ACCORD: Autonomous Cognitive Cyber Defense for Online Resilient Cloud-Enabled Digital Twin Systems

IEEE Publication Technology Department

***Abstract*—Cloud-enabled Digital Twin (CDT) systems are critical yet vulnerable to multi-layer cyberattacks. This paper presents Autonomous Cognitive Cyber Defense for Online Resilient CDT Systems (ACCORD), a four-phase framework for anomaly detection, forensic reasoning, and adaptive mitigation. Phase 1 preprocesses raw telemetry into mission-aligned representations; Phase 2 detects anomalies using spiking neural networks over temporal windows; Phase 3 constructs a knowledge graph to infer attack intent, root causes, and propagation paths; Phase 4 employs graph-augmented Deep Q-Networks for mission-aware response. ACCORD provides interpretable forensic insights, accurately identifies anomalies, and executes resilient mitigation with minimal disruption. ACCORD demonstrates consistently high and stable performance across evaluation scales, with minimal variability and near-optimal mean scores. The performance metrics confirm reliable alignment with ground truth under class imbalance. Compared to the strongest baseline, it achieves a 96.18% reduction in FNR, a 80.92% reduction in FPR, alongside broad improvements in precision, recall and asymmetric F-scores, highlighting robust, generalizable anomaly detection suitable for large-scale deployment.**

***Index Terms*—Anomaly Detection, Autonomous Cyber Defense, Cloud Digital Twin, Cognitive Forensics, Reinforcement Learning, Spiking Neural Networks.**

I. Introduction

DIGITAL Twin (DT) technology has emerged as a transformative paradigm for real-time monitoring, predictive maintenance, decision support, and operational optimization across manufacturing, healthcare, energy, transportation, and smart cities [1]. With nearly 86% of organizations deploying DTs in production [2], their strategic significance is rapidly growing. Cloud integration further enhances DT capabilities through scalability, accessibility, and collaborative analytics, but also increases cyber exposure, threatening data integrity, synchronization, and mission continuity across tightly coupled cyber–physical systems [3].

The global DT market is projected to grow from USD 35 billion in 2024 to USD 379 billion by 2034 [4], expanding the attack surface for adversarial manipulation, data poisoning, stealthy multi-stage intrusions, and model exploitation [5]. Cloud-enabled DTs (CDTs) face heightened risks due to high-dimensional, heterogeneous streaming telemetry and complex inter-layer dependencies. Existing solutions are largely reactive, focusing on anomaly detection without sufficient reasoning about propagation dynamics, adversarial uncertainty, or recovery strategies, highlighting the need for resilient, cognition-aware cyber defense frameworks.

A. Related Work

Related work on DT security and anomaly intelligence demonstrates consistent progress but largely concentrates on detection. Computational intelligence approaches such as DPFS-BM and DP-AlexNet aim to preserve privacy while enabling large-scale DT graph analytics and improving accuracy and efficiency [6]. DT-aware frameworks leverage the coupling between physical systems and virtual twins to enhance monitoring fidelity and fault diagnosis by combining model-based knowledge with data-driven learning [7]. Multimodal and edge–cloud pipelines further improve precision through heterogeneous telemetry fusion, supported by contrastive learning, attention mechanisms, and curriculum strategies for complex anomaly differentiation [8]–[11]. Widely adopted detectors such as One-Class SVM, Autoencoders, Variational Autoencoders, and clustering remain foundational across DT and IoT analytics [12]–[15]. Recent work promotes lightweight, low-latency pipelines and microservice abstractions for real-time operations [16], [17], while privacy and governance research exposes vulnerability to poisoning attacks and motivates federated and blockchain-based collaboration [18], [19]. However, these systems primarily optimize detection accuracy and latency, and provide limited support for resilience, propagation control, and autonomous mitigation.

B. Existing Limitations Addressed by ACCORD

Despite meaningful progress, several critical gaps remain. Detection pipelines often lack continuous adaptation and resilience in evolving adversarial environments [7], [8]. Multimodal and edge–cloud solutions frequently rely on static fusion rules that degrade under shifting data reliability [9], [11]. Privacy-preserving analytics such as DPFS-BM and DP-AlexNet protect sharing and training processes but do not address cascading failures or mission continuity [6]. Robustness studies expose susceptibility to poisoning and stealth attacks while offering limited real-time remediation [18]. Federated and blockchain-enabled frameworks improve trust management yet lack mechanisms for propagation-aware cyber defense and autonomous decision support [19]. These limitations underscore the need for cognition-enabled cyber defense capable of perceiving evolving risk, reasoning about dependencies, and sustaining resilient CDT operations.

Autonomous Cognitive Cyber Defense for Online Resilient Cloud-Enabled Digital Twin Systems (ACCORD) is

introduced as a unified cognitive framework that views cyber defense as a closed-loop process, integrating perception, inference, forensics, and mission-aware mitigation to safeguard CDT environments against dynamically evolving threats.

The main contributions are as follows:

- A cognition-demanding threat model that captures uncertainty, dependency-driven propagation, stealth behavior, and mission constraints across CDT layers.
- An autonomous cognitive defense architecture that unifies telemetry preprocessing, adaptive detection, forensics reasoning, and mission-aware mitigation in a continuous feedback loop.
- Propagation-aware mitigation strategies that preserve essential services while preventing cascading degradation across interconnected systems.
- Comprehensive experimental evaluation demonstrating improved robustness, reduced cascading risk, and enhanced recovery performance under complex adversarial scenarios.

C. Paper Organization

Section **??** introduces the system architecture, outlines the underlying threat model, and formally states the research problem. Section **??** presents the proposed DS-CTI framework, including detailed descriptions of CDT learning through decentralized intelligence (Section **??**) and the integrated self-healing mechanism (Section **??**). Section **??** elaborates on the operational workflow of the model and provides a comprehensive complexity analysis. Section **??** describes the experimental environment and reports extensive performance evaluations, comparative studies, and formal security analyses. Finally, Section **??** concludes the paper by summarizing key findings and outlining promising avenues for future research.

II. Problem Formulation

This section formalizes the problem in three parts. The *system model* (Section II-A) describes the CDT entities, their interactions, and observable anomalies. The *cognition-demanding threat model* (Section II-B) captures adaptive adversaries exploiting temporal, structural, and mission-level dependencies. The *problem definition and design goals* (Section II-C) specify the optimization objectives, constraints, and assumptions guiding the cognition-aware defense framework.

A. System Model

Consider an online Cloud-Enabled Digital Twin (CDT) ecosystem in which physical assets, sensors, and actuators are continuously mirrored by cloud-hosted digital counterparts. Let the set of DT applications be $\mathcal{A} = \{A_1, \ldots, A_Z\}$, deployed on virtual nodes $\mathcal{VN} = \{VN_1, \ldots, VN_Q\}$ and mapped onto physical nodes $\mathcal{PN} = \{PN_1, \ldots, PN_P\}$ under the control of the cloud platform $\mathcal{CP}$. Each application A_k executed on VN_j at PN_i generates multi-modal telemetry $\mathbf{x}_{ijk}(t) \in \mathbb{R}^d$ capturing network flows, resource usage, control feedback, and synchronization states. Continuous bidirectional communication ensures coherence between the physical environment and its digital representation. The clients operating these applications are represented by $\mathcal{C} = \{C_1, \ldots, C_n\}$, where a client may behave benignly (C^B) or act as an adversary while remaining concealed (C^m). Applications may become compromised due to injected code, configuration errors, or remote exploitation, and abnormal behavior can propagate across interdependent virtualized components.

Each application A_i is executed through a set of online CDT tasks $\mathbb{W} = \{\mathcal{W}_1, \ldots, \mathcal{W}_K\}$ managed by $\{C_1, \ldots, C_n\}$, forming a tightly coupled cyber–cloud environment in which security, performance, and synchronization are mutually dependent.

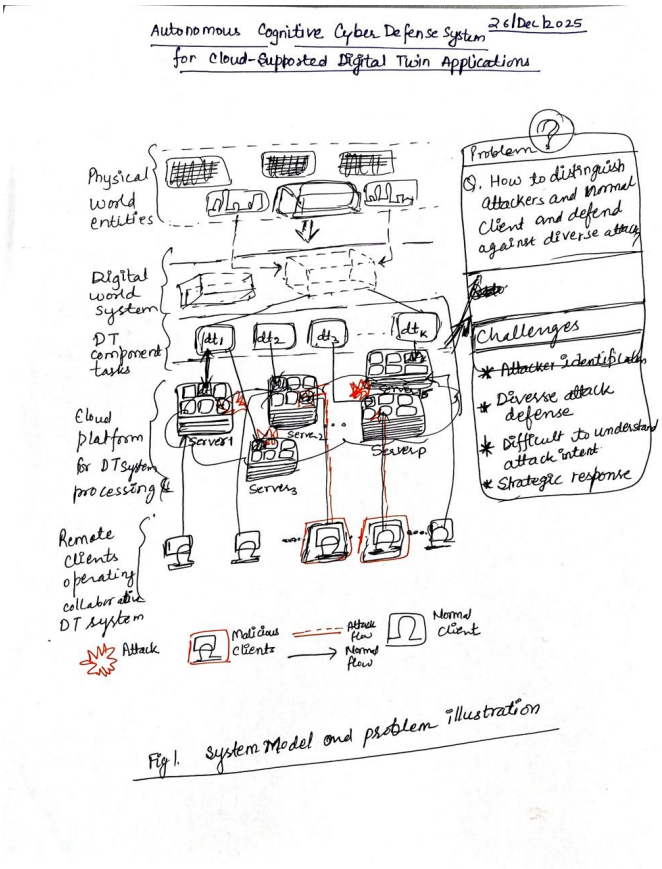


Fig 1. System Model and problem illustration

Fig. 1: System model and problem illustration.

B. Cognition-Demanding Threat Model

The CDT environment is assumed to operate under intelligent, adaptive adversaries capable of exploiting cyber, virtualized, and cyber–physical interdependencies. An attacker may possess partial knowledge of system topology, resource allocation rules, or vulnerable components, and may adapt behavior in response to observed defenses. Formally, a threat process is modeled as $\mathcal{T}$ composed of multiple threats including Stealthy Drift–Inducing Threats (δ_t), Dependency-Aware Cascading Threats ($\mathcal{R}_{\text{cas}}$), Adversarial Resource Manipulation ($U_i(t)$), Adaptive Evasion and Response Poisoning ($\mathcal{T}_{t+1}$), and Mission Manipulation Threats (Ξ_i), defined below.

Definition 1 (Stealthy Drift–Inducing Threat)**.** *A threat that introduces slow deviations that remain locally acceptable but accumulate over time:*

$$\delta_t = D(\mathbf{x}_t, \mathcal{X}_B) \leq \epsilon, \qquad \sum_{u=t-\Delta}^{t} \delta_u > \eta, \tag{1}$$

where $\mathbf{x}_t$ is telemetry at time t, $\mathcal{X}_B$ is the benign baseline, $D(\cdot)$ is a distance metric, ϵ is tolerance, Δ is the observation window, and η is the drift threshold.

Definition 2 (Dependency–Aware Cascading Threat)**.** *A threat that exploits inter-application dependencies so that a local anomaly propagates and triggers system-wide degradation:*

$$\mathcal{R}_{\text{cas}} = \sum_{(i,j)\in\Omega} \Xi_i \kappa_{ij}, \tag{2}$$

where Ω denotes execution or data-flow dependencies ($A_i \to A_j$), $\Xi_i \in \{0,1\}$ indicates whether A_i is anomalous, and κ_{ij} quantifies the sensitivity of A_j to the failure of A_i.

Definition 3 (Adversarial Resource Manipulation)**.** *A threat in which workloads respect local limits while inducing global overload:*

$$U_i(t) = U_i^B(t) + \psi_i(t), \quad U_i(t) \leq U_{\max}, \tag{3}$$

$$\sum_{i\in\mathcal{VN}} U_i(t) > \Gamma_{\max}, \tag{4}$$

where $U_i(t)$ is node utilization, $\psi_i(t) \geq 0$ is adversarial load, $U_{\max}$ local capacity, and $\Gamma_{\max}$ the global stability threshold.

Definition 4 (Adaptive Evasion and Response Poisoning)**.** *A threat in which the adversary adapts to defenses and manipulates feedback:*

$$\mathcal{T}_{t+1} = \mathcal{F}(\mathcal{T}_t, \theta_t, \Pi_t), \tag{5}$$

$$\mathbb{E}[\hat{\Xi} \mid \tilde{\mathbf{x}}] \neq \mathbb{E}[\Xi \mid \mathbf{x}], \tag{6}$$

where θ_t denotes IDS parameters, Π_t the mitigation policy, $\mathcal{F}(\cdot)$ the adaptation function, and $\tilde{\mathbf{x}}$ falsified telemetry.

Definition 5 (Mission Manipulation Threat)**.** *A threat that preserves nominal monitoring indicators while degrading mission performance:*

$$\Xi_i = 0, \qquad J(\mathit{CDT}) - J^* \geq \zeta, \tag{7}$$

where $J(\cdot)$ denotes the mission objective and J^* the nominal value achievable in the absence of adversarial perturbations.

C. Problem Definition and Design Goals

Given the cognition–demanding threats in Section II-B, the objective is to realize a cognition-driven decision process that jointly reasons about temporal dynamics, dependency propagation, and mission impact under uncertainty. Let $\Psi : (\mathbf{x}, \Xi, \Omega) \to \{\textit{risk estimation, anomaly attribution, intent inference}\}$, where $\mathbf{x}$ denotes telemetry, Ξ threat indicators, and Ω execution/data-flow dependencies. The outputs of Ψ feed a higher-level cognition layer Φ that evaluates propagation risk and selects mitigation actions:

$$\Phi : \Psi \to (\rho_{ijk}, \pi_{ijk}), \tag{8}$$

where $\rho_{ijk} \geq 0$ denotes the expected cascading/mission risk associated with application A_k executed on VN_j at PN_i, and π_{ijk} is the selected policy (e.g., isolation, throttling, migration). The optimization objective is

$$\min_{\Psi,\Phi} \mathbb{E}[\rho_{ijk}] \quad \text{s.t.} \quad J(\text{CDT}) \geq J^* - \zeta, \tag{9}$$

subject to constraints:

- *Drift-awareness:* detect cumulative drift (Eq. (1)) without excessive false alarms.
- *Propagation control:* $\mathcal{R}_{\text{cas}} \leq \tau_{\text{cas}}$ (Eq. (2)).
- *Resource stability:* $U_i(t) \leq U_{\max}$ and $\sum_{i\in\mathcal{VN}} U_i(t) \leq \Gamma_{\max}$ (Eq. (3)).
- *Evasion robustness:* $\mathbb{E}[\hat{\Xi} \mid \tilde{\mathbf{x}}] \approx \mathbb{E}[\Xi \mid \mathbf{x}]$ (Eq. (5)).
- *Mission integrity:* mission degradation bounded by Eq. (7).

Overall, the CDT problem is to enable timely, uncertainty-aware mitigation that avoids over-blocking while preventing cascading failures across interdependent CDT assets. The CDT cognition framework is guided by the following design goals:

- Fuse temporal memory, dependency reasoning, and mission context to infer risk and intent under partial, noisy, or adversarial observations.
- Prioritize mitigation actions that limit dependency-driven cascades while preserving essential services and avoiding unnecessary blocking.
- Select control policies that stabilize resource utilization and ensure $J(\text{CDT}) \geq J^* - \zeta$.
- Continuously adapt estimates and policies to remain robust against drift, adversarial evasion, and response poisoning.

III. Proposed Model

This section introduces the *Autonomous Cognitive Cyber Defense for Online Resilient Cloud-Enabled Digital Twin Systems* (ACCORD) model for securing Cloud Digital Twin (CDT) environments. ACCORD supports end-to-end anomaly detection, cognition-driven forensics, and adaptive mitigation with minimal disruption across four coordinated phases: **Phase 1: Telemetry Pre-processing**; **Phase 2: Detection Layer**; **Phase 3: Cognition-Based Forensics**; and **Phase 4: Cognitive Response**. The architecture of ACCORD model is illustrated in Fig. 2.

A. Phase 1: Cloud Digital Twin Telemetry Pre-processing Unit

The preprocessing unit converts raw CDT telemetry into consistent, noise-aware, cognition-ready inputs aligned with the threat processes in Section II-B. Each application A_k running on VN_j at PN_i emits $\mathbf{x}_{ijk}(t) \in \mathbb{R}^d$. The pipeline integrates four steps: sanitization, numerical normalization, categorical encoding, and temporal windowing. These operations preserve drift signals (Eq. (1)), dependency propagation (Eq. (2)), and mission-aware structure (Eq. (7)), strengthening downstream cognition and mitigation. Sanitization maps malformed tokens to missing values, normalizes

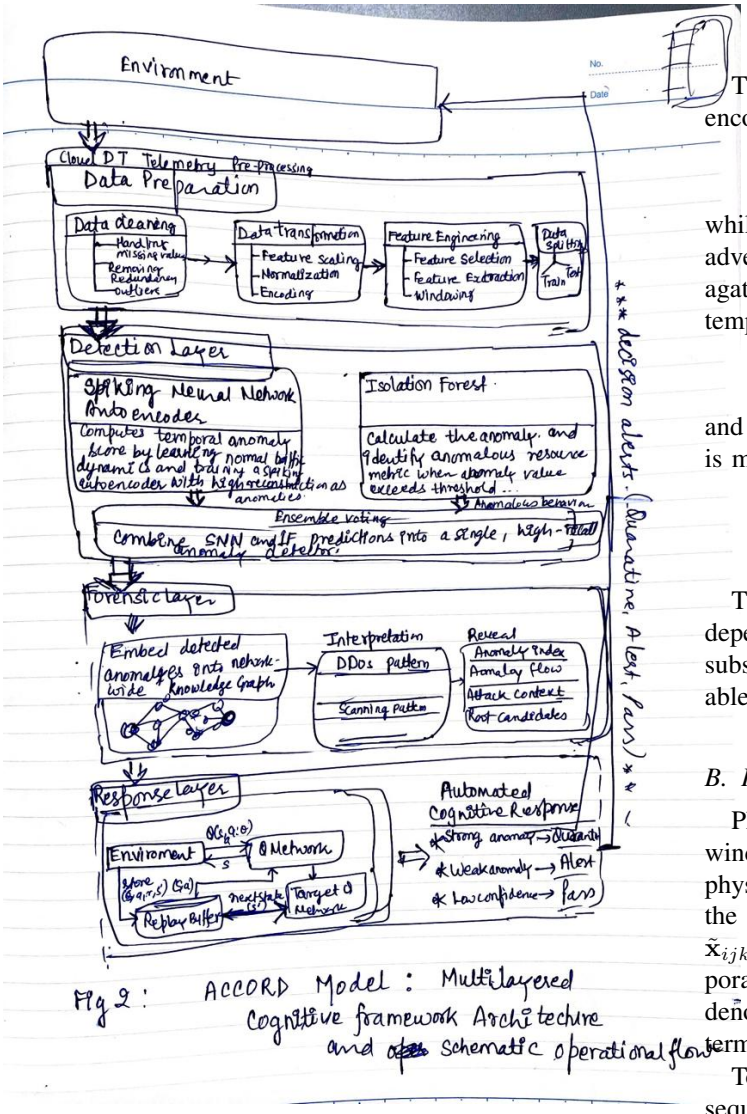


Fig. 2: ACCORD Model: Architecture and Operational Design

DNS and SSL booleans, coerces non-convertible numerics, and removes high-cardinality identifiers to avoid memorization that hides gradual drift and cascade effects, as formalized in Eqs. (10)–(12):

$$x_{r,c} = \begin{cases} \text{NaN} & \text{if } x_{r,c} \in \{--,\}, \\ x_{r,c} & \text{otherwise.} \end{cases} \tag{10}$$

$$\text{map(true"}) = 1, \qquad \text{map(false"}) = 0, \tag{11}$$

$$x_{r,c} \leftarrow \begin{cases} \text{float}(x_{r,c}) & \text{if convertible,} \\ \text{NaN} & \text{otherwise.} \end{cases} \tag{12}$$

For numerical attributes $\mathcal{N}$, median imputation stabilizes missing values (Eq. (13)) and z-normalization standardizes scale (Eq. (14)), supporting models that reason over drift and resource pressure (Eq. (3)):

$$\hat{x}_{r,c} = \begin{cases} x_{r,c} & \text{if } x_{r,c} \neq \text{NaN}, \\ \text{median}(\mathcal{N}_c) & \text{otherwise.} \end{cases} \tag{13}$$

$$\tilde{x}r, c = \frac{\hat{x}r, c - \mu_c}{\sigma_c}, \quad \sigma_c > 0. \tag{14}$$

The categorical attributes $\mathcal{C}$ are mode-imputed and one-hot encoded using

$$\phi(x_{r,c}) = \big[\mathbb{I}(x_{r,c} = v_1), \ldots, \mathbb{I}(x_{r,c} = v_{m_c})\big], \tag{15}$$

while unseen categories are ignored, reducing sensitivity to adversarial evasion (Eq. (5)). To expose early onset and propagation dynamics, telemetry is segmented into overlapping temporal windows with length $T = 25$ and stride 1:

$$\mathbb{W}t = \tilde{\mathbf{x}}ijk(t), \ldots, \tilde{\mathbf{x}}_{ijk}(t + T - 1), \tag{16}$$

and each window is labeled anomalous if any constituent event is malicious:

$$Y(\mathbb{W}_t) = \begin{cases} 1, & \exists, u \in [t, t + T - 1] : y_u = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{17}$$

This integrated pipeline preserves drift, captures cascading dependencies, and maintains mission relevance, ensuring that subsequent detection and cognition modules operate on reliable and threat-aligned representations.

B. Phase 2: Detection Layer

Phase 2 performs fine-grained anomaly detection over the windowed CDT telemetry generated in Section III-A. For each physical node PN_i, virtual node VN_j, and application A_k, the detection pipeline operates on normalized feature vectors $\tilde{\mathbf{x}}_{ijk}(t) \in \mathbb{R}^d$. These vectors are grouped into overlapping temporal windows $\mathbb{W}_t = \{\tilde{\mathbf{x}}_{ijk}(t), \ldots, \tilde{\mathbf{x}}_{ijk}(t+T-1)\}$, where T denotes the window length, thereby capturing localized short-term behavioral dynamics of the underlying CDT entities.

To explicitly model temporal event dynamics, each feature sequence in $\mathbb{W}_t$ is transformed into a Poisson-rate spike train generated via Bernoulli rate coding. Specifically, the probability of a spike event for feature f at time u is proportional to its normalized intensity, as expressed in Eq. (18), where $S_u^{(f)} \in \{0, 1\}$ denotes the spike event and $f = 1, \ldots, d$ indexes the feature dimensions. At each discrete timestep, spike generation for each feature is modeled as an independent Bernoulli trial, where the probability of emitting a spike is proportional to the normalized feature intensity.

$$P\Big(S_u^{(f)} = 1\Big) \propto \text{Norm}\Big(\tilde{x}_{ijk}^{(f)}(u)\Big). \tag{18}$$

The resulting spike trains are processed by an encoder–decoder SNN composed of Leaky-Integrate-and-Fire (LIF) neurons, enabling biologically inspired modeling of temporal dependencies. The membrane potential evolution of each neuron follows Eq. (19), where v_u denotes the membrane potential at time u, I_u represents the synaptic input current, and $0 < \beta < 1$ controls membrane leakage. A neuron emits a spike when $v_{u+1} \geq \theta$, after which the membrane potential is reset. During training, surrogate gradient techniques are employed to overcome the non-differentiability of the spiking function.

$$v_{u+1} = \beta v_u + I_u. \tag{19}$$

Let C_f and $\hat{C}_f$ denote the observed and reconstructed spike counts, respectively, for feature f over window $\mathbb{W}_t$. The SNN is trained exclusively on windows corresponding to normal system behavior by minimizing the reconstruction-based SNN loss defined in Eq. (20). This objective penalizes deviations between reconstructed and true spike statistics, thereby enforcing accurate temporal encoding of benign operational patterns:

$$\mathcal{L}_{\text{SNN}} = \frac{1}{d}\sum_{f=1}^{d}\left(C_f - \hat{C}_f\right)^2. \tag{20}$$

During inference, the temporal anomaly severity of each window is quantified using the reconstruction discrepancy in Eq. (21):

$$s_{ijk}^{T}(t) = \frac{1}{d}\sum_{f=1}^{d}\left|C_f - \hat{C}_f\right|, \tag{21}$$

where larger values indicate stronger deviations from learned normal dynamics. A window is flagged as anomalous according to the decision rule in Eq. (22), where τ_T denotes an adaptive temporal threshold estimated from normal operational data:

$$\hat{y}_{ijk}^{T}(t) = \begin{cases} 1, & s_{ijk}^{T}(t) \geq \tau_T, \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

C. Phase 3: Cognition-Based Forensics Layer

Phase 3 elevates anomaly indications generated in Section III-B from raw alerts to structured forensic hypotheses. Rather than treating window-level anomaly flags $\hat{y}_{ijk}(t) \in \{0,1\}$ as terminal decisions, this phase contextualizes them within the communication, dependency, and control structure of the Cloud Digital Twin (CDT). The objective is to infer attack intent, identify root-cause entities, and reconstruct likely propagation corridors across physical, virtual, and application layers. For each anomalous window $\mathbb{W}_t$ associated with application A_k executing on virtual node VN_j hosted by physical node PN_i, the corresponding communication tuple (u, v) is extracted, representing source and destination entities identified via network addressing and service bindings. All such interactions are incrementally integrated into a directed knowledge graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where vertices $v \in \mathcal{V}$ denote physical hosts, virtual machines, services, controllers, or applications, and directed edges $e = (u, v) \in \mathcal{E}$ represent observed communication flows or dependency relationships. Each vertex is associated with a latent representation $\phi(v) \in \mathbb{R}^p$ to enable relational and structural reasoning. Edge-level flow statistics accumulate temporal evidence linking anomaly occurrence to communication structure. Specifically, for each directed edge (u, v), the total number of observed windows F_{uv}, the number of anomalous windows A_{uv}, and the resulting anomaly concentration ratio ρ_{uv} are defined as Eq. (23):

$$F_{uv} = \sum_{t} \mathbf{1}_{(u,v)\in\mathbb{W}_t}, \tag{23}$$

$$A_{uv} = \sum_{t} \mathbf{1}_{(u,v)\in\mathbb{W}_t}\, \hat{y}_{ijk}(t), \tag{24}$$

$$\rho_{uv} = \frac{A_{uv}}{F_{uv} + \epsilon}, \tag{25}$$

where $\epsilon > 0$ prevents numerical instability. The ratio ρ_{uv} quantifies the persistence of anomalous behavior along a given interaction edge, serving as a key indicator of malicious concentration. To characterize exposure and propagation potential, node-level structural properties are computed directly from $\mathcal{G}$. The in-degree and out-degree of each node v are given by Eq. (26):

$$d^{\text{in}}(v) = |\{u : (u, v) \in \mathcal{E}\}|, \qquad d^{\text{out}}(v) = |\{w : (v, w) \in \mathcal{E}\}|. \tag{26}$$

High in-degree reflects aggregation or victimization tendencies, whereas high out-degree indicates dissemination, probing, or lateral movement capability. Cognition-guided interpretation is achieved by jointly reasoning over graph structure and anomaly severity indicators derived from the detection layer. For each anomalous window mapped to edge (u, v) at time t, a forensic hypothesis score vector $\boldsymbol{\pi}_{uv}(t) \in \mathbb{R}^4$ is constructed as Eq. (27):

$$\boldsymbol{\pi}_{uv}(t) = \Xi\Big(d^{\text{in}}(v), d^{\text{out}}(u), \rho_{uv}, s_{ijk}^{T}(t), \bar{s}_{ijk}^{S}(t)\Big), \tag{27}$$

where, $\Xi(\cdot)$ denotes a cognition function that fuses structural indicators with temporal and spatial anomaly severity. Large destination in-degree combined with high anomaly concentration biases interpretation toward convergent attack scenarios, while elevated source out-degree with persistent anomalies favors spreading, scanning, or reconnaissance behavior. This biasing mechanism enables risk-aware interpretation by reducing the likelihood of misattributing victims as attackers. The dominant forensic context is selected by Eq. (28):

$$\hat{c}_{uv}(t) = \arg \max_{\substack{\gamma\in\{\text{DDoS},\\ \text{Scan,Heavy,Iso}\}}} \boldsymbol{\pi}_{uv}^{(\gamma)}(t), \tag{28}$$

yielding one of four cognitively meaningful categories: destination under siege (DDoS), source-driven spreading or scanning, dedicated heavy attack, or isolated anomalous behavior. The role attribution identifies the primary entity of forensic interest by mapping the inferred context to either the source or destination endpoint is given by Eq. (29):

$$r_{uv}(t) = \Lambda\big(\hat{c}_{uv}(t), u, v\big), \tag{29}$$

where $\Lambda(\cdot)$ associates victim-centric contexts (e.g., DDoS) with the destination node and propagation-centric contexts (e.g., scan or heavy attack) with the source node. Forensic reasoning extends beyond individual edges through causal path analysis on $\mathcal{G}$. For any candidate path $\pi = (v_1, \ldots, v_m)$ implicated in an incident, a path-responsibility score is computed as Eq. (30):

$$\Omega(\pi) = \prod_{\ell=1}^{m-1}\left(\rho_{v_\ell v_{\ell+1}} \cdot \kappa_{v_\ell v_{\ell+1}}\right), \tag{30}$$

where $\kappa_{v_\ell v_{\ell+1}}$ encodes dependency strength (e.g., service coupling, control hierarchy, or resource binding). High $\Omega(\pi)$ values highlight likely propagation corridors and identify structurally critical intervention points. Each anomalous window thus yields an Attributed Relational Graph (ARG) record of the form $(t, (u, v), \hat{y}_{ijk}(t), \hat{c}_{uv}(t), r_{uv}(t), \Omega(\pi))$. These records preserve causal evidence for downstream response

layers and enable post-hoc validation through cross-analysis between ground-truth attack labels and graph-derived forensic interpretations. By tightly coupling detection outputs with communication-aware structural reasoning, Phase 3 transforms raw anomaly signals into coherent, interpretable, and mission-aligned forensic narratives consistent with CDT topology and operational intent.

D. Phase 4: Cognitive Response Layer

Phase 4 maps cognitively interpreted forensic evidence from Section III-C to mission-aware mitigation actions. Decisions are guided by reasoning over a knowledge graph (KG) $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \Phi)$, where nodes represent (PN_i, VN_j, A_k) entities, edges encode communication or functional dependencies, and Φ stores anomaly-aware structural and statistical attributes derived from forensic analysis, while symbolic role attribution is used exclusively for reward shaping. For each anomalous window $\mathbb{W}_t$, a compact cognition-aware state vector $\mathbf{s}_{ijk}(t) \in \mathbb{R}^{15}$ is constructed as in Eq. (31), aggregating detection severity, structural fan-in/fan-out, link anomaly concentration, and KG-derived semantic indicators.

$$\mathbf{s}_{ijk}(t) = [x_1, \ldots, x_{15}]^\top. \tag{31}$$

Each component x_m corresponds to a log-scaled KG-derived statistic encoding source and destination activity, anomaly involvement, degree structure, and local SNN severity. The symbolic forensic context $c_{ijk}(t)$ is excluded from the state representation and is used solely for reward computation, preventing semantic label leakage into policy learning.

The discrete response space $\mathcal{A} = \{\text{Pass}, \text{Alert}, \text{Block}\}$ is optimized using a Deep Q-Network (DQN). The state–action value function is defined in Eq. (32), and the optimal action is selected according to Eq. (33).

$$Q_\theta(\mathbf{s}, a) = \mathbb{E}\left[\sum_{\ell \geq 0} \gamma^\ell r_{t+\ell+1} \mid \mathbf{s}_t = \mathbf{s}, a_t = a\right], \tag{32}$$

$$a^\star = \arg\max_{a \in \mathcal{A}} Q_\theta(\mathbf{s}_{ijk}(t), a). \tag{33}$$

Mission-aware reward shaping incorporates ground-truth attack presence $y_{ijk}(t)$ and KG-inferred operational context $c_{ijk}(t)$ via Eq. (34), promoting targeted containment while penalizing collateral impact.

$$r_t = \mathcal{R}(a_t, y_{ijk}(t), c_{ijk}(t)). \tag{34}$$

Learning follows the Bellman target in Eq. (35), with parameters updated by minimizing the temporal-difference loss in Eq. (36) using a target network Q_{θ^-}.

$$y_t = r_t + \gamma \max_{a'} Q_{\theta^-}(\mathbf{s}_{t+1}, a'), \tag{35}$$

$$\mathcal{L}_{\text{DQN}} = \left(y_t - Q_\theta(\mathbf{s}_t, a_t)\right)^2. \tag{36}$$

By interacting with the KG-augmented environment, the agent learns cognitively aligned policies that Block confirmed attackers, avoid blocking victims or mission-critical services, and escalate uncertain cases via alerts, thereby closing the cognition-to-response loop.

IV. Operational Design and Complexity Analysis

The ACCORD framework operates through four coordinated phases that transform raw Cloud Digital Twin (CDT) telemetry into cognition-driven, mission-aware mitigation actions. The pipeline standardizes heterogeneous inputs, performs temporal–spatial anomaly inference, constructs cognitively meaningful forensic contexts, and executes adaptive responses with minimal operational disruption. Algorithm 1 summarizes the end-to-end operational workflow.

Algorithm 1: Operational Workflow of ACCORD

Input: Raw CDT telemetry $\mathbf{x}_{ijk}(t)$, knowledge graph $\mathcal{G}$, RL policy parameters θ
Output: Anomaly labels $\hat{y}_{ijk}(t)$, forensic contexts $\hat{c}_{uv}(t)$, mitigation actions a_t

Phase 1: Telemetry Preprocessing.
Sanitize, impute, normalize, and encode $\mathbf{x}_{ijk}(t)$; construct overlapping windows $\mathbb{W}_t$ and derive window-level representations.
Phase 2: Detection Layer.
Compute temporal anomaly severity $s^T_{ijk}(t)$ using sequence-based modeling; compute spatial deviation score $s^S_{ijk}(t)$ using graph-aware aggregation across interacting entities; derive window-level anomaly indicators $\hat{y}_{ijk}(t)$.
Phase 3: Cognition-Based Forensics.
Embed anomalous interactions into the knowledge graph $\mathcal{G}$; accumulate flow statistics $(F_{uv}, A_{uv}, \rho_{uv})$; infer forensic context $\hat{c}_{uv}(t)$ and root entity $r_{uv}(t)$; estimate propagation likelihood $\Omega(\pi)$ over candidate paths.
Phase 4: Cognitive Response.
Form cognition-aware state $\mathbf{s}_{ijk}(t)$ from detection and forensic indicators; select mitigation action $a_t \in \{\text{Pass}, \text{Alert}, \text{Block}\}$ using DQN; update policy Q_θ during training based on observed reward.

A. Computational Complexity

Let n denote the number of telemetry records, d the feature dimension, T the window length, $|\mathcal{E}|$ the number of interaction edges in the knowledge graph, $|\mathcal{V}|$ the number of entities, and $|A|$ the size of the response action space. Telemetry preprocessing, including sanitization, imputation, normalization, encoding, and window construction, incurs $\mathcal{O}(nd)$ time complexity. Temporal anomaly inference processes d features across T time steps, yielding $\mathcal{O}(ndT)$ complexity, while spatial analysis across co-existing entities introduces an additional $\mathcal{O}(nd \log n)$ cost under sparse interaction and indexed graph access assumptions. Cognition-based forensics scale linearly with observed interactions, requiring $\mathcal{O}(|\mathcal{E}|)$ time to update flow statistics, assign forensic contexts, and evaluate candidate propagation paths, with causal reconstruction remaining near-linear due to bounded path lengths. The cognitive response layer evaluates a Deep Q-Network over a fixed state dimension $s = 15$, incurring $\mathcal{O}(|A|s)$ computation per decision

step. Consequently, the overall computational complexity of ACCORD is $\mathcal{O}\big(n(dT + d\log n) + |\mathcal{E}| + |A|s\big)$, supporting near-linear scalability and distributed execution across CDT nodes. Memory complexity is dominated by telemetry buffering $\mathcal{O}(nd + nT)$, knowledge graph storage $\mathcal{O}(|\mathcal{V}| + |\mathcal{E}|)$, and reinforcement learning parameters $\mathcal{O}(s|A|)$, resulting in linear memory growth aligned with infrastructure scale.

V. Performance Evaluation

A. Experimental Setup

All experiments were conducted in a CPU-only Google Colab environment using Python 3.x. Local development was performed on a 64-bit Windows 10 system with an AMD Ryzen 7 7435HS (3.10 GHz) processor and 16 GB RAM. The framework consists of three modules: (i) an SNN-AE implemented with `snntorch` and `PyTorch` for unsupervised window-level anomaly detection via neuron-wise reconstruction error; (ii) a knowledge-graph cognition layer for forensic inference; and (iii) a DQN agent in `PyTorch` for mission-aware response optimization in a custom environment (`HybridNetworkEnv`). Preprocessing used `pandas`, `NumPy`, and `scikit-learn` for feature selection, imputation, encoding, normalization, and temporal windowing. Evaluation was performed on the TON_IoT dataset [20]. Table I reports the experimental parameters.

TABLE I: Experimental configuration and hyperparameters

Component	Parameter	Value / Setting	Tool / Library
System Setup	CPU & Memory	AMD Ryzen 7 (3.10 GHz), 16 GB RAM	Windows 10, Google Colab (CPU)
SNN-AE	Hidden Units / Window Size	64 / 25	`snntorch` + `PyTorch`
	Neuron / Gradient	LIF / Fast Sigmoid (β=0.5)	Default in `snntorch`
	Optimizer / LR / Epochs	Adam / 10^{-3} / 20	`torch.optim`
DQN Module	Episodes / γ / ε-decay	300 / 0.95 / 0.985	Custom `PyTorch` RL
	Reward Weights	Context-dependent (victim/attacker/normal)	Custom reward shaping
Preprocessing	Scaling / Encoding / Imputation	Standard+MinMax / One-hot / Median-Mode	`scikit-learn`, `pandas`
Dataset	Evaluation Source	TON_IoT network traces	Public benchmark

B. Dataset Description

Experiments use the TON_IoT dataset [20], a large-scale benchmark from the UNSW Cyber Range and IoT Labs for anomaly detection in IoT and industrial networks. It comprises 211,043 network flow records with 44 features across Network, DNS, SSL/TLS, and HTTP layers, collected from a heterogeneous testbed of IoT devices, edge gateways, and cloud systems. The class distribution is 76.28% anomalous and 23.72% benign, reflecting realistic attack scenarios including DoS, DDoS, Port Scanning, MITM, and Ransomware. The dataset exhibits feature sparsity, heavy-tailed distributions, and class imbalance, which pose challenges for deep anomaly detection models. Table II summarizes the dataset characteristics.

TABLE II: Dataset Summary

Aspect	Value
Source	UNSW Cyber Range and IoT Labs
Records	211,043
Features	44 per flow
Protocol Layers	Network, DNS, SSL/TLS, HTTP
Class Distribution	76.28% anomalous, 23.72% benign
Attack Types	DoS, DDoS, Port Scan, MITM, Ransomware
Feature Encoding	Numeric and categorical with one-hot encoding
Statistical Traits	Sparse and heavy-tailed
Training Data	10,000 normal samples, excluded from test set
Use Case	Anomaly detection and model validation

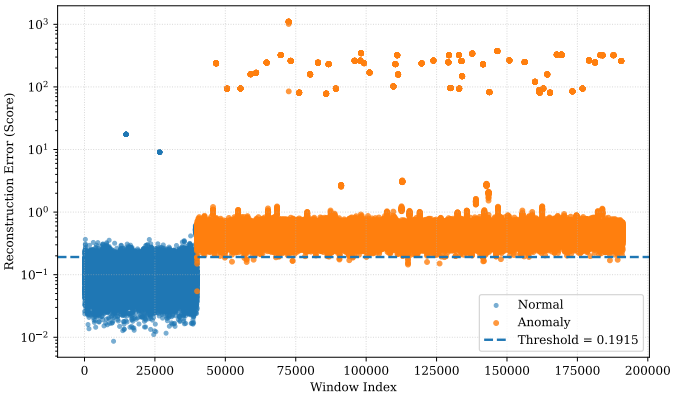


Fig. 3: Anomaly scores per window.

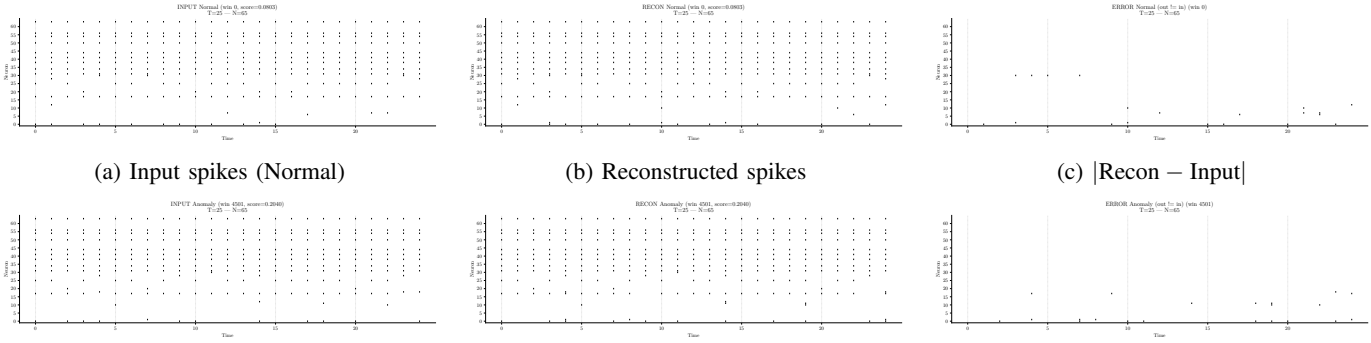
C. Numerical results

1) Anomaly detection analysis: Fig. 3 shows that anomalous windows yield higher reconstruction mismatch than normal behavior. Only 17.78% of neurons fire during inference, achieving an 82.22% reduction in activations relative to a dense ANN, which supports energy- and latency-efficient cloud digital twin deployment.

Fig. 4 contrasts spike-raster reconstructions for normal and anomalous windows. Normal traffic shows close input–reconstruction alignment with low error, whereas anomalous windows exhibit persistent, neuron-specific mismatches over time. These localized imbalances indicate detection driven by temporal reconstruction inconsistency rather than raw firing intensity, providing robustness to transient or bursty benign traffic. Fig. 5 compares ground-truth–conditioned and prediction-based reconstructions for normal and anomalous windows. Normal traffic yields sparse, short-lived errors, whereas anomalous traffic produces broad, persistent neuron-wise mismatches in both modes. This consistent separation indicates detection driven by intrinsic reconstruction imbalance rather than ground-truth conditioning, ensuring robustness under deployment.

Fig. 6 shows representative false positives and false negatives of the reconstruction-based detector. False positives occur when benign windows exhibit localized neuron-time discrepancies that elevate anomaly scores, while false negatives arise when anomalous patterns overlap with the learned normal manifold, reducing reconstruction error. The errors remain structured, indicating borderline pattern similarity rather than model instability.

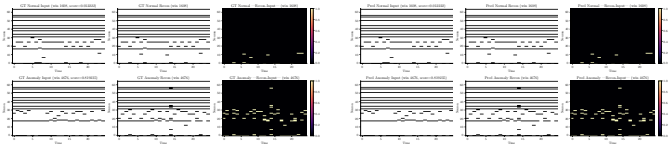
2) Cognition Forensic analysis: The SNN applies a fixed high-percentile reconstruction-error threshold for unsupervised detection, while a separate F1-optimal graph-level threshold selected from precision–recall analysis on training windows is fixed for all downstream stages, preventing label leakage and ensuring reproducibility. Using this threshold, a boosted knowledge graph (KG) is built over test traffic with nodes as IP addresses and directed edges as source–destination flows. Each node records cnt, bad_cnt, max_snn, and fan-in and fan-out degrees, where high bad_cnt with large fan-out indicates source-spreading behavior and high bad_cnt with large fan-in indicates destination-focused load. Fig. 7 shows the interaction



(a) Input spikes (Normal) (b) Reconstructed spikes (c) |Recon − Input|

(d) Input spikes (Anomaly) (e) Reconstructed spikes (f) |Recon − Input|

Fig. 4: Spike-raster comparison of normal (top) and anomalous (bottom) windows, showing accurate reconstruction for normal traffic and neuron-wise mismatches for anomalies, indicating detection via reconstruction imbalance.



(a) Ground-truth. (b) Prediction.

Fig. 5: SNN Spike-based autoencoder behavior shown via input, reconstruction, and error heatmaps.

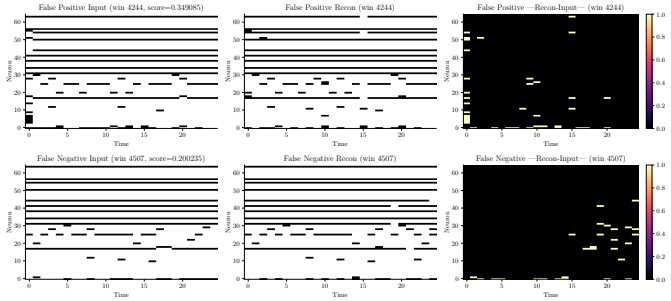


Fig. 6: False-positive and false-negative case studies illustrating reconstruction discrepancies in the SNN autoencoder.

graph, with node color as log-scaled peak SNN score, size as $\log_{1p}$ traffic volume, and shape denoting degree imbalance to support qualitative analysis and ARG extraction.

The prominent nodes in the boosted KG are summarized using a degree-imbalance heuristic: nodes with fan-out $>$ fan-in are classified as source-like, and nodes with fan-in $\geq$ fan-out as victim-like. Within each group, nodes are ranked by anomalous-window count bad_cnt, with fan-out or fan-in as a secondary criterion, and the top-k entries are reported. Table III presents the top-5 source-like and victim-like IPs. These categories reflect structural connectivity rather than ground-truth roles. IP 192.168.1.30 shows the highest bad_cnt among source-like nodes with high fan-out, indicating recurrent anomalous source-side activity.

An *Attack Reasoning Graph (ARG)* is constructed as an attributed relational graph using local degree cues (fan-in, fan-out) and SNN packet-level anomaly scores to provide coarse traffic context for downstream policy learning. Fig. 8 cross-

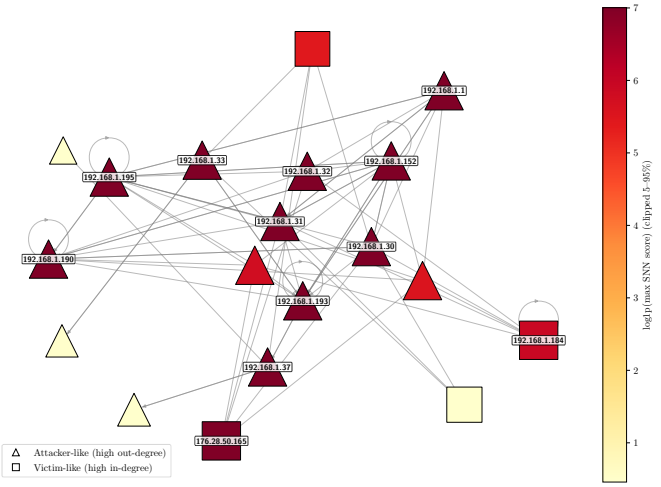


Fig. 7: Global KG of SNN-identified anomalous flows for qualitative ARG extraction.

TABLE III: Top-5 suspicious source and victim IPs from the boosted KG (test set). Max SNN values are ≈1099 for major attackers and ≈300–1100 for victims.

(a) Sources (source-like; high fan-out)

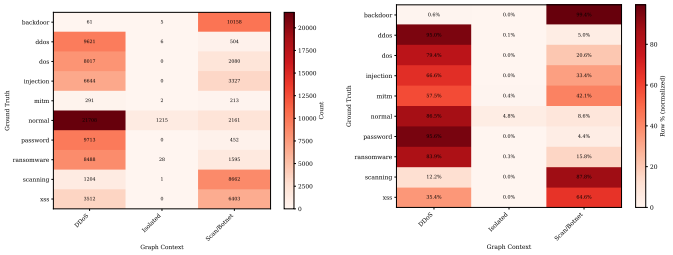
IP	bad_cnt	Fan-out
192.168.1.30	32375	99
192.168.1.193	25390	14
192.168.1.190	25053	229
192.168.1.152	21099	67
192.168.1.31	15924	98

(b) Victims (victim-like; high fan-in)

IP	bad_cnt	Fan-in
192.168.1.184	7218	5
192.168.1.1	5567	7
176.28.50.165	4852	5
192.168.1.194	3511	4
192.168.1.49	3006	3

tabulates ground-truth classes with three ARG contexts. The count view shows volumes, and the normalized view shows per-class tendencies: volumetric attacks cluster in *DDoS*, scanning and botnet behaviors in *Scan/Botnet*, and single-host anomalies in *Isolated*. This serves as a consistency check, not a performance metric. *Limitation.* The coarse, degree-based abstraction may conflate benign aggregation with volumetric patterns or split attacks across contexts.

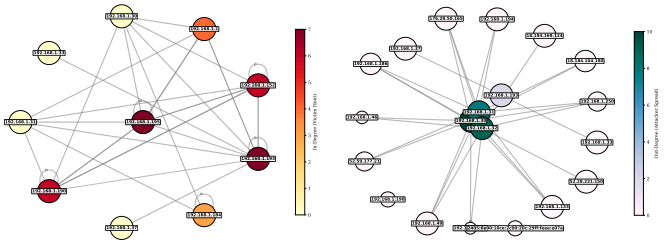
The ARG provides a coarse structural abstraction and exhibits ambiguity for low-propagation attacks and high fan-



(a) ARG context vs ground truth (counts).

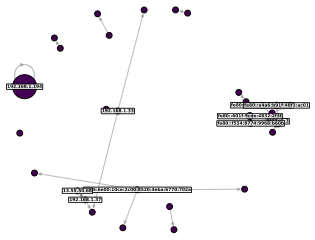
(b) ARG context vs ground truth (row-normalized %).

Fig. 8: ARG context verification via counts and normalized mappings across DDoS, Isolated, and Scan/Botnet buckets.



(a) Destination under siege.

(b) Source spreading.



(c) Isolated anomalies.

Fig. 9: ARG-derived topologies of verified anomalies showing destination-focused, source-spreading, and isolated patterns.

in benign flows. As shown in Fig. 8, classes span multiple context buckets and benign traffic can appear DDoS-like due to aggregation. The RL policy resolves this ambiguity by jointly reasoning over ARG topology, SNN scores, and historical state, using ARG as a scalable prior while enforcing mission-aware decisions. Fig. 9 visualizes induced subgraphs of SNN-verified anomalies. *Destination under siege* shows hub-like fan-in aggregation, *Source spreading* shows fan-out propagation, and *Isolated anomalies* form sparse, weakly connected components. Visuals are for interpretability, with top-N nodes and layouts chosen for readability.

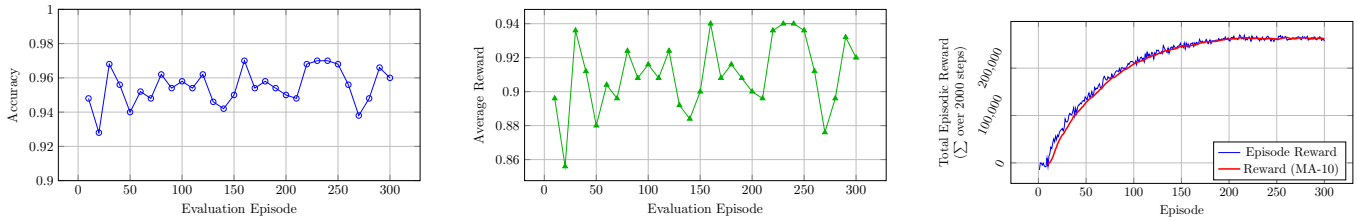
3) Response layer analysis: Fig 10 summarizes the training dynamics and periodic evaluation performance of the proposed DQN-based cognitive response agent operating within the `HybridNetworkEnv`. The periodic evaluation accuracy in Fig. 10(a) remains consistently high, stabilizing around 95–97%, indicating rapid convergence to a robust response policy across normal, victim-under-siege, and attacker-originated scenarios. Fig 10(b) shows sustained positive evaluation rewards with limited variance, confirming alignment with the mission-aware reward design and effective avoidance of self-induced denial-of-service. The episodic training reward in Fig. 10(c) increases monotonically and gradually saturates, with close agreement between instantaneous rewards and the moving average (window = 10), demonstrating stable learning and policy convergence under ε-greedy exploration. Having established policy stability and correctness, we next evaluate the operational responsiveness of the learned controller.

The RL controller is evaluated using *segment-based response latency*, which measures the delay until the first correct action after a ground-truth condition begins. The test stream is partitioned into maximal contiguous segments of identical condition, each assigned a target action: PASS for normal traffic, ALERT for victim-under-siege anomalies, and BLOCK for attacker anomalies. Samples are contiguous at window resolution, ensuring true temporal evaluation. For a segment $S = [s, e)$, latency is $L(S) = \min\{\, t - s \mid t \in [s, e),\ a_t = a^*(S) \,\}$, where a_t is the action at step t and $a^*(S)$ is the target action. Latency is measured in decision steps and is zero for immediate responses. Fig. 11 reports CDFs with median and 95th percentile for PASS, ALERT, and BLOCK. Segments without a correct action are treated as failures or right-censored. The metric reflects time-to-detection, containment, and recovery.

The RL agent uses a 15-dimensional hybrid state that combines global graph-context statistics with local SNN anomaly evidence. Fig. 12 visualizes representative states for normal, victim, and attacker nodes. Dimensions 1–5 capture source-side volume, anomaly intensity, and fan-out behavior; Dimensions 6–10 capture destination-side volume, anomaly counts, and fan-in. Dimension 15 provides window-level SNN evidence for short-term irregularities. As shown, normal states remain low across dimensions, victim nodes exhibit elevated destination-side activity and fan-in, and attacker nodes show elevated source-side activity and fan-out. Dimensions 11–14 re-encode in/out degrees to reinforce topological cues under sparse or noisy conditions.

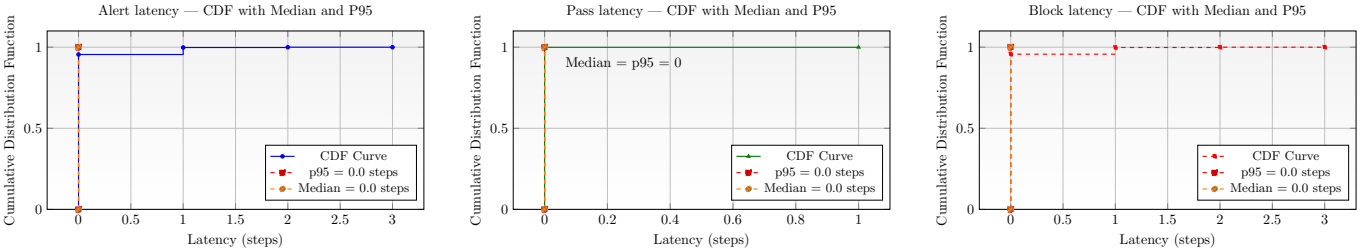
Fig. 13 shows the learned policy in a 2-D projection defined by destination in-degree and log-scaled SNN anomaly score. Points are colored by the selected action: PASS, ALERT, or BLOCK. The decision regions are structured: low score and low connectivity map to PASS, moderate scores under moderate connectivity map to ALERT, and high scores with high in-degree map to BLOCK. The figure indicates that the agent jointly exploits graph context and SNN evidence to produce coherent, interpretable decisions.

Fig. 14 contrasts RL policy behavior on attacks-only traffic (Fig. 14a) and the full dataset (Fig. 14b). Rows denote detected contexts and columns denote actions (*PASS*, *ALERT*, *BLOCK*). Anomalous flows use graph-derived context from fan-in and fan-out, with the continuous SNN score retained as a confidence feature in the state. For reporting, benign traffic is aggregated as *Normal*; the agent itself relies only on ARG-derived state, not labels. The attack-only view isolates adversarial behavior, while the full view shows preserved service continuity with strong containment, indicating robust context-aware decisions despite coarse ARG abstraction.



(a) Accuracy (b) Average Reward (c) Training Reward

Fig. 10: Training and evaluation metrics of the RL agent. (a) Periodic evaluation accuracy. (b) Periodic average evaluation reward. (c) Total episodic training reward with moving average (window = 10).



(a) Alert Latency (b) Pass Latency (c) Block Latency

Fig. 11: Empirical CDFs of RL action latency for (a) ALERT, (b) PASS, and (c) BLOCK. Dashed lines denote the median and 95th percentile in decision steps, where zero indicates an immediate response.

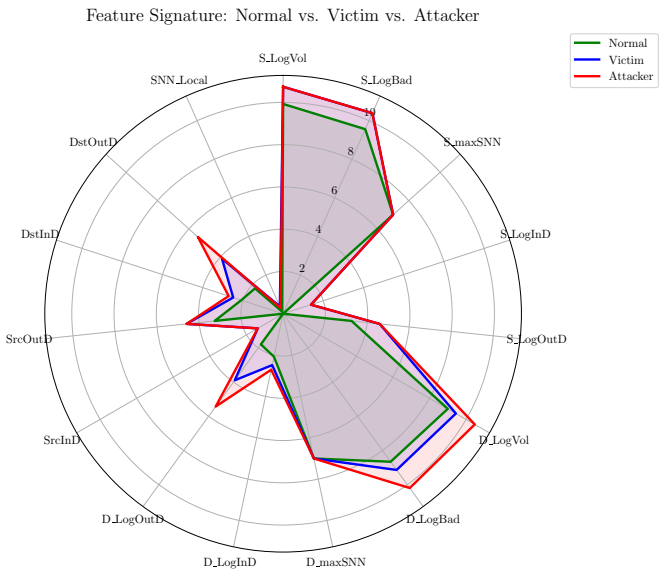


Fig. 12: Radar comparison of the 15-D state for normal, victim, and attacker nodes, highlighting graph context and SNN evidence.

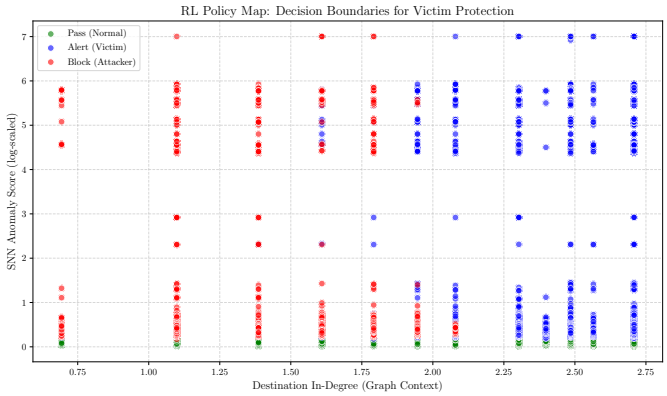


Fig. 13: 2-D view of the RL policy by destination in-degree and log-scaled SNN score.

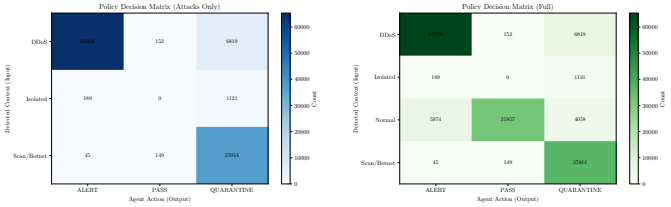
TABLE IV: ACCORD Core Classification Metrics

Size	Precision	Recall	F_1	Balanced Accuracy	MCC	Cohen's κ
20000	0.99792	0.99515	0.99653	0.99357	0.98328	0.98325
40000	0.99734	0.99519	0.99627	0.99258	0.98224	0.98222
60000	0.99732	0.99523	0.99627	0.99258	0.98233	0.98232
80000	0.9975	0.99546	0.99648	0.99302	0.98327	0.98326
100000	0.99767	0.9954	0.99653	0.99331	0.98352	0.9835
120000	0.99765	0.99555	0.9966	0.99333	0.98381	0.9838
140000	0.99762	0.99544	0.99653	0.99323	0.98347	0.98346
152816	0.99772	0.99543	0.99657	0.99342	0.98371	0.9837

4) ACCORD Comprehensive Analysis: Table IV reports classification metrics across training sizes. The model achieves $F_1 > 0.996$, balanced accuracy near 0.993, and MCC and Cohen's $\kappa > 0.98$, indicating robust and consistent class discrimination.

Fig. 15 summarizes performance across training sizes. ROC-AUC remains at 0.995–0.996 and PR-AUC near 0.998, indicating strong class separation. FPR ranges from 0.008 to 0.010 and FNR from 0.004 to 0.005, showing a favorable error trade-off. Brier score (0.004–0.006) and log loss (0.165–0.180) indicate stable probability calibration.

Table V reports supplementary metrics across training sizes, including Accuracy, Specificity, G-Mean, Jaccard, and F_β ($\beta = 0.5, 2$). Specificity and G-Mean remain near 0.99, with



(a) Attacks only (b) Full dataset

Fig. 14: Policy decision matrices for attack-only and full-traffic evaluations.

(a) ROC-AUC and PR-AUC (b) FPR and FNR (c) Calibration Metrics

Fig. 15: Performance across training sizes: (a) AUC, (b) FPR–FNR trade-off, and (c) calibration via Brier score and log loss. .

TABLE V: Supplementary Classification Metrics

Size	Accuracy	Specificity	G-Mean	Jaccard	$F_{0.5}$	F_2
20000	0.9093	0.99199	0.99357	0.99309	0.99736	0.9957
40000	0.9096	0.98996	0.99258	0.99256	0.99691	0.99562
60000	0.91	0.98992	0.99257	0.99257	0.9969	0.99565
80000	0.91015	0.99058	0.99302	0.99298	0.99709	0.99587
100000	0.91017	0.99122	0.9933	0.99308	0.99721	0.99585
120000	0.91047	0.99112	0.99333	0.99322	0.99723	0.99597
140000	0.91028	0.99101	0.99322	0.99308	0.99718	0.99588
152816	0.91046	0.9914	0.99341	0.99317	0.99726	0.99589

stable Jaccard and F_β, indicating balanced precision–recall performance.

To assess role-consistent and safety-aware behavior, three novel ACCORD-compliant metrics are introduced and defined over actions {PASS, ALERT, BLOCK}. Each event has an ideal action: normal PASS, victim ALERT, attacker BLOCK. Let T be the total events.

Victim Protection Rate (VPR). Let V_t be victim events and V_b those wrongly BLOCKed:

$$\mathrm{VPR} = 1 - \frac{V_b}{V_t}. \tag{37}$$

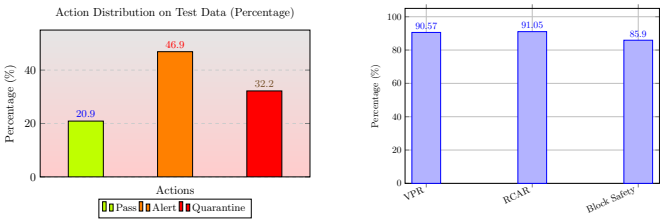
Role-Consistent Action Rate (RCAR). Let N_c, V_c, and A_c be correct PASS, ALERT, and BLOCK decisions:

$$\mathrm{RCAR} = \frac{N_c + V_c + A_c}{T}. \tag{38}$$

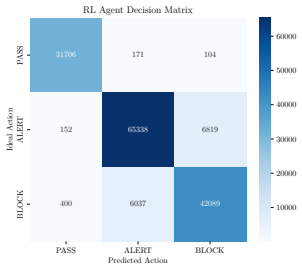
Block Precision Score (BPS). Let B_{tot} be total BLOCK actions and B_{safe} those applied to attackers:

$$\mathrm{BPS} = \frac{B_{\text{safe}}}{B_{\text{tot}}}. \tag{39}$$

Fig. 16 supports the high RCAR and VPR scores. The role–action matrix in Fig. 16c compares ideal context (rows) with agent actions (columns) and shows strong diagonal dominance, indicating role-consistent behavior. Normal traffic is mostly PASS (31,706) with few ALERT (171) or BLOCK (104).



(a) Action distribution. (b) VPR, RCAR and BPS.



(c) Decision matrix (ideal vs predicted).

Fig. 16: Policy analysis on the test set: (a) action distribution, (b) VPR and RCAR, and (c) ideal vs. selected actions across PASS, ALERT, and BLOCK.

TABLE VI: RL Specific Metrics Across Test Cases

Test Size	RCAR	VPR	BPS
20000	0.9093	0.90498	0.85359
40000	0.9096	0.9059	0.85656
60000	0.91	0.9057	0.85791
80000	0.91015	0.90681	0.85932
100000	0.91017	0.90582	0.85855
120000	0.91047	0.90584	0.85822
140000	0.91028	0.90553	0.8585
152816	0.91046	0.9057	0.85875

Victim contexts are primarily ALERT (65,338) with limited BLOCK (6,819) and rare PASS (152). Attacker contexts are largely BLOCK (42,089), with occasional ALERT (6,037) and rare PASS (400), reflecting conservative boundary behavior.

Table VI reports ACCORD-compliant RL metrics across training sizes. RCAR remains near 0.91, indicating role-appropriate actions. VPR stays at 0.905–0.907, showing strong victim protection. BPS (0.854–0.859) reflects conservative, attacker-focused BLOCK decisions.

As shown in Fig. 17, model performance improves rapidly in the low-data regime and converges as the training dataset size increases. Beyond the convergence point, both metrics remain stable with no observable degradation, indicating robust generalization and data-efficient learning.

Table VII compares a block-all heuristic with the ACCORD RL policy. The heuristic blocks all anomalous traffic, yielding VPR $= 0.00\%$, whereas ACCORD preserves 90.32% of victim flows by issuing ALERT instead of BLOCK, demonstrating victim-aware mitigation and reduced collateral impact.

D. Comparison Analysis

Table VII compares a block-all heuristic with the ACCORD RL policy. The heuristic blocks all anomalous traffic, yielding

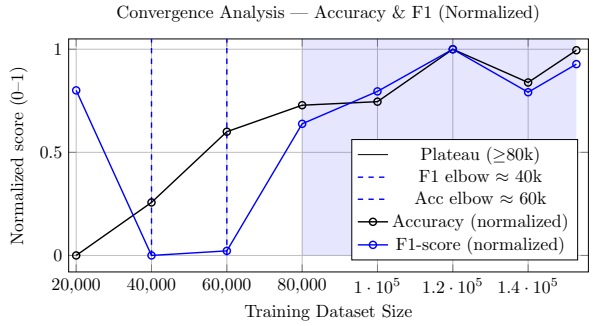


Fig. 17: Convergence vs. training size, with normalized Accuracy and F1; elbows at 40k (F1) and 60k (Accuracy), plateau beyond 80k..

TABLE VII: Victim Protection Comparison

Method	VPR (%)	Behavior
Heuristic (Block-All)	0.00	Blocks victim traffic
RL (ACCORD)	90.40	Alerts without disruption

VPR $= 0.00\%$, whereas ACCORD preserves 90.32% of victim flows by issuing ALERT instead of BLOCK, demonstrating victim-aware mitigation and reduced collateral impact.

Table IX reports mean $\pm$ std across test subsets. The proposed model achieves the highest scores with minimal variance, near-optimal $F_{0.5}$ and F_2, and low false-positive and false-negative rates, indicating robust separation. Baselines show lower means and higher variance, reflecting sensitivity to scaling and imbalance.

Table X reports mean performance with 95% confidence intervals. The proposed model shows the narrowest intervals across all metrics, indicating high stability and reliable detection, particularly for $F_{0.5}$, F_2, FNR, and FPR. Baselines exhibit wider intervals, reflecting greater sensitivity to data variability.

ACCORD model demonstrates consistently high and stable performance across all evaluation scales, with minimal variability and near-optimal mean scores. Agreement metrics (MCC, Cohen's κ) confirm reliable alignment with ground truth under class imbalance, supporting large-scale deployment. Compared to the strongest baseline, it achieves substantial relative improvements, including 96.18% reduction in FNR, 80.92% reduction in FPR, 76.55% gain in MCC, and 21.67% gain in Jaccard, alongside broad improvements in precision, recall, and asymmetric F-scores, highlighting robust, generalizable anomaly detection.

Fig. 18 compares bounded performance metrics across increasing test sizes using radar plots. The ACCORD model consistently forms the largest, near-circular polygon, with high precision, recall, balanced accuracy ($\approx$0.99) and strong agreement metrics (MCC, κ $\approx$0.98–0.99). Baselines exhibit pronounced metric asymmetries, with MCC and κ below 0.65 at small sizes and further contraction at larger scales, while precision often remains high but recall and balanced accuracy drop ($\approx$0.80–0.88). ACCORD maintains balanced geometry and near-unity ROC/PR-AUC across all sizes, reflecting stable, globally consistent performance.

VI. Conclusion and Future Work

This paper presented *ACCORD*, an autonomous cognitive cyber defense framework for Cloud Digital Twin (CDT) environments. ACCORD integrates preprocessing for telemetry, anomaly detection based on spiking neural networks, cognition-driven forensics, and adaptive response based on reinforcement learning to provide interpretable, mission-aware and resilient protection. Experimental results demonstrate that ACCORD achieves high detection accuracy, robust forensic reasoning, and effective mitigation with minimal disruption, outperforming state-of-the-art methods across multiple evaluation metrics.

The future work will focus on extending ACCORD to support multi-CDT federated environments, incorporating adversarial robustness against sophisticated attacks, and exploring hybrid neuro-symbolic reasoning for richer causal inference. Additionally, integrating energy-efficient models and real-time policy adaptation will enhance scalability and operational sustainability for large-scale industrial deployments.

References

[1] P. Empl, D. Koch, M. Dietz, and G. Pernul, "Digital twins in security operations: State of the art and future perspectives," *ACM Computing Surveys*, 2024.

[2] HCL Technologies, "Digital twin trends 2024," https://www.hcltech.com/trends-and-insights/digital-twin-trends-2024?utm_source=chatgpt.com, 2024.

[3] B. Breve, G. Cimino, and V. Deufemia, "Hybrid prompt learning for generating justifications of security risks in automation rules," *ACM Transactions on Intelligent Systems and Technology*, vol. 15, no. 5, pp. 1–26, 2024.

[4] Security Info Watch, "Zero hour: The promise and peril of digital twins in security systems," https://www.securityinfowatch.com/ai/article/55293883/zero-hour-the-promise-and-peril-of-digital-twins-in-security-systems?utm_source=chatgpt.com, 2024.

[5] M. Kuštelega, R. Mekovec, and A. Shareef, "Privacy and security challenges of the digital twin: systematic literature review." *Journal of Universal Computer Science (JUCS)*, vol. 30, no. 13, 2024.

[6] Z. Lv, D. Chen, H. Feng, A. K. Singh, W. Wei, and H. Lv, "Computational intelligence in security of digital twins big graphic data in cyber-physical systems of smart cities," *ACM Transactions on Management Information Systems (TMIS)*, vol. 13, no. 4, pp. 1–17, 2022.

[7] C. Gao, H. Park, and A. Easwaran, "An anomaly detection framework for digital twin driven cyber-physical systems," in *Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems*, 2021, pp. 44–54.

[8] Y. Wu, H. Cao, G. Yang, T. Lu, and S. Wan, "Digital twin of intelligent small surface defect detection with cyber-manufacturing systems," *ACM Transactions on Internet Technology*, vol. 23, no. 4, pp. 1–20, 2023.

[9] H. Liu, X. Huang, M. Jia, T. Jia, J. Han, Z. Wu, and Y. Li, "Uac-ad: Unsupervised adversarial contrastive learning for anomaly detection on multi-modal data in microservice systems," *IEEE Transactions on Services Computing*, vol. 17, no. 6, pp. 3887–3900, 2024.

[10] J. Huang, Y. Yang, H. Yu, J. Li, and X. Zheng, "Twin graph-based anomaly detection via attentive multi-modal learning for microservice system," in *2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2023, pp. 66–78.

[11] Q. Xu, S. Ali, and T. Yue, "Digital twin-based anomaly detection with curriculum learning in cyber-physical systems," *ACM Transactions on Software Engineering and Methodology*, vol. 32, no. 5, pp. 1–32, 2023.

[12] J. Pang, X. Pu, and C. Li, "A hybrid algorithm incorporating vector quantization and one-class support vector machine for industrial anomaly detection," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8786–8796, 2022.

[13] H. Torabi, S. L. Mirtaheri, and S. Greco, "Practical autoencoder based anomaly detection by using vector reconstruction error," *Cybersecurity*, vol. 6, no. 1, p. 1, 2023.

TABLE VIII: Model Performance Comparison at Test Size = 150,000

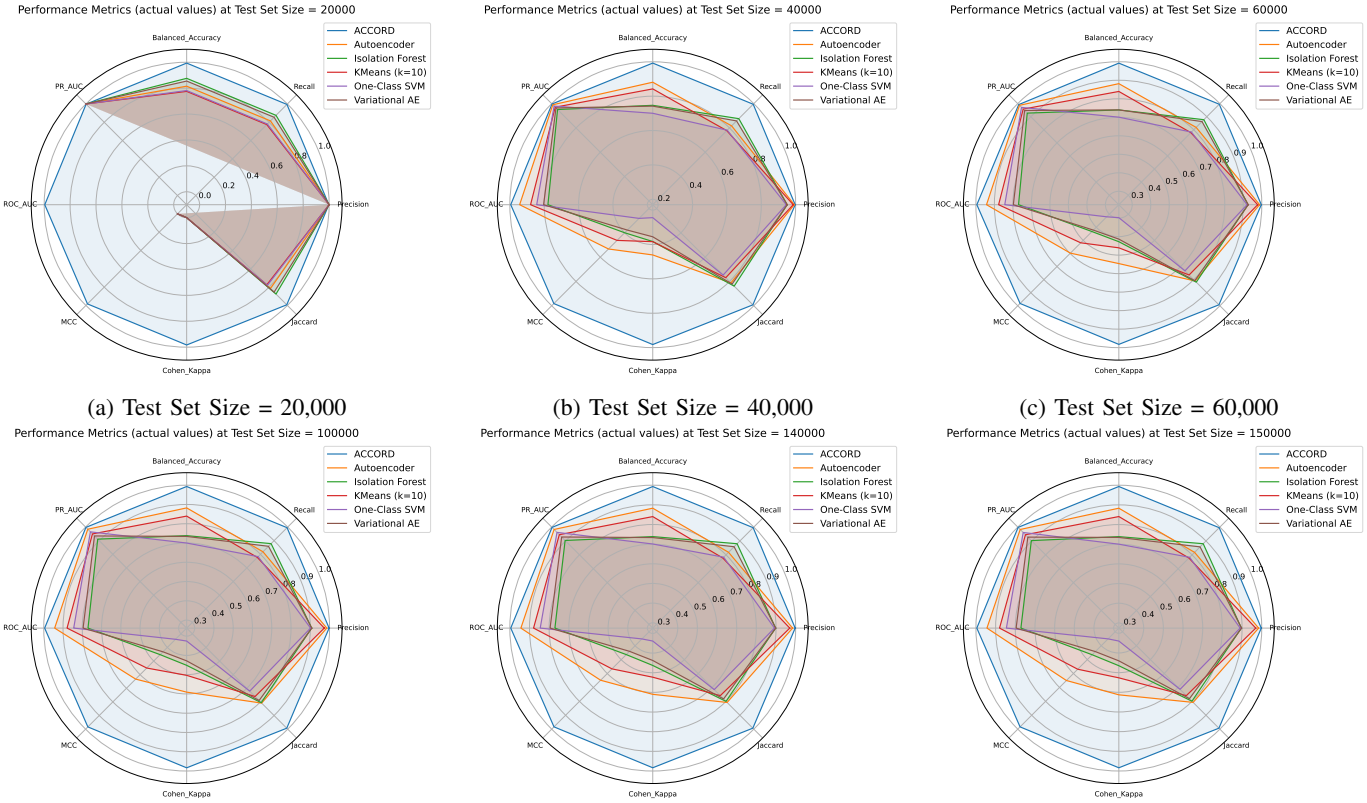
Model	Precision	Recall	F1_Score	Balanced_Accuracy	MCC	Cohen_Kappa	Jaccard	ROC_AUC
ACCORD	0.9977	0.9954	0.9966	0.9973	0.9959	0.9914	0.0086	0.0046
Isolation Forest	0.8966	0.8803	0.8884	0.8933	0.8835	0.5971	0.4029	0.1197
One-Class SVM	0.8904	0.7827	0.8331	0.8666	0.8021	0.6178	0.3822	0.2173
Autoencoder	0.9843	0.8182	0.8936	0.9459	0.8468	0.9481	0.0519	0.1818
Variational AE	0.8976	0.8576	0.8771	0.8893	0.8653	0.6115	0.3885	0.1424
KMeans (k=10)	0.9698	0.7774	0.8630	0.9241	0.8096	0.9040	0.0960	0.2226

TABLE IX: Model Performance Summary (Mean ± Standard Deviation)

Model	F0.5	F2	FNR	FPR	Jaccard	MCC	Precision	Recall	Specificity
Autoencoder	0.9483 ± 0.0037	0.8472 ± 0.0007	0.1819 ± 0.0010	0.0477 ± 0.0164	0.8098 ± 0.0030	0.5569 ± 0.1976	0.9876 ± 0.0053	0.8181 ± 0.0010	0.8523 ± 0.2915
Isolation Forest	0.9112 ± 0.0264	0.8864 ± 0.0049	0.1214 ± 0.0018	0.3602 ± 0.1233	0.8161 ± 0.0255	0.4006 ± 0.1411	0.9200 ± 0.0344	0.8786 ± 0.0018	0.5398 ± 0.1847
KMeans (k=10)	0.9290 ± 0.0073	0.8105 ± 0.0014	0.2226 ± 0.0009	0.0866 ± 0.0297	0.7632 ± 0.0060	0.4857 ± 0.1730	0.9766 ± 0.0102	0.7774 ± 0.0009	0.8134 ± 0.2782
One-Class SVM	0.8846 ± 0.0268	0.8057 ± 0.0049	0.2174 ± 0.0008	0.3444 ± 0.1178	0.7292 ± 0.0224	0.2986 ± 0.1065	0.9148 ± 0.0365	0.7826 ± 0.0008	0.5556 ± 0.1900
Variational AE	0.9069 ± 0.0261	0.8684 ± 0.0061	0.1436 ± 0.0033	0.3475 ± 0.1189	0.7975 ± 0.0251	0.3802 ± 0.1343	0.9208 ± 0.0341	0.8564 ± 0.0033	0.5525 ± 0.1890
Proposed Model	**0.99714 ± 0.00017**	**0.99580 ± 0.00013**	**0.00464 ± 0.00015**	**0.00910 ± 0.00071**	**0.99297 ± 0.00026**	**0.98320 ± 0.00060**	**0.99759 ± 0.00020**	**0.99536 ± 0.00015**	**0.99090 ± 0.00071**

TABLE X: Model Performance Summary (Mean ± 95% Confidence Interval)

Model	F0.5	F2	FNR	FPR	Jaccard	MCC	Precision	Recall	Specificity
Autoencoder	0.9483 ± 0.0018	0.8472 ± 0.0003	0.1819 ± 0.0005	0.0477 ± 0.0077	0.8098 ± 0.0014	0.5569 ± 0.0925	0.9876 ± 0.0025	0.8181 ± 0.0005	0.8523 ± 0.1364
Isolation Forest	0.9112 ± 0.0124	0.8864 ± 0.0023	0.1214 ± 0.0008	0.3602 ± 0.0577	0.8161 ± 0.0119	0.4006 ± 0.0660	0.9200 ± 0.0161	0.8786 ± 0.0008	0.5398 ± 0.0864
KMeans (k=10)	0.9290 ± 0.0034	0.8105 ± 0.0006	0.2226 ± 0.0004	0.0866 ± 0.0139	0.7632 ± 0.0028	0.4857 ± 0.0810	0.9766 ± 0.0048	0.7774 ± 0.0004	0.8134 ± 0.1302
One-Class SVM	0.8846 ± 0.0126	0.8057 ± 0.0023	0.2174 ± 0.0004	0.3444 ± 0.0551	0.7292 ± 0.0105	0.2986 ± 0.0499	0.9148 ± 0.0171	0.7826 ± 0.0004	0.5556 ± 0.0889
Variational AE	0.9069 ± 0.0122	0.8684 ± 0.0028	0.1436 ± 0.0015	0.3475 ± 0.0556	0.7975 ± 0.0118	0.3802 ± 0.0629	0.9208 ± 0.0160	0.8564 ± 0.0015	0.5525 ± 0.0885
Proposed Model	**0.99714 ± 0.00012**	**0.99580 ± 0.00009**	**0.00464 ± 0.00010**	**0.00910 ± 0.00049**	**0.99297 ± 0.00018**	**0.98320 ± 0.00042**	**0.99759 ± 0.00014**	**0.99536 ± 0.00010**	**0.99090 ± 0.00049**



(a) Test Set Size = 20,000 (b) Test Set Size = 40,000 (c) Test Set Size = 60,000

(d) Test Set Size = 100,000 (e) Test Set Size = 140,000 (f) Test Set Size = 150,000

Fig. 18: Radar plots of bounded metrics (Precision, Recall, Balanced Accuracy, PR-/ROC-AUC, MCC, κ, Jaccard) showing relative consistency and geometric balance across test-set sizes.

[14] Z. K. Shahid, S. Saguna, and C. Åhlund, "Variational autoencoders for anomaly detection and transfer knowledge in electricity and district heating consumption," *IEEE Transactions on Industry Applications*, vol. 60, no. 5, pp. 7437–7450, 2024.

[15] M. C. Dani, H. Doreau, and S. Alt, "K-means application for anomaly detection and log classification in hpc," in *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*. Springer, 2017, pp. 201–210.

[16] J. Liu, J. Jia, H. Zhang, Y. Yun, L. Wang, Y. Zhou, H. Dai, and D. Dou, "Efficient federated learning using dynamic update and adaptive pruning with momentum on shared server data," *ACM Transactions on Intelligent Systems and Technology*, vol. 15, no. 6, pp. 1–28, 2024.

[17] Z. Li, M. Duan, B. Xiao, and S. Yang, "A novel anomaly detection method for digital twin data using deconvolution operation with attention mechanism," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 7278–7286, 2023.

[18] S. Li, W. Wu, Y. Meng, J. Li, H. Zhu, and X. S. Shen, "Data poisoning attack against anomaly detectors in digital twin-based networks," in *ICC 2023 - IEEE International Conference on Communications*, 2023, pp. 13–18.

[19] A. Islam, H. Karimipour, T. R. Gadekallu, and Y. Zhu, "A federated unlearning-based secure management scheme to enable automation in

smart consumer electronics facilitated by digital twin," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 1, pp. 62–74, 2025.

[20] N. Moustafa, G. Creech, and J. Slay, "Ton_iot datasets: A new generation of realistic datasets for iot and iiot cybersecurity and anomaly detection research," https://research.unsw.edu.au/projects/toniot-datasets, 2021.