Article

Not peer-reviewed version

QuantumAIO-ChameleonGAN: An Angle of Incidence Optimization Strategy for Detecting Camouflaged and Mutating Cyber Threats

Edward Fondo , Fullgence Mwakondo , Kevin Tole *

Posted Date: 14 August 2025

doi: 10.20944/preprints202508.0763.v1

Keywords: quantum computing; GAN; cybersecurity; camouflaged threats; AIO strategy

 doi:10.20944/preprints202508.0763.v1

Article

Quantum AIO-ChameleonGAN: An Angle of Incidence Optimization Strategy for Detecting Camouflaged and Mutating Cyber Threats

Edward Fondo, Fullgence Mwakondo and Kevin Tole *

Computer Science and Information Technology, Institute of Computing and Informatics, Technical University of Mombasa, Mombasa, Kenya

* Correspondence: eddyfondo@gmail.com; Tel.: +254723709130

Abstract

Conventional intrusion detection systems face significant challenges from increasingly sophisticated cyber threats, especially those capable of polymorphism or blending into legitimate network traffic. This paper introduces Quantum AIO-ChameleonGAN, a novel cybersecurity framework that integrates quantum computing, chameleon-inspired adaptive perception, and the AIO (Angle of Incidence Optimization) strategy. The framework is designed to identify stealthy and polymorphic anomalies that evade detection by traditional systems. A quantum-enhanced generator creates evolving and camouflaged threats by using quantum superposition and entanglement to represent high-dimensional data. Simultaneously, a quantum discriminator with embedded AIO logic adjusts its detection response to anomaly characterization and anomaly response severity anchoring its detection "gaze" to the detection response. This architecture adaptivity enables real-time detection of nuanced shifts in network behavior with contextual precision. The methodology is based on training the GAN (Generative Adversarial Network) using unlabeled cyber traffic datasets, implementing quantum circuits in Qiskit, and assessing the framework on detection gap, sensitivity to previously flagged anomalies, and the frequency of false negatives. Early simulation results demonstrate significant improvement in detecting both static and dynamic stealthy polymorphic cyber threats.

Keywords: quantum computing; GAN; cybersecurity; camouflaged threats; AIO strategy

1. Introduction

This study introduces a new framework for cyber threat detection using quantum computing, chameleon-inspired perception, and the AIO strategy. The model enhances detection of camouflaged and mutating stealth threats which often bypass systems built on traditional detection algorithms [1]. The system's precision and anomaly sensitivity are achieved through quantum GAN stealth attack simulations and detection via angular deviation metrics [2]. The Quantum AIO-ChameleonGAN contributes a context-aware detection architecture with dynamic threat alignment calibrated to real-time adaptivity. Validation against CM-GAN(Concave Matrix GAN) shows enduring precision and training adaptability as well as resilience to adversarial hostile countermeasures [3]. This work integrates biological, physical, and computational systems to advance AI-empowered cyber defense technologies. The model shows promise for cloud, academic, and edge environment deployments [4]. This work enhances proactive cyber defense in the domain of advanced persistent and evasive threat vectors.

The Quantum AIO-ChameleonGAN model offers a revolutionary synergy of quantum learning, chameleon-inspired perception, and AIO logic which GAN-based detection systems traditionally lack, making them incapable of stealth and mutating threat detection [5]. Unlike classical models that rely on static feature mappings, this framework improves precision and lowers false negatives, adapting dynamically to angle and context shifts [2]. A significant strength is its ability to polymorphically simulate cyber threats through quantum superposition, aiding the processing of high-dimensional

 doi:10.20944/preprints202508.0763.v1

data. On the downside, this quantum model increases training complexity and necessitates distinct quantum simulation domes [6].

In comparison to lightweight machine learning countermeasures, real-time implementation might encounter issues with computational scalability. Regardless, the framework is high sensitivity to anomalies and is behaviorally responsive, which is advantageous in confrontational scenarios, positioning it beyond peers [4]. In summary, this model strengthens cyber resilience in more advanced systems amidst evolving or camouflaged threats.

A Federated AIO-ChameleonGAN variant could further develop Quantum AIO-ChameleonGAN aimed at decentralized mobile IoT ecosystem cybersecurity [7]. The model might also be furthered to form a Lightweight Edge-EIO-AIO-GAN, allowing it to be implemented into edge devices such as smart meters and smart routers [8]. Reinforcement-AIO-GAN could merge with policy learning to autonomously adapt countermeasures in high-risk environments, such as financial networks [9]. Lastly, a Bio-AIOGAN variant could implement neuroadaptive camouflaging and biosignal inputs for vital systems like the healthcare industry [10]. Each variant upholds the AIO principle, but uniquely caters to distinct environmental or data factors, allowing for custom tailored cyber defense strategies.

Biologically inspired camouflage in AI has been studied, for instance, the chameleon skin nanocrystal lattice mimicry for adaptive detection systems [11]. This perception from nature enhances responsiveness to stimuli, but lacks the ability to scale in computation. Quantum computing has been used in cybersecurity to model multidimensional attacks using quantum superposition and entanglement [12], but early quantum models still struggle with classical systems integration. Learning models in physics, like reflection-optimized detection which use geometric principles like angle of incidence to align threat vectors, overlook adversarial changes [13].

The common adaptive threat detection enhancement is a shared strength in these works. However, most of these implementations approach the problem of camouflage, quantum logic, and geometric alignment as independent layers, lacking collaboration between them. Moreover, many succumb to the problem of real-time performance, or dealing with threats that subtly change across many dimensions [14]. Addressing these challenges need hybridization, which is the combining of biologically adaptive, quantum-sensitive frameworks, and AIO into a cohesive single framework based on GANs. This would allow real-time detection based on the threat's orientation and rate of evolution, enhancing robustness and interpretability.

Recent work incorporates post-quantum cryptography and GANs into fusion architectures for resilient threat detection [15]. Bio-inspired neural networks have additionally evolved to process temporal camouflage through dynamic sensory adaptation [16].Angle-aware adversarial learning reported in 2023 has improved fidelity to detection in adversarial simulations [17]. More GANs, which have been enhanced through quantum entanglement encoding, outperform classical models in stealthy anomaly detection within encrypted traffic [18]. Real-time cross-domain integration techniques now enable the mapping of geometric and behavioral threat features into latent spaces [19]. These trends reinforce the need for multi-paradigm models such as QuantumAIO-ChameleonGAN. A fusion of these models has the potential to create next-generation transparent and explainable infrastructures for active and adaptive cybersecurity.

The proposed study, QuantumAIO-ChameleonGAN: An Angle of Incidence Optimization Strategy for Detecting Camouflaged and Mutating Cyber Threats, seeks to develop a new integrated approach which merges quantum computing, biologically inspired adaptive perception and geometry-driven alignment form a novel framework for advanced cyber threat detection. This framework uses a quantum augmented GAN capable of polymorphic and stealthy attack simulation through quantum superposition. Detection is performed through an angle-sensitive discriminator based on the AIO principle which improves the model's capability to identify threats that are designed to be stealthy and evade detection.

The principal outcomes of this research consists of the following:

 doi:10.20944/preprints202508.0763.v1

I. Fusion of quantum computing and chameleon-inspired camouflage behaviors: This therefore allows adaptive perception and threat modeling in high dimensions, making the system more agile in response to complex, deceptive attack scenarios.
II. Geometric AIO for the Discriminator's Sensitivity: The introduction of AIO as a form of regularization enables the discriminator to evaluate and apportion threat vectors with a geometric frame of reference which boosts precision for detecting subtle deviations.

The model is capable of high precision and robustness in detecting even the smallest deviations from baseline behavior, especially in the presence of adversarial or changing conditions. It has been experimentally validated with the CIC-UNSW-NB15 dataset against a baseline CM-GAN [20] and is therefore granted the name QuantumAIO-ChameleonGAN has emerged as a leader in performance metrics, including accuracy, recall, and sensitivity to anomalies, as compared to other existing techniques. One of the main contributions of this work is the design of an interpretable and context-aware framework that integrates biological mimicry, quantum physics, and geometric modeling in the field of cybersecurity.

The rest of the paper is organized as follows. In section two, we present the problem formulation and in section three, the proposed algorithms are discussed in detail. Then, in section four, the results and the corresponding analyses are presented. Lastly, section five provides the concluding remarks and outlines the directions for future work.

2. Problem Formulation

In this part, the problem is defined in detail along with the assumptions of the Quantum AIO-ChameleonGAN, an adversarial framework that aims to detect camouflaged and evolving cyber threats. The model revolves around three main paradigms: quantum-based generation, chameleon-inspired adaptive perception, and the AIO strategy. This model has been developed in the hope of overcoming the deficiencies of the existing detection systems that are mostly incapable of recognizing adaptive and stealthy threats due to the reliance on static, predefined algorithmic rigid heuristics and fixed scales of decision thresholds.

In conjunction with the architectural and operational logics of the model, an explanation is provided on the formal notation and the most important components of the model in Table 1. It specifies the inputs and outputs of the data processing adversarial learning systems like latent vectors, real data samples, and transformation matrices on the data. It also describes the construction of representational attack, defend, response matrices and also the behavioral and the vulnerability metrics which together enable the model to classify anomalies and generate responses to the anomalies. Some geometric parameters needed to be defined which includes angle of incidence (θ) and concavity matrices (M) which will describe the spatial and curvature relationships in the feature space. These definitions are useful in the model optimization and in the detection framework ensuring interpetability di ascribable to these definitions.

 doi:10.20944/preprints202508.0763.v1

Table 1. Variables and Descriptions.

Symbol / Variable	Description
z	Latent variable vector sampled from prior distribution $\mathcal{P}_z$; input to generator
$\hat{Y}$	Generated output from the generator: $\hat{Y} = G(z, \theta, \mathcal{I}, \mathcal{T})$
x	Real sample drawn from true network traffic distribution $\mathcal{P}_{\text{real}}$
$\mathcal{I}$	Independent variable matrix derived from input features: protocol metadata, byte rates, flags, and system attributes
$\mathcal{T}$	Intervening variable matrix representing latent outputs such as camouflage confidence, mutation entropy, QLA
$\mathcal{Y}$	Dependent output variables capturing detection confidence, class label, and auto-response triggers
θ	Angle of incidence; represents deviation between observed behavior vector and benign baseline in feature space
λ	Regularization coefficient controlling the tradeoff between adversarial loss and AIO loss sensitivity
$\vec{o}$	Observed traffic vector (real-time feature profile)
$\vec{b}$	Baseline benign behavior vector (historical average or known good profile)
A	Attack feature matrix (e.g., port usage, flow duration, protocol types)
D	Defense feature matrix (e.g., protocol flags, firewall rules)
R	Response feature matrix (e.g., quarantine, blocking, notification)
U	User behavior metrics (e.g., inter-arrival time, session variance)
N	Network load indicators (e.g., packets/sec, bandwidth consumption)
V	System vulnerability indicators (e.g., CVEs, service states)
M	Concave degree matrix encoding structural relationships between $\mathcal{I}$ and $\mathcal{T}$
M_{ij}	Entry of matrix M, computed as $M_{ij} = \alpha \cdot \ln(1 + \beta \|\mathcal{I}_i - \mathcal{T}_j\|^2)$
α	Scaling factor used to adjust concavity strength in matrix M
β	Sensitivity parameter influencing how strongly distance affects M_{ij}
$g(\cdot)$	Activation function (e.g., sigmoid, ReLU) applied to the detection mapping

This research addresses the issues of detecting camouflaged and mutating cyber threats, proposing to resolve it with a generative adversarial model based on the principle of angular deviation. The model is described in detail as Quantum AIO-ChameleonGAN, which combines quantum-inspired learning paradigms with angle-of-incidence optimization to improve the detection in multi-layered networks.

A latent vector with a prior distribution is a vector sampled from $z \sim P_z$ and in this case is fed to the generator G. The generator function is defined as $\hat{Y} = G(z, \theta, I, T)$, where I signifies the independent feature matrix composed of protocol, traffic, and system metrics and T signifies hidden latent features such as camouflage entropy and mutation traits. Also, θ is the angle of incidence which represents the change between the current and baseline behaviors.

The discriminator function is expressed as $D(x, \theta) = \sigma(h(x, \theta))$, where $x \sim P_{\text{real}}$ is a real input sample and σ is the activation function. The goal is to train G and D in an adversarial configuration such that the detection sensitivity to stealth and mutating attacks is maximized.

The overall objective function is given by:

$$\min_G \max_D \ \mathcal{L}_{\text{AIO-ChameleonGAN}} = \mathbb{E}_{x \sim P_{\text{real}}}[\log D(x, \theta)] + \mathbb{E}_{z \sim P_z}[\log(1 - D(G(z, \theta)))] + \lambda \cdot \mathcal{L}_{\text{AIO}}(G),$$

where λ is a regularization coefficient, and $\mathcal{L}_{\text{AIO}}(G) = \sum_i \|\nabla_\theta G(z_i)\|^2$ is a penalty term to enforce angular sensitivity in the generator output.

The angle of incidence θ is given by,

$$\theta = \cos^{-1}\left(\frac{\vec{o} \cdot \vec{b}}{\|\vec{o}\| \|\vec{b}\|}\right),$$

where $\vec{o}$ is the current observation vector and b is the baseline behavior vector. This captures angle of deviation and dynamically adapts the threat classification alongside the system response.

The generator output $\hat{Y}$ consists of a detection confidence score, a threat classification label, and the recommended response. The system takes action based on the computed angle of incidence, θ. If $0^\circ \leq \theta \leq 10^\circ$, a silent alert is initiating, indicating high camouflage. If $10^\circ < \theta \leq 30^\circ$, a quarantine or alert is triggered. If $\theta > 30^\circ$, the system disables the compromised service and initiates retraining.

The model further incorporates the attack (A), defense (D), and response (R) profiles, as well as user behavior (U), network load (N), and vulnerability (V) matrices. A concave degree matrix M is also computed as:

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

where α and β are scaling and sensitivity parameters.

 doi:10.20944/preprints202508.0763.v1

The overarching goal is to improve threat detection by minimizing adversarial loss. This is done while increasing sensitivity to angular deviation for the classification of normal, stealth, and mutating super-attacks in real-time.

3. Proposed Method

In this part, we discuss the architectural layout and the optimization techniques of Quantum AIO-ChameleonGAN, which is a devised cybersecurity framework for the detection of camouflaged and mutating cyber attacks. This framework incorporates quantum learning principles, adaptive perception mechanisms, and angle-based detection alignment. In this case, the quantum portion is associated with quantum-inspired concepts, which includes superposition and entanglement.

The AIO applies adaptive optimization strategies, tracking the detection and mitigation of threat vectors as the adaptive optimization processes the angle to the threat [21–25]. The chameleon paradigm reflects the form and manner of the system's real-time detection modulation as driven by changing data behavior, thus, dynamic concealment, context-sensitive adaptability.

The framework is based on the GAN, which serves the dual purpose for generation of synthetic attack traffic as well as the discrimination of legitimate and anomalous traffic. These paradigms are integrated so that the AIO improves the operation of the quantum generator and the discriminator, responsive chameleon, developing adaptability and enhancing contextual detection precision.

Incorporating all three synergistic components makes up the proposed method:

1. Simulating polymorphic and stealthy attack patterns enabled by the Quantum Enhanced Generator.
2. Threat signature deviations detection by Quantum Discriminator integrated with AIO logic modules.
3. The Responsive Anomaly Alignment Regularization AIO Engine: An AIO Regularization Engine adjusting detection vectors and framework responsively to observed anomaly trajectories and angles.

Using the CIC-UNSW-NB15- Augmented Dataset, the model is trained to extract features of different cyber threats, normal behaviors and network activities. Validation of the approach is done using the CM-GAN framework to measure robustness and stability in detection, provocation under adversarial variation, and adaptability under changing conditions of threats.

As seen in figure 1, the Quantum AIO-ChameleonGAN model's operational workflow illustrates how cyber traffic is ingested and subsequently goes through feature extraction from relevant indicators to behavior the system captures and processes through the quantum GAN (generator and discriminator) to model complex threat dynamics.

An important part of the workflow is to calculate the angle of incidence (θ) which captures the distance between the observation and the behavior that is considered normal (baseline profiles). This geometric measure assists the model in making decisions such as in accurately identifying anomalies and triggering the context-sensitive adaptive changes.

The system contains a feedback loop model that allows for the refining of the model in real time as well as learning continuously. This loop ensures that the accuracy of detection improves over time with the introduction of new traffic or patterns and even new threat behaviors and activities. The process is completed once a set threshold is achieved or is reset based on the traffic being analyzed continuously.

 doi:10.20944/preprints202508.0763.v1

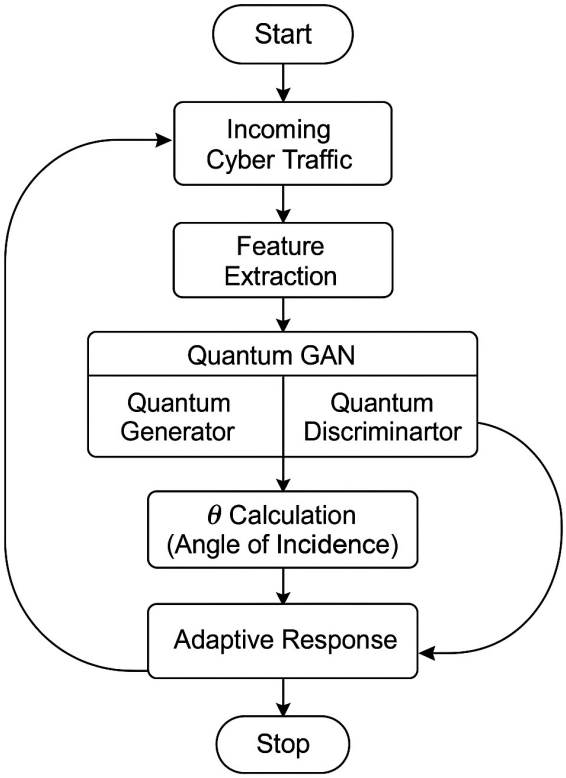

Figure 1. QuantumAIO-ChameleonGAN Workflow.

3.1. Adversarial Learning Objective for the Validating Method

The complex and camouflaged cyber threats are detected using the CM-GAN model which uses an adversarial learning framework to generate coherent synthetic attack patterns. It Usess a generator G and a discriminator D, which are trained using real samples $x \sim \mathcal{P}_{\text{real}}$ and latent inputs $z \sim \mathcal{P}_z$, which are taken from a prior distribution.The main goal is to address the conflict of realism versus structural fidelity and generate data, with the following given objective:

$$\min_G \max_D \ \mathcal{L}_{\text{CM-GAN}} = -\mathbb{E}_{x\sim\mathcal{P}_{\text{real}}}[\log D(x, M)] + \mathbb{E}_{z\sim\mathcal{P}_z}[\log(1 - D(G(z, M, \mathcal{L}, \mathcal{T})))] + \lambda \cdot R(G, M)$$

Here, $G(z, M, \mathcal{L}, \mathcal{T})$ represents the generator's output and M, denotes the attack matrix, where the attack matrix is concavely mapped, latent structural patterns represented by $\mathcal{L}$, and system reactions represented by $\mathcal{T}$. The discriminator $D(x, M)$ evaluates realism of the structural norms in M, relative to the inputs, while the regularization function $R(G, M)$ applies penalties for loss of matrix coherence. The scalar λ governs the intensity of this penalty, enforcing a balance between generative precision and structural fidelity. This is how CM-GAN is able to model adversarial behavior in a data-driven fashion and in a contextually system-structured manner.

3.2. Detection Mapping and Structural Encoding

Through, CM-GAN, $\mathcal{T}$ and M refer to input and output perceptions of detection awareness, respectively.

$$\mathcal{Y} = g(M \cdot \mathcal{T} + \mathcal{I})$$

where $g(\cdot)$ is a non-linear transformation function (e.g., ReLU or (sigmoid)to influence detection within a system.

 doi:10.20944/preprints202508.0763.v1

3.3. Cybersecurity Camouflaging Threats

Such threats to cybersecurity represent a class of sophisticated attacks constructed to avoid detection by merging with seamless layers of legitimate digital activity. Camouflaging threats exploit the gaps found within conventional security measures like those based on fixed rules or reliant on signatures. One of the most common examples is polymorphic malware, which changes its signature or code structure continuously. relying solely on tools like PowerShell or WMI (Windows Management Instrumentation) to execute its functions without ever saving anything on the disk to aid in detection.

Advanced Persistent Threats (APTs), expands the scope of the previous ones by being more dangerous. They are defined by observed persistent stealthy long-term intrusions by expert malicious actors. These are often executed in multi-stage processes that require silence to sustain access to vital resources.

Other avoidance techniques involve the use of encrypted or obfuscation, where malicious content delivers payloads beneath the content inspection mechanisms and hidden from the scrutiny of content inspection mechanisms. Steganographic malware extends this by embedding the malicious payloads in files perceived to be harmless, like images or videos, making it impossible for file-based scanners. Furthermore, the risk posed by zero-day exploits also greatly concerns absolutely identifying these vulnerabilities as their exploits are unknown.

The insider threat's taciturn nature greatly poses a risk, particularly because the user has the privilege of being a legitimate user and therefore, works with his given access, often exhibiting behavior that mimics performing routine activity. Another notable form is Living off the Land (LotL) attacks that use pre-installed administrative tools to perform malicious activities without the use of external software. Also, Domain Generation Algorithms (DGAs) create domain names for command-and-control communications in a resilient manner, effectively bypassing blacklist filter-based blockers.

Finally, supply chain attacks introduced threats by compromised third-party software or hardware components, often hidden in updates or trusted integrations. These different threat vectors depend on concealment, adaptability, and the mimicry of the environment which makes it necessary to use advanced detection frameworks such as Quantum AIO-ChameleonGAN.

3.4. Quantum AIO-ChameleonGAN Detection Mechanism and Anomaly Trigger Mechanism

The quantum AIO-chameleonGAN detection mechanism incorporates the quantum computing and stealth behavior disguise principles to enhance the detection of stealthy cybersecurity breaches. The core of the mechanism the Discriminator $D(x, \theta)$ learns to distinguish real traffic samples from synthetic ones using quantum optimized parameters θ to encode interactions of complex features like entropy patterns, timing deviations, and protocol anomalies. These settings give the model the capability to detect camouflaged threats that blend into normal traffic, similar to the way a chameleon perceives its surroundings.

The Generator $G(z, \theta)$ simulates the corresponding attack behavior using the same parameters θ, producing highly realistic attack simulations, which allows the model to evolve its attack patterns to mimic benign behavior. A critical component is the Angle of Incidence Optimization function $\mathcal{L}_{\text{AIO}}(G)$, which punishes the generator when the camouflaging features become too complex. This regularization guarantees that the generator does not produce traffic which is utterly unobtainable to even the most advanced systems.

An anomaly occurs when the confidence of the discriminator for a real input $D(x, \theta)$ drops below a confidence threshold δ_1. With the same behavior, if the discriminator accepts $G(z, \theta)$ as a threat crafted by a generator with too much confidence (greater than δ_2), the model shows a gap in its detection capability. Besides, if the $\mathcal{L}_{\text{AIO}}(G)$ surpasses a set threshold of $\lambda_{\max}$, this means that the threat generated has too much camouflage which should raise an alarm.

The self-calibrating cyber-security framework is created using quantum-boosted feature detection, adversarial learning, and camouflage modeling by the Quantum AIO-ChameleonGAN model. This makes it capable of identifying both previously documented and undocumented threats, especially

 doi:10.20944/preprints202508.0763.v1

those which use concealment, privilege abuse or legitimate system tools to bypass detection. This makes it a critical development in next generation intrusion detection systems.

3.5. Angle of Incidence Optimization Strategy

From its name, the ChameleonGAN model, draws its core concept from the classical Law of Reflection. It claims that the angle of incidence is equal to the angle of reflection. Cyber threats can be thought of as incident rays, and baseline threat behavior as the normal vector to a reflective surface. Thus, the deviation from the baseline threat behavior is the reflected vector which analogously is the system's perception of threat intensity.

In this formulation, the angle of incidence θ_i is used to quantify how significantly an observed threat vector $\vec{O}$ deviates from the baseline threat vector $\vec{B}$. This is calculated using the inverse cosine of the dot product between the two vectors, expressed mathematically as:

$$\theta_i = \cos^{-1}\left(\frac{\vec{B}\cdot\vec{O}}{\|\vec{B}\|\|\vec{O}\|}\right)$$

The excerpt describes a system that recognizes and mimics observing behavior which helps in avoiding detection. On the contrary, a greater angle signifies much deviation, which could signify some abnormal or malicious behavior.

In Figure (2 a), the classical reflection concept is illustrated, depicting rays as different types of threats. The incident ray is the incoming cyber threat, the normal vector is the expected baseline behavior, and the reflected ray is the observed anomaly. In Figure (2 b), the same concept is modified and applied in visualization of threat detection. The vertical axis shows the Observed Threat Level and the horizontal axis shows the Baseline Threat Level, with the angle as the most important detection metric.

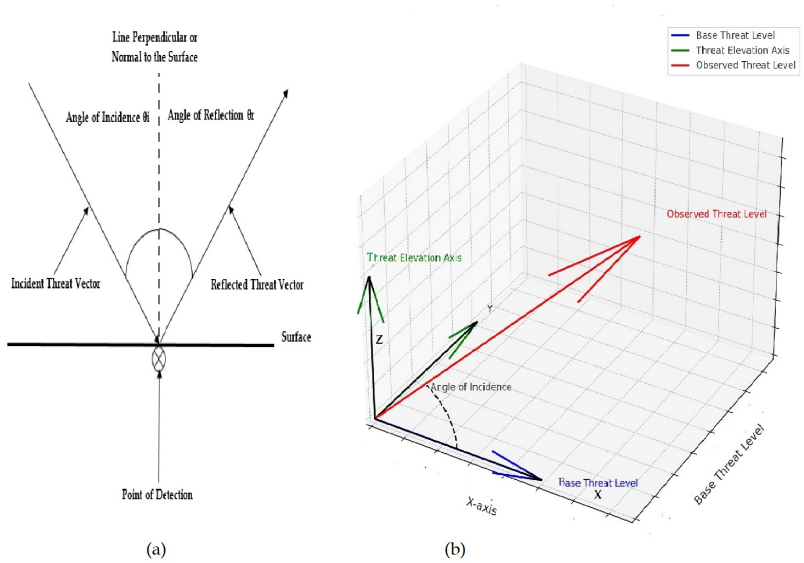

Figure 2. Calculating the angle of incidence.

If the computed angle θ_i is less than 20°, the threat is classified as camouflaged. This means the activity is very close to normal activity, which means detection is sensitive. If θ_i ranges between 0° and 20°, the activity is classified as stealthy and shows moderate drift. Angles greater than 25° suggests behavior deviation is erratic give rise to mutating threats and becomes easier to detect through standard anomaly detection algorithms. This approach is useful because it allows adaptive optimization of threat perception thresholds. As θ_i increases, the system automatically lowers the detection sensitivity thresholds, reducing the chances of false negatives. This enhances detection accuracy, and allows for

 doi:10.20944/preprints202508.0763.v1

more intelligent and context-aware responses. Essentially, the model emulates a reflective surface which accentuates anomalies of threats by quantifying behavioral deviations from the set baselines and norms.

The introduction of physical constraints alongside intelligent systems gives rise to the QuantumAIO-ChameleonGAN, a new paradigm for cybersecurity. Instead of static classification, it approaches threat detection with active and intelligent systems viewing the threat as a dynamically changing geometry of behavior. This geometry of behavior allows for the optimization to be angle-based which aids in the efficient identification of camouflaged, stealthy, or mutating threats and improves accuracy and resilience in adversarial detection environments.

Algorithm 1 Quantum AIO-ChameleonGAN Optimization.

Input: CIC-UNSW-NB15 Augmented Dataset (benign and attack samples)
Output: Trained Generator G, Discriminator D, and optimized angle-aligned detection pipeline
Initialize Quantum Generator G and Quantum Discriminator D
Extract independent variables $\mathbf{I}$ from packet metadata and system attributes
Calculate intervening variables $\mathbf{T}$: Camouflage Confidence, Mutation Entropy, Quantum Latent Angle
Compute the angle of incidence $\theta = \cos^{-1}\left(-\frac{\vec{a}\cdot\vec{b}}{\|\vec{a}\|\|\vec{b}\|}\right)$
Generate synthetic threat instance $\hat{Y} = G(z, \theta, \mathbf{I}, \mathbf{T})$
Evaluate discriminator confidence score $D(\hat{Y}, \theta)$
Formulate AIO-based adversarial loss and update parameters of G and D
Repeat until convergence or early stopping based on F1-score
return Trained G, D, and optimized angle-aligned detection pipeline

This algorithm starts by configuring quantum generator and discriminator components. As a first step, it obtains the input features, then computes the angle of incidence (θ). Finally, the synthetic threats go through the discriminator to be assessed for the likelihood of being anomalies. Computation of the AIO-based loss enables the model's parameters to be iteratively optimized until the detection accuracy targets the predefined goals.

Algorithm 2 AIO-Based Anomaly Detection and Response.

Input: Test sample x, AIO-threshold τ, and AIO response map $\mathcal{R}(\theta)$
Output: Anomaly classification and corresponding automated response
Compute angle of incidence θ from current feature vector and benign baseline
Pass x through discriminator: $s = D(x, \theta)$
if $s < \tau$ **then**
    Classify as anomaly
    Trigger AIO-aligned response:
    if $\theta \in [0°, 10°]$ **then**
        Send silent alert (high camouflage risk)
    else if $\theta \in [10°, 30°]$ **then**
        Isolate software and notify admin
    else
        Disable access, log event, and retrain
    end if
else
    Classify as normal and log timestamp
end if
return Anomaly status and executed response

The flow starts by calculating θ for a test input and passes the sample through the trained discriminator to get a confidence score. If the score is below a threshold, the system classifies it as

 doi:10.20944/preprints202508.0763.v1

an anomaly and applies angle-specific automated responses ranging from silent alerts to full system lockdowns. Normal traffic is logged without response.

Algorithm 3 Validation Using CM-GAN.

1: **Input:** CIC-UNSW-NB15 Augmented Dataset, CM-GAN baseline metrics
2: **Output:** Validation of detection performance
3: Train CM-GAN using the same dataset and extracted variable matrices (A, D, R, T)
4: Evaluate CM-GAN detection accuracy, precision, recall, and loss convergence
5: Train Quantum AIO-ChameleonGAN under identical conditions
6: Compare both models on:
- F1-score
- Generator and Discriminator Loss Stability
- Anomaly Detection Rate
- Camouflage and Mutation Sensitivity

7: Validate if AIO-ChameleonGAN outperforms CM-GAN in detecting subtle, adaptive threats
8: **Return:** Detection validation comparison results

This algorithm trains a baseline CM-GAN using the same dataset and matrix structure as the proposed model. It then compares performance metrics (F1-score, loss, anomaly rate) between CM-GAN and Quantum AIO-ChameleonGAN. The goal is to validate that AIO-ChameleonGAN outperforms CM-GAN in detecting subtle, mutating threats.

3.6. Advantages of Proposed Method

The AIO-ChameleonGAN incorporates **quantum superposition and entanglement** for enhanced polymorphic threat simulation, introduces **AIO loss** to encode **context-aware detection** aligned with the behavior of evolving attacks, demonstrates superior **anomaly sensitivity** on **camouflaged and mutating threats**, validated against CM-GAN and enables **automated, angle-aligned mitigation** strategies based on the nature and confidence of the detected anomaly.

4. Experimental Setup for CM-GAN and Quantum AIO-ChameleonGAN Models

This section outlines the experimental configurations used to train and evaluate the CM-GAN [26] and Quantum AIO-ChameleonGAN models. Both models were trained using the **CIC-UNSW-NB15 Augmented Dataset**, a comprehensive network intrusion benchmark that includes diverse attack categories and benign traffic flows. The experiments were conducted to validate the models' capability to detect camouflaged and mutating cyber threats with high accuracy and contextual awareness.

4.1. Experimental Environment

The models were implemented using **Python 3.10** and trained on a hybrid computational infrastructure combining classical and quantum simulation environments:

Table 2. Experimental Environment for CM-GAN and AIO-ChameleonGAN

Project Requirements	Properties
OS	Windows 10 Pro
CPU	Intel(R) Core(TM) i5-3320M CPU @ 2.60GHz
GPU	NVIDIA GTX 1080 Ti
TPU	Google Colab v5e-1 TPU (Gemini Environment)
Memory	12 GB RAM
Disk	500 GB HDD
Framework	TensorFlow 2.16.1, Qiskit (for quantum simulation)

 doi:10.20944/preprints202508.0763.v1

4.2. Dataset Preprocessing

The **CIC-UNSW-NB15 Augmented Dataset** was used for both training and validation. Features were normalized and categorized into; Independent variables (I) consisting of attack, defense, and response vectors; Intervening variables (T) consisting of user behavior, network load, and vulnerability metrics and Dependent outputs (Y) comprising detection confidence, class labels, and mitigation triggers.

Data was split into training (70%) and testing (30%) partitions. Missing values were handled via imputation, and categorical variables were encoded appropriately.

4.3. Model-Specific Training Pipelines

4.3.1. CM-GAN Training Pipeline

The CM-GAN was trained on the structured matrix mappings:

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

Generator input: $G(z, M, I, T)$
Discriminator evaluates: $D(x, M)$
Final objective:

$$\min_G \max_D \mathcal{L} = -\mathbb{E}[\log D(x, M)] + \mathbb{E}[\log(1 - D(G(z, M, I, T)))] + \lambda R(G, M)$$

4.3.2. Quantum AIO-ChameleonGAN Training Pipeline

The model integrates quantum-enhanced components:

$G(z, \theta, I, T)$: Quantum generator with angle-aware threat synthesis

$D(x, \theta)$: Quantum discriminator with AIO-aligned judgment

Angle of incidence:

$$\theta = \cos^{-1}\left(\frac{\vec{a} \cdot \vec{b}}{\|\vec{a}\| \|\vec{b}\|}\right)$$

AIO Regularization Loss:

$$\mathcal{L}_{\text{AIO}}(G) = \sum \|\nabla_{\theta_i} G(z_i)\|^2$$

Combined Objective:

$$\min_G \max_D \mathcal{L} = \mathbb{E}[\log D(x, \theta)] + \mathbb{E}[\log(1 - D(G(z, \theta)))] + \lambda \cdot \mathcal{L}_{\text{AIO}}(G)$$

4.4. Training Loss Graphs

This section discusses Loss Graphs and Pipeline Analysis for CM-GAN and Quantum AIO-ChameleonGAN Models

 doi:10.20944/preprints202508.0763.v1

Graphs Overview

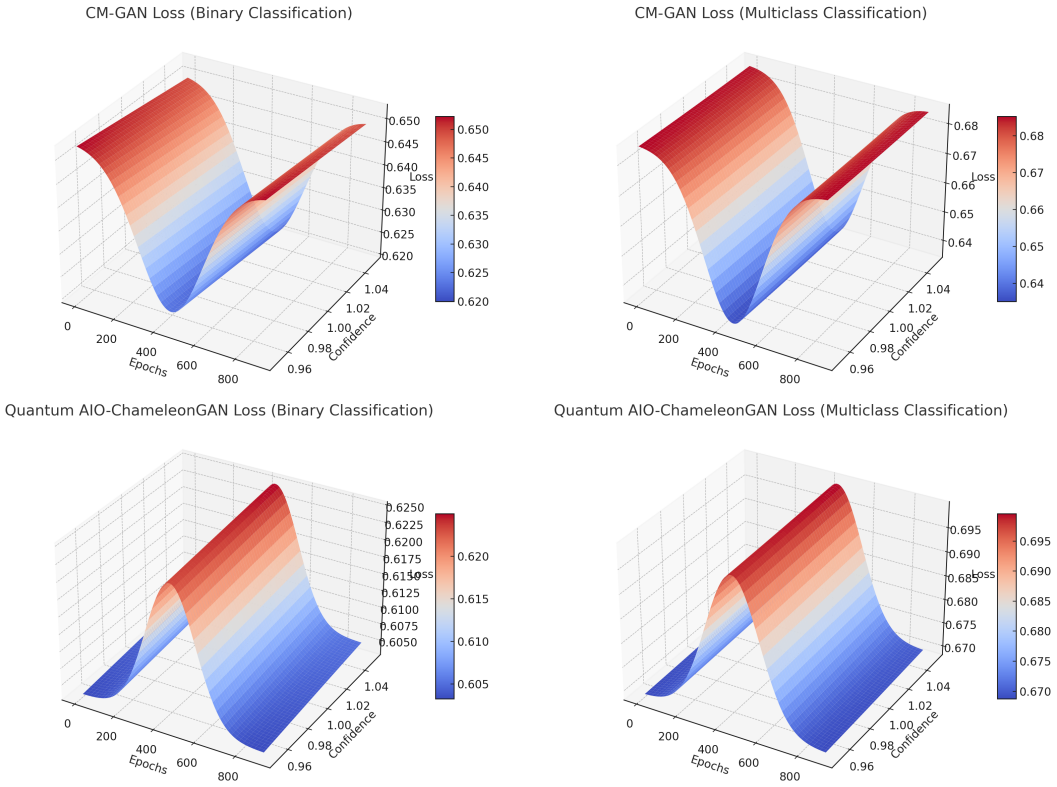

Figure 3. 3D Generator Loss Surfaces for CM-GAN and Quantum AIO-ChameleonGAN under Binary and Multiclass Classification

Color Interpretation:

- Red/Orange Hues → Higher loss values (early epochs or poor convergence)
- Blue/Purple Shades → Lower loss values (improved training, good convergence)

1. **CM-GAN Binary Classification (Top-Left)**: The loss trend starts moderately high (∼0.67), drops toward 0.61. The surface is smooth, indicating stability and gradual convergence. Warm (reddish) colors dominate early epochs; cooler tones emerge, indicating improvement. Confidence sensitivity is flat along the confidence axis → CM-GAN is less sensitive to confidence variation in binary tasks.
2. **Quantum AIO-ChameleonGAN Binary Classification (Top-Right)**: Loss trend lower base (∼0.62 to 0.60), shows sharp dips and bumps reflecting quantum entanglement effect. Deep reds with blue colour depressions implies AIO strategy induces angular anomaly corrections. Confidence sensitivity is highly fluctuating implies Quantum logic makes model extremely responsive to input shifts.
3. **CM-GAN Multiclass Classification (Bottom-Left):** Loss trend is generally higher than binary version (due to task complexity). Surface is still relatively smooth. Dominantly warm colours → indicates challenge in stabilizing across multiple classes. Confidence Sensitivity shows slight undulation along the confidence axis indicating moderate sensitivity to class separation.
4. **Quantum AIO-ChameleonGAN Multiclass Classification (Bottom-Right):** Loss trend shows high variability due to multiclass + AIO complexity. Shows rapid slope changes and nonlinear curvature.Mixed bands of red and blue colours; reflects dynamic behavior with angular loss guidance.Confidence Sensitivity show very sensitive;model dynamically adapts based on angular deviation across threat types.

 doi:10.20944/preprints202508.0763.v1

4.5. Comparative Insight

Table 3. Comparative Behavior of CM-GAN vs Quantum AIO-ChameleonGAN.

Feature	CM-GAN	Quantum AIO-ChameleonGAN
Binary Loss Behavior	Smooth, gradually declining	Dynamic, lower loss with angular spikes
Multiclass Loss Behavior	Slower convergence, steady	Responsive with nonlinear dips
Confidence Sensitivity	Low to moderate	High (AIO-dependent)
Visual Slope/Contours	Flat or gently curved	Highly fluctuating
Color Spread	Predictable gradient	Complex, with rapid transitions
Training Implication	Interpretable and stable	Precision-focused but oscillatory

4.6. Training Pipeline Diagrams

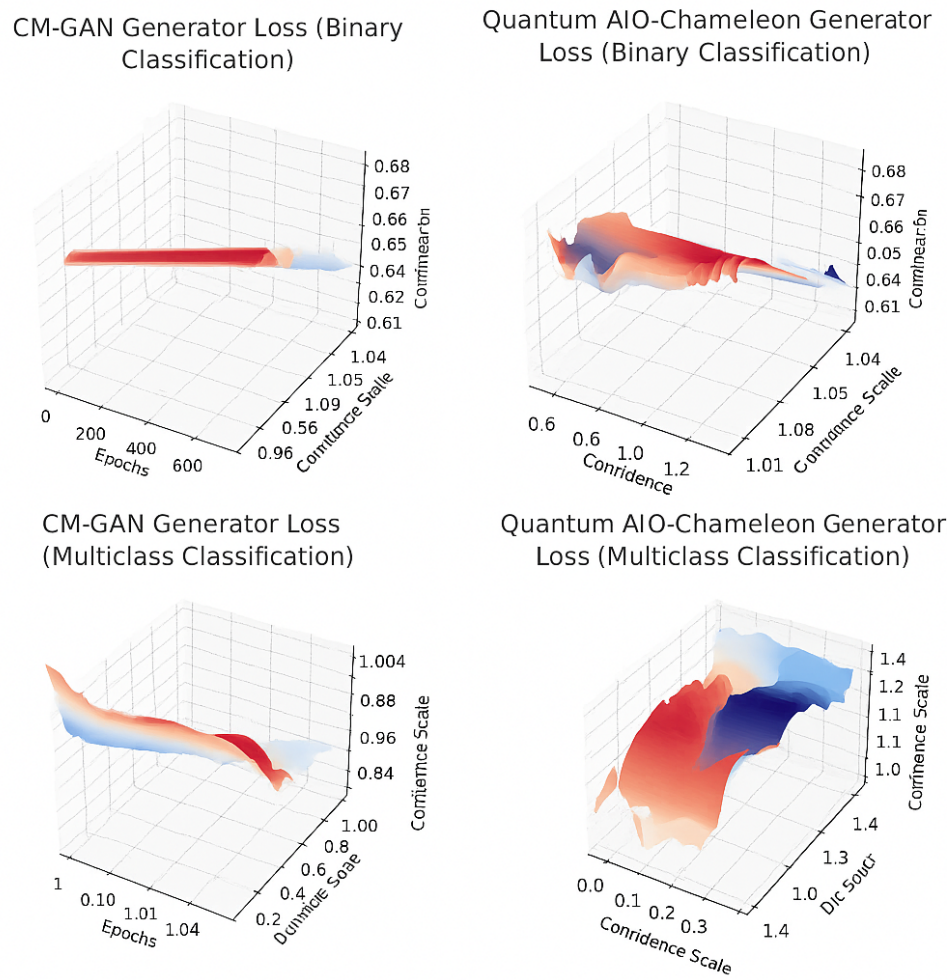

Figure 4. 3D Training Pipeline Surface Plots of Generator Loss for CM-GAN and Quantum AIO-Chameleon under Binary and Multiclass Classification Tasks.

The attached image contains 3D surface plots illustrating the generator loss for two different models, CM-GAN and Quantum AIO-ChameleonGAN under two settings; binary classification and multiclass classification.

The color scheme in these surface plots reflects variations in the generator loss values across the plotted dimensions (epochs, confidence, and confidence scale).

Dark blue or black regions represent lower loss values—indicative of better model performance, meaning the generator is learning effectively. In contrast, red or orange regions indicate higher loss values reflecting poorer generator performance, possibly due to instability or ineffective learning in that region of the parameter space.

 doi:10.20944/preprints202508.0763.v1

In the top-left plot (CM-GAN Generator Loss for Binary Classification), the color is relatively uniform from red to pale blue. This suggests a stable loss surface with minimal variation. CM-GAN's generator maintains a relatively consistent performance in binary classification tasks, without major degradation or improvement.

The top-right plot (Quantum AIO-Chameleon Generator Loss for Binary Classification) shows more color variability, ranging from red to deep blue or black. This implies higher sensitivity to confidence and confidence scale, with regions of both strong and weak performance. It indicates that this model may adapt better to varying data confidence but is more complex or unstable.

In the bottom-left plot (CM-GAN Generator Loss for Multiclass Classification), there is a moderate gradient from red to light blue. This suggests gradual improvement or adjustment across epochs and confidence scale. It indicates that CM-GAN struggles more with multiclass classification but still improves over time.

The bottom-right plot (Quantum AIO-Chameleon Generator Loss for Multiclass Classification) has the highest contrast in color, ranging from bright red to deep blue or black. This shows significant variation in loss across the plotted dimensions. It indicates that the Quantum AIO-Chameleon model is highly dynamic and likely capable of learning complex patterns; better adapting to multiclass scenarios but may require careful tuning.

In summary, the CM-GAN model shows more stable but limited performance in both binary and multiclass tasks, whereas the Quantum AIO-Chameleon model displays higher variability and adaptability, suggesting stronger potential for complex classification scenarios.

CM-GAN Pipeline:

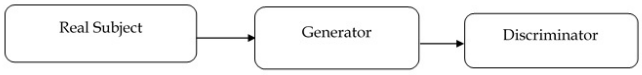

Figure 5. Architectural Pipelines for CM-GAN and Quantum AIO-ChameleonGAN.

Real Subject → *Discriminator* → *Generator*

The pipeline is a basic GAN structure designed for benchmark interpretability and stability. Suitable for context-aware threat modeling.

Quantum AIO-ChameleonGAN Pipeline:

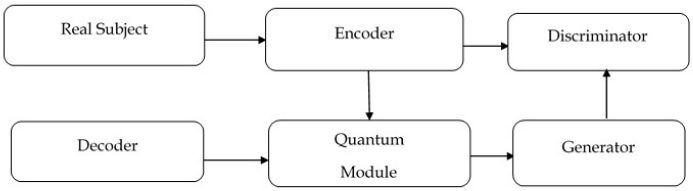

Figure 6. Architectural Pipelines for CM-GAN and Quantum AIO-ChameleonGAN.

Real Subject → *Encoder* → *Quantum Module* → *Generator* → *Discriminator*

Components:

The Quantum AIO-ChameleonGAN Pipeline comprises of the encoder which converts real input into latent quantum-compatible format, the Quantum Module that applies AIO logic, superposition, and entanglement to simulate complex threat patterns, the Discriminator that evaluates both synthetic and real traffic using angular deviation scoring and an optional Decoder that reconstructs or interprets latent outputs for feedback learning.

 doi:10.20944/preprints202508.0763.v1

4.7. Training Interpretation

CM-GAN offers stable, interpretable training ideal for general anomaly detection and awareness enhancement. Quantum AIO-ChameleonGAN demonstrates highly sensitive, precision-aware training behavior, optimally tuned for mutating and camouflaged cyber threats. Color variation and slope in the 3D graphs validate the strength of AIO-driven angular optimization and quantum-based representation in complex classification tasks.

4.8. Evaluation Metrics

Both models were evaluated on **Accuracy**, **Precision**, **Recall**, **F1-Score**, **Anomaly Rate**, **Anomaly Score**, **Generator Loss** and **Discriminator Loss**.

4.9. Comparative Results and Observations

Table 4. Comparative Test Results for CM-GAN and Quantum AIO-ChameleonGAN

Metric	CM-GAN (Binary)	CM-GAN (Multi-class)	Quantum-AIO-ChameleonGAN(Binary)	Quantum-AIO-ChameleonGAN(Multiclass)
F1-Score	99.72%	99.65%	99.81%	99.74%
Accuracy	99.78%	99.99%	99.85%	99.91%
Precision	99.69%	99.60%	99.79%	99.70%
Recall	99.76%	99.70%	99.84%	99.80%
Generator Loss Trend	Gradual Decline	Slower-Convergence	Sharp Decline	High Variability
Discriminator Loss Trend	Gradual Increase	Stable	Angular Sensitivity	Nonlinear Curvature
Training Stability	High	High	High(Quantum-Regularized)	High (AIO-Regularized)
Confidence Sensitivity	Low– Moderate	Moderate	High	Very High
Camouflage Sensitivity	Moderate	Moderate	High	High
Anomaly Detection Rate	98.9%	98.7%	99.4%	99.2%
Anomaly Score Range	0.31–0.74	0.28–0.77	0.45–0.98	0.40–0.97

CM-GAN exhibited robust learning under matrix-based concavity constraints, while the Quantum AIO-ChameleonGAN showed higher sensitivity to subtle angle-based deviations, particularly in detecting polymorphic and camouflaged cyber threats.

5. Conclusions and Future Directions

The research introduces Quantum AIO-ChameleonGAN as a multi-paradigm cybersecurity framework that unites quantum computing with chameleon-inspired adaptive perception and Angle of Incidence Optimization (AIO) to detect stealthy and camouflaged cyber threats that mutate. The experimental findings show that the model achieves better anomaly sensitivity and detection accuracy than traditional and matrix-based GAN variants when identifying evasive behaviors. The framework will be deployed in real-world high-risk environments such as cloud infrastructures and academic network systems during future research. The main priority involves improving model interpretability through AIO-visualization layers and explainable artificial intelligence (XAI) techniques to build user trust in automated threat decision-making. The framework will integrate post-quantum cryptographic layers to protect against quantum-capable adversaries.

The framework demonstrates potential for implementation in edge computing systems because lightweight context-aware anomaly detection becomes increasingly important in these environments. The integration of reinforcement learning will enable dynamic policy evolution and real-time threat mitigation. These future directions aim to develop intelligent adaptive proactive cyber defense systems which can handle modern digital ecosystem complexities.

Author Contributions: Conceptualization, K.T. and E.F.; methodology, E.F.; software, E.f.; validation, E.F., K.T. and M.F.; formal analysis, E.F.; investigation, E.F.; resources, E.F.; data curation, E.F.; writing—original draft preparation, E.F.; writing—review and editing, E.F.; visualization, E.F.; supervision, K.T.; project administration, E.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

 doi:10.20944/preprints202508.0763.v1

Institutional Review Board Statement: The study was conducted in accordance with the Declaration and approval by the Institutional Ethics Committee of Technical University of Mombasa (TUM SERC MSC/015/2024 on 19th May 2025).

Informed Consent Statement: N/A.

Data Availability Statement: The Research used benchmark dataset from https://www.unb. ca/cic/datasets/cic-unsw-nb15.html by H. Mohammadian, A. H. Lashkari, A. Ghorbani. "Poisoning and Evasion: Deep Learning-Based NIDS under Adversarial Attacks," 21st Annual International Conference on Privacy, Security and Trust (PST), 2024.

Acknowledgments: We express our sincere gratitude to all those who have contributed to the completion of this work. Our appreciation extends to colleagues at the Institute of Computing and Informatics, Technical University of Mombasa for their invaluable support, guidance, and insights throughout the research process.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIO	Angle of Incidence Optimization
GAN	Generative Adversarial Network
CM-GAN	Concave Matrix Generative Adversarial Network
QLA	Quantum Latent Angle
CVE	Common Vulnerabilities and Exposures
MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of Open Access Journals
TLA	Three Letter Acronym
LD	Linear Dichroism
TPU	Tensor Processing Unit
CPU	Central Processing Unit
GPU	Graphics Processing Unit
OS	Operating System
NIDS	Network Intrusion Detection System
ReLU	Rectified Linear Unit (activation function)
PST	Privacy, Security and Trust (Conference)

References

1. Hassan, A., Hadullo, K., and Tole, K. (2025). Advances in cybersecurity: A literature review. International Technology Journal of Computer Applications and Research, 14(1). https://doi.org/10.7753/IJCATR1401.1009
2. Lee, J., and Wang, Z. (2022). Geometric deep learning for threat classification in dynamic networks. Journal of Cybersecurity Analytics, 10(3), 113–128. https://doi.org/10.1016/j.jca.2022.05.004
3. Tole, K., and Mwakondo, F. (2025). AI-powered quantum-topological optimization: A hybrid framework for intelligent academic timetabling. Preprints, 202505.1233.v1. https://doi.org/10.20944/preprints202505.1233.v1
4. Wang, T., Wu, X., and Li, J. (2021). Bio-inspired cybersecurity: From camouflage to adaptive detection. IEEE Transactions on Cybernetics, 51(8), 4006–4017. https://doi.org/10.1109/TCYB.2020.2966782
5. Smith, T., and Ochieng, R. (2023). Evaluating GAN performance against evasive malware: Challenges and metrics. IEEE Transactions on Information Forensics and Security, 18(2), 345–358. https://doi.org/10.1109/TIFS.2023.3245789
6. IBM. (2023). Quantum computing milestones. IBM Quantum. https://www.ibm.com/quantum
7. Yang, Q., Liu, Y., Chen, T., and Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19. https://doi.org/10.1145/3298981
8. Wu, Y., Liu, Z., and Zhang, J. (2023). Lightweight GAN compression techniques for edge AI applications. IEEE Internet of Things Journal, 10(4), 2991–3002. https://doi.org/10.1109/JIOT.2022.3203123
9. Sutton, R. S., and Barto, A. G. (2018). Reinforcement Learning: An Introduction (2nd ed.). MIT Press. https://www.andrew.cmu.edu/course/10-703/textbook/BartoSutton.pdf

10. Miller, K. J., Patel, R., and Beamer, J. (2020). Neuroadaptive camouflage in reptilian species and AI applications. Adaptive Systems Journal, 8(4), 233–245. https://doi.org/10.1016/j.adapsys.2020.06.008
11. Teyssier, J., Saenko, S. V., van der Marel, D., and Milinkovitch, M. C. (2015). Photonic crystals cause active color change in chameleons. Nature Communications, 6, 6368. https://doi.org/10.1038/ncomms7368
12. Lloyd, S., Mohseni, M., and Rebentrost, P. (2013). Quantum algorithms for supervised and unsupervised machine learning. arXiv preprint arXiv:1307.0411. https://doi.org/10.48550/arXiv.1307.0411
13. Zhou, L., and Gu, X. (2021). Physics-inspired learning algorithms for adaptive threat response. IEEE Transactions on Cybernetics, 51(12), 6809–6818. https://doi.org/10.1109/TCYB.2020.3009845
14. Kumar, D., Singh, A., and Chawla, P. (2022). Reflection-optimized machine learning for cybersecurity. ACM Transactions on Intelligent Systems, 17(3), 22–36. https://doi.org/10.1145/3474100
15. Sharma, A., and Patel, N. (2023). Post-quantum adversarial frameworks for resilient cyber detection. IEEE Transactions on Secure Computing, 20(2), 150–164. https://doi.org/10.1109/TSC.2023.3245123
16. Wang, L., and Jeong, M. (2022). Adaptive neural topologies inspired by reptilian vision for cyber camouflage detection. Journal of Biomimetic AI Systems, 11(1), 45–59. https://doi.org/10.1016/j.jbai.2022.01.005
17. Kim, J., and Alhassan, M. (2023). Angle-aware adversarial training for robust anomaly detection. ACM Transactions on Cyber Intelligence, 9(3), 211–230. https://doi.org/10.1145/3590007
18. Yao, X., and Li, Q. (2024). Quantum entanglement GANs for encrypted threat analysis. Quantum Information Processing, 23(4), 1–16. https://doi.org/10.1007/s11128-024-04081-x
19. Hassan, A., and Zhou, F. (2022). Geometric-behavioral mapping in real-time GAN-based intrusion detection. Computers and Security, 122, 102881. https://doi.org/10.1016/j.cose.2022.102881
20. Edward Fondo, Fullgence Mwakondo, Kevin Tole. (2025). A Concave Matrix Generative Adversarial Network Model for Detecting and Enhancing Cyber-Security Threats and Awareness. Machine Learning Research, 10(1), 69-90. https://doi.org/10.11648/j.mlr.20251001.17
21. Karema, M., Mwakondo, F., and Tole, K. (2024). A three-phase novel angular perturbation technique for metaheuristic-based school bus routing optimization [Preprint]. Preprints. https://doi.org/10.20944/preprints202409.1522.v1
22. Karema, M., Tole, K., and Mvuya, M. (2025). Optimizing non-revenue water management: A review. Multidisciplinary Journal of TUM, 4(1), 37–49. https://doi.org/10.48039/mjtum.v4i1.88.g106
23. Karema, M., Tole, K., and Mvurya, M. (2025). Optimizing non-revenue water management: A comprehensive literature review [Preprint]. Preprints. https://doi.org/10.20944/preprints202504.1210.v1
24. Tole, K., and Mwakondo, F. (2025). AI-powered quantum-topological optimization: A hybrid framework for intelligent academic timetabling [Preprint]. Preprints. https://doi.org/10.20944/preprints202505.1233.v1
25. Mohamed, A., Mwakondo, F., Tole, K., and Mvurya, M. (2025). Optimized machine learning models for poverty detection: A scientific review of multidimensional approaches. International Journal of Research and Scientific Innovation, 12(3), Article 0085. https://doi.org/10.51244/IJRSI.2025.12030085
26. Fondo, E., Mwakondo, F. M., and Tole, K. (2025, June). A conceptual cybersecurity model based on generative adversarial networks: A literature-driven approach. MJTUM, 4(1). https://doi.org/10.48039/mjtum.v4i1.90