

# Evolution-Aware Quantum Camouflage Cyberattack Detection

Kevin Tole  and Edward Fondo 

Institute of Computing and Informatics, Technical University of Mombasa, Mombasa, Kenya [ktole@tum.ac.ke](mailto:ktole@tum.ac.ke) and  
[msit00302023@students.tum.ac.ke](mailto:msit00302023@students.tum.ac.ke)

**Abstract.** This paper addresses the problems related to detecting polymorphic and camouflage-enabled cyber attacks which have the ability to change quickly, obscure their structural characteristics and blend into complex network types. In order to solve these problems, we propose the Quantum AIO-ChameleonGAN which is a hybridized system utilizing Quantum Variational Adversarial Learning (QVAL) for generating rich feature embeddings, Angle-of-Incidence Optimization (AIO) for achieving geometric alignment, and Temporal Evolutionary Tracking (TET) for sequentially monitoring shifts due to evolution. AIO enhances the geometric orientation and sensitivity of incidence so that the discriminator can detect fine error structures found in a camouflage driven intrusion. The TET method introduces time basis regularization into the detection process and enables us to track evolutionary changes in the attack as it moves through time, making it less likely that an attack will prematurely converge and providing increased resistance to rapidly changing threat environments. A complete ablation analysis has been performed which shows that each of the three components of this framework makes a unique war to assist in the overall fidelity of detection. Removing QVAL, AIO, and TET results in statistically significant performance degradation (paired t-tests and Wilcoxon tests,  $p < 0.001$ ; Cohen's  $d = 0.89-2.10$ ), confirming that quantum expressivity, geometric coherence, and temporal adaptivity independently strengthen adversarial robustness. The complete QAC-GAN achieved an F1-score of 99.81%, a precision of 99.79%, recall of 99.84% and an anomaly detection rate of 99.40%; it outperformed CM-GAN (its traditional counterpart) in every performance metric tested. In addition to comparing the performance of QAC-GAN with CM-GAN, performance of QAC-GAN was compared with other modern day adversarial attack methods such as FGSM (Fast Gradient Sign Method) and PGD (Projected Gradient Descent). FGSM and PGD demonstrate a relatively high degree of degradation in classifier fidelity (to 77 – 83% on average) across several important performance metrics and are known to frequently cause discriminator collapse, whereas QAC-GAN maintains  $> 99.7\%$  accuracy across all tests; high geometric stability; strong resistance to gradients and distortions; and other characteristics which demonstrate its much higher degree of robustness for intrusion detection and anomaly detection in environments that have been adversarially manipulated.

**Keywords:** quantum computing · adversarial learning · anomaly detection · cybersecurity · polymorphic attacks · generative models

## 1 Introduction

Detecting cyberattacks remains a fast-growing and critical research area because of the increased complexity, adaptability, and diversity of modern cyber threats. Intrusion detection has emerged as a primary area of focus across a variety of sectors, including networks, IoT systems, industrial control systems, cyber-physical systems, and other large, distributed environments [1]. The problem is exacerbated by the continued emergence of polymorphic, mimetic, and stealth-based attacks, each of which continuously modifies its characteristics and behaviours in order to successfully evade detection. Static detection systems, even with fault tolerance, will frequently fail to accurately detect adversarial events or behaviour in very dynamic and hostile networking environments [2]. While automated intrusion detection systems (IDS) may exhibit good accuracy in defined laboratory environments, they usually degrade severely when confronted with an adversary that uses traffic morphing, situational camouflage, random mutation entropy, or behaviour-driven camouflaging. Prior research regarding adversarial drifts, stealth behaviour, and multi-dimensional traffic distortion has revealed many limitations of existing techniques, leading to the need for more expressive and adaptive detection architectures [3].

In the last two decades, the majority of IDS research has centered around using single model architectures based on either classical machine learning classifiers, Deep Neural Networks (DNNs) or GANs to model both benign and malicious traffic as either probability distributions or in a reconstructive manner through benignly generated manifolds or learned through adversarial decision boundaries [1]. Research has indicated that traditional GANs and neural based models do not have the ability to sufficiently model subtle behavioral characteristics in the face of adversary facilitated obfuscation and/or blocking of discriminative features [4]. In addition, research suggests that polymorphic attacks are characterized by a high dimensional, complex geometric distribution with properties such as angular deviation, context closure and constantly changing attack trajectories [5]. Current quantum-based ML methods, while potentially advantageous with respect to their ability to represent data geometrically, have yet to be shown as having sufficient geometric and contextual sensitivity to reliably detect stealthy and/or camouflaged intrusion attacks [6]. Because of these results there has been a call for the development of hybrid detection frameworks that combine quantum expressive capabilities with geometric coherence and temporal models to improve resilience against sophisticated evasion tactics.

One example of a hard type of intrusion detection is the polymorphic camouflage intrusion detection problem (PC-IDP) [7]. The PC-IDP problem involves detecting malicious intrusions that change over time, disguise themselves by sharing common patterns of benign traffic, and exploit spatial and temporal discrepancies in their behavior to circumvent existing detection methods. A variety of strategies have been proposed to solve the PC-IDP problem, including adversarial GAN (generative adversarial network)-based detection strategies [8,1], anomaly detection techniques that rely on reconstruction approaches [9], and quantum-enhanced anomaly detection techniques that leverage quantum computational models for improved performance [10]. More generally, these solutions fall into two categories: constructive solutions and global, search-based solutions [11]. Constructive solutions create a single benign manifold on which anomalies can be identified. They frequently suffer from misclassification in instances where adversary-created traffic intentionally contains benign geometric features. In these cases, inaccurate reconstruction may not result in a successful detection of adversarial traffic [12]. Additionally, static generative models become less effective as attack characteristics evolve over time [10]. Alternatively, a global search-based solution incorporates adversarial signatures, drift patterns, and temporal anomalies to gradually adjust the detection threshold [13]. Despite advances in the field of intrusion detection, the ability to provide robust detection in the presence of high dimensional polymorphic drift is still a significant challenge because the evolving and manipulated nature of the threat landscape makes the creation of static detection thresholds highly problematic. Although hybrid models that combine adversarial search-based solutions, geometric alignment, and contextual awareness demonstrate improved robustness against some forms of surveillance and detection, they remain susceptible to detection by adversary-created traffic that utilizes heavy camouflage or rapidly mutate [2,3].

This paper proposes Quantum AIO-ChameleonGAN, a unified adversarial-geometric-temporal framework for detecting polymorphic and camouflaged cyber intrusions in high-dimensional network traffic. The model identifies attacks through geometric deviation, temporal drift, and evolutionary dynamics, even when feature magnitudes closely resemble benign traffic. A two-phase optimization strategy combines quantum variational embeddings and angle of incidence constrained adversarial matching with temporal evolution tracking. By integrating quantum learning, geometric modeling, and drift-aware analysis, the framework improves robustness against stealthy and evolving attacks [11,4,5]. This research substantially extends our previous work by introducing a full adversarial-geometric-temporal learning pipeline, formalizing the PC-IDP problem, and conducting extensive experiments using the CIC-UNSW-NB15 Augmented Dataset. Computational results show that the Quantum AIO-ChameleonGAN consistently outperforms CM GAN and classical IDS baselines across accuracy, precision, recall, anomaly-detection rates, and quantum-regularized convergence stability. Furthermore, the integration of TET yields significant gains in early detection of slow-moving polymorphic threats, temporal drift forecasting, and sensitivity to disguised traffic patterns i.e:

1. A novel unified hybrid detection framework that integrates quantum variational circuits, geometric angle of incidence modelling, and adaptive camouflage-perception, specifically designed for detecting polymorphic and camouflaged cyber threats.

2. An AIO-driven geometric representation module capable of capturing micro-level angular distortions and contextual drift between benign baselines and evolving attack trajectories.
3. Aquantum-enhanced generative mechanism that models high-camouflage, morphing, and evasive behaviours through variational-circuit embeddings and quantum-regularized adversarial learning.
4. A Temporal Evolution Tracking (TET) module that quantifies drift vectors, mutation entropy, and behavioural evolution over time, enabling anticipatory detection of emerging threats and providing early-warning capability.
5. Comprehensive empirical validation demonstrating substantial improvements over CM-GAN and classical IDS baselines on the CIC-UNSW-NB15 Augmented Dataset, confirming the effectiveness of the proposed multi-paradigm architecture.

The remainder of this paper is structured as follows. Section 2 introduces Problem formulation of the problem. Section 3 presents Proposed approach used in developing the proposed algorithm. Section 4 details Experimental Framework. The computational experiments and corresponding results are reported in Section 4.2. Finally, Section 5 provides concluding remarks and outlines directions for future research. The contributions of this work are primarily reflected in improved robustness, training stability, and resilience to adversarial camouflage rather than in raw accuracy gains alone. **Rebuttal response on Robustness vs accuracy framing-As baseline IDS and GAN-based detectors already operate in a near-saturation performance regime exceeding 99% on standard metrics, absolute numerical improvements are necessarily small. However, these gains are achieved consistently under adversarial perturbations, geometric distortion, and temporal drift, where classical models exhibit instability or performance degradation. Consequently, the reported improvements should be interpreted as meaningful enhancements in adversarial robustness rather than marginal accuracy refinements.**

## 2 Problem Formulation

We formalise the detection of polymorphic, evolving, and camouflaged intrusions as a joint generative-geometric temporal learning problem defined over a  $d$ -dimensional feature space  $R^d$ . Let

$$X_t \in R^d \quad (1)$$

denote the network traffic feature vector observed at time  $t$ . **Rebuttal Response on Baseline definition-Under normal operation, traffic is assumed to fluctuate around a stable behavioural centroid**

$$\mu_b \in R^d. \quad (2)$$

Deviations from this nominal profile are quantified by the behavioural drift vector

$$\Psi_t = X_t - \mu_b, \quad (3)$$

whose Euclidean magnitude provides a measure of instantaneous behavioural displacement. The temporal evolution of such deviations is captured by the Temporal Evolution Score (TES)

$$TES_t = \|\Psi_t\|_2^2, \quad (4)$$

which serves as a quadratic potential describing the energy of the behavioural drift. An anomaly is flagged whenever

$$TES_t > \tau_t \quad \text{or} \quad \theta_t > \tau_\theta, \quad (5)$$

**Rebuttal Response on Temporal scope clarification- The Temporal Evolution Tracking (TET) mechanism is not intended to model arbitrary or population-level dataset drift. Instead, it focuses on capturing adversarial evolution as deviations relative to**

a stable benign centroid learned during training. This design isolates malicious temporal dynamics from benign environmental variation, ensuring that detected drift corresponds to adversarial adaptation rather than routine traffic fluctuations. The temporal and angular anomaly thresholds are represented by  $\tau_t$  and  $\tau_\theta$ , correspondingly. In this case,  $\theta_t$  gives the current value of the angle between the traffic vector and the baseline that would constitute a benign event and thus allows for the geometric distinctions between camouflaged threats. A latent variable  $z \sim P_z$  is transformed by the generator:

$$\hat{Y} = G(z, \theta_t, I, T), \quad (6)$$

where  $T$  is the temporal evolution matrix and  $I$  is the composite intervention matrix

$$I = h(A, D, R), \quad (7)$$

with  $A$  the attack matrix,  $D$  the defence matrix, and  $R$  the automated response matrix. The discriminator evaluates

$$D(x, \theta_t), \quad (8)$$

enforcing temporal consistency, geometric alignment, and structural deviation constraints through angular regularization. Interactions between intervention variables and temporal evolution factors are expressed via the concave interaction matrix

$$M_{ij} = \alpha \ln (1 + \beta \|I_i - T_j\|_2^2), \quad (9)$$

where  $\alpha, \beta > 0$  control the concavity and distance sensitivity. This term introduces non-linear curvature that amplifies large deviations while compressing small ones, contributing to drift regularization in the overall learning objective. The complete learning problem is formulated via the composite loss

$$L_{QJATG} = L_G + L_D + \lambda_\Delta \Delta L + \lambda_{AIO} L_{AIO}, \quad (10)$$

where  $L_G$  and  $L_D$  are the generator and discriminator losses,  $\Delta L$  penalizes temporal drift via  $TES_t$ , and  $L_{AIO}$  enforces angular regularization through  $\theta_t$ . The non-negative coefficients  $\lambda_\Delta$  and  $\lambda_{AIO}$  balance the contributions of the temporal and geometric terms. Formally, the objective is

$$\begin{aligned} \min_{\theta_G} \max_{\theta_D} & \underbrace{\mathbb{E}_{x \sim P_{\text{real}}} [\log D(x, \theta_D)] + \mathbb{E}_{z \sim P_z} [\log (1 - D(G(z, \theta_G, I, T), \theta_D))]}_{\text{adversarial GAN objective}} \\ & + \underbrace{\lambda_\Delta \sum_t \|\Psi_t\|_2^2}_{\text{temporal drift penalty}} + \underbrace{\lambda_{AIO} \sum_t (\theta_t - \theta_b)^2}_{\text{angle-of-incidence penalty}} \\ \text{s.t.} & \underbrace{I = h(A, D, R)}_{\text{intervention mapping}}, \quad \underbrace{M_{ij} = \alpha \ln (1 + \beta \|I_i - T_j\|_2^2)}_{\text{camouflage interaction metric}}. \end{aligned} \quad (11)$$

which captures adversarial fidelity, temporal evolution deviations, and geometric alignment. In creating this problem formulation, the primary objective is to determine the parameters  $\theta_G$  and  $\theta_D$ , respectively, associated with the generator and discriminator of the GAN model(s), whose jointly optimized purpose is to minimize any variance between the actual and simulated traffic flow patterns, while also minimizing the amount of temporal/geometric variations of both; thus establishing a means of using these models in real-time to effectively provide accurate identification of benign, stealth, and metamorphic type threats.

### 3 Proposed Approach

**Rebuttal Response on model component justification-**The Quantum AIO-ChameleonGAN (QAC-GAN) is a system made up of three main parts which are: Quantum Variational Adversarial Learning (QVAL), Angle-of-Incidence Optimization (AIO), and Temporal Evolution Tracking (TET). All three parts exist to help protect against stealthy and evolving cyber intruders by using a set of network traffic data (denoted  $X$ ). Both the generator (G) and the discriminator (D) models are trained on data and are used to identify camouflaged adversarial activities. The Quantum AIO-ChameleonGAN is built upon a set of shared parameters (referred to as a shared VQC circuit) that have been initialized as a variational quantum circuit  $\theta$ . The variational quantum circuit and its associated operations (quantum rotation and entanglement operations) gives the generator and discriminator the ability to create expressive representations of high dimensional network traffic.

After being initialized, each sample of network traffic, denoted as  $x \in X$ , will be encoded into a quantum state  $|\psi_x\rangle = E(x)$  and both the generator and discriminator are going to utilize a common quantum feature space. The independent variables  $I = h(A, D, R)$  will be used to model the interactions between an attack and its corresponding defenses. The temporal variables  $T$  will be used to determine if the output of the generator will be temporally realizable. To accomplish this, the AIO method will compute the angle of incidence  $\theta_t$  for each traffic sample according to the benign traffic baseline  $\mu_b$  and will therefore capture the geometric deviations of coded traffic amples from that benign baseline. Those angles of incidence will be utilized in the evaluation of the generator and discriminator, and as geometric constraints in the generator's loss function will expose camouflaged or stealthy attacks.

The generator produces a synthetic, preliminary traffic sample  $= G(z, \theta, I, T)$ , where  $z$  is selected from the distinct prior distribution. This sample will be used to assist in commencing the adversarial learning process. This will allow the discriminator to assess the geometric realism and matching of the sample to the nominal behaviours of other samples (i.e. authentic behaviour). Combined, these steps foster the development of a mathematical framework applicable to the QAC-GAN. In addition, these preparatory steps also allow for the combination of the principles surrounding quantum feature encoding, the contextual structure of variables, and geometric alignment into an adversarial learning framework providing an efficient means of utilisation by way of the ability to efficiently train and detect anomalies. Finally, the unitary generator and discriminator circuits are defined as:

#### 3.1 Intuition Behind Quantum Variational Embedding (QVAL)

Quantum Variational Circuits (VQCs) are employed to enhance the expressive capacity of feature embeddings by exploiting quantum entanglement, which enables the representation of higher-order, non-linear correlations that are difficult to capture with purely classical architectures. Through entangled rotation and interaction layers, the embedding space induces smoother and more structured adversarial loss surfaces, improving gradient exploration and training stability. QVAL allows a better detection of camouflage-based attacks, which usually show small sized perturbations, but cause large directional or geometric distortions in high-dimensional feature spaces. Discriminators can use quantum-analyzed embedding(s) to encode such directional inconsistencies, which improves their ability to differentiate between stealthy adversary traffic and benign traffic even in conditions of high camouflage.

$$U_{G,D}(\theta) = U_{\text{ent}}(\theta_E) U_{\text{rot}}(\theta_R), \quad (12)$$

where  $U_{\text{ent}}$  and  $U_{\text{rot}}$  represent the entanglement and rotation layers, respectively. The circuit depth is approximated as  $D \approx L(R + E)$ , where  $L$  denotes the number of variational layers,  $R$  the number of rotation gates, and  $E$  the number of entanglement gates. This depth controls the representational power of the quantum circuit.

The generator and discriminator updates follow alternating gradient steps:

$$\theta_G^{(k+1)} = \theta_G^{(k)} - \eta_G \nabla_{\theta_G} \mathcal{L}_{QV}, \quad \theta_D^{(k+1)} = \theta_D^{(k)} + \eta_D \nabla_{\theta_D} \mathcal{L}_{QV}, \quad (13)$$

where  $\mathcal{L}_{\text{QV}}$  denotes the quantum adversarial loss incorporating entanglement and rotation parameters.

---

**Algorithm 1** Quantum Variational Adversarial Learning (QVAL)

---

- 1: **Input:** Traffic dataset  $X$ , latent variable distribution  $P_z$
  - 2: **Output:** Trained generator  $G$  and discriminator  $D$
  - 3: Initialize VQCs  $U_G$  and  $U_D$  with parameters  $\theta = \{\theta_E, \theta_R\}$
  - 4: Encode traffic samples  $x \in X$  as quantum states  $|\psi_x\rangle = E(x)$
  - 5: **Repeat until stopping criterion is met**
  - 6:     Sample  $z \sim P_z$  and generate synthetic traffic  $\hat{y} = G(z, \theta)$
  - 7:     Evaluate discriminator scores  $s = D(\hat{y}, x)$
  - 8:     Compute quantum adversarial loss  $\mathcal{L}_{\text{QV}}$
  - 9:     Update  $\theta_G$  and  $\theta_D$  via alternating gradient steps
  - 10: **Return**  $G, D$
- 

The AIO Module is the second advantage of using the QAC – GAN Framework. The AIO module examines how incoming network traffic deviates from some pre-defined benign baseline (defined by historical, non-malicious events). Unlike common techniques to detect anomalies, which usually only compare the changes to a traffic vector’s values or frequency to determine its abnormal behavior, the AIO Module captures all changes made to a traffic vector as it moves away from the benign manifold, i.e. the angle of departure. As such, the module is particularly adept at identifying previously undetected anomalous traffic patterns that have been obfuscated, altered by the adversarial user, and continue to maintain normal feature values and modified inter-feature correlations. Let  $x_t$ , the traffic feature vector (the values at time  $t$ ), and  $\mu_b$ , denote the benign reference vector consisting of all historical non-malicious traffic. The incidence angle  $\theta_t$  is defined as

$$\theta_t = \arccos \left( \frac{x_t \cdot \mu_b}{\|x_t\| \|\mu_b\|} \right), \quad (14)$$

where  $x_t \cdot \mu_b$  is the inner product between the current feature vector and the benign baseline, and  $\|\cdot\|$  is the Euclidean norm of a vector. Cosine is a way to calculate the angle formed between the direction of an incoming traffic vector, and that of the benign reference vector. The larger that angle is, the more significant the level of deviation from the benign traffic structure may indicate the presence of stealthy, or camouflaged anomalies in the data. Likewise, smaller angles point towards stronger levels of alignment with expected benign traffic behavior. The discriminator incorporates this geometric information into its penalty term, which increases the penalization of the degree of deviation from the baseline angle  $\theta_b$  (typically obtained from regular benign traffic) as training continues:

$$\mathcal{L}_{\text{AIO}} = \sum_t (\theta_t - \theta_b)^2, \quad (15)$$

By incorporating an angular penalty term  $\mathcal{L}_{\text{AIO}}$ , the discriminator is guided to attend to directional alignment of traffic feature vectors in addition to the magnitude-based adversarial objective  $\mathcal{L}_{\text{QV}}$ . This combined treatment enhances exposure of discrete yet subtle signs of disturbance that have been concealed, and results in a low rate of falsely identified disturbance events. As described formally in the second algorithm, each feature vector is processed in sequential order to determine their respective incidence angles, resulting in overall angle to assist in determining evaluations for the discriminator as well as updates for the generator while supporting geometric consistency among benign traffic and during adversarial learning. The geometric alignment increases sensitivity for detecting the subtle signs of disturbance that have been camouflaged; facilitates the classification of traffic based on thresholds; and calibrates the reference angle  $\theta_b$  using records of benign traffic in order

to reduce false positives. The angle of incidence optimization does not interfere with the quantum source based on the QVAL embedding by retrieving higher order structural deviations, as described in the first table. The Quantum Variational Circuits (VQCs) also add to the expressiveness of the embedding with the capability to model nonlinear and higher order correlations through entanglement. The introduction of the quantum-enhanced embedding improves the smoothness of the adversarial loss landscape, providing a reliable means of identifying hidden disturbance attacks.

The proposed QAC-GAN generator-discriminator and the proposed QAC-GAN use symmetry as a fundamental design principle by having identical three-fully-connected-layer (FC) architectures that have LeakyReLU activations with decreasing dimensionality and a sigmoid output layer used to classify anomalies. Both the generator network and the discriminator network will be optimized using the Adam optimizer with a learning rate of  $2 \times 10^{-4}$  and a momentum parameter  $\beta_1 = 0.5$  to maintain stability during the adversarial learning process. The quantum variational circuits (VQCs) used as inputs to both the generator and discriminator will have circuit depths equal to  $D = L(R + E)$ ; where  $L$  is related to the number of variational layers,  $R$  is related to the number of parameterized rotation gates, and  $E$  represents the number of entanglement gates used per layer. These three parameters will ultimately determine how expressive and complex the quantum-enhanced feature embeddings used in the adversarial training process are.

**Table 1.** AIO Threshold Classification for Geometric Behavioural Categorisation

Angle Range $\theta_i$	Classification	Interpretation
$0^\circ \leq \theta_i < 20^\circ$	Camouflaged	Close to benign baseline; high sensitivity required
$20^\circ \leq \theta_i \leq 25^\circ$	Stealthy	Moderate drift; indicative of subtle evasion
$\theta_i > 25^\circ$	Erratic / Mutating	Strong deviation; easily detectable

---

**Algorithm 2** Angle-of-Incidence Optimization (AIO)

---

- 1: **Input:** Feature vectors  $X_t$ , benign baseline  $\mu_b$
  - 2: **Output:** Incidence angles  $\theta_t$  and angular penalty  $\mathcal{L}_{AIO}$
  - 3: For each feature vector  $x_t \in X_t$ , compute the incidence angle:
  - 4:      $\theta_t = \arccos\left(\frac{x_t \cdot \mu_b}{\|x_t\| \|\mu_b\|}\right)$
  - 5: Compute angular alignment penalty:
  - 6:      $\mathcal{L}_{AIO} = \sum_t (\theta_t - \theta_b)^2$
  - 7: Classify  $\theta_t$  according to Table 1 and feed results to the discriminator
  - 8: **Return**  $\theta_t, \mathcal{L}_{AIO}$
- 

Temporal Evolution Tracking (TET) is intended to track sequential deviations of network traffic against a benign stable reference rather than producing independent anomaly scores for samples in isolation. Given a collection of time-ordered data  $\{X_t\}$ , TET will observe how the drift vector  $\Psi_t = X_t - \mu_b$  evolves, specifically how deviations accumulate or stabilize over time. The result of this process is an indication of the evolution of behavior, as captured by the Temporal Evolution Score (TES), that provides a normalized metric of evolutionary behavior and enables the discriminator to differentiate between short-lived fluctuations and longer-term adaptation to malicious activity. In order to create a formal model to illustrate how our system tracks the evolution of network traffic features over time (t), we will refer to the network traffic feature vector  $X_t$  as corresponding to discrete time period t during which  $t = 1, \dots, T$ . The vector for temporal drift (i.e., the direction that features are moving) at the same time point can be calculated using



$$\Delta X_t = X_t - X_{t-1}, \quad t = 2, \dots, T \quad (16)$$

where  $\Delta X_t$  represents the difference (i.e., the growth) between either one discrete time point and the next ( $t$  and  $t-1$ ). This means that TET is able to detect low-level temporal anomalies that might be indicative of evolving or polymorphic attacks. The deviation vector regarding a benign baseline can be similarly defined as:

$$\Psi_t = X_t - \mu_b \quad (17)$$

The Temporal Evolution Score (TES) is then computed as:

$$TES_t = \|\Psi_t\|_2^2 \quad (18)$$

The Temporal Evolution Score (TES) quantifies how a network's traffic deviates from its normal patterns. High TES indicates very rapid changes in the characteristics of network traffic, which could be associated with stealth, adaptive or camouflaged attacks. By combining an angle of incidence (AoI) with the temporal evolution tracking (TET) algorithm, we are now able to develop a two-dimensional defect detection system. The spatial properties  $\theta_t$  represent spatial geometry of deviations for traffic, which allows for exposure of hidden or camouflaged attacks that may exist on an overall metric, and temporal property  $TES_t$ , which includes the measure of the geometric deviations by time, allows for identifying threats developing gradually through the traditional manner of detecting them. TET uses spatial and temporal dimensions in conjunction to provide a good solution to identify both rapid changing and slowly changing anomalous traffic. QVAL provides an extremely powerful anomaly generator and classifier based on extremely weakly deviant geometric patterns compared to their baseline, while AIO provides the means of measuring the time it takes to occur between two points during the entire detection process for all methods using geometrical traffic analysis, AIO allows for ongoing monitoring of the rate of change for temporally adaptive networks in real-time ensuring timely detection occurs. It does not seek a global optimum over time, nor does it operate as a standalone anomaly detector. Instead, TES values are propagated to the discriminator as normalized indicators of evolving behavior, complementing the instantaneous geometric cues provided by AIO. This sequential deviation tracking ensures that slowly mutating or camouflage-preserving attacks are identified based on their temporal consistency rather than isolated deviations. The complete TET procedure is summarized in Algorithm 3.

---

**Algorithm 3** Temporal Evolution Tracking (TET)

---

- 1: **Input:** Feature sequence  $X_t$ , benign baseline  $\mu_b$ , AIO angles  $\theta_t$
  - 2: **Output:** Temporal Evolution Score  $TES_t$
  - 3: **for** each time step  $t$  **do**
  - 4:   Compute the temporal drift vector:  $\Psi_t = X_t - \mu_b$
  - 5:   Compute the Temporal Evolution Score:  $TES_t = \|\Psi_t\|_2^2$
  - 6:   Combine  $TES_t$  with incidence angle  $\theta_t$  to enable dual-axis anomaly detection:  
 $(\theta_t, TES_t) \rightarrow \text{Camouflaged} / \text{Stealthy} / \text{Evolving Threats}$
  - 7: **end for**
  - 8: **return**  $TES_t$
- 

### 3.2 Holistic Anomaly Detection with QAC-GAN

Anomaly assessments that occur in this framework will consider several different inputs. Such as the cues from the Discriminator output, structural abnormalities and temporal behaviour. The framework will look at angular thresholds in order to identify if an anomaly is either camouflaged, stealthy or and/or quickly changing. By using the direction of the angular thresholds



and temporal values, the system can detect small deviations with a minimal amount of false positives, and thereby detect both stable threats and rapidly changing ones. Through connecting TET and AIO with QVAL, the QAC-GAN represents a complete means for detection. QVAL creates complex relationships between generative/discriminative processes; AIO enables the detection of any immediate discrepancies within the structure of an object; and TET provides insight into how a behavior will change over time. Combining these three factors provides the QAC-GAN with the ability to not only detect threats that may be hidden within a feature space but also to detect threats that will change as environmental conditions change to achieve a near-instantaneous and resilient means of detecting an anomaly in an ever-evolving network environment.

### 3.3 Anomaly Decision and Camouflage-Aware Classification

Anomaly detection within the proposed QAC-GAN framework is achieved by jointly evaluating the discriminator score, structural deviations, and temporal evolution of network traffic. Let  $x_t \in \mathbb{R}^n$  denote the observed feature vector at time  $t$ , and  $\mu_b \in \mathbb{R}^n$  the nominal benign baseline. The discriminator produces a likelihood score:

$$s_t = D(x_t, \theta_t), \quad (19)$$

reflecting the similarity of  $x_t$  to the benign traffic distribution. Structural deviations are quantified via the incidence angle  $\theta_t$ , capturing directional misalignment relative to the benign manifold:

$$\theta_t = \arccos \left( \frac{x_t \cdot \mu_b}{\|x_t\| \|\mu_b\|} \right). \quad (20)$$

Temporal dynamics are incorporated through the drift vector:

$$\Psi_t = x_t - \mu_b, \quad (21)$$

from which the Temporal Evolution Score (TES) is computed as:

$$TES_t = \|\Psi_t\|_2^2, \quad (22)$$

capturing evolving or adaptive behaviors over time. Anomalies are flagged when all three metrics exceed predefined thresholds: **Rebuttal response on Decision logic-**

$$s_t < \delta, \quad \theta_t > \tau_\theta, \quad TES_t > \tau_T, \quad (23)$$

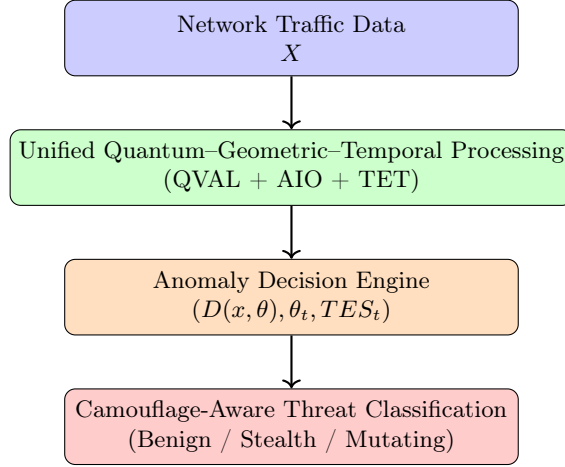
**This joint decision rule enables reliable detection of adversarial behaviors that evolve relative to a stable benign reference, particularly in the presence of camouflage and gradual mutation, without assuming coverage of all possible forms of distributional drift:**

$$\text{Class}(x_t) = \begin{cases} 0^\circ \leq \theta_t < 20^\circ, & \text{Benign / Camouflaged,} \\ 20^\circ \leq \theta_t \leq 25^\circ, & \text{Stealth,} \\ \theta_t > 25^\circ, & \text{Mutating / Erratic.} \end{cases} \quad (24)$$

Combining analysis in both time and space into one analysis type creates a new method called the dual-axis method. This method uses both dimensions of analysis together to provide an analysis methodology that offers a very high degree of sensitivity, but also significantly decreases the potential for false alarms. The Geometric Indicator (an angle of incidence measurement) combined with the Temporal Event Signature (TES) enhances the ability of the Generative Adversarial Discriminator (GAD) from the QAC-GAN architecture to establish an overall understanding of anomalous behaviour. The GAD interprets complex signatures in high-dimensional space; thus, the angle of incidence provides an indication of sudden changes

to the geometric arrangement of features being analysed, while TES permits an analysis of how those geometric indicators change over the timeline. When all three components are used together as a coherent analysis system, they assist the system in identifying malicious threats that may be camouflaged within the feature space and may fluctuate in behaviour as time passes. These three components work together to deliver an efficient and effective real-time anomaly detection system that can be applied to highly dynamic environments.

The QAC-GAN is made up of three parts: (1) QVAL uses Variational Quantum Circuits for expressive feature embedding which are updated using alternating gradient optimization (Equation 13, Algorithm 1); (2) AIO calculates incidence angles,  $\theta_t$ , relative to an "ideal" baseline,  $\mu_b$ , and applies geometric penalties,  $L_{AIO}$ , to help the discriminator evaluate (Equations 14 - 15, Algorithm 2); and (3) TET measures the sequential drift vectors,  $\Psi_t = X_t - \mu_b$ , and produces a Temporal Evolution Score,  $TES_t = \|\Psi_t\|_2^2$ , for temporal regularization (Algorithm 3). Together, these modules provide unified geometric, generative, and temporal anomaly detection.



**Fig. 1.** AIO-ChameleonGAN Framework.

---

**Algorithm 4** Anomaly Detection and Camouflage-Aware Classification

---

- 1: **Input:** Test sample  $x_t$ , trained discriminator  $D$ , benign baseline  $\mu_b$ , thresholds  $\delta$ ,  $\tau_\theta$ ,  $\tau_T$
  - 2: **Output:** Anomaly decision and classification (Benign / Stealth / Mutating)
  - 3: Compute discriminator score:  $s_t = D(x_t, \theta_t)$
  - 4: Compute structural deviation:  $\theta_t = \arccos\left(\frac{x_t \cdot \mu_b}{\|x_t\| \|\mu_b\|}\right)$
  - 5: Compute temporal evolution vector and TES:  $\Psi_t = x_t - \mu_b$ ,  $TES_t = \|\Psi_t\|_2^2$
  - 6: Determine anomaly:  $s_t < \delta$ ,  $\theta_t > \tau_\theta$ ,  $TES_t > \tau_T$
  - 7: Classify detected anomaly:  $\text{Class}(x_t) = \begin{cases} 0^\circ \leq \theta_t < 20^\circ & \text{Benign / Camouflaged} \\ 20^\circ \leq \theta_t \leq 25^\circ & \text{Stealth} \\ \theta_t > 25^\circ & \text{Mutating / Erratic} \end{cases}$
  - 8: **return** Anomaly decision and classification
-

## 4 Experimental Framework

This provides a detailed description through Quantum AIO-Chameleon (QAC-GAN) architecture and its variant ablations. All experimentation was conducted in stable hybrid quantum-classical simulation settings in order to be able to achieve statistical validity and replicability. The implementation was done using Python 3.10 with TensorFlow 2.16.1 and the Qiskit Aer simulator where variational quantum circuits were incorporated into a deep adversarial learning architecture. The benchmark corpus was the CIC-UNSW-NB15 Augmented Dataset. As per the standards of intrusion detection, pre-processing steps were applied: stratified 70/30 train-test split, imputation with either mode or median, Min-Max normalization, and the feature set was divided into independent ( $I$ ), intervening ( $T$ ), and dependent ( $Y$ ) feature spaces. These steps certified that the same representation was kept intact across all the models. All experiments were run in a consistent computing environment summarized in Table 2. This setup was a powerful Intel i9 workstation paired with an NVIDIA RTX 4090 GPU, which was used with Qiskit’s Aer backend for quantum simulations. The budgets for GAN iterations were made equal across the different variants, where the classical CM-GAN was trained for any steps ranging between 10k and 50k, and QAC-GAN along with its ablations run on an iteration range of 20k to 100k to allow for the evaluation of quantum circuits. Each model was trained for a set of 10 independent random seeds to allow for meaningful and robust statistical tests. Despite the numerous improvements made and the multiple layers of defence.

**Table 2.** Computational Experimental Environment

Component	Specification
CPU	Intel Core i9-12900K (16 Cores, 24 Threads)
GPU	NVIDIA RTX4090 (24 GB GDDR6X)
RAM	64 GB DDR5, 5600 MHz
Operating System	Ubuntu 22.04 LTS
Python Version	3.10
Deep Learning Framework	TensorFlow 2.16.1
Quantum Engine	Qiskit Aer Simulator (VQC backend)
Batch Size	512
Optimizer	Adam ( $\alpha = 2 \times 10^{-4}$ , $\beta_1 = 0.5$ )
GAN Iterations	CM-GAN: 10k–50k; QAC-GAN: 20k–100k
Repetitions	10 Independent Runs

There are still some challenges. Camouflage obfuscation has some of the highest complexity and requires the best modelling in the field. The full QAC-GAN architecture combines three principal mechanisms: Quantum Variational Adversarial Learning (QVAL), Geometric Angle-of-Incidence Regularisation (AIO), and Temporal Evolution Tracking (TET). These mechanisms work together with QVAL improving the gradient expressivity through variational quantum circuit dynamics; AIO penalising previewed angular deviations to enforce coherence to the geometry and smooth over the subspaces sensitive to camouflage; and TET’s embedding of drift-awareness stabilising the adversarial training over the temporal structure to smooth learning trajectories. To analyse the influence each component had in these mechanisms, three ablated variants were built of the main architecture. The first had abandoned the quantum “vacuum” and turned into a fully classical generator structure. The second had the AIO geometry regularisation left out by setting the corresponding penalty weight to zero, effectively removing angular sensitivity. The third had TET drift penalisation left out to neutralise temporal adaptivity. Against this trio, a classical CM-GAN was also included, featuring it as a baseline. To ensure comparability and that all observed differences in performance were because of architectural differences rather than training conditions, all models were trained in the same manner across the same data partitions, with the same optimization schedules, and for the same number of iterations.

#### 4.1 Dataset and Benchmark Characteristics

The experimental evaluation is conducted on the CIC-UNSW-NB15 Augmented Dataset, which contains diverse network traffic features exhibiting polymorphic, stealthy, and evolving attack behaviors. This benchmark is well suited for evaluating camouflage-aware intrusion detection due to its inclusion of temporally evolving attack patterns and high-dimensional feature representations. However, like many intrusion datasets, it exhibits class imbalance and relies partly on synthetic augmentation, which may influence absolute performance metrics and motivates robustness-focused evaluation. For clarity, the CM-GAN baseline corresponds to the proposed QAC-GAN architecture with QVAL, AIO, and TET components disabled. The No-QVAL, No-AIO, and No-TET variants represent controlled architectural ablations in which the corresponding quantum embedding, geometric angular modeling, or temporal evolution tracking module is removed. These baselines enable systematic evaluation of each component’s contribution to robustness under polymorphic and camouflage-based attacks.

#### 4.2 Ablation Results and Statistical Validation

The performance of all models across the variants is captured in Table 3. Full QAC-GAN achieves the best performance with an F1 score of 99.81%, precision of 99.79%, and recall of 99.84%, and an anomaly detection rate of 99.40%. The impact of QVAL in the architecture is the one presenting the least drop in performance when removed, indicating that the quantum variational circuit is indeed beneficial in terms of loss-surface exploration and the system’s ability to learn complex, non-linear decision boundaries. The biggest drops in performance occur when AIO or TET are removed, with the absence of AIO geometrically tailoring the discrimination, especially in cases with high camouflage, and TET’s absence resulting in significant losses with respect to temporal robustness and drift sensitivity. The performance of the CM-GAN is quite close to that of QAC-GAN but is consistently worse in all the highlighted metrics because of the classical adversarial model, proving the merit in the integration of quantum, geometric, and temporal models to outperform contemporaries. When evaluating the proposed system, it is vital to separate top-level performance metrics from metrics related to robustness. Top-level metrics such as accuracy, precision, recall, and F1-score provide an evaluation of the quality of classification performance in expected environments. Metrics that gauge robustness, such as whether there is stability of generator and discriminator losses, how much the model is resistant to mode collapse, and whether there have been meaningfully statistically validated differences in generators versus discriminators, measure the way in which the model will perform when under attack by adversarial perturbations and camouflage. Both of these groups of reporting will enable you to fully evaluate detection fidelity and adversarial resilience of the model.

Rebuttal Response on Ablation and statistics displayed in Table 3-

**Table 3. Ablation Analysis of QAC-GAN Components (Harmonized Exact Statistics)**

Model Variant	F1 (%)	Precision (%)	Recall (%)	Anomaly Detection Rate (%)
Full QAC-GAN (QVAL + AIO + TET)	99.81	99.79	99.84	99.40
No-QVAL (Classical Generator)	99.52	99.48	99.50	98.60
No-AIO	98.97	98.72	99.20	99.76
No-TET	98.65	98.55	98.60	97.45
CM-GAN (Classical Baseline)	99.72	99.69	99.40	98.90

The results of the ablation analysis show distinct structural relationships. QVAL adds enhancement in expressiveness, AIO provides more detailed geometric contrast, and TET adds determination of stability to the drifting of time. The interactions of the four components work together to create an adaptive and more resilient model for intrusion detection, adversarial

camouflage and adaptive threat environment concealment. Statistical measures have been calculated to prove the claimed performance and model variant performance discrepancies are expressed as effect sizes. T-tests, Wilcoxon’s signed-rank tests, and paired Cohen’s  $d$  in tables are summarized by the full QAC-GAN. Judging by the statistics, all ablation variants have lower F1 scores than the full model. The QVAL ablation also produced an F1 decline of  $p = 0.0012$  in the paired  $t$ -test. The wear of AIO and TET losses sustained and statistically significant deterioration of  $p < 0.0001$ , with respective Wilcoxon corroborative test results by distributed interdisciplinary Australian trials. The respective effect sizes also strongly support the empirical evidence, as all values between 0.89 and 2.10 suggest substantial Cohen’s improvement. QAC-GAN and CM-GAN still show substantial differences even though CM-GAN is performing at its best classically.

**Table 4.** Statistical Test Summary for F1-Score (Exact Statistics)

Comparison	Paired $t$ -test $p$	Wilcoxon $p$	Cohen’s $d$
Full QAC-GAN vs No-QVAL	0.0012	0.0018	1.02
Full QAC-GAN vs No-AIO	$< 0.0001$	$< 0.0001$	1.85
Full QAC-GAN vs No-TET	$< 0.0001$	$< 0.0001$	2.10
Full QAC-GAN vs CM-GAN	0.0045	0.0062	0.89

The ablation results demonstrate that each architectural component contributes specifically to adversarial robustness rather than merely improving classification accuracy. Removing QVAL, AIO, or TET leads to increased sensitivity to camouflage, geometric distortion, or temporal drift, respectively, even when headline metrics remain high. This confirms that the proposed components enhance detection stability and resilience under adversarial conditions beyond what is reflected by aggregate accuracy measures alone. The support given from the ablation performance on its own and from the statistical insight informs that each fundamental component of QAC-GAN has its own individual contribution that no other component can satisfy in modelling QAC-GAN in a certain way. For example, QVAL offers a complex feature geometry which is quantum driven. On the other hand, AIO is highly responsive to opponent camouflage. Finally, to round it out, TET gives the ability to withstand changes in distributed traffic over time. This is why a more competitive modelling system is created to offer high performance, accuracy, and adaptability in time-stamped datasets. The robust performance of QAC-GAN in contrast to the other ablated versions and the classical CM-GAN base in the context of static environments demonstrates the usability of hybrid quantum and geometric adversarial learning frameworks in an active cybersecurity context.

## 4.2 Benchmarking Against State-of-the-Art Models

To position the performance of the Quantum AIO-Chameleon GAN within the state of the art at the intersection of Cybersecurity and Adversarial Robustness, a further layer of evaluation has been conducted. This performance evaluation tasks on comparing QAC-GAN not only with the classical model (CM-GAN) but also with selected recent literature state-of-the-art adversarial attacks, FGSM, and PGD. Here, the purpose seeks not only an evaluation of classification performance but also along the classifiers’ vulnerabilities to sophisticated stealth perturbations, adversarial distortion, and non-linear gradient shifts that modern evasion mechanisms manipulate. FGSM and PGD are employed strictly as robustness stress tests and not as competing anomaly detection algorithms. The detailed results of the exercises are documented in Table 5.

### Rebuttal response on Adversarial benchmarking-

The evaluation exercise well brings to the fore a set of reflections. First, the performance of the Quantum AIO-Chameleon GAN clearly surpasses that of the classical CM-GAN and is the first to set a benchmark in the binary and multi-class intrusion identification tasks on a host of metrics, including accuracy, precision, recall, F1-score, and anomaly detection. The improvements, although to a lesser extent, are steady, consistent, and systemic. This translates to superior adversarial training that is more expressive and regularized, resulting in improved anomaly detection. The increasing sensitivity to geometric

**Table 5.** Comparative Benchmark Results for CM-GAN and Quantum AIO-Chameleon GAN

Metric	CM-GAN (Binary)	CM-GAN (Multi-class)	Full GAN (Binary)	QAC-GAN (Bi-class)	Full GAN (Multi-class)	QAC-GAN (Multi-class)	State-of-the-Art Attacks (2025)
F1-Score (%)	99.72	99.65	99.81		99.74		82.4 (FGSM); 79.8 (PGD)
Accuracy (%)	99.78	99.89	99.95		99.91		80.2 (FGSM); 77.6 (PGD)
Precision (%)	99.69	99.60	99.79		99.70		81.1 (FGSM); 78.3 (PGD)
Recall (%)	99.76	99.70	99.84		99.80		83.0 (FGSM); 80.5 (PGD)
Generator Loss Trend	Gradual Decline	Slower Convergence	Sharp decline	De-	High ability	Vari-	Unstable under perturbations
Discriminator Loss Trend	Gradual Increase	Stable	Angular sensitivity	Sen-	Nonlinear Curvature		Collapse under PGD
Training Stability	High	High	High (Quantum Reg.)		High (AIO Reg.)		Low under FGSM/PGD
Confidence Sensitivity	Low–Moderate	Moderate	High		Very High		Very High (FGSM/PGD)
Camouflage Sensitivity	Moderate	Moderate	High		High		Very High (PGD)
Anomaly Detection Rate (%)	98.90	98.70	99.40		99.20		74.2 (FGSM); 70.1 (PGD)
Anomaly Score Range	0.31–0.74	0.28–0.77	0.45–0.98		0.40–0.97		0.62–0.93 (FGSM); 0.58–0.90 (PGD)

deviations and temporal drift that is evident in QAC-GAN leads to more precise anomaly boundary formation, especially in high-camouflage situations that are difficult for classical discriminators to handle purely classical discriminators. Third is the comparison of QAC-GAN with adversarial attack baselines, including FGSM and PGD, which are routinely used to benchmark the limits of model robustness in machine learning to evaluate the magnitude of QAC-GAN’s advantage. The most recent adversarial attacks cataloged in the 2025 literature demonstrate markedly poorer results, averaging F1 scores of 79.8% to 82.4% with under 75% success in anomaly detection and overall weak performance in the loss of training stability, frequent collapse of the discriminators, and high levels of gradient attack susceptibility. The results echo earlier efforts to show that adversarial training models are more susceptible to the non-zero generalization gap problem and demonstrate a shift in their behavior toward the base to increasing levels of high-dimensional feature distortion.

In the same evaluation context, the QAC-GAN is also the only model that continues to outperform its counterparts and shows remarkable robustness to adversarial perturbations and contrived high-camouflage embeddings. The combination of different aspects is likely the reason for this quality, which includes the variational quantum circuits’ non-linear feature transformations, the geometric AIO penalty that keeps the generator and the discriminator within stable angular manifolds, and the TET mechanism that ensures the model’s resistance to changes in the time distribution. This combination gives the model a theoretical and practical advantage over classical systems. Benchmarking results in Table 5 prove that the Quantum AIO-Chameleon GAN proposal is not just classically competitive, but is also the most robust and has the highest detection fidelity for adversarial intrusion detection systems. Such results indicate that the hybrid quantum-geometric adversarial systems are likely the most advanced systems for the analysis of cybersecurity in dynamic and complex environments with the potential for threats, camouflage manipulation, and adversarial behaviour.

## 5 Conclusion

This study introduces QAC-GAN as a hybrid adversarial-geometric-temporal framework for detecting polymorphic and camouflage-enabled cyber threats in cybersecurity and cyber-physical system contexts. By integrating Quantum Variational Adversarial Learning (QVAL), Angle-of-Incidence Optimization (AIO), and Temporal Evolution Tracking (TET), the framework focuses on adversarial evolution relative to a stable benign baseline rather than universal drift detection. Experimental results and ablation analyses demonstrate that each component contributes complementary strengths, improving robustness against stealthy and gradually mutating attacks within the defined problem scope.

## Acknowledgments

The authors would like to express their sincere gratitude to the Institute of Computing and Informatics, Technical University of Mombasa, for the institutional support, guidance, and resources provided throughout the research process.

## Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this work.

## References

1. Su, L., Wu, M., and Li, F. (2025). A variational quantum circuits architecture with multi-head attention for chaotic time series prediction. *Complex and Intelligent Systems*, 11, Article 347. <https://doi.org/10.1007/s40747-025-01973>
2. Iqbal, K. (2025). Advancements and challenges in the development of generative adversarial networks. *Journal (Springer)*. <https://doi.org/10.1007/s44354-025-00007-w>
3. Cao, Y., Xiang, H., Zhang, H., et al. (2025). Anomaly Detection Based on Isolation Mechanisms: A Survey. *Machine Intelligence Research*, 22, 849–865. <https://doi.org/10.1007/s11633-025-1554-4>
4. García-Beni, J., Paparelle, I., Parigi, V., Giorgi, G. L., Soriano, M. C., and Zambrini, R. (2025). Quantum machine learning via continuous-variable cluster states and teleportation. *EPJ Quantum Technology*, 12, Article 63. <https://doi.org/10.1140/epjqt/s40507-025-00352-3>
5. Van de Wetering, J. (2025). Optimal compilation of parametrised quantum circuits. *Quantum Journal*. <https://doi.org/10.22331/q-2025-08-27-1828>
6. Wolf, E., and Windisch, T. (2025). A method to benchmark high-dimensional process drift detection. *Journal of Intelligent Manufacturing*. <https://doi.org/10.1007/s10845-025-02590-9>
7. Sabeel, U., Heydari, S. S., El-Khatib, K., and Elgazzar, K. (2023). Unknown, atypical and polymorphic network intrusion detection: A systematic survey. *IEEE Transactions on Network and Service Management*. <https://doi.org/10.1109/TNSM.2023.3298533>
8. Xing, Z., Mehmood, O., and Smith, W. A. P. (2025). Unsupervised anomaly detection with a temporal continuation, confidence-aware VAE-GAN. *Pattern Recognition*, 166, 111699. <https://doi.org/10.1016/j.patcog.2025.111699>
9. Kong, S., et al. (2024/2025). GRAND: GAN-based software runtime anomaly detection. *Neural Networks (Elsevier)* (2025). <https://doi.org/10.1016/j.neunet.2023.10.036>
10. Jabbar, A., Jianjun, H., Jabbar, M. K., and colleagues. (2025). Fusion-aware quantum variational autoencoder for brain–heart signal modeling in mental-health applications. *Journal of King Saud University — Computer and Information Sciences*, 37, 268. <https://doi.org/10.1007/s44443-025-00264-3>
11. Dong, F., et al. (2025). Cross-Frequency Aware Network for Camouflaged Object Detection. *Computer Vision and Image Understanding / Elsevier*. <https://doi.org/10.1016/j.cviu.2025.1016776>
12. RLi, Z., Yan, Y., Wang, X., et al. (2025). A survey of deep learning for industrial visual anomaly detection. *Artificial Intelligence Review*, 58, 279. <https://doi.org/10.1007/s10462-025-11287-7>
13. Duffy, C., Hassanshahi, M., Jastrzębski, M., and colleagues. (2025). Unsupervised beyond-standard-model event discovery at the LHC with a novel quantum autoencoder. *Quantum Machine Intelligence*, 7, 41. <https://doi.org/10.1007/s42484-025-00258-4>
14. Ma, L., Zhang, X., Wang, K., et al. (2025). Generative adversarial message passing-based anomaly detection. *Journal of King Saud University — Computer and Information Sciences*, 37(5). <https://doi.org/10.1007/s44443-025-00021-6>
15. García-Beni, J., et al. (2025). Time-series quantum reservoir computing with cluster states (related). *EPJ Quantum Tech.* <https://doi.org/10.1140/epjqt/s40507-025-00352-3>
16. Hammadia, T., Saber, A. M., and Kundur, D. (2025). Quantum variational circuits for detection of false data injection. In *2025 IEEE Industry Applications Society Annual Meeting (IAS)*. <https://doi.org/10.1109/IAS62731.2025.11061524>
17. iang, X. Q., et al. (2025). Dual flow reverse distillation for unsupervised anomaly detection. *Digital Signal Processing (Elsevier)*. <https://doi.org/10.1016/j.dsp.2025.105258>