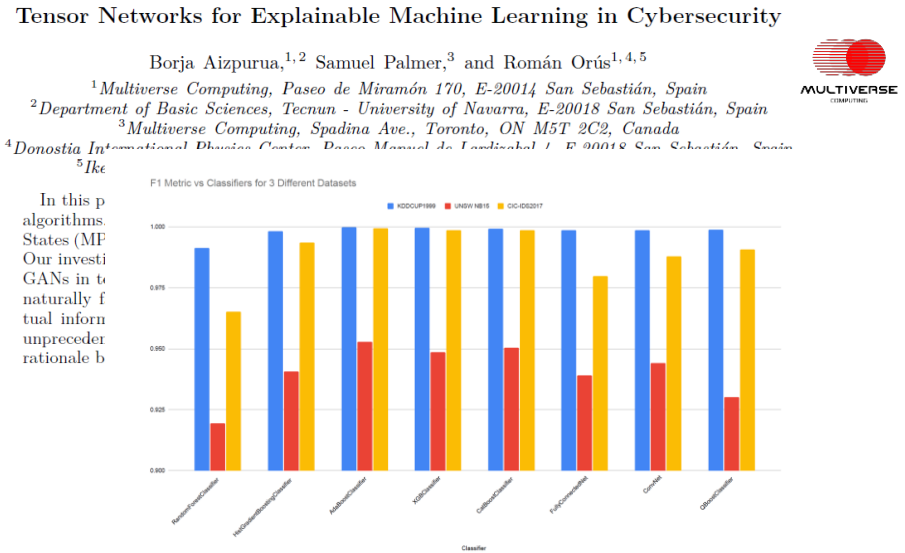


Gate based implementation

1. Same QBM not feasible with limited number of qubits.
2. Different generative model to compare results on same dataset.

RELATED WORKS

Despite project time lag, AQACYB partners have been involved in other cyber projects e.g. Multiverse has developed solution with quantum-inspired solutions (TN) and Qboost.



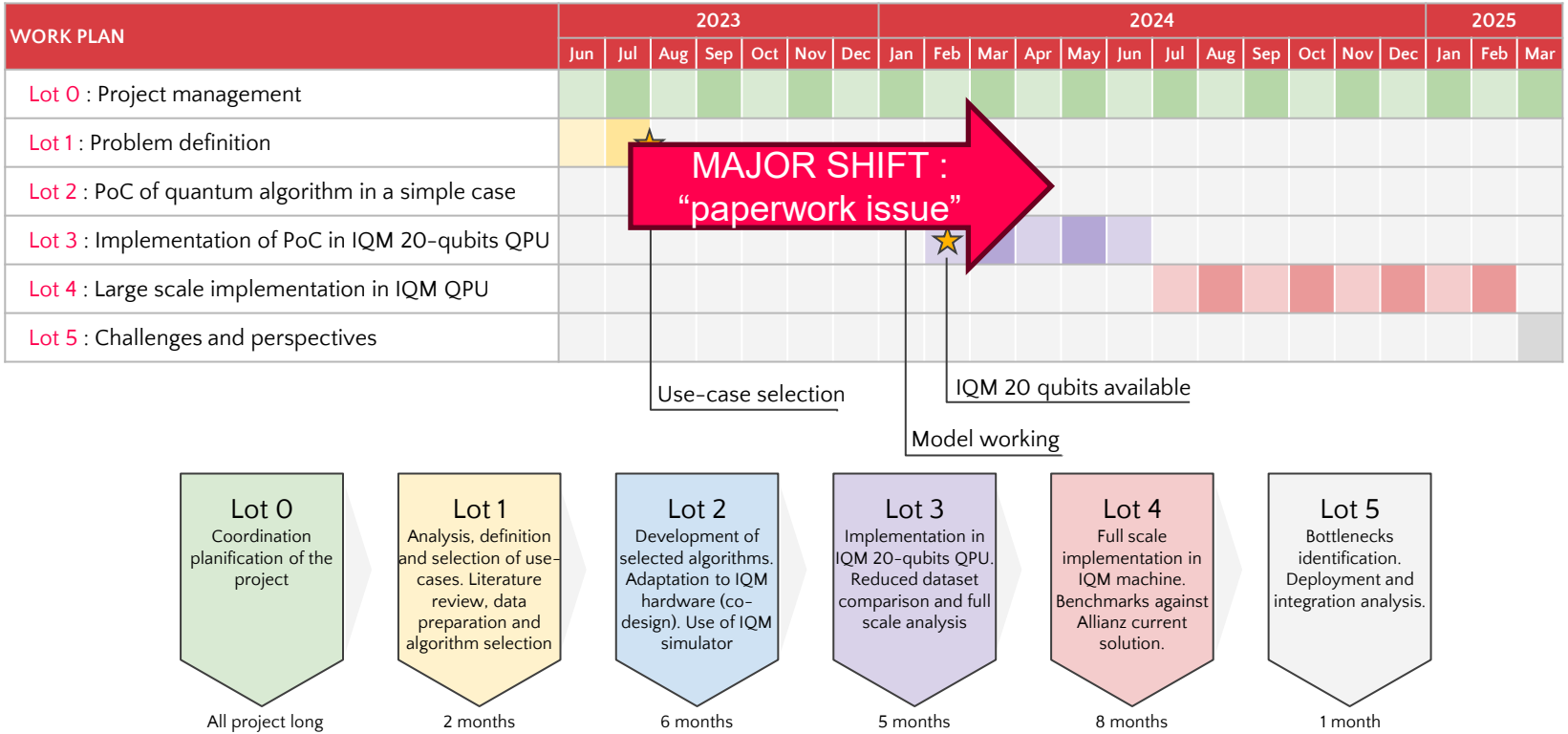
Tensor Networks for Explainable Machine Learning in Cybersecurity

Borja Aizpurua,[1,2] Samuel Palmer,[3] and Román Orús[1,4,5]

[1] *Multiverse Computing, Paseo de Miramón 170, E-20014 San Sebastián, Spain*
[2] *Department of Basic Sciences, Tecnun - University of Navarra, E-20018 San Sebastián, Spain*
[3] *Multiverse Computing, Spadina Ave., Toronto, ON M5T 2C2, Canada*
[4] *Donostia Int*
[5] *Ike*

In this p
algorithms
States (MF
Our investi
GANs in t
naturally f
tual inforn
unprecedei
rationale b

TIMELINE OVERVIEW



NEXT STEP

Allianz red team is building a specific dataset

Accordingly envisaged approaches, quantum machine learning models, will highly depend on the problem type unsupervised vs supervised, the data quality and the different attributes of the dataset (imbalance, size, etc.) :

	Classical (Benchmarking)	Quantum and Quantum-Inspired
Supervised	**Random Forest & Boosting methods. Additionally, fully connected neural networks (FCNN) and convolutional neural networks (CNN)..**	**QBoost, quantum neural networks, VQA, etc**
Unsupervised	**DBSCAN, SVM, Variational Autoencoders, Isolation Forest, GAN.**	**TN-based GM**

→ Approach will depend also on what we can do with the IQM QPU, the IQM simulator and the superconducting quantum circuits (e.g. adaptation of Allianz & LMU work on IQM QPU).
→ The exploration of highly innovative approaches could also potentially surpass the methods described above.


Thank you !