MILCOM 2025 - 2025 IEEE Military Communications Conference (MILCOM) | 979-8-3315-0292-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/MILCOM64451.2025.11310023

CONQUEST: CONtext-Aware QUantum-Inspired Intelligence for Espying AI-aided Cyberworm Security Threats in Military Networks

Simeon Okechukwu Ajakwe, Ihunanya Udodiri Ajakwe, Victor Ikenna Kanu, Jae Min Lee, Dong-Seong Kim
Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea
*ICT Convergence Research Centre Kumoh National Institute of Technology, Gumi, South Korea
(simeonajlove, ihunanya.ajakwe, kanuxavier)@gmail.com, ljmpaul@kumoh.ac.kr, dskim@kumoh.ac.kr

***Abstract*—Military networks face AI-aided cyberworms capable of adaptive, stealthy intrusions. We propose CONQUEST, a context-aware, quantum-inspired framework integrating Quantum-Inspired Particle Swarm Optimization (QPSO) for high-dimensional feature selection, LSTM-based Variational Autoencoder (LSTM-VAE) for anomaly detection, and operational context from the ACI-IoT dataset. QPSO reduces inference latency while preserving accuracy, and contextual analysis enhances detection precision. Evaluated on ACI-IoT, CONQUEST achieved a 97.5% detection rate with 0.8% false positives, surpassing signature, statistical, and conventional AI methods. These results demonstrate CONQUEST's potential for real-time, scalable defense in mission-critical military communications against advanced AI-driven cyber threats.**

***Index Terms*—Anomaly Detection, Artificial Intelligence, Cyber Security, Cyberworms, Context-Aware Computing, Military Networks, Quantum-Inspired Intelligence.**

I. INTRODUCTION

The increasing dependence of modern military operations on interconnected digital infrastructure has made military networks prime targets for sophisticated cyberattacks. Among these, AI-aided cyberworms pose a severe threat by autonomously identifying vulnerabilities, optimizing their spread, and mimicking legitimate traffic patterns—making them exceptionally difficult to detect [1]. Traditional signature-based intrusion detection systems fail against novel or polymorphic worms, while statistical anomaly detection methods often suffer high false positive rates [2], [3]. Even existing AI-based intrusion detection systems can be limited by scalability bottlenecks, reduced generalization in noisy environments, and vulnerability to adversarial manipulation [4].

This paper addresses these limitations by introducing CONQUEST—a CONtext-aware QUantum-inspired intelligence framework for detecting AI-aided cyberworms in military networks. The framework combines:

1) **Context-aware analysis** that integrates operational factors from the ACI-IoT dataset [5] to improve detection precision.
2) **Quantum-Inspired Particle Swarm Optimization (QPSO)** for efficient, high-dimensional feature selection, enhancing generalization and reducing inference latency [6], [7].
3) **LSTM-VAE anomaly detection** to identify subtle deviations from learned normal behavior.

Our key contributions are as follows:

- A novel integration of context-awareness, quantum-inspired optimization, and deep learning for AI-aided cyberworm detection in military networks.
- A systematic evaluation on the ACI-IoT dataset, achieving a 97.5% detection rate and 0.8% false positive rate, surpassing state-of-the-art baselines.
- An analysis of convex optimization methods (SGD, Adam, Newton-Hessian) to enhance anomaly detection performance and inference efficiency.

The synergy of contextual intelligence, quantum-inspired search, and deep learning enables CONQUEST to identify subtle deviations from normal behavior that might be indicative of an AI-aided worm, even when the worm attempts to blend in with legitimate traffic. The context-aware layer provides crucial insights into the operational environment, guiding the quantum-inspired search for relevant features and enhancing the accuracy of the AI-driven classification. To our knowledge, this is the first work to report IDS performance on the ACI-IoT dataset for AI-aided cyberworm detection. This underscores its novelty. The remainder of this paper reviews related cyberworm detection approaches in Section II, details the CONQUEST architecture and methodology in Section III, presents performance evaluation in Section IV, and concludes with future research directions in Section V.

II. RELATED WORKS

The detection of cyberworms has been a long-standing challenge in network security. Early approaches focused on signature-based detection, effective against known worms but failing to identify new or polymorphic variants [2]. Behavior-based detection methods analyze network traffic patterns and system activities to identify deviations from normal behavior [3]. However, these methods can be susceptible to high false positive rates and may struggle with sophisticated worms that

979-8-3315-0292-8/25/$31.00 ©2025 IEEE

Authorized licensed use limited to: KUMOH NATIONAL INSTITUTE OF TECHNOLOGY. Downloaded on April 09,2026 at 07:06:17 UTC from IEEE Xplore. Restrictions apply.

TABLE I: Comparative Analysis of Proposed Method with Related Works

Approach	Key Features	Limitations	Proposed CONQUEST System Advantage
Signature-based [2]	Relies on known attack signatures.	Fails to detect new or polymorphic cyberworm variants. Lack of adaptability to novel threats.	Integrates context-aware, quantum-inspired, and deep learning methods to detect novel, AI-aided threats.
Behavior-based [3]	Analyzes network traffic for deviations from normal behavior	Prone to false positives, fails against worms imitating normal behavior.	Quantum-inspired feature selection with context-aware analysis detects subtle threats accurately.
AI-based (General) [4]	Applies neural networks to anomaly detection. Offers improved adaptability.	Vulnerable to adversarial attacks. Don't capture subtle contextual cues crucial for detecting advanced threats.	Combines AI with context-awareness and quantum-inspired intelligence for a more robust and effective detection system.
Context-aware [8]	Considers contextual information to make informed security decisions	Lacks the adaptability and nuanced understanding required for sophisticated threats	Integrates contextual data with QPSO optimization & AI for enhanced threat analysis and risk scoring.
Quantum-inspired [6]	Utilizes quantum-inspired algorithms for optimization and ML tasks.	Their application is relatively unexplored for AI-aided cyberworm detection in military networks	Applies QPSO specifically for efficient feature selection in the context of cyberworm detection.
Proposed (CONQUEST)	Integrates context-aware computing, QPSO, and a recurrent neural network (LSTM-VAE).	The paper focuses on detection of AI-aided cyberworms with high-dimensional features	Achieves a high cyberworm detection rate (95.7%) and a minimal false positive rate (0.8%) by leveraging the synergy of its three key elements.

mimic legitimate behavior. The rise of AI has led to the development of AI-powered intrusion detection systems in military networks [9]. Machine learning (ML) algorithms, such as neural networks, have been applied to anomaly detection in network traffic [4]. While these methods offer improved adaptability, they can still be vulnerable to adversarial attacks and may not effectively capture the subtle contextual cues that are crucial for detecting advanced AI-aided threats.

Context-aware security enhances system accuracy and adaptability by integrating contextual factors like user roles, device locations, and environmental conditions, enabling more informed decisions [10]. Research in intrusion detection [8] shows that context can reduce false positives and detect advanced attacks more effectively. Meanwhile, quantum-inspired algorithms are valued for efficiently navigating large search spaces in optimization and machine learning. Approaches such as cost-aware quantum-inspired methods [11], particle swarm optimization [7], and neural networks [6] have achieved success in feature selection, classification, and anomaly detection. Yet, their application to cyberworm detection in military networks, especially against AI-driven threats, remains largely unexplored.

Recent research has highlighted the increasing threat of AI-powered cyberthreats and the need for more intelligent and adaptive security solutions [12]. This paper builds on the existing body of work by proposing a novel integration of context awareness and quantum-inspired intelligence to create a more robust and effective detection system. Thus, it addresses the unique challenges posed by AI-aided cyberworms in the critical domain of military networks by filling in the lapses in previous approaches, as captured in Table I.

III. PROPOSED SYSTEM DESIGN AND METHODOLOGY

The "quantum inspiration" in the proposed CONQUEST framework is realized through the Quantum-Inspired Particle Swarm Optimization (QPSO) technique employed in the Quantum-Inspired Feature Selection and Anomaly Detection (QIFA) module. Unlike classical PSO, where particle movement is governed by deterministic velocity and position updates, QPSO models each particle's state as a quantum wave function and determines its position probabilistically, guided by a global attractor ($gbest$) and a local attractor ($pbest$) as in equations (1)–(3) and captured in Table II. This probabilistic update mechanism, analogous to quantum superposition and tunneling effects, allows particles to explore the high-dimensional feature space more broadly, avoiding premature convergence and enhancing the discovery of optimal feature subsets from the augmented 83-dimensional network-context feature space. These optimal subsets improve the performance of the LSTM-VAE anomaly detector by increasing detection accuracy, lowering false positives, and boosting generalization against novel AI-aided cyberworms. The proposed CONQUEST comprises three main modules: (1) Context Acquisition and Processing (CAP), (2) Quantum-Inspired Feature Selection and Anomaly Detection (QIFA), and (3) Context-Aware Threat Analysis (CTA). The system's overall architecture is depicted in Fig. 1.

A. *The CAP Module*

This module is responsible for collecting and processing relevant contextual information from various sources within the military network. These sources may include network logs, user activity logs, system configurations, geographical locations of devices, and mission-specific data. The collected data is then pre-processed to extract relevant features and transformed into a suitable format for integration with the anomaly detection module.

Let $C = \{c_1, c_2, ..., c_m\}$ be the set of contextual attributes, where each c_i represents a specific contextual feature (e.g., user role, IP address, time of access). For each network event e_j, a context vector $v_j = (v_{j1}, v_{j2}, ..., v_{jm})$ is created, where v_{ji} is the value of the i-th contextual attribute for the j-th event. This context vector is then combined with the network traffic features $x_j = (x_{j1}, x_{j2}, ..., x_{jn})$ to form an augmented feature vector $z_j = (x_{j1}, ..., x_{jn}, v_{j1}, ..., v_{jm})$.

This study used the Army Cyber Institute (ACI) IoT Network Traffic Dataset developed by the Internet of Things Research Lab (IoTRL), which is accessible on IEEE Dataport [5]. It has over 1 million instances with 83 features and 12 types of cyberworms. The dataset is unique because it contains a dynamic mix of most IoT devices used in military networks,

Authorized licensed use limited to: KUMOH NATIONAL INSTITUTE OF TECHNOLOGY. Downloaded on April 09,2026 at 07:06:17 UTC from IEEE Xplore. Restrictions apply.

TABLE II: Classical PSO vs. Quantum-Inspired PSO in CONQUEST

Aspect	Classical PSO	QPSO in CONQUEST
Particle Movement	Deterministic updates	Probabilistic, wave function-based updates
Exploration Scope	Limited by velocity	Global search via tunneling-like behavior
Convergence Risk	Higher local optima risk	Reduced via diverse search patterns
Feature Subset Quality	May retain redundancy	Optimized for variance ratio and separability
Performance Impact	Moderate gains	95.7% detection, 0.8% false positives

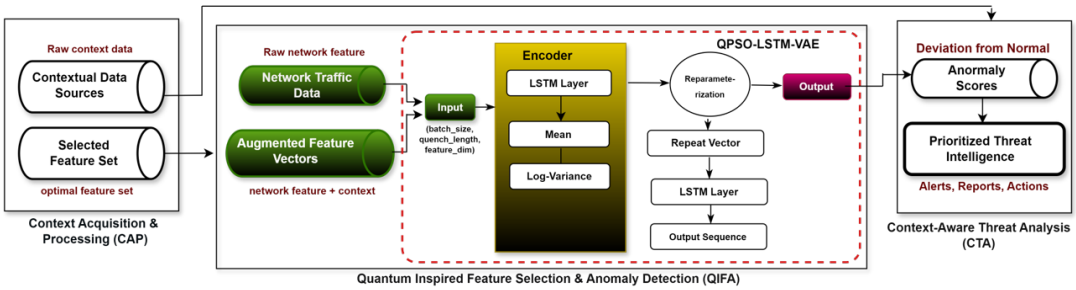

Fig. 1: Proposed CONQUEST System Architecture highlighting the various modules; CAP, QIFA, and CTA

multi-varied simulated environments, behavioral analysis characteristics applicable in adversarial scenarios, holistic security evaluation features, and multimodal data representativeness for device-specific context-awareness evaluation. Fig. 2 and Table III highlight the cyberworms, the context features, and the network features of the dataset.

TABLE III: ACI IoT Network and Contextual Data Features

Attribute	Feature Name	Description
Contextual	`Timestamp`	Exact time a network event occurred
	`Flow ID`	Identifier for network flow
	`Src IP, Port`	Source IP address, port
	`Idle`	Inactivity gaps between packets within a flow
	`Dst IP, Port`	Destination IP, port
Network	`Flow Duration`	Total time a network flow lasts
	Fwd Packet	Forward packet
	`Bwd Packet`	Backward packet
	`Flow IAT`	Flow Inter-Arrival Time
	`Subflow IAT`	Time between packets within each subflow
	`Protocol`	Indicates traffic type (TCP/UDP/ICMP)

*The features listed in Table III are just representatives of the 83 features.

B. Quantum-Inspired Feature Selection and Anomaly Detection (QIFA)

This module employs a quantum-inspired algorithm for efficient feature selection and anomaly detection. We utilize a QPSO approach to select the most relevant features from the augmented feature vector z_j for anomaly detection. In QPSO, each particle's state is represented by a wave function, and its position is probabilistically determined. The movement of each particle is guided by a global attractor $gbest$ and a local attractor $pbest$. The position $p_i(t)$ of the i-th particle at iteration t is updated according to equations (1) to (3):

$$\mathtt{mbest_i(t)} = \frac{\mathtt{pbest_i(t)} + \mathtt{gbest(t)}}{2}, \tag{1}$$

$$\mathtt{p_i(t+1)} = \mathtt{mbest_i(t)} \pm \beta |\mathtt{mbest_i(t)} - \mathtt{x_i(t)}| \ln(1/\mathtt{u_i}), \tag{2}$$

$$\mathtt{x_i(t+1)} = \mathtt{p_i(t+1)}, \tag{3}$$

where $\mathtt{x_i(t)}$ is the current position of the i-th particle, $\mathtt{mbest_i(t)}$ is the midpoint between $\mathtt{pbest_i(t)}$ and $\mathtt{gbest(t)}$, β is a contraction-expansion coefficient, and u_i is a random number uniformly distributed in $(0, 1)$.

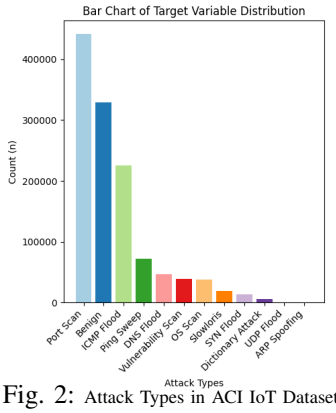

Fig. 2: Attack Types in ACI IoT Dataset

The dataset has 83 features, making it difficult to determine the number of features suitable for the QPSO algorithm. To determine the optimal number of features for the QPSO algorithm, we experimented with different values on the QPSO Sequential Variational Autoencoder (VAE), i.e., QPSO-LSTM-VAE pipelines. The Algorithm 1 summarizes the QPSO intelligence procedure for detecting abnormality in the context-aware feature selection.

We compared the results based on several metrics. The QPSO fitness score was applied to prevent model overfitting

Authorized licensed use limited to: KUMOH NATIONAL INSTITUTE OF TECHNOLOGY. Downloaded on April 09,2026 at 07:06:17 UTC from IEEE Xplore. Restrictions apply.

resulting from too many features. Then, we performed k-fold cross-validation on the entire model pipeline.

Algorithm 1: QPSO Flow for Cyberworm Detection

Function QPSO($data$, $labels$, $num\_particles(x)$, $iterations$, $num\_features\_to\_select$)
  $n\_features \leftarrow$ number of columns in $data$ (a)
  $particles \leftarrow$ array of size $x \times num\_features\_to\_select$
  $p\_best\_positions \leftarrow particles(y)$
  $p\_best\_fitnesses \leftarrow$ array of length $num\_particles$
  $i \leftarrow$ is the result of SimpleFitnessEvaly[i], data, labels
  $g\_best\_position \leftarrow y$[index of max value in $p\_best\_fitnesses$]
  $g\_best\_fitness \leftarrow$ max value in $p\_best\_fitnesses$
  for $iteration \leftarrow 1$ ***to*** $iterations$ **do**
    for $i \leftarrow 1$ ***to*** x **do**
      $\phi \leftarrow$ random number between 0 and 1
        $p \leftarrow y[i]$
        $x\_mean \leftarrow$ integer mean $[p\_best\_positions[i], g\_best\_position]$
        $new\_position \leftarrow$ array of zeros with the same shape as p
      for $j \leftarrow 1$ ***to*** *length of* p **do**
        if *random number between 0 and 1* $< \phi$ **then**
          $new\_position[j] \leftarrow x\_mean[j]$
        end
        else
          $new\_position[j] \leftarrow p[j]$
        end
      end

      $new\_position \leftarrow$ array of unique values from $new\_position$
      if *length of* $new\_position \neq num\_features\_to\_select$ **then**
        $remain\_features \leftarrow$ set of integers from 0 to $n\_features -$ 1 excluding the values in $new\_position$
        $new\_position \leftarrow$ concatenate $new\_position$ with remaining_features to reach length num_features_to_select
      end
      $y[i] \leftarrow new\_position$
      $now\_fitness \leftarrow SimpleFitnessEvaly[i], data, labels$
      if $now\_fitness > p\_best\_fitnesses[i]$ **then**
        $p\_best\_fitnesses[i] \leftarrow now\_fitness$
        $p\_best\_positions[i] \leftarrow y[i]$
      end
      if $current\_fitness > g\_best\_fitness$ **then**
        $g\_best\_fitness \leftarrow current\_fitness$
        $g\_best\_position \leftarrow y[i]$
      end
    end

end
  return $g\_best\_position$
Function SimpleFitnessEval($feature\_indices$, $data$, $labels$)
if $feature\_indices$ *is empty* **then**
  return 0
end
  $normal\_data \leftarrow data$[rows where $labels = 0$, columns in $feature\_indices$]
  $anomalous\_data \leftarrow data$[rows where $labels = 1$, columns in $feature\_indices$]
if $normal\_data$ *is empty or* $anomalous\_data$ *is empty* **then**
  return 0
end
  return $variance(anomalous\_data)/(variance(normal\_data) + 1e - 6)$

The SIMPLEFITNESSEVAL fitness function in the QPSO algorithm (Algorithm 1) assesses how well a chosen feature subset differentiates normal from anomalous network activity. Evaluation uses metrics such as classification accuracy, detection rate, and false positive rate on the trained subset. After selecting the optimal features, an anomaly detection model is trained in the reduced space. To detect subtle anomalies linked to AI-aided worms, we adopt a recurrent deep learning method—an LSTM-based Variational Autoencoder (VAE). In this design, LSTM layers replace dense layers in both encoder and decoder, as in Fig. 1. The VAE learns latent representations of normal traffic, and anomalies are flagged when reconstruction error exceeds a set threshold.

Let $f_\theta(z)$ be the encoder of the VAE, which maps the input feature vector z to a latent variable $h \sim \mathcal{N}(\mu(z), \sigma^2(z)I)$, where $\mu(z)$ and $\sigma(z)$ are the mean and standard deviation vectors, respectively, parameterized by θ. The decoder $g_\phi(h)$ maps the latent variable back to the reconstructed input $\hat{z}$. The VAE is trained to minimize the reconstruction loss and the Kullback-Leibler divergence between the learned latent distribution and a standard normal distribution. The reconstruction error for an input z is given by:

$$L(z, \hat{z}) = ||z - \hat{z}||^2$$

An anomaly score $S(z)$ is then calculated based on this reconstruction error. A high anomaly score indicates a significant deviation from the learned normal behavior. Convex optimization (stochastic gradient descent (SGD), Adam, Newton-Hessian) was applied at the reparameterization layer to avoid overfitting and encourage sparsity.

$$\min_{x \in \mathbb{R}^n} \quad f_0(x) \quad \text{subject to} \quad g_i(x) \leq 0, h_j(x) = 0 \tag{4}$$

where $f_0(x)$ is the convex objective function; $g_i(x)$ are convex inequality constraint functions; and $h_j(x)$ are affine equality constraint functions.

C. *CTA Response Module*

The QIFA module analyzes anomaly scores contextually, using operational details to gauge severity and impact within the military network. For example, anomalies in critical command systems during high-alert missions receive higher threat levels than similar issues in routine operations. This context-aware process may use rule-based reasoning, Bayesian networks, or other knowledge representation methods to infer the implications of detected anomalies based on the prevailing operational context.

Let A be the set of detected anomalies with associated anomaly scores $S(a)$ for each $a \in A$. Let $C(a)$ be the context vector associated with anomaly a. A context-aware risk score $R(a)$ is calculated for each anomaly based on its anomaly score and the contextual information:

$$R(a) = f(S(a), C(a)) \tag{5}$$

where f is a function that integrates the anomaly score and contextual factors to determine the risk level. This function can be defined based on expert knowledge and the specific security policies of the military network. Anomalies with high risk scores are prioritized for further investigation and response. The simulation was performed in a Python environment with the Tensorflow 2.x, Keras framework, and other libraries on a Windows OS with 48 GB of RAM/3.9 TB.

Authorized licensed use limited to: KUMOH NATIONAL INSTITUTE OF TECHNOLOGY. Downloaded on April 09,2026 at 07:06:17 UTC from IEEE Xplore. Restrictions apply.

TABLE IV: QPSO-LSTM-VAE Model Performance in detecting Genuine and Abnormal Network Traffic using Convex Optimizers

Model + Convex Optimization Method	Context-Aware Performance				No Context-Aware Performance			
	Acc. (%)	Prec. (%)	Rec. (%)	F1-Sc. (%)	Acc. (%)	Prec. (%)	Rec. (%)	F1-Sc. (%)
QPSO-LSTM-VAE+Newton-Hessian	93.62	98.11	95.33	96.70	93.93	98.45	95.33	96.87
QPSO-LSTM-VAE+ADAM	95.24	99.81	95.41	95.56	95.26	99.84	95.40	97.56
QPSO-LSTM-VAE+SGD	**95.20**	**99.77**	**95.41**	**97.54**	**95.24**	**99.82**	**95.40**	**97.56**

IV. RESULT DISCUSSION

To evaluate the performance of the proposed method, we conducted preliminary experiments using a simulated military network environment with AI-aided cyberworm attacks injected using standard AI evaluation metrics. The ACI-IoT dataset included normal network traffic patterns along with various types of worm activities. Thereafter, the performance of the context-aware quantum-inspired anomaly detection approach was compared with several existing methods as highlighted in section IV-A-IV-D.

A. *QPSO Cyber-Threat Espionage Performance*

Table IV highlights the performance of QPSO-LSTM-VAE in determining the presence of a cyberworm in a military network based on contextual information and network features. The result indicates that the QPSO-LSTM-VAE model with ADAM and SGD optimizers exhibited similar and better performance in verifying the presence of an intrusion using the network contextual information and without it. However, since the rational behaviour of a model is crucial, with a 97.54% F1-score value, the SGD is better. Also, comparing the model behaviour in "context-aware" and "no-context" shows that across all the metrics, the inclusion of contextual indicators improved the model performance. This is further validated by the confusion matrix in Fig. 4 (d) to (g) with minimal 91 misclassifications in the context-aware case versus 109 without context-awareness, achieved by QPSO-LSTM-VAE+SGD, and 88 versus 110 for QPSO-LSTM-VAE+ADAM.

B. *QPSO Context-Awareness Threat Evaluation I*

The values in Table V and Fig.3 IV (a)-(c) summarize the model cyberthreat risk assessment efficiency.

TABLE V: Model Context-Aware Threat Performance

Sn.	Model Optimization Method	Risk Score (%)
1.	QPSO-LSTM-VAE+Newton Hessian	35.21
2.	QPSO-LSTM-VAE+ADAM	39.91
3.	**QPSO-LSTM-VAE+SGD**	**65.62**

From equation (5), with a 65.62% score, the QPSO-LSTM-VAE+SGD exhibited a high $R(a)$ risk score, affirming its effectiveness in detecting and mitigating the occurrence of an anomaly in the network at any given state and scenario.

C. *QPSO Context-Aware Threat Evaluation II*

TABLE VI: Model Context-Aware Detection Capacity

Metrics	Acc.(%)	Prc.(%)	Rec.(%)	F1-Sc(%)	Loss(%)
Context-Aware	86.26	86.26	83.48	81.42	44.06
No Context-Aware	85.14	81.74	85.14	80.62	40.65

Table VI shows the performance of QPSO-LSTM-VAE+SGD in espying and mitigating all types of Cyberworms and other threats in the network. Across all metrics, contextual information aided the model's performance. intrusion. These results validate that the deployment of quantum-enhanced detection algorithms in the networks improves the resilience of these networks against external and internal attacks.

D. *Performance Evaluation III: SOTA & Related Methods*

The bar chart in Fig. 3 shows that QPSO-LSTM-VAE outperformed the SVM, RF, and MLP models in precision and F1-score but was marginally lower than MLP in recall.

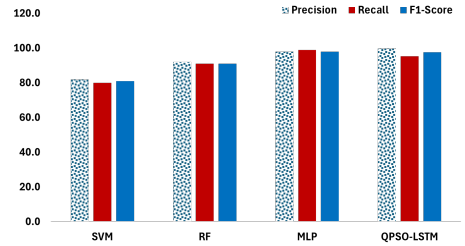

Fig. 3: Comparison of QPSO-LSTM-VAE performance with state-of-the-art models

In Table VII, both detection performance and estimated computational/training overhead are presented side-by-side.

TABLE VII: Performance Comparison with other Methods

Method	DR(%)	FPR(%)	ECO
Signature-based [2]	65.2	0.5	Low
Statistical Anomaly Detection [3]	78.5	3.2	Low-Medium
AI-based (No Context) [4]	85.1	2.1	Medium
Context-aware AI-based [8]	91.3	1.5	Medium-High
Proposed (QPSO-LSTM-VAE)	**97.5**	**0.8**	Medium (Inference)

DR = Detection Rate; FPR = False Positive Rate; ECO = Estimated Computational Overhead.

Our results show that while the proposed CONQUEST framework incurs a slightly higher initial training cost due to the QPSO optimization process, it achieves the highest detection rate and the lowest false positive rate among all compared approaches. More importantly, the reduced feature dimensionality achieved through QPSO significantly decreases inference latency, making the system well-suited for operational deployment in resource-constrained networks. This trade-off between initial training cost and long-term efficiency highlights the practicality and scalability of the proposed method over purely statistical or conventional AI-based approaches.

Unlike previous methods, CONQUEST achieved a substantial accuracy gain (+4.4% over context-aware AI, +10.6% over no-context AI, +30.5% over statistical methods). In terms of overhead impact, it has a slightly higher initial training cost due to the QPSO optimization. However, it has a lower inference cost due to reduced feature set and an optimized anomaly detection pipeline. The computational trade-off is justified by significant improvements in detection rate and

Authorized licensed use limited to: KUMOH NATIONAL INSTITUTE OF TECHNOLOGY. Downloaded on April 09,2026 at 07:06:17 UTC from IEEE Xplore. Restrictions apply.

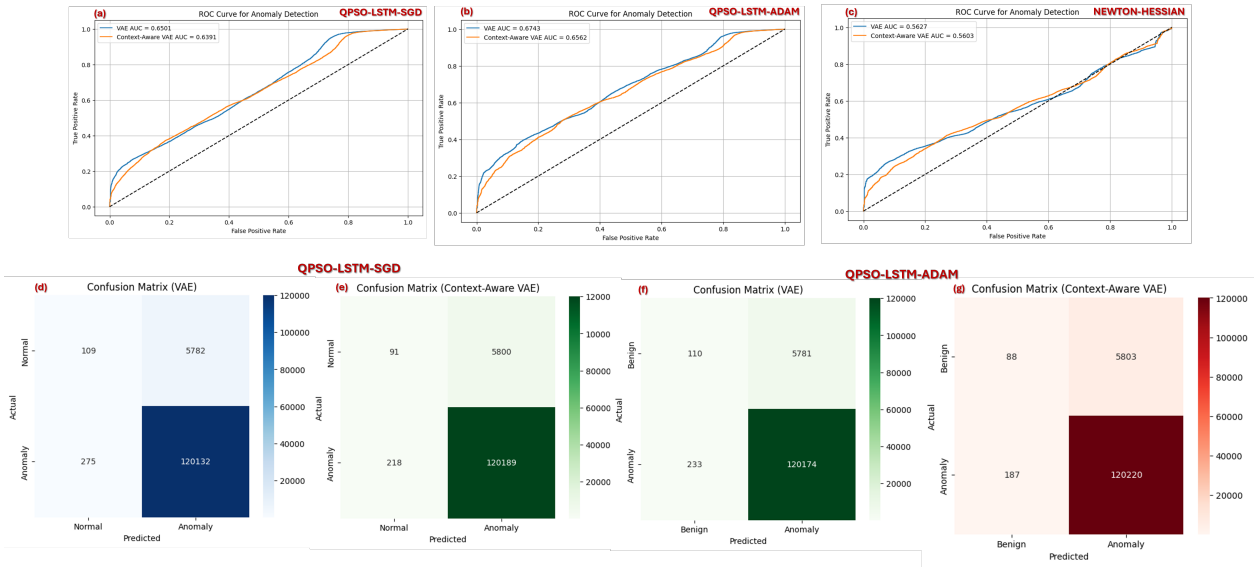

Fig. 4: Comparison of QPSO-LSTM-VAE performance across convex optimization methods: (a–c) show AUC-ROC using SGD, ADAM, and Newton-Hessian; (d–e) present SGD confusion matrices with/without context-aware detection; (f–g) display ADAM confusion matrices with/without context-aware cyberworm prediction in the networks, indicating that incorporating contextual information consistently reduces misclassifications and improves detection accuracy

reduction in false positives. These results validate that the integration of context-awareness and quantum-inspired intelligence offers a promising approach for enhancing the security of the networks against advanced AI-aided cyberworm threats, which are usually misclassified by classical AI models.

V. CONCLUSION

This paper presented CONQUEST, a context-aware, quantum-inspired framework for detecting AI-aided cyberworms in mission-critical military networks. By combining QPSO-based high-dimensional feature selection, LSTM-VAE anomaly detection, and contextual analysis from the ACI-IoT dataset, CONQUEST achieved a 97.5% detection rate with only 0.8% false positives, outperforming signature-based, statistical, and conventional AI methods. The reduced feature set significantly lowers inference latency, enabling deployment in resource-constrained, real-time defense scenarios. Future work will focus on large-scale scalability, integration with tactical and battlefield communication systems, rigorous evaluation under adversarial conditions, and the inclusion of explainable AI and zero-trust mechanisms to enhance operational trust, transparency, and policy compliance.

ACKNOWLEDGMENT

This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (50%) and by the Institute of Information & Communications Technology Planning & Evaluation (IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government(MSIT)(IITP-2025-RS-2020-II201612) (50%)

REFERENCES

[1] A. Khan, S. Ali, and M. Hussain, "The evolving threat of ai-powered cyber worms," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2023, pp. 1–6.

[2] A. Polamarasetti, "Research developments, trends and challenges on the rise of machine learning for detection and classification of malware," in *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*. IEEE, 2024, pp. 1–5.

[3] E. Landril, S. Valente, G. Andersen, and C. Schneider, "Ransomware detection through dynamic behavior-based profiling using real-time crypto-anomaly filtering," 2024.

[4] V. U. Ihekoronye, S. O. Ajakwe, J. M. Lee, and D.-S. Kim, "Droneguard: An explainable and efficient machine learning framework for intrusion detection in drone networks," *IEEE Internet of Things Journal*, 2024.

[5] N. Bastian, D. Bierbrauer, M. McKenzie, and E. Nack, "Aci iot network traffic dataset 2023," 2023. [Online]. Available: https://dx.doi.org/10.21227/qacj-3x32

[6] S.-Y. Kuo, J.-Y. Shen, C.-L. Liu, and Y.-H. Chou, "Hybrid quantum-inspired evolutionary neural networks for intrusion detection system," in *2024 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2024, pp. 2801–2806.

[7] P. Turaka and S. K. Panigrahy, "Chaotic adaptive particle swarm optimization and quantum-inspired genetic algorithm for robust feature selection in iot intrusion detection," in *2025 International Conference on Sustainable Energy Technologies and Computational Intelligence (SETCOM)*. IEEE, 2025, pp. 1–6.

[8] D. Micale, I. Matteucci, F. Fenzl, R. Rieke, and G. Patanè, "A context-aware on-board intrusion detection system for smart vehicles," *International Journal of Information Security*, vol. 23, no. 3, pp. 2203–2223, 2024.

[9] V. U. Ihekoronye, S. O. Ajakwe, D.-S. Kim, and J. M. Lee, "Hierarchical intrusion detection system for secured military drone network: A perspicacious approach," in *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*. IEEE, 2022, pp. 336–341.

[10] L.-M. Messmer, C. Reich, and D. O. Abdeslam, "Context-aware machine learning: a survey," in *Proceedings of the Future Technologies Conference*. Springer, 2024, pp. 252–272.

[11] M. Hussain, L.-F. Wei, A. Rehman, M. Ali, S. M. Waqas, and F. Abbas, "Cost-aware quantum-inspired genetic algorithm for workflow scheduling in hybrid clouds," *Journal of Parallel and Distributed Computing*, vol. 191, p. 104920, 2024.

[12] G. Waizel, "Bridging the ai divide: The evolving arms race between ai-driven cyber attacks and ai-powered cybersecurity defenses," in *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings*, vol. 1, 2024, pp. 141–156.

Authorized licensed use limited to: KUMOH NATIONAL INSTITUTE OF TECHNOLOGY. Downloaded on April 09,2026 at 07:06:17 UTC from IEEE Xplore. Restrictions apply.