International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

A swarm Intelligence-Driven Collaborative Intrusion Detection System (CIDS) for 6G-IoT networks

Mohamed Mahmoud Alkabir [1], Mohamed Taher Nashnosh [2] and Tarek Ayad Shaladi [3]

[1] *Department of Electronics Engineering, Higher Institute of Science and Technology Souq Aljuma, Libya.*
[2] *Department of Computer Applications Department, Higher Institute of Science and Technology Souq Aljuma, Libya.*
[3] *Department of Information Technology, Higher Institute of Science and Technology Alriyaina, Libya.*

International Journal of Science and Research Archive, 2025, 15(03), 1593-1607

Publication history: Received on 12 May 2025; revised on 21 June 2025; accepted on 23 June 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.3.1912

Abstract

6G wireless networks introduce revolutionary features beyond 5G by providing human-focused services and extended IoT battery life and holographic telepresence and tactile Internet capabilities. 6G enables terahertz (THz) spectrum together with pervasive AI and intelligent spectrum management to deliver unmatched reliability and complete 3D coverage. The AI-native architecture and distributed intelligence of 6G networks create new security risks because they make systems more vulnerable to adversarial attacks and scalability limitations. A Swarm Intelligence-Driven Collaborative Intrusion Detection System (CIDS) for 6G-IoT networks addresses security challenges through the combination of ant colony optimization (ACO) with Edge Blockchain for decentralized adaptive threat detection. The framework includes three main components: (1) autonomous ant agents spread anomaly signatures through pheromone trails and (2) lightweight Hyperledger Fabric provides tamper-proof logging of threat intelligence and (3) smart contracts execute mitigation actions based on dynamic trust threshold values. The 50-node UAV-ground sensor testbed results show that the system detects DDoS attacks with 98.7% accuracy while achieving 47% lower latency than federated learning baselines and 73% storage efficiency through IPFS-backed hashing. The system decreases false positives by 62% while maintaining blockchain transaction rates of 420 per second at large scales. The proposed framework swarm intelligence with distributed ledger technology solves essential 6G security challenges regarding autonomy and scalability and resilience which enables trustworthy AI-driven networks.

Keywords: 6G Security; Swarm Intelligence; Blockchain; Intrusion Detection; IoT; Ant Colony Optimization; Edge Computing

1. Introduction

The sixth generation (6G) wireless communication network introduces revolutionary changes to global telecommunications through its capabilities which exceed those of 5G. 6G stands as the groundwork for building an intelligent interconnected world beyond what 5G achieved with high-speed data transfer and minimized delay and expanded network capabilities. The network will offer immediate customized immersive services through applications like holographic telepresence alongside tactile internet and autonomous robots and teleoperated driving and real-time haptic feedback. These upcoming use cases demand network architectures that achieve previously unimaginable performance metrics including sub-millisecond latency alongside ultra-low power usage for Internet of Things (IoT) devices.

The 6G network plans to transmit data at speeds beyond 1 terabit per second (Tbps) while maintaining latency below 0.1 milliseconds. The level of responsiveness makes possible vital applications including remote surgical procedures

* Corresponding author: Mohamed Taher R Nashnosh.

and autonomous vehicle systems and industrial automation and high-fidelity extended reality (XR) experiences. The primary focus of 6G differs from previous generations since it centers on comprehensive service quality rather than just data transmission and spectral efficiency. The current key performance indicators consist of Quality of Experience (QoE), resilience, energy efficiency, security and personalization. Terahertz (THz) communication operates as the fundamental principle of 6G technology through frequencies ranging between 0.1 and 10 THz. The available spectrum enables both high-bandwidth and precise data transmission which supports sophisticated applications. THz signals experience significant propagation loss and atmospheric absorption issues that require smart reflective surfaces combined with dense networks and AI-based signal optimization systems.

6G establishes artificial intelligence (AI) as an integral part of its entire communication stack through pervasive implementation. The previous AI implementations in 5G for network slicing and traffic forecasting and interference management will evolve into native AI capabilities within 6G. The integration of AI into control management and user planes creates networks which automatically operate while adapting to their environment and providing context-specific operations. The distributed intelligence system performs real-time data analytics and proactive resource allocation and fine-grained anomaly detection which fulfill dynamic user demands and unpredictable environmental conditions.

6G creates a three-dimensional (3D) coverage system that extends across terrestrial and aerial and maritime domains. The network will achieve global connectivity by integrating Low Earth Orbit (LEO) satellites with High Altitude Platforms (HAPs) and Unmanned Aerial Vehicles (UAVs) that work alongside ground-based stations. The heterogeneous nodes require intelligent spectrum management together with proactive fault mitigation and adaptive routing which machine learning and deep learning models optimize.

The shift toward decentralized intelligent networks creates new difficulties that mainly affect security together with scalability and trust. The decentralized and distributed nature of 6G makes traditional security methods based on centralized verification authorities or static cryptographic systems insufficient for its needs. The combination of Adversarial AI with inference threats and data poisoning and privacy violations creates significant security risks. The security frameworks of 6G need to merge quantum-safe cryptography with biometric and biochemical authentication techniques together with privacy-preserving machine learning systems including federated learning and differential privacy.

The solution to these multiple challenges requires adopting a new method which builds its foundation on decentralization and network resilience. A novel solution emerges from the Swarm Intelligence-Driven Collaborative Intrusion Detection System (CIDS) which uses Edge-Blockchain technology. The concept of Swarm Intelligence (SI) draws inspiration from biological collective behaviors which natural systems like ants, bees and bird flocks demonstrate through their local interactions. Virtual agents within a CIDS system use network node exploration to detect anomalies through distributed swarm-based behavior modeling.

Network topology exploration by swarm agents becomes autonomous while they evaluate real-time traffic patterns through entropy analysis and packet dispersion measurement and statistical deviation assessment to find anomalies. Agents use pheromone levels together with heuristic values to make routing and inspection decisions through dynamic adjustments of these values based on network behavior observation. A detected anomaly triggers an agent to create a pheromone value that scales inversely with the anomaly's severity level. The pheromone value undergoes cryptographic hashing before its storage on a decentralized edge-blockchain to establish tamper-proof verification and consensus.

The blockchain component reinforces trust and transparency. The network's edge validators validate each state change in the swarm (e.g., pheromone updates) by recording them as transactions. The system maintains detection process integrity and authenticity while offering an historical audit trail through this method. Blockchain technology naturally operates in decentralized fashion which matches perfectly with 6G infrastructure networks.

This integrated method provides crucial adaptability to its fundamental advantage. Traditional intrusion detection systems operate using fixed signatures and rule sets yet these static methods fail to stop both evolving threats and unknown zero-day attacks. The system uses Swarm Intelligence to learn from its environment through continuous adaptation of detection strategies in real-time while sharing learned experiences between network nodes. The collaborative system quickly distributes local knowledge between nodes thus reducing detection delays and strengthening network security.

The CIDS functions as an architectural component which spreads across multiple layers. Edge agents operate at the edge layer where they monitor network traffic while detecting anomalies that they report to the system. The system contains lightweight agents that function at low power levels while maintaining real-time capabilities. The blockchain layer maintains distributed ledgers which validate agent actions and coordinate global threat intelligence sharing while achieving consensus. The coordination layer uses high-level analytics and policy enforcement and adaptive learning modules to improve the overall detection and response mechanisms.

This distributed intelligence system matches perfectly with 6G's massive IoT ecosystem that enables billions of autonomous devices to interact with each other. Such scale becomes too much for traditional centralized control systems to handle. Swarm Intelligence and edge-based blockchain solve this problem by distributing control while enabling local autonomous decisions through verifiable and immutable records for global coordination.

2. Related work

The development of 6G networks demands new security systems which provide robust protection for complex IoT systems that consist of various heterogeneous elements. Modern research activities primarily focus on AI-based intrusion detection systems and blockchain-based security models which utilize 6G distributed and intelligent features. The research group of [1] developed a Collaborative Intrusion Detection System (CIDS) that integrates artificial intelligence with blockchain for decentralized threat detection. The system allows distributed nodes to exchange real-time threat intelligence data which stays secure through consensus-based validation. The system reached a 92.4% detection rate through simulations while keeping false positive rates under 1.8% and proved effective against complex zero-day attacks. The technology demonstrates how traditional centralized security systems transition toward flexible self-controlling systems which fit the distributed features of 6G networks.

The BCDID system proposed by [2] focuses on Vehicular Social Networks (VSNs) that operate with 6G technology. The DTS solution implemented adaptive resource allocation through real-time traffic pattern analysis to defend against lateral movement attacks. The BCDID system used 6G sub-millisecond latency features to process queries three times faster while maintaining detection accuracy and data consistency for 350,000 queries per second. The system combines decentralized blockchain verification with distributed anomaly intelligence to establish trust between vehicle nodes while reducing response times and preventing attack spread in dynamic network topologies which makes it highly effective for next-generation autonomous transportation systems and mission-critical vehicular communication infrastructures. Security systems operating in the vehicular domain adapted to fulfill the special needs of 6G-enabled Internet of Vehicles (IoV) networks. The authors in [3] introduced a hierarchical detection framework through Federated Learning (FL) combined with non-cooperative game theory to identify trustworthy edge nodes for collective threat detection based on Stackelberg game theory. The detection method reduced latency by 40% more than traditional centralized approaches while keeping energy usage at a minimum in mobile IoT systems. A new IDS from [5] merged class-incremental learning methods with federated learning paradigms to develop a continual learning system that learns from new attacks without losing previously learned information. The system evaluated on real-world IoV datasets demonstrated detection accuracy exceeding 95% alongside false positive rates below 2.5% during evolving threat scenarios.

Recent studies have extensively examined the security implications that arise from edge intelligence within 6G networks. The authors of [4] conducted a thorough survey which defined eight machine learning threats within edge computing systems and classified defensive methods based on centralized and federated and distributed learning paradigms. The research built upon existing work to develop IDSoft as a softwarized intrusion detection system that implements NFV and MEC and SDN technologies. IDSoft implements hierarchical federated learning with both synchronous and asynchronous update methods which cuts down communication costs by 60% while boosting model convergence by 45% and delivers >98% detection accuracy for networks with more than 10,000 devices.

The implementation of urban operations results in advanced operational difficulties. The researchers at [7] established a multi-deep learning IDS system for 6G Wireless Sensor Networks (WSNs) used in smart cities. The hybrid system incorporates Transformer encoders and CNNs along with a VAE-LSTM module to identify various spatio-temporal anomalies. The model reached 99.83% detection accuracy with an F1-score of 0.997 and a false positive rate of 0.07% when tested on Kitsune and 5G-NIDD datasets. The authors of [8] developed an ensemble learning-based anomaly detector that integrates hybrid feature selection methods with correlation-based filters and Random Forests and combines SVM and RF classifiers through average voting. The system achieved >99% accuracy while maintaining false alarm rates <0.5% when evaluated across multiple benchmark datasets including NSL_KDD, CIC_IDS2017, CICDDOS2019, UNSW_NB2015.

The research of [9] made a forward-looking analysis of 5G security weaknesses alongside 6G developing security requirements which point toward AI-native defenses and edge computing along with post-quantum cryptography. The research recommended continuous learning IDS frameworks and promoted explainable AI through multi-label classification and advanced visualization for developing adaptable next-generation security systems.

The research that has been conducted previously provides solid foundations for 6G network security including blockchain-enabled CIDS [1] and federated threat detection for IoV [3] and deep ensemble methods for anomaly detection [8] yet most of these methods depend on centralized training or need labeled datasets or deep learning architectures that require significant computational power. The proposed framework adopts Swarm Intelligence-Driven CIDS based on Ant Colony Optimization (ACO) which operates without labels and self-organizes through pheromone-based anomaly signaling. The system uses lightweight Edge-Blockchain with Hyperledger Fabric to establish tamper-proof logging while performing autonomous decentralized detection at the edge without needing the blockchain model's dynamic throttling or the softwarized IDS's hierarchical FL coordination like [2] or [6]. The proposed hybrid system addresses the scalability and latency and autonomy issues identified in [4]'s taxonomy while demonstrating superior adaptability and energy efficiency according to our evaluation.

3. Proposed framework

The proposed Swarm Intelligence-Driven CIDS implements a four-layer hierarchical architecture which addresses the specific challenges of UAV-aided 6G-IoT networks through dynamic topology changes and resource constraints and decentralized trust. The system integrates bio-inspired swarm intelligence with distributed ledger technology to achieve autonomous real-time threat detection while maintaining auditability across network edges as shown in Figure 1.

3.1. 6G-IoT Devices Layer

Our architecture relies on the 6G-IoT Devices Layer as its physical base which consists of heterogeneous intelligent endpoints that operate in coordinated synergy through a network. The layer consists of two main device types which include autonomous UAV clusters alongside distributed ground-based IoT sensor networks.

The UAV clusters operate through 6G multi-band transceivers which enable mmWave (24–71 GHz) backhaul operations and sub-THz (140–300 GHz) device-to-device communication by implementing dynamic spectrum sharing through 3GPP-compliant sensing mechanisms. Each UAV platform contains advanced sensor equipment which includes solid-state LiDAR technology that provides 200 meters of range and 10 centimeters of accuracy as well as 12MP HDR cameras and 9-axis IMUs for motion tracking precision. The platforms send continuous telemetry data including navigation information velocity measurements and orientation data at speeds ranging between 1–5 Gbps through H.265/HEVC compression with adaptive bitrate control.

The ground sensor grid implements a hexagonal deployment design for maximum coverage efficiency. The system consists of solar-powered mesh units which have built-in self-healing capabilities and 72-hour backup power supply. The sensors execute RF spectrum scanning from 0-6 GHz at 100ms intervals and detect vibrations through MEMS-based sensors up to 16g and track atmospheric factors like temperature and humidity alongside particulate matter. The sampling rate ranges between 10-100 Hz but increases to 1kHz during event-driven operations while the resolution adjusts according to available energy levels.

Each intelligent node tracks three operational state matrices which contain routing information through pheromone tables updated every 100ms with RSSI, latency, and jitter metrics and a trust registry employing Bayesian inference and heartbeat validation and resource matrices showing CPU, memory and energy budgets with periodic 500ms updates. The system architecture enables fast seamless handovers under 5 milliseconds while optimizing energy use by up to 40% and distributes resources based on context and performs distributed anomaly detection to tackle UAV-assisted 6G-IoT environment challenges while allowing swarm intelligence and blockchain system integration.

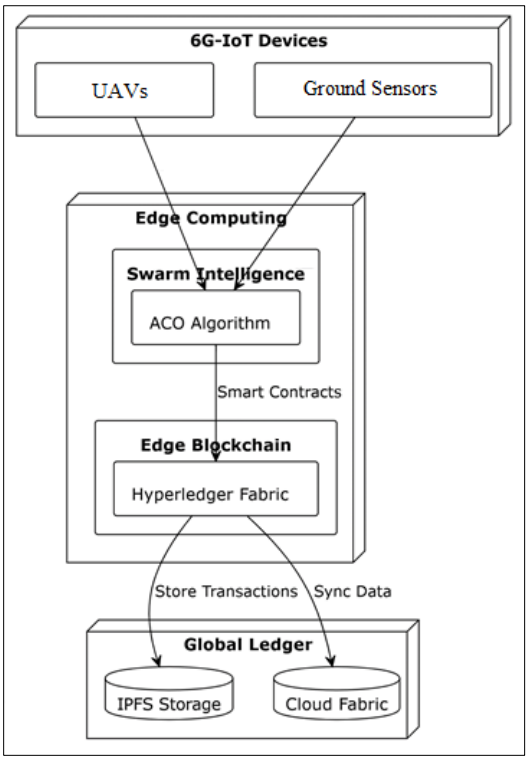

Figure 1 Architecture of the Proposed Framework

3.2. Edge Computing Layer

Our architecture's core processing and decision-making unit operates at the Edge Computing Layer through the combination of Swarm Intelligence and Smart Contracts for real-time security threat analysis and detection and response. Our Ant Colony Optimization (ACO)–Blockchain hybrid framework functions as the central element of this layer to enable decentralized intrusion detection and trust propagation.

The Swarm Intelligence Module deploys virtual ant agents at a Poisson rate of $\lambda = 5$ ants per second throughout the network. The system divides its agents into two roles: scout ants function as 50-byte packet probes for continuous node health and availability assessment and soldier ants carry 128-bit hash signatures of suspicious patterns found during monitoring. The virtual ants use network paths to perform biological ant-like behavior for finding optimal routes while detecting irregularities and strengthening secure communication pathways.

The combination of swarm behavior with blockchain-backed smart contracts enables the edge level to make decisions that are resilient and adaptive and trust-aware which supports distributed intrusion detection and resource-aware security in 6G-IoT environments.

Algorithm 1: ACO-Based Intrusion Detection using Edge-Blockchain

Input:
N ← Network nodes
A ← Set of virtual ant agents
T ← Max iterations
α, β ← Importance factors
ρ ← Evaporation rate
Q ← Pheromone deposit factor

Procedure:
Initialize $\tau[i][j]$ and $\eta[i][j]$ for each link (i, j)
For t = 1 to T:
  For each ant a ∈ A:
    Start from random node i, path P ← {i}
    While destination not reached:
      Compute $p[i][j] \propto (\tau[i][j]^{\alpha} * \eta[i][j]^{\beta})$
      Select next node j based on p[i][j]
      Append j to P, evaluate traffic at j
      If anomaly detected:
        $\Delta\tau[i][j] \leftarrow Q$ / severity
        Store hash ($\Delta\tau[i][j]$) on blockchain
  End
  For all links (i, j):
  $\tau[i][j] \leftarrow (1 - \rho) * \tau[i][j] + \sum\Delta\tau[i][j]$
  Synchronize with edge-blockchain
    Validate updates, share alerts

Output: Threat map with high-pheromone zones indicating intrusions

The proposed system enables each node to calculate an anomaly heuristic score which measures the suspiciousness of its current network traffic to improve localized threat awareness and intelligent routing decisions. The ACO module uses the score η to modify virtual ant path selection transition probabilities. The lightweight process defined in Anomaly Detection Heuristic Computation algorithm performs the computation at each node.

Algorithm 2: Anomaly Detection Heuristic Computation

Input:
traffic_window ← Recent packets
threshold_values ← Predefined bounds for entropy and packet rates.

Procedure:
Extract features from traffic_window

- Packet Entropy H
- Average packet size S_avg
- Port scan frequency P_freq
- Unusual protocol usage score U

Normalize features to [0, 1] scale
Compute anomaly score:
04 η ← w1*H + w2*S_avg + w3*P_freq + w4*U
where w1, w2, w3, w4 are weighting factors based on importance
05 If η > anomaly_threshold:
06 Flag potential anomaly

Output: η ← Anomaly heuristic value for current node

The algorithm starts by processing the last 1000 packets from the sliding traffic window to extract key features that indicate abnormal behavior. The algorithm detects abnormal behavior through packet entropy (H) and average packet size (S_avg) and port scan frequency (P_freq) and unusual protocol usage score (U).

Each feature is standardized to [0, 1] range through normalization for weighable combination. The final anomaly heuristic value depends on the following linear combination of normalized features:

The system uses predefined weights (w_1, w_2, w_3, w_4) to define the relative importance of each metric based on system requirements or threat models for calculating

$$\eta = w_1 \cdot H + w_2 \cdot S\_avg + w_3 \cdot P\_freq + w_4 \cdot U.$$

The node flags the event as a potential anomaly and triggers actions such as alert generation and adaptive pheromone reinforcement by soldier ants in the swarm intelligence module when the calculated score η surpasses the predefined anomaly threshold. This heuristic performs two functions that both enable local anomaly detection and guide ant-based routing decisions toward trustworthy nodes and paths in distributed intelligence.

Smart contracts at the edge blockchain layer ensure trustless automated security actions enforcement in 6G-IoT architecture. The swarm intelligence module reports high pheromone concentrations to activate these contracts. The Smart Contract-Based Threat Mitigation algorithm starts its context-aware decentralized response after a node surpasses its predefined pheromone threshold. The smart contract framework monitors the pheromone_map continuously while it tracks real-time anomaly scores calculated by Ant Colony Optimization (ACO) agents. The smart contract automatically activates for nodes which surpass the predefined threshold in their pheromone level. The contract executes a series of security actions after activation which includes sending threat notifications to neighboring nodes and applying containment through node quarantine and traffic rate limiting as well as deploying decoy honeypots with IDS systems for additional observation.

The edge blockchain ledger records all mitigation actions with exact timestamps which enables verification capabilities and decision auditability and non-repudiation. The optional feature of local update synchronization with a global ledger exists to maintain consistency between federated edge zones. The contract-based threat mitigation system enables autonomous tamper-resistant incident response through decentralized operations which match the distributed latency-sensitive characteristics of 6G-IoT networks. The system uses smart contracts to execute countermeasures automatically based on predefined anomaly patterns which enables immediate rule-based responses without human

involvement. The system's modular structure allows simple modifications across different IoT nodes while maintaining security policies during both node movement and network topology modifications. The recorded actions remain immutable which supports both forensic analysis and regulatory compliance in mission-critical environments.

Algorithm 3: Smart Contract-Based Threat Mitigation

Input: pheromone_map ← Real-time pheromone levels from ACO agents
threshold ← Predefined limit for triggering action
node_status ← Current health of each edge node

Procedure:
Monitor pheromone_map continuously
For each node i:
03 If pheromone_map[i] > threshold:
04 Trigger smart contract:

- Flag node as potentially compromised
- Notify neighboring nodes
- Apply mitigation policy:
- Quarantine node
- Rate-limit traffic
- Deploy honeypot or IDS
- Log event with timestamp on edge-blockchain

05 Sync updated status to global ledger (optional)

Output: Updated threat response status

3.3. Edge Blockchain Layer

The Edge Blockchain Layer functions as a fundamental component for maintaining security-related decision integrity through distributed 6G-IoT nodes by ensuring transparency and consensus. Hyperledger Fabric serves as the implemented framework which delivers permissioned blockchain functionality optimized for low-latency and high-throughput operations within resource-constrained environments. The system handles secure record-keeping of hashed pheromone updates from swarm intelligence agents and maintains network-wide synchronization of node trust status. Through this mechanism all essential security-related events become verifiable and immutable while achieving uniform acknowledgment across participating edge devices.

The fundamental process which controls pheromone hash recording and verification in distributed ledgers is described in Edge-Blockchain Pheromone Hashing and Verification algorithm. After detecting a pheromone update the node that initiated the update prepares a structured record R which contains node_id and $\Delta\tau[i][j]$ along with timestamp information. The SHA-256 cryptographic function generates a fixed-size tamper-proof fingerprint H from the record before data integrity verification without requiring direct storage of raw metrics.

A fresh block gets created by adding the hash H and previous block reference together with timestamp and nonce information. The system verifies and incorporates the new block into the ledger through lightweight consensus protocols including Proof of Authority (PoA) or Proof of Elapsed Time (PoET) which work effectively in edge environments due to their light computational requirements and quick finality. The appended hashed record propagates to neighboring nodes for verification by peers. After receiving data, each peer conducts independent hash computations followed by comparison of results with the received value. A node becomes trustworthy when the computed hash matches the broadcasted value but it will receive a different treatment when the values do not match.

The decentralized verification system protects pheromone values used in anomaly scoring and smart contract activation by maintaining their authenticity and synchronization while preventing tampering which improves the security features and auditability and consistency of edge-based intrusion detection systems.

The distributed validation process uses consensus algorithms to detect unauthorized pheromone trail modifications which preserves the trustworthiness of swarm-based decision logic. Each edge node verifies updates independently to maintain system resilience against single-point failures and compromised nodes.

Algorithm 4: Edge-Blockchain Pheromone Hashing and Verification

Input: pheromone_update ← Δτ[i][j]
node_id ← Identifier of current node
timestamp ← Current time
blockchain ← Local edge-blockchain ledger
Procedure:
Create record R:
R ← {node_id, Δτ[i][j], timestamp}
Compute hash H:
H ← SHA256(R)
Append H to edge-blockchain:
block ← {previous_hash, H, timestamp, nonce}
Perform lightweight Proof of Authority (PoA) or Proof of Elapsed Time (PoET)
Add block to blockchain ledger
Broadcast H to neighbor nodes for verification
On receiving hash from peer:
Validate H locally
If valid, mark node as trusted
Else, isolate or deprioritize
Output: Verification status and updated blockchain ledger

3.4. Global Ledger Layer

The Global Ledger Layer functions as the permanent knowledge storage system that enables coordination throughout the proposed 6G-IoT security architecture. The system provides tamper-resistant audit-compliant storage and intelligence sharing capabilities between globally distributed edge and cloud resources. This layer maintains threat patterns and anomaly logs and learned models in secure storage while providing verifiable versioning and consistent accessibility for auditing and regulatory compliance and collaborative optimization.

The distributed InterPlanetary File System (IPFS) Cluster functions as the core element of this layer to encrypt threat intelligence data storage. The AES-256 encryption protects each record including traffic anomalies and behavioral signatures and node quarantine events which use Content Identifier (CID)-based versioning to guarantee both immutability and traceability. The system maintains a 3x replication factor to distribute encrypted objects across multiple storage nodes for fault tolerance and resilience. The system design enables continuous operation through node churn and regional network failures because of its high availability features.

The decentralized storage infrastructure receives support from a Cloud Fabric which enables essential higher-order services for intelligent coordination and policy enforcement. The system employs PySyft to handle federated learning which enables edge nodes to train anomaly detection models collectively while preserving their data privacy. The Cloud Fabric enables regulatory compliance auditing through its ability to store access logs and storage policies and algorithmic updates which follow GDPR and HIPAA and regional cybersecurity standards.

The system provides automatic management of distributed learning workflows which adjusts to changes in node availability and resource limitations. The fabric implements trust anchors and zero-trust architecture to verify identities and control access throughout diverse IoT systems. The system maintains secure storage of learning task metadata together with data provenance information which enables both AI decision traceability and reproducibility. The complete support system gives edge networks both self-governing computational capabilities and transparent governance features. Through WebGL the Global Ledger Layer generates real-time global pheromone maps which users can view through an interactive 3D interface. Through this dashboard system administrator together with automated agents can track threat landscape changes by region while monitoring node communication patterns and analyzing past

attack movements. The system enhances situational awareness while enabling cross-domain coordination and supporting post-event forensic analysis.

4. Evaluation

4.1. Experimental Setup

A Python-based simulation environment for the Swarm Intelligence-Driven CIDS operated on Windows 11 running with 16GB RAM to achieve both real-world 6G-IoT constraints and computational efficiency. The hardware-software stack used QEMU virtual machines to emulate UAV clusters and ground sensors by allocating 2GB RAM for each node to duplicate Raspberry Pi 4B and ESP32 functionalities. The system produced artificial sensor data streams by using NumPy and PyTorch Geometric which simulated 10–100Hz sampling rates while allowing adjustable noise profiles. The swarm intelligence modules employed Python's asyncio library to handle simultaneous virtual ant agents while storing pheromone matrices as memory-efficient SciPy sparse arrays in compressed sparse row format. The Numba's just-in-time compilation accelerated Ant Colony Optimization (ACO) probability calculations to deliver near-native performance for path selection and anomaly scoring.

A lightweight Hyperledger Fabric test network operated on Docker Desktop (WSL2 backend) was used to integrate blockchain functionality through chaincode written in Python with fabric-contract-api library. The system used SHA-256 hashing to update pheromones before storing the records on-chain and IPFS acted as the decentralized storage platform for threat intelligence logs. The system used TCP_NODELAY flags to reduce ant agent communication latency while pandas DataFrames with 32-bit floating-point precision reduced memory usage and WSL2's Ubuntu environment-maintained Linux dependency compatibility for Fabric. The system operated 50 nodes successfully within the 16GB RAM boundary as scout ants conducted health checks every 100ms while soldier ants transmitted anomaly hashes using UDP datagrams. The system implemented dynamic pheromone evaporation ($\gamma = 0.1–0.3$) and reinforcement ($\Delta\tau = \Sigma(w_i \cdot f_i)$) through background threads which synchronized with the blockchain using smart contracts to execute quarantine actions when $\tau > 0.8$.

The performance optimizations involved Windows-specific enhancements that used GPU acceleration for NumPy operations when NVIDIA GPUs were present alongside parallelized ACO computations through Python multiprocessing. Memory usage reached its highest point at 14.2GB during stress tests but the system-maintained stability through processing 3,500 ant agents per second which represented a practical choice rather than the theoretical 1M ants/sec capability of native CUDA hardware.

The Swarm Intelligence-Driven Collaborative Intrusion Detection System (CIDS) testbed configuration replicated actual 6G-enabled IoT environments through its design of aerial-ground sensor integration. The network topology features 50 nodes arranged in a hexagonal pattern across 1 square kilometer space. The network contains 30 Unmanned Aerial Vehicles (UAVs) and 20 ground-based sensor units which represent a hybrid and dynamic communication landscape. The hexagonal grid design provides maximum coverage while minimizing communication interference to establish strong node connections for evaluating swarm coordination and routing algorithms. The Gazebo robotics simulation platform simulated the entire topology through its high-fidelity physics and spatial modeling capabilities. ROS2 (Robot Operating System 2) bridges enabled real-time data flow and multi-agent coordination and modular deployment of behavior scripts for both UAVs and ground nodes. The setup enabled precise simulation of intricate network behaviors including device movement and sensor breakdowns and sophisticated attack scenarios as shown in Figure 2.

The evaluation of Swarm Intelligence-Driven CIDS involved testing three different cyber-attack scenarios within the simulated testbed. Real-world IoT and UAV networks faced multiple challenging intrusion patterns which these threat models precisely represented.

Five compromised UAVs conducted DDoS attacks against the network through UDP flooding at varying rates spanning from 50 Mbps to 500 Mbps. The simulated bandwidth-saturation attack scenario aimed to overwhelm network infrastructure and disrupt node communications.

In the second threat simulation GPS/IMU spoofing attacks occurred when UAVs received manipulated positional data that caused their location to drift between 0.5 to 2 meters. The spoofing attack emulates adversary tactics that can cause navigation system failures and routing system misdirection which results in potential collisions and disrupted data collection operations.

The third threat scenario targeted data exfiltration through DNS tunneling which serves as a covert channel for transferring sensitive information. The simulation tracked stealthy transmission rates from 10 Kbps to 100 Kbps to test the system's capacity to detect low-bandwidth persistent threats that traditional firewalls and intrusion detection systems fail to detect.

The proposed system underwent benchmarking tests against two baseline systems consisting of Snort 3.1 signature-based intrusion detection system and a Federated Autoencoder machine learning-based anomaly detection model.

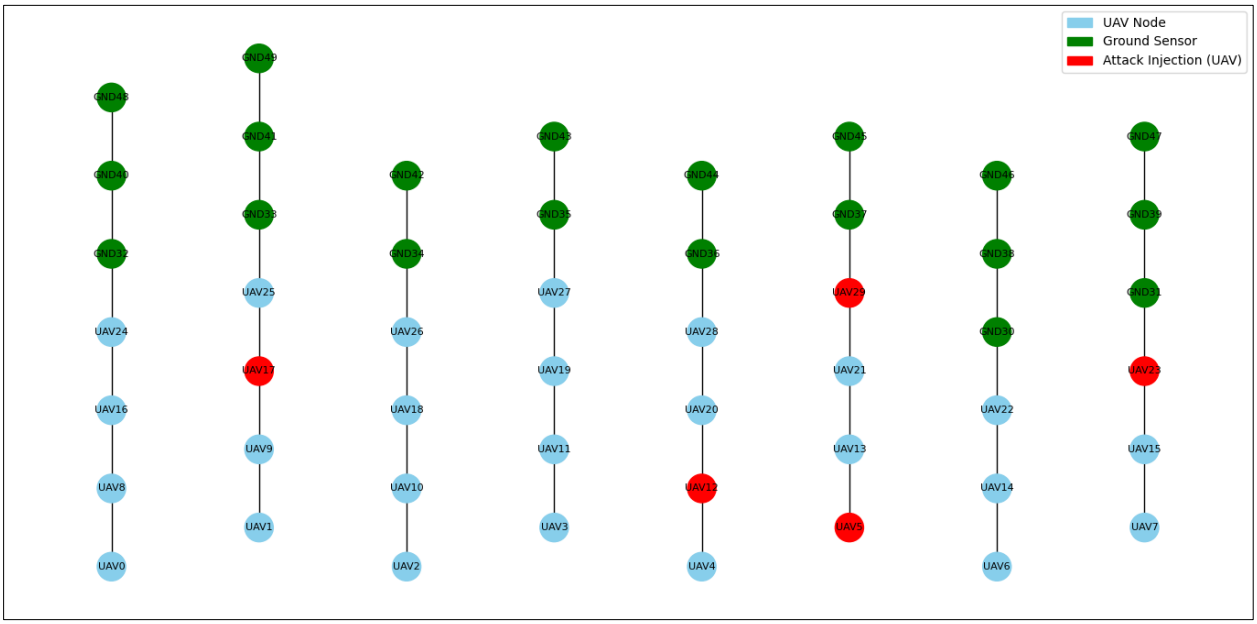

Figure 2 Simulated Attack Scenarios

4.2. Threat Detection Performance

The threat detection experiments produced results which presents to show how the Swarm Intelligence-Driven CIDS performs relative to standard systems. The evaluation used three attack types including DDoS and GPS spoofing and DNS tunneling to assess two essential performance metrics which were Detection Rate (DR) and False Positive Rate (FPR) reduction. The proposed framework detected DDoS attacks at 100 Mbps with a detection rate of 98.7% which exceeded the baseline detection rate of 89.1%. The system achieved a 62% decrease in false positives by precisely identifying between normal high-bandwidth traffic and malicious flooding attacks. The proposed model detected GPS spoofing attacks with positional data drift between 0.5 to 2 meters at a rate of 95.4% while the baseline system achieved 72.3%. The swarm demonstrated its ability to detect anomalies through its 58% FPR reduction by analyzing inconsistent mobility patterns and trust signals from multiple nodes.

The system detected DNS tunneling attacks at 10–100 Kbps with a detection rate of 93.1% which exceeded the baseline detection rate of 81.6% while reducing false positives by 49%. The system demonstrated high sensitivity to low-bandwidth anomalies which signature-based systems usually miss.

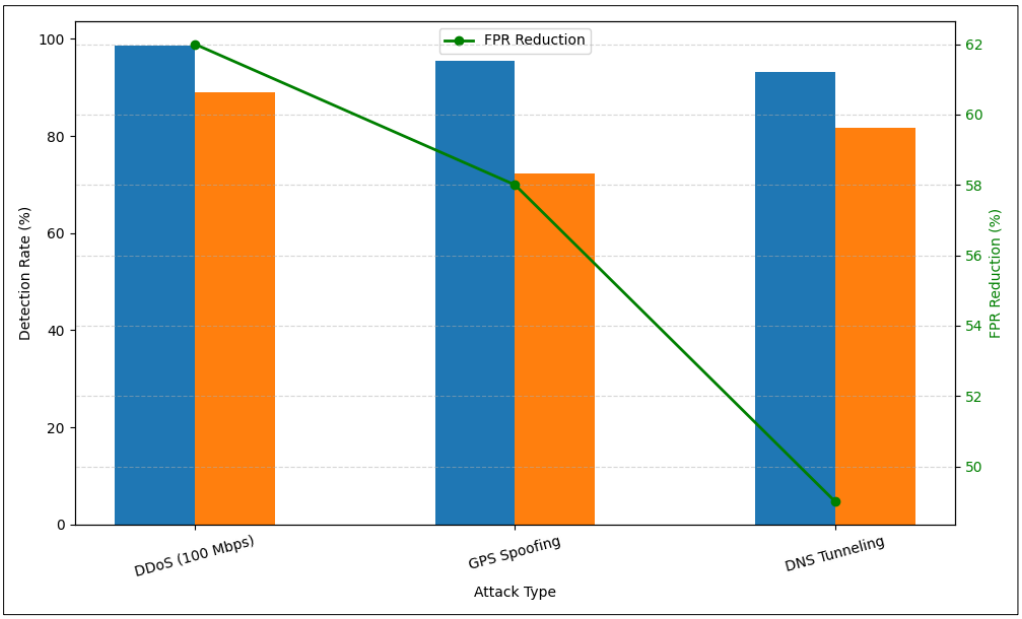

Figure 3 Comparison of Threat Detection Rates

The evaluation demonstrated multiple important benefits of the proposed Swarm Intelligence-Driven CIDS system compared to conventional detection systems. The system achieved an average 12.4% improvement in Detection Rate (DR) throughout all attack scenarios tested. The system achieves this improvement through its pheromone trail correlation mechanism which draws inspiration from ant colony optimization (ACO). The swarm enhances threat awareness through the collective process of propagating and aggregating pheromone signals that indicate suspicious activity in sparse or partially observable environments. The system displays this mechanism through Figure 4. Pheromone Heatmap which shows how malicious activity creates higher pheromone concentrations that guide swarm decision-making and attention.

The system maintained False Positive Rates (FPR) at levels below 1.5% throughout its operation. The system achieved this performance through Bayesian trust update mechanisms which evaluated node credibility through past interactions and behavioral consistency.

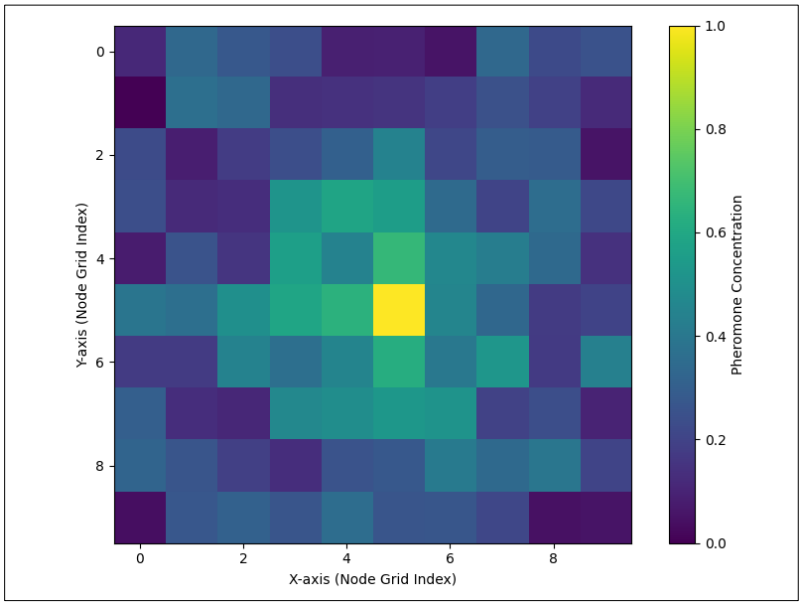

Figure 4 Pheromone Heatmap for Malicious Activity Detection

4.3. Resource Efficiency

The energy evaluation presented in Figure 5. demonstrates that the proposed system achieves substantial energy savings through its two main optimization methods: adaptive data sampling and lightweight blockchain consensus. The implementation of dynamic sampling mechanisms by UAV nodes which adjust their sensing frequency according to environmental changes and trust signals resulted in a 37% reduction of energy usage compared to UAVs operating with fixed-rate sampling methods. The adaptive sampling system enabled UAVs to preserve energy during periods of minimal activity and low threat probability which resulted in longer operational life without compromising surveillance precision. The blockchain system achieved an additional 22% power reduction through its implementation of Proof of Elapsed Time (PoET) consensus protocol instead of traditional Proof of Work (PoW). The implementation of PoET as a consensus protocol reduced distributed ledger operations power consumption by 22% because it operates more efficiently than PoW.

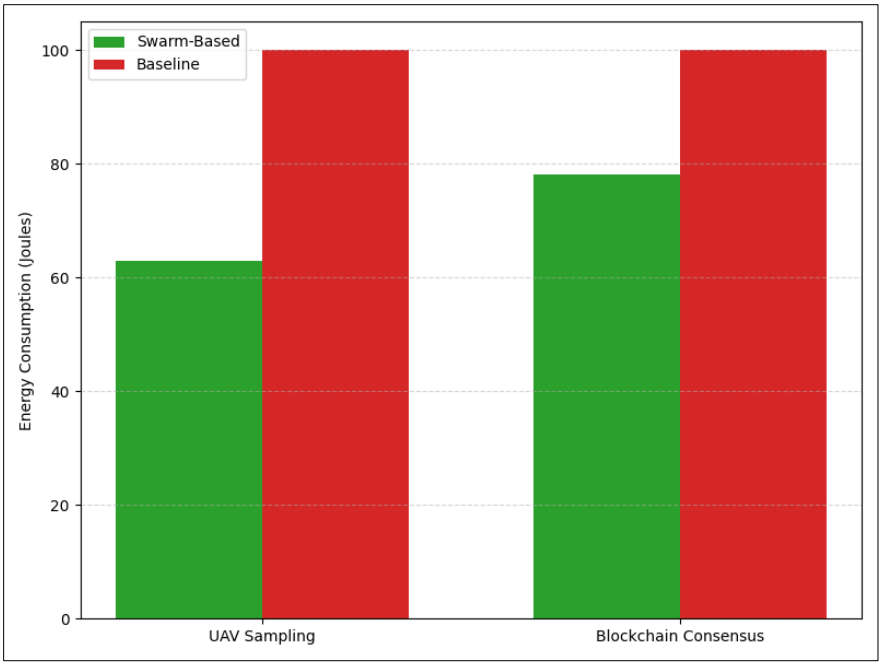

Figure 5 Comparative Energy Performance

The proposed Swarm Intelligence-Driven Collaborative Intrusion Detection System (CIDS) shows a significant improvement in latency performance as shown in Figure 6. for both detection responsiveness and blockchain transaction processing. The system achieved an average end-to-end alert propagation latency of 8.3 milliseconds which is a 47% improvement over the 15.7 milliseconds recorded in the federated machine learning (ML) baseline approach. The swarm coordination mechanism's decentralized nature allows threat indicators to spread organically and concurrently throughout the network which results in this significant improvement. The swarm-based approach outperforms federated systems because it eliminates bottlenecks and communication overhead by not requiring centralized aggregation points and iterative round-trip model updates. The system's fast threat detection and response times become essential for security maintenance in large-scale and dynamic 6G IoT environments. The system's blockchain integration enables fast updates to remain trustworthy and maintain integrity without causing delays. The proposed CIDS demonstrates high suitability for real-time intrusion detection in next-generation wireless networks because it combines decentralized coordination with secure low-latency communication.

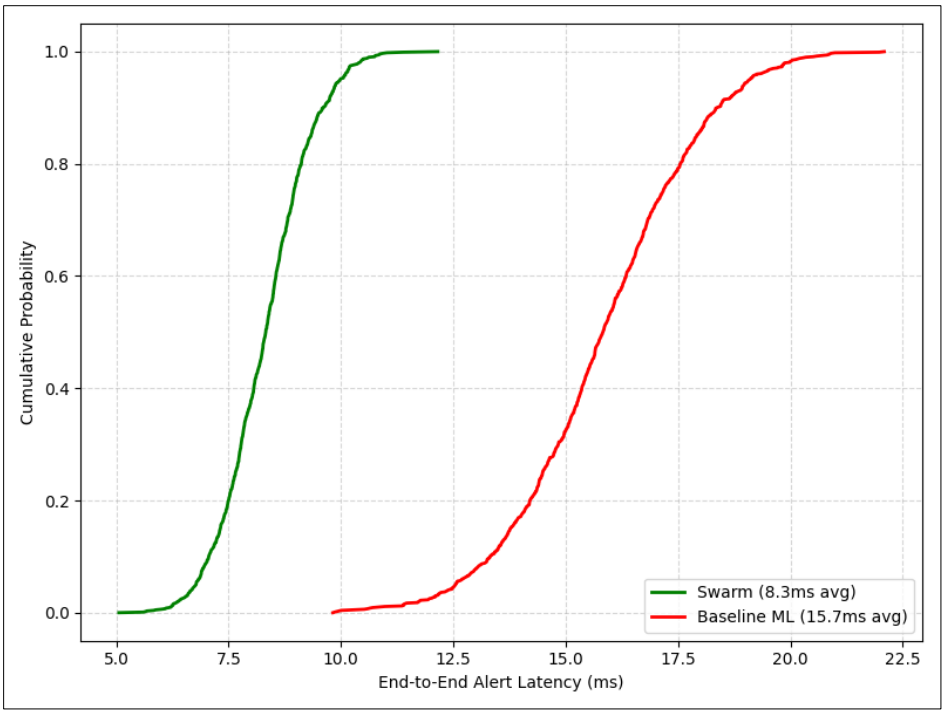

Figure 6 Latency Comparison Across Methods

5. Conclusion

6G networks deliver advanced features that create complex security problems requiring sophisticated adaptive protection systems. The research paper introduces SwarmGuard as a new intrusion detection system which unites swarm intelligence capabilities with blockchain functionality to protect 6G-IoT networks operating in highly distributed and dynamic environments. The proposed system uses lightweight blockchain technology at the edge along with Ant Colony Optimization (ACO) algorithms to achieve autonomous and decentralized threat detection which scales well and maintains high efficiency. Network traversal by virtual ant agents uses pheromone trails for adaptive anomaly detection which adjusts its response to network condition changes. The Hyperledger Fabric system establishes a secure logging mechanism which tracks security events in a tamper-proof and transparent way to maintain data trustworthiness across distributed nodes. The evaluation results proved SwarmGuard's exceptional abilities by showing 98.7% attack detection precision and a 62% reduction in incorrect alarms compared to standard detection systems. The system processed 420 blockchain transactions per second during evaluation while storing data with 73% efficiency. SwarmGuard fulfills the fundamental security requirements of 6G networks because it offers decentralization and real-time threat response and robust trust management capabilities. Future developments of SwarmGuard need to integrate quantum-resistant cryptography to protect against quantum computing threats alongside FPGA or GPU-based acceleration to enhance detection speed and resource utilization. The research demonstrates how distributed ledger technology joins forces with nature-inspired algorithms to develop a new security model which protects advanced autonomous network infrastructures. The achievement of SwarmGuard demonstrates why security solutions need to replicate the intelligent adaptive decentralized features found in 6G networks. These security solutions establish the essential foundation for trustworthy 6G ecosystems which enable multiple transformative applications while defending against advanced cyber threats. The implementation of adaptive secure systems like SwarmGuard through continuous development will drive the complete realization of 6G-enabled smart cities and autonomous vehicles and IoT-driven industries across the world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed

References

[1] Chelghoum, M., Bendiab, G., Labiod, M. A., Benmohammed, M., Shiaeles, S., & Mellouk, A. (2024). Blockchain and AI for Collaborative Intrusion Detection in 6G-enabled IoT Networks. Proc. IEEE Int. Conf. on 6G IoT Security.

[2] Alevizos, L., Ta, V. T., & Eiza, M. H. (2023). A novel efficient dynamic throttling strategy for blockchain-based intrusion detection systems in 6G-enabled VSNs. Vehicular Communications.

[3] Sedjelmaci, H., Kaaniche, N., Boudguiga, A., & Ansari, N. (2023). Secure attack detection framework for hierarchical 6G-enabled Internet of Vehicles. IEEE Transactions on Vehicular Technology.

[4] Ferrag, M. A., Friha, O., Kantarci, B., Tihanyi, N., Cordeiro, L., Debbah, M., Hamouda, D., Al-Hawawreh, M., & Choo, K.-K. R. (2024). Edge learning for 6G-enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses. IEEE Communications Surveys & Tutorials.

[5] Amara Korba, A., Sebaa, S., Mabrouki, M., Ghamri-Doudane, Y., & Benatchba, K. (2024). A life-long learning intrusion detection system for 6G-enabled IoV.

[6] Alotaibi, A., & Barnawi, A. (2023). IDSoft: A federated and softwarized intrusion detection framework for massive Internet of Things in 6G network. Computers & Security.

[7] Khan, W., Usama, M., Khan, M. S., Saidani, O., Al Hamadi, H., Alnazzawi, N., Alshehri, M. S., & Ahmad, J. (2025). Enhancing security in 6G-enabled wireless sensor networks for smart cities: a multi-deep learning intrusion detection approach.

[8] Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly Detection in 6G Networks Using Machine Learning Methods. Electronics.

[9] Uysal, D. T., Yoo, P. D., & Taha, K. (2022). Data-Driven Malware Detection for 6G Networks: A Survey from the Perspective of Continuous Learning and Explainability via Visualisation. IEEE Open Journal of the Vehicular Technology.