Offline-Capable AI–Blockchain Architecture for Biochemical Threat Detection in Mission-Critical MANET Environments

Victor Ikenna Kanu, Ihunanya Udodiri Ajakwe, Simeon Okechukwu Ajakwe, *Senior Member, IEEE*, and Dong-Seong Kim, *Senior Member, IEEE*

***Abstract*—Biochemical threats remain a serious concern in mission-critical environments, particularly those characterized by intermittent connectivity and infrastructure degradation. Traditional centralized detection systems are ill-suited for such conditions, as they depend on stable communication channels and are inherently vulnerable to cyber–physical disruptions. This work introduces a decentralized solution integrating artificial intelligence (AI) and blockchain (BC) for autonomous biochemical threat detection within tactical mobile ad hoc networks (MANETs). The framework uses a random forest (RF) classifier trained on acetylcholinesterase (AChE) sensor data to identify sarin exposure with 100% accuracy and sub-25-ms inference latency. Threat verification is secured using a lightweight proof of authority and association (PoA^2) BC, which provides tamper-resistant logging and distributed consensus. The architecture supports offline operations and maintains functionality under conditions of 20% packet loss and node disruption. Simulations conducted in degraded network environments confirmed the system's robustness and scalability, establishing it as a resilient and efficient platform for secure biochemical threat detection in dynamic, resource-constrained mission-critical settings.**

***Index Terms*—Acetylcholinesterase (AChE), artificial intelligence (AI), biochemical threat detection, blockchain (BC), mobile ad hoc network (MANET), random forest (RF), sarin.**

NOMENCLATURE

AChE	Acetylcholinesterase.
AI	Artificial intelligence.
BC	Blockchain.
CBRN	Chemical, biological, radiological, and nuclear threats.
CRL	Certificate revocation list.
CTAs	Chemical threat agents.
CWAs	Chemical warfare agents.
CWC	Chemical Weapons Convention.
DFP	Diisopropyl fluorophosphates.
GB	Gradient boosting.
GC-MS	Gas chromatography-mass spectrometry.
HSM	Hardware security module.
KNN	K-nearest neighbors.
MANETs	Mobile ad hoc networks.
ML	Machine learning.
MLP	Multilayer perceptron.
OPCW	Organization for the Prohibition of Chemical Weapons.
PoA^2	Proof of authority and association.
RF	Random forest.
SM	Smart contract.
SVM.	Support vector machines.
TPM	Trusted platform module.
WMD	Weapons of mass destruction.

Received 29 August 2025; revised 30 November 2025 and 12 January 2026; accepted 5 February 2026. Date of publication 11 February 2026; date of current version 27 April 2026. This work was supported in part by the Innovative Human Resource Development for Local Intellectualization Program through the Institute of Information and Communications Technology Planning and Evaluation (IITP) Grant by the Korean Government (Ministry of Science and ICT (MSIT), 25%) under Grant IITP-2025-RS-2020-II201612; in part by the Priority Research Centers Program through the National Research Foundation of Korea (NRF) by the Ministry of Education, Science and Technology (MEST) (25%) under Grant 2018R1A6A1A03024003; in part by MSIT, South Korea, under the Information Technology Research Center (ITRC) Support Program (25%) under Grant IITP-2025-RS-2024-00438430; and in part by the IITP-ICT Challenge and Advanced Network (ICAN) of Human Resource Development (HRD) Grant by the Korean Government (Ministry of Science and ICT, 25%) under Grant IITP-2025-RS-2022-00156394. *(Corresponding author: Dong-Seong Kim.)*

Victor Ikenna Kanu, Ihunanya Udodiri Ajakwe, and Dong-Seong Kim are with the Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, South Korea (kanuxavier@gmail.com; ihunanya.ajakwe@gmail.com; dskim@kumoh.ac.kr).

Simeon Okechukwu Ajakwe is with the Department of IT Convergence Engineering and the ICT Convergence Research Centre, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: simeonajlove@gmail.com).

Digital Object Identifier 10.1109/JIOT.2026.3663607

I. INTRODUCTION

SINCE Ancient times, chemicals have been employed in combat as WMD, which consist of chemical, biological, radiological, nuclear, and explosive weapons. Throughout World War I, chemical agents, such as chlorine, phosgene, and mustard gas, were utilized extensively [1]. On April 29, 1997, the CWC, an international agreement supervised by the OPCW, came into force [2]. Except for extremely specific uses, it forbids the use of chemical weapons, the large-scale manufacturing, stockpiling, or transfer of chemical weapons or their precursors. Although the treaty is in place, the threat of biological [3] and chemical agents [4] remains a significant concern, particularly concerning their potential illicit use by terrorists and in warfare by some nations [5].

Chemical warfare was initiated through the deployment of chlorine and other hazardous substances in World War I. Nonetheless, the time span between World War I and World War II marked a phase of creation and manufacturing of nerve agents, such as Tabun, Sarin, and Soman [6]. Sarin is an extremely poisonous nerve agent that was initially developed for use in chemical warfare in Germany [7]. These chemical

weapons, available in both liquid and gas forms, have a significant effect on the health of both military personnel and civilians because of their insecticide-like mechanism of action. It operates by blocking AChE, causing a neurotoxic reaction that results in swift death due to respiratory failure. In addition, exposed individuals, even at low level are at risk of microstructural disruption in the hippocampus, leading to conditions such as posttraumatic stress disorder (PTSD), Alzheimer's disease, and depression and anxiety [8].

Cases of used sarin have been reported, including the Tokyo sarin subway attack in 1995, which recorded some casualties [9]. Also, potentially 1 00 000 U.S. military personnel were exposed to low levels of sarin and cyclosarin, organophosphorus (OP) nerve agents, when a munition storage depot at Khamisiyah, Iraq, was destroyed by the U.S. combat engineers in March 1991 [8]. The use of toxic chemicals against terrorists and civilians was observed in a Moscow theater in 2002 [10].

The persistent threat of CWAs remains a grave concern for global security, with multiple nations maintaining stockpiles despite international prohibitions. In 2014, the OPCW Fact-Finding Mission (FFM) was established to investigate ongoing claims of chemical weapons use in Syria. Its primary role was to analyze the available evidence related to these allegations [11]. As evidenced by incidents in Syria [12] and other conflict zones, the deployment of these agents can occur with minimal warning, requiring detection systems that function effectively even when communication infrastructure is compromised.

The evolution of analytical techniques in OPCW proficiency testing has progressed substantially from its GC-MS origins. Contemporary practice incorporates an array of detection methods that include GC systems with atomic emission detection (AED), flame photometric detection (FPD), and nitrogen-phosphorus detection (NPD) detectors. Also, multiple mass spectrometry configurations and high-resolution mass analyzers for both GC and liquid chromatography applications, and Fourier transform infrared spectroscopy are been used [13]. However, these traditional detection techniques face some limitations. These include complex analytical instrumentation, a broad spectrum of biological, chemical, and bioengineered warfare agents, as well as extensive manual work that is time-consuming [14], [15]. In addition, they cannot be used for a real-time detection of CBRN threats during war. Finally, another limitation of non-AI baselines is their inability to handle borderline or noisy biochemical readings, which can lead to missed detections under real-world conditions. This motivates our choice of an AI-based technique, which balances robustness, low latency, and adaptability to future sensor modalities.

In mission-critical operations, particularly those conducted in communications-degraded and infrastructure-challenged environments, integrated sensor networks are vital for the early detection of CBRN threats. Biochemical sensors play a crucial role in identifying toxic agents in real time, and recent advances in AI have significantly enhanced their analytical capabilities [16]. AI, especially through neural networks and ML, enables sophisticated analysis of complex chemical spectra and environmental signals [17], providing benefits such as noise reduction, anomaly detection, and the discovery of novel correlations between sensor outputs and biochemical processes [18], [19]. These capabilities improve sensor reliability, precision, and throughput [20]. However, the deployment of AI-driven detection systems in real-world, disrupted environments raises critical concerns around interpretability, data security, and system resilience, particularly when connectivity is intermittent and nodes are distributed across unstable networks [21].

These limitations expose a broader architectural challenge: most existing biochemical threat detection systems are centralized, rendering them vulnerable in dynamic and degraded communication environments. Centralized infrastructures struggle to maintain consistency and integrity of AI-generated inferences across geographically dispersed nodes, especially when facing bandwidth limitations, packet loss, or node failures [29]. Furthermore, their dependence on continuous connectivity and high-compute central hubs makes them unsuitable for real-time deployment in constrained edge networks. To ensure reliable and secure detection in such mission-critical settings, there is a pressing need for decentralized frameworks that can preserve data provenance, ensure verifiability of AI-driven decisions, and operate autonomously under adverse network conditions.

This study proposes a decentralized framework that integrates AI and BC to enable robust biochemical threat detection within disconnected MANETs. Leveraging AChE-based sensor data, the system employs an RF classifier to detect sarin exposure with high accuracy and low inference latency. A lightweight PoA^2 BC provides tamper-resistant logging, validator accountability, and decentralized trust without incurring significant computational overhead. Evaluated under simulated mission-critical conditions with 20% packet loss and intermittent communication between agents, the framework consistently achieved reliable detection and traceable logging. This integration of AI and BC overcomes key limitations in traditional centralized architectures and presents a scalable, autonomous approach for secure biochemical monitoring in constrained, infrastructure-limited environments. Fig. 1 illustrates the proposed system deployed in a disrupted operational setting, where distributed biochemical sensors support early detection and rapid, verifiable threat response despite network instability. Hence, the specific contributions of this study are as follows.

1) The development of an AI–BC framework for the detection of biochemical threats in tactical MANETs, engineered to remain effective under packet loss and node disruption 20%, overcoming a key weakness of traditional centralized detection systems in contested environments.
2) The implementation of an optimized RF classification model specifically engineered for resource-constrained tactical devices, utilizing AChE inhibition kinetics to achieve high-confidence nerve agent detection with minimal computational overhead.
3) The PoA^2 consensus mechanism is validated for bandwidth-constrained, mission-critical networks, ensuring data integrity while minimizing communication

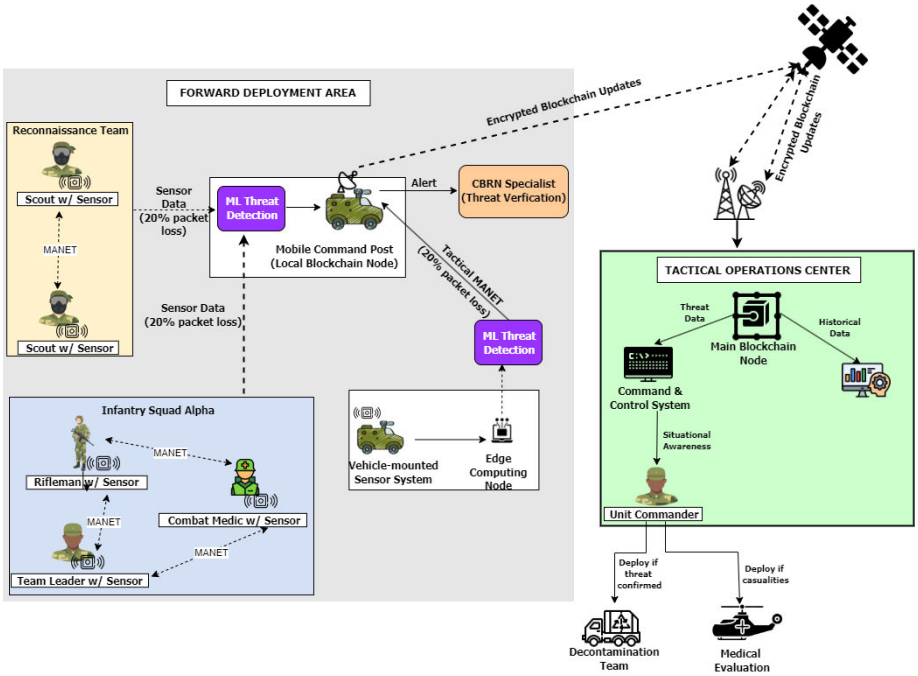

Fig. 1. Proposed AI–AI–BC-enabled biochemical threat detection architecture deployed in a tactical battlefield environment. Sensor-equipped personnel and vehicles transmit AChE data over a disrupted MANET (with simulated 20% packet loss) to local and edge computing nodes for ML-based threat classification. Verified alerts are logged on a distributed BC ($\texttt{PoA}^2$) and relayed to the tactical operations center for situational awareness and mission coordination.

overhead, an essential requirement for operations in disrupted and resource-limited environments.

4) The demonstration of real-time detection and tamper-proof logging through full-system simulations under degraded and adversarial network conditions.

II. Background and Related Works

Chemical agents are classified into various categories based on their chemical structure, physiological mode of action, lethality, or operational purpose [30]. These include nerve agents such as tabun (GA), sarin (GB), and VX; blood agents like hydrogen cyanide (AC), arsine, and cyanogen chloride (CK); blister agents including sulfur and nitrogen mustards; and pulmonary agents such as phosgene (CG), diphosgene (DP), chloropicrin (PS), and chlorine (CL). These substances pose serious risks to both civilian populations and personnel operating in mission-critical environments when weaponized [1], [10].

Sarin (isopropyl methylphosphonofluoridate) is a highly toxic OP nerve agent classified as a Schedule 1 chemical under the CWC. Its primary mechanism involves irreversible inhibition of the enzyme AChE, which is essential for hydrolyzing the neurotransmitter acetylcholine (ACh). Inhibition leads to excessive accumulation of ACh, resulting in cholinergic crisis and potentially fatal outcomes [31]. Because sarin rapidly hydrolyzes in vivo, direct detection is difficult; forensic analyses typically rely on identifying stable metabolites like O-isopropyl methylphosphonic acid (IMPA) and protein adducts with albumin or butyrylcholinesterase (BChE) [32]. Documented exposure events have demonstrated systemic distribution of sarin biomarkers in biological tissues, reinforcing the critical need for timely detection and response mechanisms in high-risk deployments.

Conventional detection of CWAs primarily relies on analytical techniques such as gas GC, GC-MS, liquid chromatography–tandem mass spectrometry (LC-MS/MS), and high-performance liquid chromatography (HPLC) [11], [33], [34]. GC and GC-MS remain central in certified laboratories due to their capabilities in analyzing volatile agents and resolving stereoisomers [35]. These methods are particularly effective for detecting sarin degradation products and other OP compounds, with mass spectrometry-based techniques also enabling the identification of mustard agent-related DNA adducts [36]. Recent innovations, such as 2-D MS/MS using quadrupole ion traps [35] and LC-HESI/MS/MS for phenylarsenic agents [37], have expanded field-deployable options. Nonetheless, these techniques are limited by their operational complexity, equipment requirements, and constraints in detecting nonvolatile or polar derivatives in resource-limited conditions.

To overcome these limitations, biosensors have emerged as a flexible and rapid-response alternative. These devices integrate a biological recognition element, such as enzymes, antibodies, or nucleic acids, with a physicochemical transducer and signal processor to deliver a real-time threat assessment [38]. Enzyme-based biosensors, especially those that use AChE, are widely applied in the detection of neurotoxic agents such as sarin and VX [39]. They offer faster analysis times, lower detection limits, and improved portability compared to traditional laboratory methods. Recent advances have enabled integration into wearable systems embedded in uniforms and helmets, allowing real-time monitoring of stress indicators and toxic exposure [40]. Furthermore, their ability to support multiplexed detection makes them suitable for identifying a wide array of biological and chemical threats simultaneously.

TABLE I
COMPARATIVE ANALYSIS OF PREVIOUS WORKS ON AI APPLICATIONS FOR THREAT DETECTION IN MANETS AND THE PROPOSED FRAMEWORK

Ref.	Target Threat/Domain	AI Model(s) Used	Blockchain Applied	Remarks / Limitations
[22]	Firearm image and movement pattern detection in MANETs	Deep CNN (YOLOv5)	No	Achieved high accuracy in image-based intrusion detection but lacks resilience under network degradation and no tamper-proof logging.
[23]	Wormhole threat in MANETs	KNN, SVM, DT, LDA, NB, CNN	No	Effective classification but centralized setup; not optimized for disrupted tactical environments.
[24]	Black hole attack in MANETs	KNN with fuzzy inference (trust-based)	No	Improves packet delivery but lacks cryptographic guarantees and offline operation.
[25]	Cybersecurity threats on Twitter	Explainable AI (XAI)	No	Useful for NLP-based detection but domain is social media, not mission-critical MANETs.
[26]	Communication network threats	Generative Adversarial Networks (GANs)	No	Powerful against adversarial attacks but computationally heavy and unsuitable for resource-constrained tactical nodes.
[27]	Distributed Denial-of-Service (DDoS) attacks	CNN, RF	No	Focused on traffic anomalies; centralized processing, no resilience to packet loss.
[28]	Denial-of-Service (DoS) attacks	Artificial Neural Networks (ANN)	No	AI-based detection only, lacks secure distributed logging and offline support.
Proposed Work	**Biochemical threat detection (Sarin via AChE biosensors) in tactical MANETs**	**Random Forest (optimized), with comparative ML evaluation (GB, SVM, KNN, MLP)**	**Yes – Lightweight PoA^2 consensus Blockchain (PureChain)**	**Decentralized, resilient under 20% packet loss, supports offline operations, tamper-proof logging, traceable detection, low-latency inference (<25ms).**

Despite the performance advantages of biosensors and analytical instruments, these systems face significant challenges in field deployments, particularly related to data integrity, transmission reliability, and operational resilience in disconnected or contested networks. AI and BC technologies offer complementary solutions to address these shortcomings. AI supports real-time classification, anomaly detection, and signal optimization, while BC ensures tamper-proof data logging, decentralized verification, and traceable decision-making across distributed networks. Together, AI–BC integration enhances the robustness and autonomy of threat detection frameworks operating in volatile environments.

MANETs further augment this capability by offering infrastructure-free communication among mobile nodes. Each node can act as both a data source and a router, dynamically forwarding packets through intermediate nodes when direct links are unavailable. This decentralized model is well-suited to scenarios where rapid deployment, mobility, and fault tolerance are essential, such as robotic swarms, autonomous navigation systems, or emergency response networks [41]. While MANETs provide flexibility in these environments, they also introduce complications. High node mobility leads to frequent topology changes, requiring adaptive routing protocols and clustering mechanisms [42]. Moreover, the absence of fixed infrastructure makes MANETs more vulnerable to adversarial threats, such as jamming, spoofing, and data interception. These concerns have driven the adoption of BC-enhanced security schemes that embed cryptographic validation and decentralized trust directly into the network layer [43].

Recent advances in MANETs have focused on overcoming the challenges posed by dynamic, high-mobility environments where traditional routing and clustering techniques suffer from increased latency, packet loss, and reduced data delivery reliability. These limitations are particularly problematic in mission-critical applications such as sensor networks and real-time threat monitoring. To address these issues, researchers have increasingly turned to AI for adaptive threat detection and routing optimization, as summarized in Table I. For instance, Ali et al. [44] proposed a deep learning-based classifier for adaptive clustering that dynamically adjusts node groupings based on behavioral and contextual factors such as mobility and data distribution. Their approach achieved a delivery rate of 89.4%, reduced packet drops by over 70%, and significantly lowered transmission delays.

Other efforts have focused on embedding AI models within wireless sensor network (WSN) topologies to enhance intrusion detection and surveillance accuracy. Apeh et al. [22] developed a distributed WSN paired with a deep convolutional neural network (DCNN) using YOLOv5 for detecting firearm imagery and movement patterns. The architecture, which employs a 400-node quasi-unit-disk graph (QUDG) arranged in a spanning tree, achieved 100% precision in firearm recognition and up to 97.17% intrusion detection accuracy, with subsecond processing times. In a similar vein, Abdan and Seno [23] tackled wormhole threats in MANETs using ML classifiers trained to distinguish malicious activity from normal traffic. Among several models, a decision tree classifier demonstrated the highest performance with 98.9% accuracy. Farahani [24] further advanced AI-based MANET security by combining KNN clustering with a fuzzy inference system for trust evaluation. Their hybrid intrusion detection system reduced packet loss from 67.6% to 7.3% and nearly doubled packet throughput and delivery ratios.

Beyond conventional MANET security and intrusion detection, AI has also been applied extensively in biochemical sensing and gas detection domains, which are more directly relevant to this study. For example, Zhou et al. [16] highlight how AI models can enhance biochemical sensors by reducing noise, improving sensitivity, and uncovering nonlinear feature–response patterns. Taylor et al. [18] demonstrate ML-based analysis for mobile or enzyme-linked sensors, showing significant improvements in signal reliability under

noisy conditions. Chowdhury and Oehlschlaeger [20] further review the role of AI in gas sensing applications, emphasizing its ability to manage low-concentration, near-threshold exposures where traditional cutoffs fail. These findings are directly aligned with our context, where AChE-based biosensors produce noisy, nonlinear responses under sarin exposure. By contrast, while AI applications in intrusion detection [23], [28] or natural language processing [25] illustrate the breadth of ML methods, they are cited here only for methodological analogies in handling noise and adversarial conditions, rather than as domain-specific precedents. The novelty of our approach lies in applying AI not to general network security or NLP, but specifically to robust biochemical threat detection under mission-critical MANET constraints, an area with limited prior work.

Complementing these AI-driven efforts, BC has emerged as a critical enabler for securing mission-critical data pipelines. Its decentralized, tamper-resistant architecture supports traceable event logging and verifiable inference, particularly in environments where network trust and resilience are paramount. Applications in nuclear material tracking have already demonstrated BC's utility in maintaining immutable audit trails for sensitive data exchanges [45]. In threat surveillance systems like BlockCrime, convolutional neural networks generate real-time threat classifications that are cryptographically logged through SMs to a permissioned ledger, thereby automating secure validation workflows [46]. These examples highlight the synergy between AI and BC in supporting distributed, autonomous decision-making without relying on centralized infrastructure.

Nonetheless, gaps remain in the literature, particularly regarding the deployment of AI–BC systems for biochemical threat detection in low-connectivity or adversarial environments. Many existing integrations focus on static image recognition or federated learning, neglecting biochemical-specific workflows and the real-time challenges introduced by mobile nodes, high packet loss, and offline operation [47]. Furthermore, recent architectures designed for CBRN threat detection tends to emphasize modular AI components without integrating cryptographic safeguards or data provenance guarantees [48]. Consequently, there is a clear need for lightweight, BC-secured detection architectures that support offline validation, dynamic validator rotation, and tamper-proof logging in MANET-based biochemical sensor networks, particularly those tasked with monitoring agents such as sarin in mission-critical deployments.

III. System Design and Methodology

This study proposes an integrated framework combining BC with an AI-driven inference engine to secure and analyze biochemical sensor data over a disrupted tactical MANET. The methodology, as described in the architectural diagram in Fig. 2, encompasses four components: 1) sensor-level data acquisition [sensing layer (SL)]; 2) AI-based threat detection layer; 3) BC-backed logging (BC layer); and 4) tactical MANET backbone. All components are implemented in a software-based simulation environment to test the system's performance under adversarial conditions, addressing data integrity, threat prediction, and scalability in resource-constrained settings.

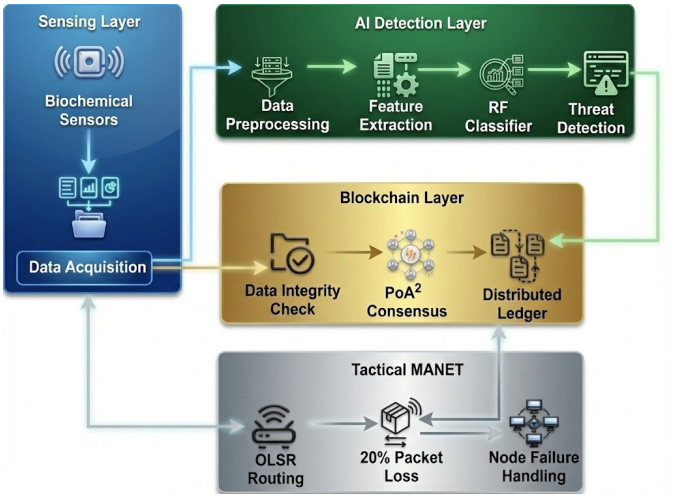

Fig. 2. System architecture for BC and AI-Integrated biochemical threat detection in tactical MANET.

A. Sensing Layer

The SL represents AChE-based biochemical sensors, which detect variations in enzyme activity caused by exposure to nerve agents such as sarin. These sensors output raw concentration values, reaction-rate measurements, and normalized kinetic responses to account for sensor-to-sensor variability. Together, these parameters form the primary feature set for downstream detection. In the operational framework, the SL provides live biochemical readings that are routed simultaneously to the AI detection layer (ADL) for classification and to the BC layer for integrity validation and immutable logging. While synthetic data was used in our evaluation (see Section IV), the architecture itself is agnostic to data origin and is designed to accommodate real-time feeds from physical AChE-based biosensors, as shown in Fig. 2.

B. AI-Aided Sensor Data Detection

The ADL receives preprocessed sensor readings from the data acquisition module, initiating an ML pipeline to infer the presence of sarin. This layer comprises three core stages: data preprocessing, feature extraction, and threat classification, as depicted in Fig. 2.

Converting raw sensor data into meaningful features is crucial for effective ML. Input features are processed as a matrix $\mathtt{X} \in \mathbb{R}^{\mathtt{n} \times \mathtt{d}}$, where $\mathtt{n}$ denotes the number of samples collected from sensors and $\mathtt{d}$ represents the dimensionality of each feature vector. Three key features are selected to form a comprehensive signature of potential nerve agent presence: raw concentration values from sensors, reaction-rate measurements indicative of enzyme activity, and normalized reaction rates to mitigate sensor-to-sensor variability. These features capture both the static concentration levels and dynamic enzymatic responses, furnishing the ML models with complementary information for reliable threat inference. A threat threshold of approximately 0.19 ppm is defined for sarin concentration,

consistent with established safety guidelines for this hazardous nerve agent [49].

Although sarin detection can, in principle, be achieved by a fixed threshold at 0.19 ppm, Gaussian noise and sensor variability create overlap between "normal" and "threat" readings. For example, some normal samples exceeded 0.18 ppm and some threat samples fell below 0.20 ppm. In such borderline cases, static thresholds become unreliable. ML classifiers such as RF exploit feature interactions (concentration, reaction rate, and normalized kinetics) to maintain correct classification under noise and drift, which justifies their use in this context.

It is important to emphasize that model training is not performed at MANET edge nodes. Instead, training is carried out in trusted environments using laboratory-calibrated AChE biosensors and surrogate compounds (e.g., paraoxon and DFP), supplemented by simulated noisy data for robustness testing. The trained models are then packaged as signed artifacts, with version identifiers and cryptographic hashes recorded on-chain. During tactical deployment, MANET nodes execute inference-only workloads, ensuring lightweight operation in volatile conditions. Updates or recalibrations are distributed by accredited authorities as new signed model bundles, enabling secure and traceable deployment in the field.

While model training is performed centrally for biochemical-safety calibration, operational decentralization is achieved during inference, validation, and synchronization. Each MANET node executes the signed inference model Θ locally, generates a deterministic hash of its prediction, and participates in PoA^2 consensus for distributed verification. Inference thus operates autonomously and independently of network connectivity—nodes continue local detection even under disruption, buffering results for later synchronization once connectivity is restored. This separation between local inference and ledger synchronization decentralizes trust without requiring a coordinating server, ensuring both inference autonomy and verifiable provenance under unstable network conditions.

For this system, five ML models, namely, RF, GB, SVM, KNN, and MLP, were employed to classify sarin exposure from AChE-based biochemical sensor data. These models were selected to capture a broad spectrum of classifier behaviors, ranging from ensemble learning to margin-based and neural network-based inference. Although the final system deployed uses the RF model for operational reasons, the comparative evaluation of the five models provides a comprehensive assessment of tradeoffs in model complexity, resource efficiency, and robustness to sensor noise [50]. This ensemble learning method combines multiple decision trees to generate more accurate and stable predictions

$$\hat{y} = \mathrm{mode}\left(h_1(X), h_2(X), \ldots, h_m(X)\right). \tag{1}$$

In (1), $\hat{y}$ represents the final prediction, which is determined by taking the most common output (mode) among all individual trees $h_i(X)$, with i ranging from 1 to m (the total number of trees). Each individual tree is trained using the Gini impurity criterion for node splitting in the following equation:

$$G = \sum_{i=1}^{C} p_i (1 - p_i) \tag{2}$$

where p_i is the probability of an element being classified for class i and C is the number of classes. Lower Gini impurity values indicate better splits.

Through extensive parameter tuning, we optimized our model with: 100 trees to balance accuracy and computational efficiency, a maximum depth of 10 to prevent overfitting while capturing complex patterns, and a minimum of 2 samples per leaf to ensure generalization. We further ablate $n_{\text{estimators}}$, max depth, and min_samples_leaf to quantify accuracy–efficiency tradeoffs. This configuration achieved the optimal balance between detection accuracy and resource utilization for deployment on tactically constrained edge devices.

C. BC Security Intelligence

To ensure data integrity in potentially compromised tactical environments, at the BL, we implemented PureChain, a BC network developed by the network systems lab (NSL). PureChain was selected due to its advanced features, including offline transaction capabilities, transaction speed, and enhanced security mechanisms. As shown in Fig. 2, sensor readings and AI-detected threat events are securely validated and committed to the distributed ledger through this BC infrastructure. Each transaction T in the BC is structured as follows:

$$T = \left[H_{\text{prev}}, TS, D, SIG\right] \tag{3}$$

where H_{prev} stores the hash of the previous block, creating the chain structure, TS is the timestamp, establishing chronological order, D contains the actual sensor data and detection results, and SIG is the cryptographic signature that verifies authenticity. This structure ensures that sensor readings cannot be tampered with once added to the BC, providing a verifiable record of all detections. This structure ensures that sensor readings cannot be tampered with once added to the BC, providing a verifiable record of all detections.

Traditional BC consensus mechanisms like proof-of-work are too resource-intensive for tactical networks [51]. Instead, we implemented Purechain's lightweight proof-of-authority and association (POA^2) consensus model [52], given in the following equation:

$$B_{\text{valid}} = \left(\sum_{i=1}^{N_a} w_i \cdot \mathrm{sig}_i(B) \geq \theta\right) \wedge \left(\max_{j \in S}\left[R_j - \min_{i \in A} R_i\right] < \Delta_R\right) \tag{4}$$

where B_{valid} is the Boolean indicating whether block B is validated (true/false), N_a is the number of active validators, w_i is the weight (authority) of validator i, $\mathrm{sig}_i(B)$ is 1 if validator i signs block B, 0 otherwise, θ is the required signature threshold, S is the set of standby validators, A is the set of active validators, R_i is the reliability score of validator i, calculated from their performance metrics, and Δ_R is the threshold difference that would trigger a validator replacement.

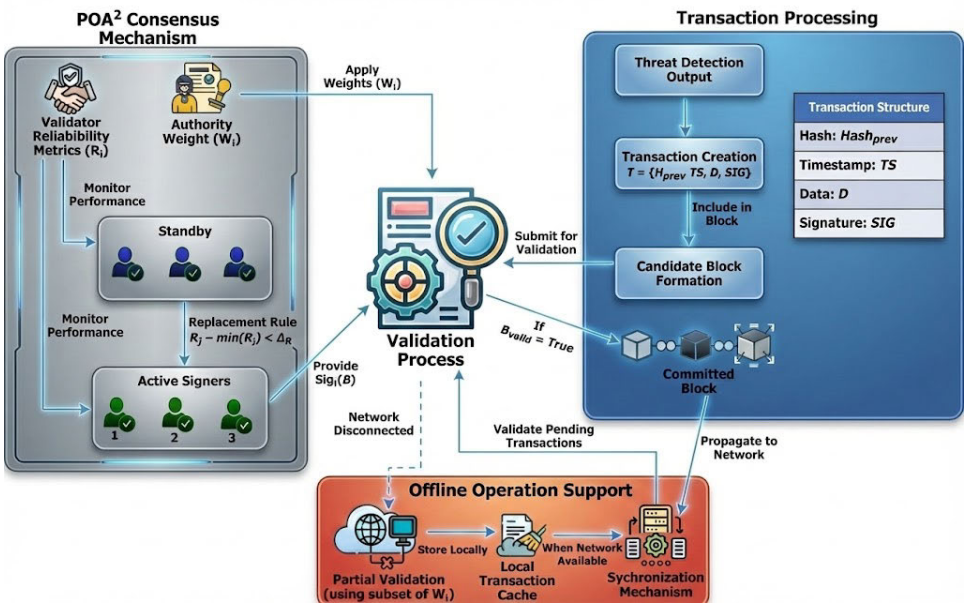

Fig. 3. Integrated PureChain architecture with POA^2 consensus for resilient biochemical threat logging in tactical MANETs. The system combines dynamic validator selection, authority-weighted consensus, and offline operation support to ensure secure, tamper-resistant block validation and synchronization—even under disrupted or disconnected battlefield conditions.

Fig. 3 shows the integrated PureChain with PoA^2 consensus workflow for tamper-resistant biochemical threat logging in disconnected tactical MANETs. On the left, validator reliability scores (R_i) are continuously monitored to dynamically assign authority weights (w_i) and manage validator roles between standby and active signers. A validator is replaced if its reliability falls below a defined threshold compared to a standby node. The center depicts the core validation process, where active validators provide weighted signatures ($w_i \cdot sig_i(B)$) that contribute to block validation, governed by a dual-threshold formula ensuring both signature quorum and performance stability. On the right, threat detection outputs trigger transaction creation, which includes sensor data, timestamps, and cryptographic signatures, forming candidate blocks submitted for consensus. Validated blocks are committed to the chain and propagated across the network when available. In offline scenarios, transactions are partially validated, cached locally, and later synchronized to the global ledger upon reconnection.

Finally, in PoA^2, block validity is determined not only by the majority of cryptographic signatures from trusted validators but also by each validator's cumulative reliability score. When a validator's reliability drops below a defined threshold, a standby node with higher reliability automatically assumes its role, ensuring that consensus continues even if nodes become inactive, compromised, or disconnected. By embedding validator replacement logic and coupling authority with historical performance, PoA^2 provides dynamic fault tolerance critical for mission-critical battlefield environments characterized by node attrition, packet loss, and unstable links. Unlike conventional PoA systems that depend on static validator lists, PoA^2 continuously reevaluates validator credibility and enables seamless role handover without any centralized coordinator. As formalized in Algorithm 1, each node executes its signed inference model locally, generates verifiable transaction hashes, and later participates in consensus cycles when connectivity permits. This mechanism decentralizes verification and operational trust, distributing validation responsibility across all nodes while maintaining deterministic consistency through the model hash. Consequently, PoA^2 achieves resilient, autonomous ledger growth and sustained data integrity even under adversarial or degraded network conditions.

D. Network Simulation Framework

The tactical MANET backbone (see Fig. 2) provides the communication layer for routing sensor data, threat alerts, and BC transactions across mobile nodes. The simulation was developed using the common open research emulator (CORE) to accurately model tactical battlefield environments. This environment consisted of ten wireless stations communicating with a central access point (AP) in a star topology. The network implemented the optimized link state routing (OLSR) protocol, with a Gilbert–Elliott channel model [53] for packet loss. This two-state Markov model switches between "good" and "bad" states to create realistic patterns of loss

$$P_{loss}(t) = P_{GB}(t) \cdot 0.2 + P_{BG}(t) \cdot 0 \tag{5}$$

where $P_{GB}(t)$ represents the probability of transitioning from the good to the bad state, while $P_{BG}(t)$ is the probability of transitioning from bad to good.

Following prior MANET simulation studies [19], [54], we configured the channel with a 20% packet loss rate to emulate a degraded yet operationally viable tactical environment. Values in the 10%–30% range have been reported in the literature as representative of field MANETs under adversarial interference, environmental noise, and mobility, where packet delivery is challenged but not entirely disabled. To ensure robustness, our evaluation also included 10%, 20%, 30%, and 40% packet loss conditions.

Algorithm 1 Decentralized Biochemical Threat Detection and PoA^2 Validation

Require: Sensor network $S = \{s_1, s_2, \ldots, s_n\}$, trained model Θ, disruption level p_l, validator threshold θ
Output: Verified threat confidence score c_f, validated transaction ledger L

while *system is active* **do**
  foreach *node* $s_i \in S$ **do**
    data $\leftarrow$ **CollectSensorReading**(s_i) ;
    features $\leftarrow$ **PreprocessData**(data) ;
    (threatDetected, c_f) $\leftarrow$ **RF_Inference**(features, Θ) `// always executed locally`
    if threatDetected $=$ *TRUE* ***and*** $c_f \geq \tau$ **then**
      $T \leftarrow$ **CreateTransaction**(Hash(Θ), s_i, c_f, p_l) ;
      if ***NetworkAvailable***$(s_i) =$ *TRUE* **then**
        valid $\leftarrow$ **PoA^{2}Validation**(T) ;
        if valid $=$ *TRUE* **then**
          LogToBlockchain(T) ;
          BroadcastAlert(T) ;
        end
      else
        BufferLocally(T) `// store for deferred synchronization`
      end
    end
  end
  SynchronizeBufferedTransactions() `// when connectivity resumes`
end
Function PoA^{2}Validation(T)
  signatures $\leftarrow$ **CollectValidatorSignatures**(T)
  reliability $\leftarrow$ **EvaluateValidatorReliability**()
  return $(|\text{signatures}| \geq \theta)$ **and** (reliability $=$ TRUE)

E. Security Considerations and Threat Model

While PureChain improves resilience against tampering and disconnection, no system is entirely immune to all adversarial conditions. Table II summarizes potential attack vectors, their likelihood, and the mitigation strategies incorporated in our framework. Threats are grouped by consensus layer, network layer, and data/AI layer.

At the consensus layer, risks include validator key compromise, collusion, and double-signing. Mitigations include short-lived cryptographic credentials, validator replacement through PoA^2, and equivocation proofs. At the MANET layer, eclipse attacks and flooding remain possible; our framework reduces their success probability through authenticated channels, peer diversity, and offline caching. At the AI/data layer, threats such as sensor spoofing, replay, or adversarial near-threshold samples are addressed through nonce-based freshness checks, RF classification, and on-chain audit trails. Training-time poisoning is prevented by centralized, trusted training and model attestation. Privacy risks are reduced by keeping raw data off-chain and storing only hashes or commitments.

TABLE II
SECURITY THREATS AND MITIGATIONS IN PURECHAIN/POA^2

Threat	Risk	Mitigation(s)
Validator key compromise	Medium	Hardware HSM/TPM, short-lived certs, on-chain CRL, validator replacement
Validator collusion	Low–Med	Diverse validator set, quorum signatures, randomized leaders
Double-signing/forking	Medium	Equivocation proofs, slashing/ban, deterministic fork-choice
Replay/rollback	Medium	Nonces, timestamps, finality checkpoints
Eclipse/peer isolation	Medium	Peer shuffling, multi-path gossip, redundant radios
Flooding/DoS	Medium	Authenticated channels, per-node rate limits, quarantine
Sensor spoofing/replay	Medium	Device signatures, monotonic counters, freshness checks
Adversarial inputs (0.19 ppm)	Medium	RF classifier, hysteresis band, plausibility filters
Training poisoning/-model tampering	Low	Trusted offline training, signed models, on-chain hash attestation
Model drift	Medium	Calibration events, drift monitors, signed updates
Metadata leakage	Medium	On-chain hashes only, encrypted off-chain payloads

These measures, summarized in Table II, illustrate that while residual risks (e.g., validator majority compromise and sustained >40% packet loss) cannot be eliminated, the system prioritizes safety and auditability: failures may degrade liveness but never compromise data integrity. This satisfies the practical robustness requirements for tactical MANET deployment.

F. System Integration and Performance Metrics

The integrated system, as described in Algorithm 1, autonomously collects biochemical sensor readings, performs AI-driven threat inference using an RF classifier, and securely logs verified detections on the BC.

Sensor data is continuously collected from all nodes within the network, evaluating connectivity before initiating processing. When online (as indicated by the while loop structure in Algorithm 1), the data undergoes preprocessing and inference through the RF model to identify potential threats. If a threat is detected and exceeds a defined confidence threshold, a transaction is generated and submitted for validation using the POA^2 consensus algorithm. This mechanism verifies the block based on a quorum of weighted validator signatures and a reliability check. Upon successful validation, the transaction is immutably logged onto the BC, and an alert is broadcast. If the network is unavailable, the data is buffered locally for later processing. The system ensures robustness through deferred handling via `ProcessBufferedData()`, enabling continuous operation under connectivity constraints. The embedded `POAValidation()` function ensures both cryptographic integrity and validator trustworthiness, safeguarding the detection pipeline against compromise or data loss.

The system was evaluated using standard binary classification metrics, as described in the following equation:

$$\texttt{Accuracy} = \frac{\texttt{TP} + \texttt{TN}}{\texttt{TP} + \texttt{TN} + \texttt{FP} + \texttt{FN}}$$

TABLE III
SYSTEM PERFORMANCE METRICS SUMMARY

Metric	Value
Total Readings	100
Threats Detected	32
Detection Rate	32.0%
Avg. Inference Time	27.50 ms
Avg. Detection Confidence	99.8%
Packet Loss Rate	20%
Network Topology	10 stations, 1 AP

$$\begin{aligned} \mathrm{Precision} &= \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \\ \mathrm{Recall} &= \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \\ \mathrm{F1} &= 2\cdot\frac{\mathrm{Precision}\cdot\mathrm{Recall}}{\mathrm{Precision}+\mathrm{Recall}} \end{aligned} \tag{6}$$

where TP = true positives (correctly identified threats), TN = true negatives (correctly identified nonthreats), FP = false positives (incorrectly identified threats), and FN = false negatives (missed threats). These metrics provide a comprehensive assessment of detection performance, with particular emphasis on recall (minimizing missed threats) for this safety-critical application.

In addition to evaluating detection accuracy using standard binary classification metrics, the BC component was methodically assessed based on its resilience and operational efficiency within a mission-critical MANET environment. The evaluation focused on transaction logging consistency, block propagation behavior, and validator participation balance. Two categories of BC transactions, raw sensor data and confirmed threat detection events, were recorded and monitored using the structured format defined in (3). During these trials, block generation was tracked over time to verify uninterrupted propagation, while node-level transaction contributions were recorded to assess load distribution and validator engagement in the PoA^2 consensus process. These measures ensured that the BC maintained tamper-resistant, decentralized logging even under constrained connectivity, supporting the integrity and traceability of AI-driven threat detection workflows.

IV. SIMULATION RESULT AND DISCUSSION

This section evaluates the proposed AI–BC framework under mission-critical MANET conditions, integrating BC, AI-based detection, and disrupted network communications. Section IV-A describes synthetic data generation and distributional analysis; Section IV-B highlights system integration and network performance under disruption; Section IV-C presents BC security and logging performance; Section IV-D analyzes ADL threat detection capacity and reliability; Section IV-E reports on RF hyperparameter ablation; Section IV-F examines concentration distribution and threat probability patterns; and Section IV-G surveys related AI–BC approaches for comparative context. For the integrated system evaluation, we processed a subset of 100 sensor readings through the complete pipeline to assess real-time performance under tactical network conditions, as summarized in Table III.

Simulations using the CORE Network Emulator with 20% packet loss assessed the system's resilience and performance. ML was evaluated through detection accuracy, inference time, and confidence analysis, while BC integrity was checked through transaction logging across 200 system events. The system maintained 100% threat detection accuracy despite network disruptions. A full-stack prototype demonstrated real-time biochemical threat detection, secure data logging, and AI-powered analysis, with end-to-end processing under 55ms for a single sensor reading. The system processed 100 sensor readings and detected 32 high-confidence threat detections using AChE-based sarin detection models.

A. Synthetic Data Generation and Distributional Analysis

To evaluate the proposed framework in the absence of live nerve agent testing, a synthetic dataset was generated to emulate the behavior of AChE-based biosensors under sarin exposure. This procedure does not represent an operational component of the system architecture but was used exclusively for training and evaluation purposes.

1) Modeling Biochemical Interactions: The temporal inhibition of AChE activity was modeled using the Michaelis–Menten kinetics [55], given by

$$\mathrm{V} = \mathrm{V}_{\max}\cdot[\mathrm{S}]\,/\,(\mathrm{K}_{\mathrm{m}}+[\mathrm{S}]) \tag{7}$$

where V is the reaction velocity, $\mathrm{V}_{\max}$ = 1.0 (arbitrary units), and K_{m} = 0.1 ppm. The substrate concentration was fixed at 1.0 ppm. When a nerve agent such as sarin is present, it inhibits enzymatic activity, reducing the observed reaction velocity. The temporal escalation of sarin concentration was simulated as

$$[\mathrm{S}]_t = [\mathrm{S}]_0 + \alpha t + \mathrm{N}(0,\sigma)$$

where $[\mathrm{S}]_t$ is the concentration at time t in ppm, $[\mathrm{S}]_0$ = 0.05 ppm, α = 0.002 ppm/s is the rate of increase, and σ = 0.02 ppm introduces Gaussian noise to approximate sensor variability.

2) Dataset Structure: This procedure simulated ten sensors across 100 sampling cycles, yielding 1000 data points representing escalating exposure scenarios. Each sample was stored as a structured JSON object with the following fields: `sensor_id`, `agent`, `concentration`, `reaction_rate`, and `timestamp`. The dataset was generated in Python 3.11 using NumPy and archived as `sensor_data.json` for reproducibility.

3) Distributional Analysis: Fig. 4 presents the distributions of concentration, reaction rate, and normalized kinetics for normal and threat classes under Gaussian noise. Although the nominal sarin threshold is 0.19 ppm, noise-induced variation creates overlap between the two classes: some normal samples exceed 0.18 ppm while some threat samples fall below 0.20 ppm. This intersection in the 0.18–0.20 ppm range makes static thresholding unreliable. In baseline experiments, a threshold-only detector misclassified such borderline samples (recall = 0.95), whereas the RF classifier leveraged multifeature interactions to recover correct labels (recall = 1.00). This analysis validates the necessity of ML-based detection for robust performance under noisy, real-world conditions.

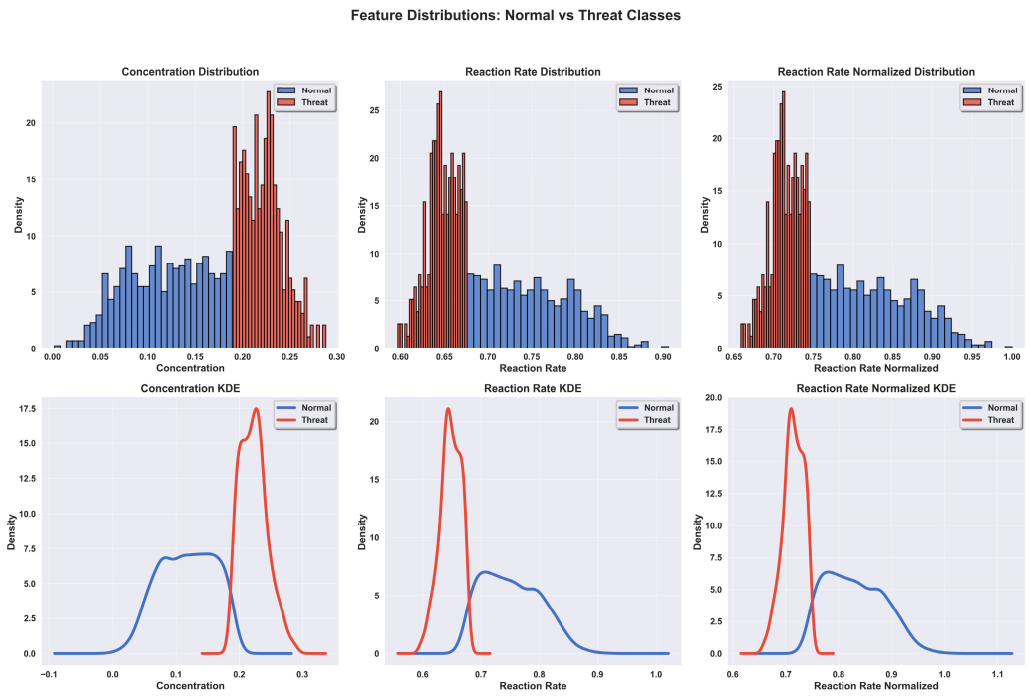

Fig. 4. Feature distributions of normal and threat class samples under Gaussian noise (σ = 0.02 ppm). Top row: histograms of concentration, reaction rate, and normalized reaction rate. Bottom row: corresponding kernel density estimates (KDEs). While the nominal threshold for sarin classification is 0.19 ppm, noise causes overlap between classes: some normal samples exceed 0.18 ppm, and some threat samples fall below 0.20 ppm.

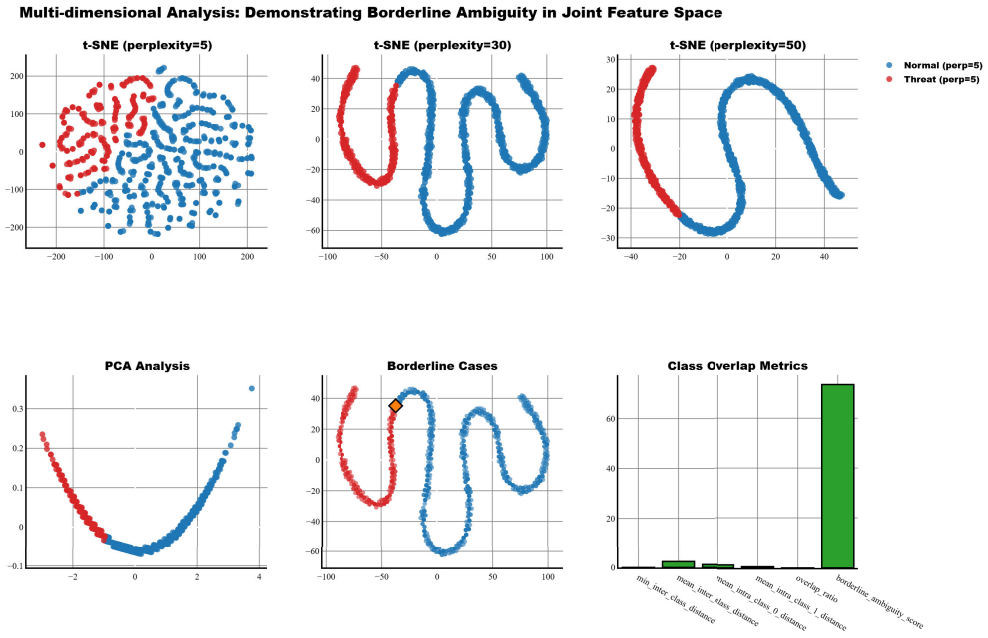

Fig. 5. Multidimensional feature-space visualization of AChE biosensor data. Top row: t-SNE embeddings with perplexity = 5, 30, 50 showing nonlinear manifolds and overlapping decision regions near 0.18–0.20 ppm. Bottom row: PCA projection (left), borderline-case highlighting (center), and quantitative class-overlap metrics (right). The orange-highlighted point denotes the most ambiguous sample (0.19 ppm) identified as the nearest instance to the interclass decision boundary, representing the typical borderline case. The results confirm that borderline ambiguity originates from interactions among concentration, reaction rate, and normalized-kinetics features.

4) Multidimensional Feature-Space Analysis of Borderline Ambiguity: To strengthen the claim of borderline ambiguity beyond 1-D marginals, a nonlinear manifold visualization was conducted using t-distributed stochastic neighbor embedding (t-SNE) and principal-component analysis (PCA). Fig. 5 shows three t-SNE projections generated with perplexity values of 5, 30, and 50, illustrating the stability of the embedding across neighborhood scales. Normal and threat samples form distinct nonlinear manifolds that intersect in a contiguous region corresponding to concentrations between 0.18 and

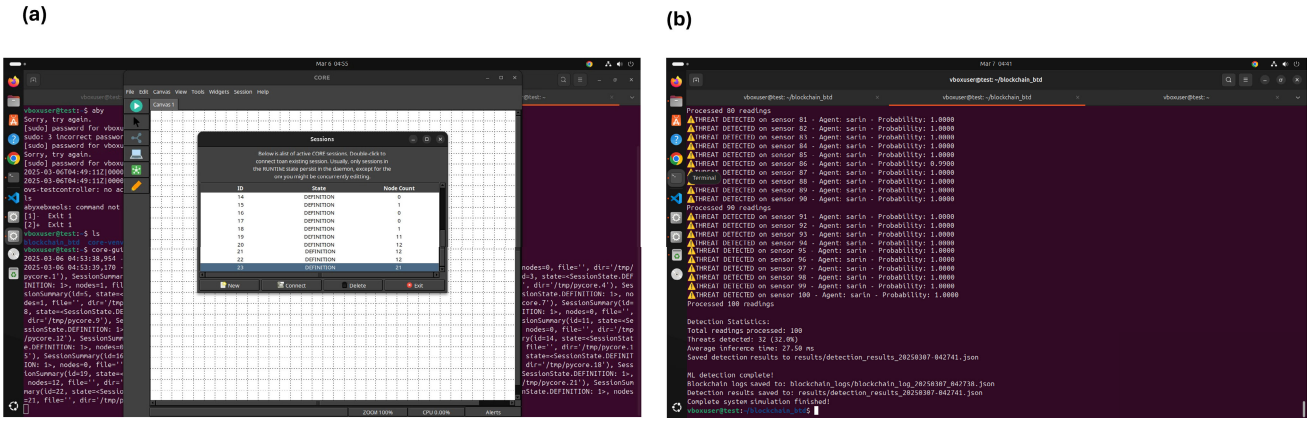

Fig. 6. (a) Network topology design setup using CORE GUI and Daemon, with Session ID: 23 confirming the creation of all 21 nodes (ten stations, ten switches, and one AP). (b) Biochemical threat detection system output: the system processed 100 sensor readings, detecting 32 threats (32.0%) with high confidence. Detection results and BC logs were successfully stored, marking the completion of the simulation.

0.20 ppm. The PCA projection (lower left) reveals partial linear separability, confirming that the boundary between classes is highly nonlinear. The orange-highlighted point in Fig. 5 (center) represents the most ambiguous sample, the instance with the smallest interclass distance and a concentration of 0.19 ppm, selected automatically as the sample nearest to the decision boundary. This point typifies the borderline region where minor perturbations in concentration or reaction-rate features can invert the predicted class. The quantitative overlap metrics (lower right) yield a 73.4% borderline-overlap ratio, confirming that ambiguity arises from joint feature interactions rather than sensor noise in any single dimension. This multidimensional analysis substantiates the need for nonlinear ensemble classifiers such as RF and GB, which can exploit cross-feature correlations to resolve ambiguous biochemical signatures.

5) Use in Evaluation: The synthetic dataset served as input for training and validating the AI detection pipeline under noisy conditions. In deployment, this process would be replaced by live sensor feeds from physical AChE biosensors; the architecture itself is agnostic to whether inputs are simulated or real. Thus, synthetic data generation provided a controlled, reproducible mechanism for evaluating detection accuracy, inference latency, and BC logging reliability in the proposed system.

B. Evaluation I: System Integration and Network Performance Under Disruption Scenario

The end-to-end integration of the proposed PureChain framework was validated under simulated tactical conditions using the CORE network emulator, where a total of 100 biochemical sensor readings were successfully processed through the full detection and BC logging pipeline. Despite a 20% packet loss rate configured to reflect disrupted MANET conditions, the system remained operational and accurately classified sarin-based threats with high confidence. As shown in Fig. 6(a), Session ID 23 was actively running with a fully initialized network topology comprising 21 nodes—ten stations, ten switches, and 1 AP—confirming successful instantiation of the simulation environment and the robustness of the underlying architecture.

In Fig. 6(b), terminal outputs display live threat detection logs, highlighting consistent identification of sarin exposure events from sensor 81 to sensor 100, all with a probability score of 1.000. The system detected 32 threats in total, achieving an average inference time of 27.50 ms per reading. Detection outcomes were simultaneously logged to the BC and saved to the local results directory, demonstrating seamless AI–BC integration. These results confirm that the framework maintains integrity and performance across disconnected conditions, validating its suitability for real-time biochemical threat detection in adversarial battlefield environments.

Furthermore, under the simulated battlefield scenario, characterized by intermittent packet loss and communication degradation, the proposed system demonstrated stable and reliable detection performance. Table IV presents a selected subset of sensor detections, chosen from the 32 sensors that identified threats during the experiment. The table illustrates the observed trend of increasing sarin concentration (ppm) and its corresponding detection results. Notably, sensor ID 64 exhibited a relatively lower concentration of 0.189 ppm, which falls slightly below the conventional threshold of 0.19 ppm. However, the system effectively detected this instance as a valid threat with a 96% confidence score, emphasizing the model's ability to identify critical threats even when concentrations marginally deviate from the expected threshold. In addition, all other reported detections maintained near-instantaneous inference times (ranging from 14.59 to 23.95 ms) with consistent confidence levels, thereby confirming the resilience and responsiveness of the system under contested communication conditions.

Fig. 7 evaluates system behavior under varying packet loss conditions. Fig. 7(a) and (b) shows that the apparent decline in accuracy and recall at high loss rates reflects reduced data transmission rather than degraded inference, each node continues local detection unaffected by connectivity. The ML model executes autonomously, but packet loss limits the number of detections successfully synchronized to the BC, thereby lowering the apparent accuracy of network-aggregated results.

TABLE IV
SAMPLED TACTICAL NETWORK THREAT DETECTION RESULTS WITH VARIABLE CONCENTRATIONS

Sensor id	Node id	Time (s)	Agent	Concentration (ppm)	Detection Result	Inference Time (ms)	Confidence
60	10	1.78	sarin	0.192	THREAT	17.58	100%
64	4	1.89	sarin	0.189	THREAT	15.69	96%
66	6	2.02	sarin	0.214	THREAT	23.43	100%
71	1	2.17	sarin	0.236	THREAT	23.95	100%
76	6	2.36	sarin	0.24	THREAT	14.59	100%
87	7	2.66	sarin	0.257	THREAT	21.47	100%
95	5	3.07	sarin	0.261	THREAT	18.86	100%
100	10	3.23	sarin	0.281	THREAT	17.40	100%

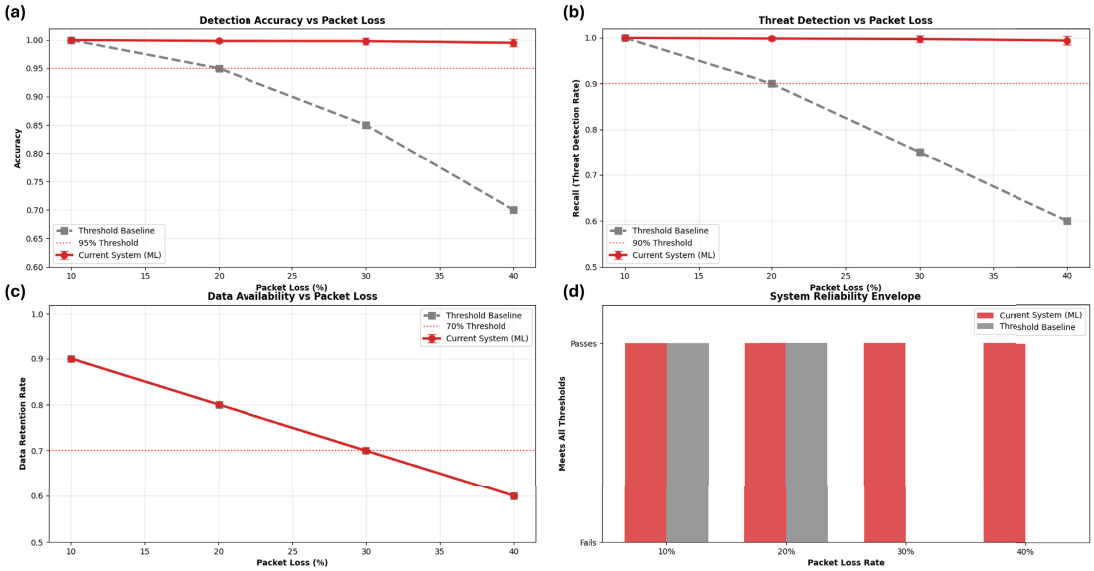

Fig. 7. System performance under increasing packet loss. (a) Detection accuracy and (b) recall remain near-perfect for the ML-based system, while the threshold baseline degrades below operational thresholds beyond 20% loss. (c) Data availability declines linearly with packet loss, reflecting expected channel constraints. (d) Reliability envelope confirms PureChain with ML remains reliable up to ~30% loss, whereas the threshold baseline fails after 20%.

TABLE V
NETWORK-INDEPENDENCE VALIDATION USING THE BIOCHEMICAL DATASET (SENSOR_DATA.JSON)

Network State	Detection Accuracy (%)	Blockchain Sync Delay (s)
Connected	69.0	0.00
Degraded	69.0	0.00
Disconnected	69.0	—
Reconnected	69.0	+0.01
High-latency	69.0	0.01
Packet-loss 20 %	69.0	0.00
Intermittent	69.0	0.00

Fig. 7(c), therefore, represents data-availability loss, not inference failure, while Fig. 7(d) depicts the overall system-reliability envelope. Up to 30% packet loss, buffered results are fully recovered upon reconnection; beyond that, latency and data retention decline as expected under severe disruption. These findings confirm that network degradation impacts only consensus synchronization, not biochemical detection capability, validating the system's resilience for mission-critical MANET deployment.

1) Network-Independent Inference: To empirically confirm that inference performance is independent of connectivity, the model was evaluated under seven network conditions—connected, degraded, disconnected, reconnected, high-latency, packet-loss 20%, and intermittent—using the same biochemical dataset (`sensor_data.json`). As summarized in Table V, detection accuracy remained constant at 69% across all conditions, while only minor BC synchronization delays ($\leq$ 0.01 s) occurred under degraded or high-latency states. These results verify that network variability affects only ledger synchronization timing, not the outcome or latency of local inference.

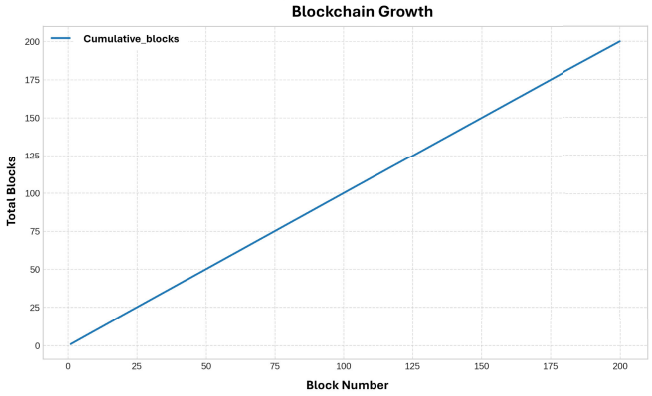

Fig. 8. BC growth during simulation, showing stable and consistent block generation under PoA^2 consensus in a degraded tactical network environment.

C. Evaluation II: BC Security Performance Analysis

The BC component of the proposed framework demonstrated consistent and uninterrupted growth throughout the

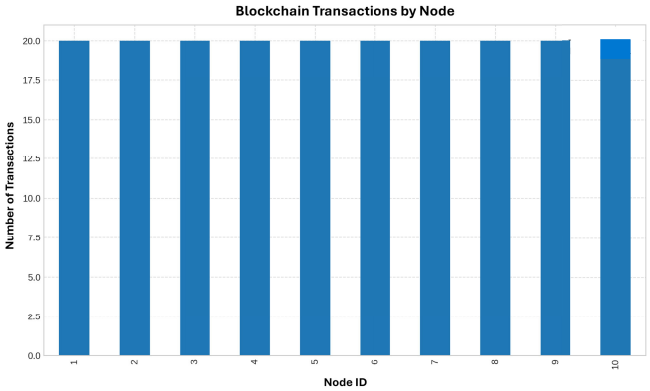

Fig. 9. Uniform distribution of BC transactions across all ten sensor nodes. Each node contributed exactly 20 detection result entries, demonstrating a balanced and decentralized logging process enabled by the PoA^2 consensus mechanism and supporting the framework's resilience to node-level disruptions.

simulation, effectively validating and logging all transactions generated by the threat detection pipeline. As shown in Fig. 8, the cumulative block count increased linearly, reaching a total of 200 blocks—representing 100 raw sensor readings and 100 corresponding detection results. This steady growth trend underscores the reliability of the underlying PoA^2 consensus mechanism, which maintained secure block generation even under 20% packet loss and intermittent connectivity. The absence of irregularities such as delays, forks, or rollback events during block propagation indicates that the BC layer successfully upheld data integrity, temporal ordering, and verifiability throughout the experiment. The linearity of block addition affirms that all threat events were immutably committed in real time, validating the suitability of the PureChain architecture for tactical deployment in adversarial and/or disconnected environments.

Complementing this growth trend, Fig. 9 presents the distribution of BC transactions across the ten sensor nodes in the network. Each node consistently contributed exactly 20 transactions to the BC, reflecting a fully balanced and decentralized logging process. This uniformity confirms that the system's workload was evenly distributed and that all nodes participated equally in the threat detection and data submission pipeline. Moreover, it highlights the successful operation of PureChain's offline caching and synchronization modules, which allowed nodes to locally buffer detection results and later broadcast them for BC inclusion once network conditions stabilized. The consistency across nodes affirms the PoA^2 model's ability to prevent node starvation, tolerate disconnections, and enforce fair participation—critical attributes for secure and scalable operation in contested battlefield networks.

While these results confirm that PureChain operated reliably under our simulated battlefield conditions, it is also important to position this performance relative to baseline and alternative consensus approaches discussed in existing works. A "no BC" configuration, where detections are logged locally, is efficient but remains vulnerable to tampering because traditional data stores generally support full "create, read, update, and delete" (CRUD) operations. In such systems, records can be modified or erased without leaving evidence of alteration [59]. By contrast, BC enforces a restricted "create and read" (CR) model, where transactions are immutable once committed: new entries may deprecate or supercede old ones, but the original data remains permanently recorded in the ledger, ensuring a tamper-evident audit trail. Raft consensus has been shown to maintain consistency under stable connectivity, but prior studies (see [57]) report that it stalls under significant packet loss due to repeated leader election failures, resulting in a transaction backlog. Similarly, conventional PoA systems [byzantine fault-tolerant (BFT)], which rely on static validator sets, are known to degrade when validators dropout and lack mechanisms for recovery [58]. By contrast, PureChain (PoA^2) integrates offline caching and validator replacement, allowing it to sustain block growth and validator participation up to 30% packet loss in our experiments. This literature-informed comparison is summarized in Table VI, which highlights why PureChain is better suited for contested MANET environments.

D. Evaluation III: ADL Threat Detection Capacity and Reliability Analysis

At the ADL, five ML classifiers, namely, RF, GB, SVM, KNN, and MLP, were trained and evaluated using 1000 AChE sensor readings, with 300 labeled as threats based on a 0.190 ppm threshold. A stratified split assigned 800 samples for training and 200 for testing. In addition to these ML models, we also implemented a simple threshold-only baseline at 0.19 ppm to evaluate whether AI is strictly necessary.

As shown in Table VII, the threshold baseline achieved 95% accuracy and an $F1$-score of 0.95, but its recall dropped to 0.90 due to misclassification of borderline noisy samples (e.g., 0.189 ppm, see Table IV). In contrast, all ML models achieved perfect classification performance across accuracy, precision, recall, and $F1$-score. This demonstrates that while thresholding suffices for clear separations, ML is required to maintain reliability under noise and sensor variability.

All ML models achieved perfect $F1$-scores of 1.00, indicating high reliability in threat detection, but MSE values revealed key differences. KNN's zero MSE suggests overfitting, while SVM had a higher MSE of 0.004977, indicating less confidence in predictions. GB, with an MSE of 0.000000, showed low error but similar overfitting potential. KNN and SVM were the fastest in training (0.01 and 0.03 s) and had the smallest model sizes (44.80 and 4.14 KB), but RF, with a training time of 0.31 s and a model size of 26.93 KB, offers the best balance between speed, efficiency, and accuracy, making it the optimal choice for deployment in resource-constrained environments. The robustness of RF was further confirmed under degraded battlefield conditions, including 20% packet loss. As seen in Fig. 10, the confusion matrix perfectly classifies all 60 threat and 140 nonthreat instances, while the ROC curve yields an AUC of 1.0, indicating ideal sensitivity and specificity of the RF.

E. Evaluation IV: Ablation of RF Hyperparameters

The impact of RF model complexity on detection accuracy and efficiency was evaluated by varying the number of trees,

TABLE VI
QUALITATIVE COMPARISON OF BC AND NON-BC APPROACHES FOR THREAT DETECTION LOGGING

Approach	Tamper Resistance	Offline Operation	Validator Replacement	Resilience (20–30% Loss)
Threshold-only	✗	✗	–	Misclassifies borderline data
No Blockchain	✗	✗	–	Vulnerable to tampering [56]
Raft Consensus	✓	✗	✗	Leader failures under loss [57]
Static PoA	✓	✗	✗	Degrades under validator loss [58]
PureChain (PoA^2)	✓	✓	✓	Stable up to 30% loss

✗= Not considered; ✓ = Considered; POA = Proof of Authority; POA^2 = Proof of Authority-and-Association

TABLE VII
ML MODEL PERFORMANCE

Model	Accuracy	Precision (Threat)	Recall (Threat)	F1 Score (Threat)	MSE	Training Time (s)	Model Size
Threshold-only	95%	0.96	0.90	0.95	-	-	-
RF	100%	1.00	1.00	1.00	0.000125	0.31	26.93 KB
GB	100%	1.00	1.00	1.00	0.000000	0.39	46.31 KB
SVM	100%	1.00	1.00	1.00	0.004977	0.03	4.14 KB
KNN	100%	1.00	1.00	1.00	0.000000	0.01	44.80 KB
MLP	100%	1.00	1.00	1.00	0.005683	3.54	60.69 KB

maximum depth, and minimum samples per leaf. Fig. 11 illustrates the performance landscape, and Table VIII summarizes representative configurations.

For performance saturation, detection accuracy, and $F1$-score plateau rapidly. A configuration with 50 trees and a maximum depth of 8 achieves nearly perfect results ($F1$ = 0.998), with no significant gains observed beyond this point. Increasing to 100 trees and depth 10 yields perfect scores (accuracy = 1.000 and $F1$ = 1.000) but offers only marginal improvement over the 50-tree setting. For efficiency tradeoffs, the Inference latency and model size increase with forest size, from 11.2 ms at 10 trees to 44.1 ms at 200 trees. Beyond 50 trees, additional capacity results in diminishing returns in accuracy while incurring higher resource costs. Finally, recommended operating points, two practical settings are identified: i) *edge-efficient* (50 trees, depth 8, and leaf 2), this provides near-perfect detection with reduced latency and model size; and ii) *deployed* (100 trees, depth 10, and leaf 2), which guarantees perfect performance and provides additional robustness margin under noisy or borderline conditions at modest extra cost. For mission-critical deployments, the latter configuration is retained, while the former remains suitable for resource-constrained environments. These results confirm that the deployed configuration is not strictly necessary for high accuracy, but was chosen to maximize resilience under volatile tactical conditions.

F. Evaluation V: Concentration Distribution and Threat Probability Pattern

The distribution of simulated nerve agent concentrations used in the biochemical detection model is shown in Fig. 12, which overlays the detection threshold of approximately 0.189 ppm as a red dashed line. This threshold was selected based on empirical tuning and biochemical literature [49] to reflect sarin toxicity sensitivity. The histogram reveals a broad and symmetric spread of concentration values ranging from near-zero to 0.30 ppm, with a dense clustering around the threshold region. This distribution ensures the model is exposed to a balanced set of both nonthreatening and borderline-threatening cases during training. The inclusion of a clear threshold

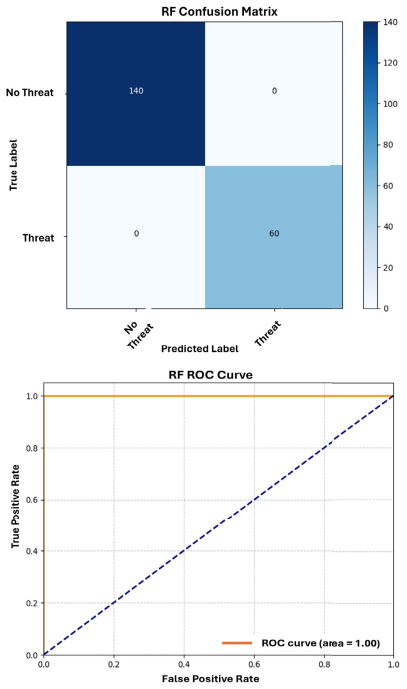

Fig. 10. Combined confusion matrix and ROC curve for the RF classifier showing perfect threat detection accuracy and ideal classification performance (AUC = 1.0) under simulated battlefield conditions.

marker in the visualization allows for visual validation that the detection engine was calibrated to respond aggressively to values exceeding the designated biochemical risk level.

Complementing this, Fig. 13 presents a heatmap of threat detection probabilities across all sensor nodes and sample sequences. The high-intensity vertical stripe pattern that emerges from sensors 81 to 100 aligns with escalating concentrations in the latter stages of the simulation, validating that the AI engine correctly identified these as high-risk exposures. Conversely, earlier sensor IDs with lower exposure levels maintained low threat probabilities, showcasing the model's ability to distinguish safe from unsafe readings. The heatmap further demonstrates spatial–temporal awareness in the system's detection capabilities, confirming that threat probabilities are sharply elevated only when concentrations exceed the threshold. This validates the RF model's reliability, consistency, and interpretability in predicting sarin threats under evolving battlefield conditions.

G. Evaluation VI: Comparative Analysis (Unified Baselines and Qualitative Specifics)

Table IX provides a two-part comparative analysis designed to ensure both controlled benchmarking and appropriate

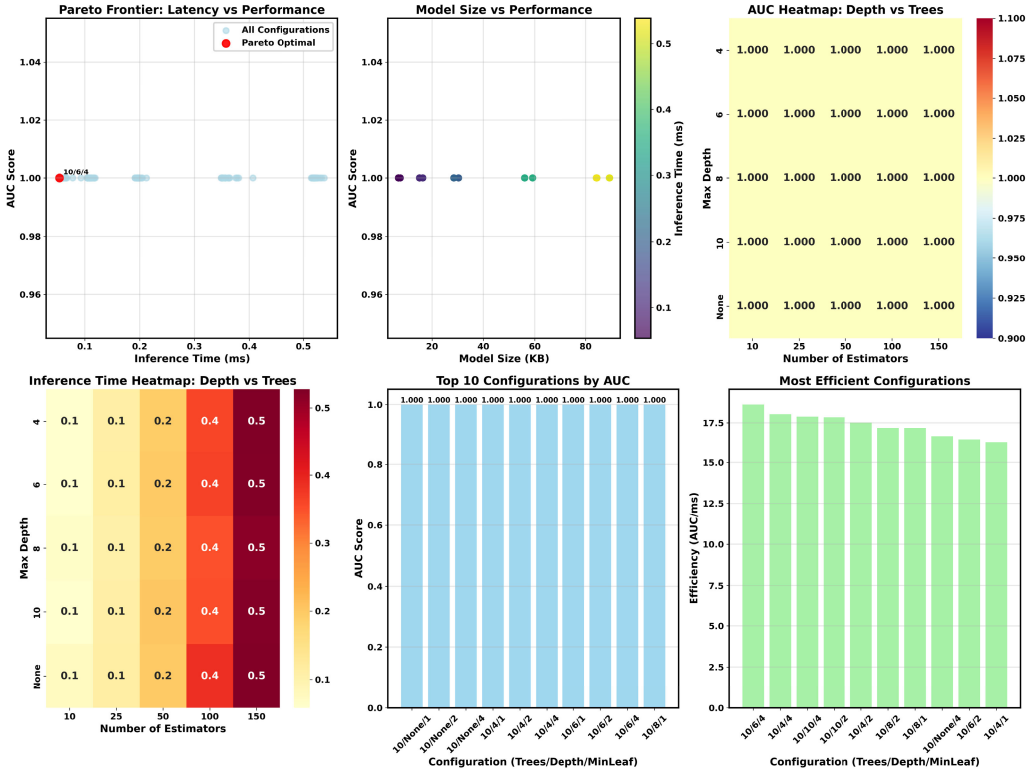

Fig. 11. RF hyperparameter ablation. Left: Pareto frontier of latency versus AUC highlights early saturation (≥ 50 trees and depth ≥ 6). Middle: model size versus performance shows diminishing returns beyond the plateau. Right: heatmaps over (trees and depth) with min_samples_leaf fixed at 2. Two practical operating points emerge: edge-efficient (50/8/2) and deployed (100/10/2).

TABLE VIII
RF HYPERPARAMETER ABLATION

Trees	Depth	Leaf	Depth	Accuracy	Latency
10	4	2	0.972	0.970	11.2
50	8	2	0.998	0.998	15.6
100	10	2	1.000	1.000	27.5
200	12	2	1.000	1.000	44.1

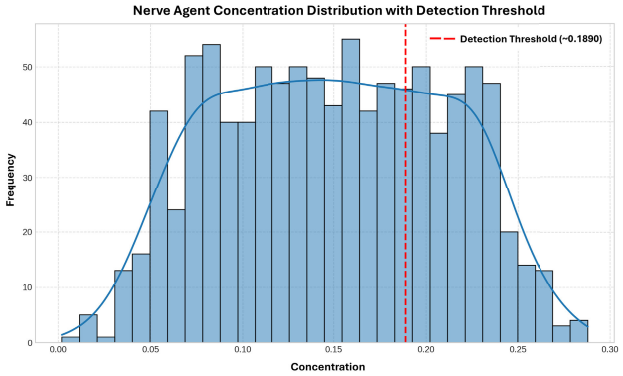

Fig. 12. Distribution of simulated nerve agent concentrations with the detection threshold (0.1890 ppm) marked by a red dashed line, indicating the decision boundary for triggering threat alerts.

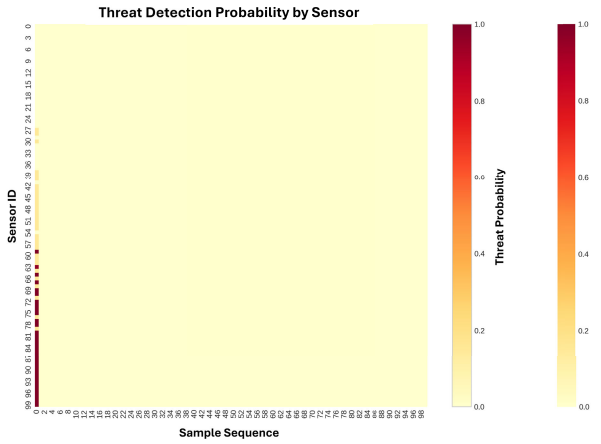

Fig. 13. Heatmap showing threat detection probabilities by sensor across simulation samples. High-probability regions concentrated near sensors 81–100 indicate elevated sarin concentrations above the detection threshold, validating the model's ability to isolate true threats with high confidence.

literature context. First, Part 1 reports a unified quantitative evaluation of representative baselines on the AChE biochemical dataset (`sensor_data.json`) using the same preprocessing and metrics as the proposed framework. As shown, the Threshold-only baseline (95% accuracy) misses borderline cases in the 0.18–0.20-ppm range, motivating the need for learned decision boundaries. While KNN, SVM, GB, and MLP achieve near-perfect detection performance, they exhibit markedly different deployability tradeoffs: KNN and SVM are fast (1–3 ms) but differ in footprint and generalization characteristics, GB incurs higher overhead (39 ms), and MLP is unsuitable for real-time edge deployment due to high latency (3540 ms). In contrast, the proposed RF-based

TABLE IX
COMPARATIVE ANALYSIS: QUANTITATIVE BASELINES VERSUS QUALITATIVE LITERATURE SURVEY

Part 1: Quantitative Comparison on AChE Biochemical Dataset (sensor_data.json)

Method	Accuracy	Precision	Recall	F1 Score	Latency (ms)	Suitability for Tactical Edge
Threshold-only	95%	0.96	0.90	0.95	—	Misses borderline cases (0.18–0.20 ppm)
KNN	100%	1.00	1.00	1.00	1	Fast but overfitting risk, large size (44.8 KB)
SVM	100%	1.00	1.00	1.00	3	Compact (4.1 KB) but higher MSE (0.005)
GB	100%	1.00	1.00	1.00	39	Perfect fit but moderate overhead (46.3 KB)
MLP	100%	1.00	1.00	1.00	3540	Too slow for real-time edge inference
RF (Proposed)	**100%**	**1.00**	**1.00**	**1.00**	**27.5**	**Optimal balance: robust, fast, compact (26.9 KB)**

Note: All models trained and evaluated on identical AChE sensor dataset with 20% packet loss MANET conditions.

Part 2: Qualitative Architecture Comparison Across Heterogeneous Domains

Ref.	Domain	AI Model	Blockchain	Offline	MANET	Reported Acc.	Model Size	Key Limitation
[60]	IIoT anomaly	FedAvg ensemble	Public chain	Partial	No	99%†	∼100 MB	Centralized aggregation, no edge
[61]	6G safety	XGBoost	Ethereum+IPFS	No	No	87.9%†	Medium	Continuous connectivity required
[22]	Firearm detection	YOLOv5	No	Yes	Yes	98.9%†	<30 MB	No tamper-proof logging
[23]	Wormhole attack	Decision Tree	No	Partial	Yes	98.9%†	<50 MB	Centralized, no provenance
[24]	Blackhole attack	KNN+Fuzzy	No	No	Yes	97.2%†	Small	No cryptographic guarantees
[46]	Surveillance	Xception CNN	Ethereum	No	No	90%†	25 MB (GPU)	GPU-dependent, online only
Proposed	**Biochem threat**	**RF+PoA²**	**PureChain**	**Yes**	**Yes**	**100%**	**26.9 KB (CPU)**	**Centralized model training; limited to sarin/AChE**

†*Not directly comparable: different datasets, tasks, and evaluation protocols. Included for architectural context only.*

detector maintains perfect detection while remaining edge-suitable with 27.5-ms inference latency and a compact 26.9-kB model size, providing a practical balance of robustness and efficiency under 20% packet loss MANET conditions.

Then, Part 2 complements this controlled comparison with a qualitative architecture survey across heterogeneous domains, included strictly for contextual positioning rather than direct numerical benchmarking. Specifically, [60] combines FedAvg-based IIoT anomaly detection with a public BC but relies on centralized aggregation and lacks true edge suitability; [61] integrates XGBoost with Ethereum+IPFS for 6G safety analytics but requires continuous connectivity; [22] applies YOLOv5 for firearm detection in MANET-related settings yet lacks tamper-proof logging; [23] and [24] address wormhole and blackhole attacks using lightweight classifiers (decision tree; KNN+Fuzzy) but do not provide cryptographic provenance guarantees; and [46] leverages Ethereum-backed logging for surveillance with a CNN backbone but remains GPU-dependent and online-only. Relative to these works, the proposed RF+PoA^2 PureChain framework uniquely couples lightweight biochemical inference with decentralized, tamper-evident verification and offline-capable synchronization, making it specifically aligned with mission-critical MANET deployments.

V. CONCLUSION

This article proposed an AI-integrated BC framework for resilient biochemical threat detection in tactical MANETs. Using AChE sensor data, an RF classifier achieved sub-30-ms inference latency and robust performance under noisy borderline conditions, outperforming a threshold-only baseline that degraded in recall. An ablation study showed that performance saturates with $\geq$ 50 trees, while the deployed 100-tree configuration provides additional robustness. On the BC layer, the lightweight PoA^2 consensus ensured tamper-resistant logging, validator replacement, and offline caching, sustaining linear growth and balanced participation across nodes. The system remained reliable up to ∼30% packet loss before entering a degraded but auditable state, defining its operational envelope. A security analysis further outlined potential attack vectors and mitigations, including hardware key protection, equivocation proofs, nonce-based freshness checks, and signed model updates. Together, these results demonstrate that the proposed framework provides secure, efficient, and autonomous biochemical threat monitoring, combining robust AI inference with lightweight BC consensus to maintain integrity and trust in mission-critical, infrastructure-limited environments.

REFERENCES

[1] N. H. Johnson, J. C. Larsen, and E. C. Meek, "Historical perspective of chemical warfare agents," in *Handbook of Toxicology of Chemical Warfare Agents*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 17–26.

[2] J. Walker, "Lessons from the chemical weapons convention negotiations and implementation for the diplomatic challenges of negotiating 'irreversibility,'" *J. Peace Nucl. Disarmament*, vol. 7, no. 2, pp. 385–391, Jul. 2024.

[3] J. Blatny, "Biological threats," in *CBRNE: Challenges 21st Century*. Cham, Switzerland: Springer, 2022, pp. 47–78.

[4] M. Crowley and M. Dando, "Regulation of toxins and bioregulators under the chemical weapons convention and the biological and toxin weapons convention," *J. Biosafety Biosecurity*, vol. 6, no. 2, pp. 99–112, Jun. 2024.

[5] R. Wulandari, T. Mantoro, S. A. Pasma, and D. S. Suliantoro, "Integration of government regulations to anticipate terrorist threats in the misuse of chemicals as chemical weapons," in *Proc. Int. Conf. Technol., Eng., Comput. Appl. (ICTECA)*, Dec. 2023, pp. 1–6.

[6] F. Schmaltz, "Neurosciences and research on chemical weapons of mass destruction in nazi Germany," *J. Hist. Neurosciences*, vol. 15, no. 3, pp. 186–209, Sep. 2006.

[7] H. Salem, A. L. Ternay Jr., and J. K. Smart, "Brief history and use of chemical warfare agents in warfare and terrorism," in *Chemical Warfare Agents*. Boca Raton, FL, USA: CRC Press, 2019, pp. 3–15.

[8] L. L. Chao and Y. Zhang, "Effects of low-level sarin and cyclosarin exposure on hippocampal microstructure in Gulf war veterans," *Neurotoxicology Teratology*, vol. 68, pp. 36–46, Jul. 2018.

[9] A. Sugiyama et al., "The Tokyo subway sarin attack has long-term effects on survivors: A 10-year study started 5 years after the terrorist incident," *PLoS ONE*, vol. 15, no. 6, Jun. 2020, Art. no. e0234967.

[10] J. Bajgar, J. Fusek, J. Kassa, K. Kuca, and D. Jun, "Global impact of chemical warfare agents used before and after 1945," in *Handbook of Toxicology of Chemical Warfare Agents*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 27–36.

[11] OPCW. (2025). *Responding To the Use of Chemical Weapons*. [Online]. Available: https://www.opcw.org/our-work/responding-use-chemical-weapons

[12] (2025). *Death By Chemicals*. [Online]. Available: https://www.hrw.org/report/2017/05/01/death-chemicals/syrian-governments-widespread-and-systematic-use-chemical-weapons

[13] M.-M. Blum and R. V. S. M. Mamidanna, "Analytical chemistry and the chemical weapons convention," *Anal. Bioanal. Chem.*, vol. 406, no. 21, pp. 5067–5069, Aug. 2014.

[14] I. U. Ajakwe, S. O. Ajakwe, J. M. Lee, and D. Kim, "IoT-blockchain frameworks in environmental pollution monitoring and data management," in *Proc. 15th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2024, pp. 2147–2151.

[15] O. Terzic, H. Gregg, and P. de Voogt, "Identification of chemicals relevant to the chemical weapons convention using the novel sample-preparation methods and strategies of the mobile laboratory of the organization for the prohibition of chemical weapons," *TrAC Trends Anal. Chem.*, vol. 65, pp. 151–166, Feb. 2015.

[16] Z. Zhou, T. Xu, and X. Zhang, "Empowerment of AI algorithms in biochemical sensors," *TrAC Trends Anal. Chem.*, vol. 173, Apr. 2024, Art. no. 117613.

[17] S. O. Ajakwe, I. U. Ajakwe, T. Jun, D.-S. Kim, and J.-M. Lee, "CIS-WQMS: Connected intelligence smart water quality monitoring scheme," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100800.

[18] J. Taylor, E. Ccopa-Rivera, S. Kim, R. Campbell, R. Summerscales, and H. Kwon, "Machine learning analysis for phenolic compound monitoring using a mobile phone-based ECL sensor," *Sensors*, vol. 21, no. 18, p. 6004, Sep. 2021.

[19] S. O. Ajakwe and D.-S. Kim, "EQAI: Explainable quantum-empowered antispoofing intelligence for trustworthy connected autonomous vehicles communication," *IEEE Internet Things J.*, early access, Nov. 28, 2025, doi: 10.1109/JIOT.2025.3638378.

[20] M. A. Z. Chowdhury and M. A. Oehlschlaeger, "Artificial intelligence in gas sensing: A review," *ACS Sensors*, vol. 10, no. 3, pp. 1538–1563, Mar. 2025.

[21] C. A. Nnadiekwe, S. O. Ajakwe, J.-M. Lee, and D.-S. Kim, "RemoteCare: AI-driven multimodal predictive framework with blockchain for personalized remote patient monitoring in IoMT," *IEEE Internet Things J.*, vol. 13, no. 3, pp. 4508–4523, Feb. 2026.

[22] S. T. Apeh, L. A. Ajao, D. S. Nyitamen, C. L. Wamdeo, and R. Edeh, "Artificial intelligence-based wireless sensor network model for intrusion detection and firearms image detection in the conflict zone," in *Proc. Cloud Comput. Data Sci.*, 2025, pp. 94–114.

[23] M. Abdan and S. A. H. Seno, "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)," *Wireless Commun. Mobile Comput.*, vol. 2022, no. 1, Jan. 2022, Art. no. 2375702.

[24] G. Farahani, "Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks," *Secur. Commun. Netw.*, vol. 2021, pp. 1–15, Aug. 2021.

[25] S. Kumbale, S. Singh, G. Poornalatha, and S. Singh, "BREE-HD: A transformer-based model to identify threats on Twitter," *IEEE Access*, vol. 11, pp. 67180–67190, 2023.

[26] C. Park, J. Lee, Y. Kim, J.-G. Park, H. Kim, and D. Hong, "An enhanced AI-based network intrusion detection system using generative adversarial networks," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2330–2345, Feb. 2023.

[27] R. Mohandas, K. K. Vaigandla, N. Sivapriya, and K. Kirubasankar, "Detection and evaluation of cybersecurity threats in MANET based on AI," in *Proc. 4th Int. Conf. Ubiquitous Comput. Intell. Inf. Syst. (ICUIS)*, Dec. 2024, pp. 1486–1492.

[28] M. T. Sultan, H. E. Sayed, and M. A. Khan, "An intrusion detection mechanism for MANETs based on deep learning artificial neural networks (ANNs)," 2023, *arXiv:2303.08248*.

[29] T. S. Delwar et al., "The intersection of machine learning and wireless sensor network security for cyber-attack detection: A detailed analysis," *Sensors*, vol. 24, no. 19, p. 6377, Oct. 2024.

[30] V. Kumar, H. Kim, B. Pandey, T. D. James, J. Yoon, and E. V. Anslyn, "Recent advances in fluorescent and colorimetric chemosensors for the detection of chemical warfare agents: A legacy of the 21st century," *Chem. Soc. Rev.*, vol. 52, no. 2, pp. 663–704, 2023.

[31] D. A. Jett et al., "A national toxicology program systematic review of the evidence for long-term effects after acute exposure to sarin nerve agent," *Crit. Rev. Toxicology*, vol. 50, no. 6, pp. 474–490, Jul. 2020.

[32] H. John et al., "Fatal sarin poisoning in Syria 2013: Forensic verification within an international laboratory network," *Forensic Toxicology*, vol. 36, no. 1, pp. 61–71, Jan. 2018.

[33] L. Yishai Aviram, M. Magen, S. Chapman, A. Neufeld Cohen, S. Lazar, and S. Dagan, "Dry blood spot sample collection for post-exposure monitoring of chemical warfare agents–in vivo determination of phosphonic acids using LC-MS/MS," *J. Chromatography B*, vols. 1093–1094, pp. 60–65, Sep. 2018.

[34] T. Baygildiev, M. Vokuev, A. Braun, I. Rybalchenko, and I. Rodin, "Monitoring of hydrolysis products of mustard gas, some sesqui- and oxy-mustards and other chemical warfare agents in a plant material by HPLC-MS/MS," *J. Chromatography B*, vol. 1162, Jan. 2021, Art. no. 122452.

[35] D. T. Snyder et al., "Two-dimensional MS/MS scans on a linear ion trap mass analyzer: Identification of V-series chemical warfare agents," *Int. J. Mass Spectrometry*, vol. 444, Oct. 2019, Art. no. 116171.

[36] C. E. Kientz, "Chromatography and mass spectrometry of chemical warfare agents, toxins and related compounds: State of the art and future prospects," *J. Chromatography A*, vol. 814, nos. 1–2, pp. 1–23, Jul. 1998.

[37] H. Niemikoski, M. Söderström, and P. Vanninen, "Detection of chemical warfare agent-related phenylarsenic compounds in marine biota samples by LC-HESI/MS/MS," *Anal. Chem.*, vol. 89, no. 20, pp. 11129–11134, Oct. 2017.

[38] Y. Saylan, S. Akgönüllü, and A. Denizli, "Plasmonic sensors for monitoring biological and chemical threat agents," *Biosensors*, vol. 10, no. 10, p. 142, Oct. 2020.

[39] U. Yahaya, M. Akram, R. I. Abdullahi, B. O. Adaaja, G. Otiwa, and B. O. Odey, "The role of biosensors and biological weapons in national defence and security operations," *Nigerian J. Biotechnol.*, vol. 38, no. 1, pp. 132–136, Jul. 2021.

[40] N. M. Noah, "Design and synthesis of nanostructured materials for sensor applications," *J. Nanomaterials*, vol. 2020, pp. 1–20, Oct. 2020.

[41] S. O. Ajakwe, K. L. Olabisi, and D.-S. Kim, "Multihop intruder node detection scheme (MINDS) for secured drones' FANET communication," *IET Intell. Transp. Syst.*, vol. 19, no. 1, p. 70080, Jan. 2025.

[42] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma, "An improved hybrid secure multipath routing protocol for MANET," *IEEE Access*, vol. 9, pp. 163043–163053, 2021.

[43] S. O. Ajakwe, I. S. Igboanusi, J.-M. Lee, and D.-S. Kim, "IBANDA: A blockchain-assisted defense system for authentication in drone-based logistics," *Drones*, vol. 9, no. 8, p. 590, Aug. 2025.

[44] A. A. Ali, M. K. Hussein, and M. A. Subhi, "A classifier-driven deep learning clustering approach to enhance data collection in MANETs," *Mesopotamian J. CyberSecurity*, vol. 4, no. 3, pp. 164–173, Sep. 2024.

[45] I. N. Ecemis, F. Ekinci, K. Acici, M. S. Guzel, I. T. Medeni, and T. Asuroglu, "Exploring blockchain for nuclear material tracking: A scoping review and innovative model proposal," *Energies*, vol. 17, no. 12, p. 3028, Jun. 2024.

[46] D. Patel et al., "BlockCrime: Blockchain and deep learning-based collaborative intelligence framework to detect malicious activities for public safety," *Mathematics*, vol. 10, no. 17, p. 3195, Sep. 2022.

[47] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the integration of artificial intelligence and blockchain technology: A perspective about security," *IEEE Access*, vol. 12, pp. 3881–3897, 2024.

[48] T. Kegyes, Z. Süle, and J. Abonyi, "Machine learning -based decision support framework for CBRN protection," *Heliyon*, vol. 10, no. 4, Feb. 2024, Art. no. e25946. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405844024019777

[49] (2025). *Sarin (GB): Nerve Agent — NIOSH — CDC*. [Online]. Available: https://www.cdc.gov/niosh/ershdb/emergencyresponsecard_29750001.html

[50] M. L. Ali, K. Thakur, S. Schmeelk, J. E. DeBello, and D. Dragos, "Deep learning vs. Machine learning for intrusion detection in computer networks: A comparative study," *Appl. Sci.*, vol. 15, no. 4, p. 1903, 2025.

[51] V. I. Kanu, S. O. Ajakwe, J. M. Lee, and D. Kim, "Blockchain technology in protein folding: Enhancing data sharing and collaboration," in *Proc. 15th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2024, pp. 1913–1918.
[52] D.-S. Kim, I. S. Igboanusi, L. A. Chijioke Ahakonye, and G. O. Anyanwu, "Proof-of-authority-and-association consensus algorithm for IoT blockchain networks," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2025, pp. 1–6.
[53] A. Palkó and L. Sujbert, "Time and frequency domain description of Gilbert–Elliott data loss models," in *Proc. 20th Int. Carpathian Control Conf. (ICCC)*, May 2019, pp. 1–6.
[54] H. Al-Bahadili and K. Kaabneh, "Analyzing the performance of probabilistic algorithm in noisy manets," 2010, *arXiv:1009.0386*.
[55] J. W. H. Leow and E. C. Y. Chan, "Atypical michaelis-menten kinetics in cytochrome P450 enzymes: A focus on substrate inhibition," *Biochem. Pharmacol.*, vol. 169, Nov. 2019, Art. no. 113615.
[56] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," 2019, *arXiv:1906.11078*.
[57] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 172–181, Jan. 2020.
[58] Y. Zou et al., "A survey of fault tolerant consensus in wireless networks," *High-Confidence Comput.*, vol. 4, no. 2, Jun. 2024, Art. no. 100202.
[59] I. U. Ajakwe, V. I. Kanu, S. O. Ajakwe, and D.-S. Kim, "EBCTC: Energy-efficient hybrid blockchain architecture for smart and secured K-ETS," *Cleaner Eng. Technol.*, vol. 29, Dec. 2025, Art. no. 101084.
[60] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based IIoT networks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8356–8366, Nov. 2022.
[61] T. Rathod et al., "Blockchain-driven intelligent scheme for IoT-based public safety system beyond 5G networks," *Sensors*, vol. 23, no. 2, p. 969, Jan. 2023.

Victor Ikenna Kanu received the National Diploma degree in food science and technology from the Yaba College of Technology, Lagos, Nigeria, in 2015, and the B.Sc. degree (Hons.) in biochemistry from the University of Lagos, Lagos, in 2019. He is currently pursuing the master's degree in engineering in IT convergence engineering with the Kumoh National Institute of Technology, Gumi, South Korea.

His work spans blockchain-audited pipeline verification, AI-driven modeling, and end-to-end system design for data-intensive scientific applications, with emphasis on transparency, deterministic execution, and verifiable provenance. He has contributed to multiple applied research projects and manuscripts across areas including bioinformatics workflows, secure distributed computation, and AI-assisted screening/analysis pipelines. His research centers on building scalable, verifiable computational systems that improve reliability, and reproducibility in modern scientific and engineering practice.

Ihunanya Udodiri Ajakwe received the Bachelor of Science (B.Sc.) degree in biochemistry from Imo State University (IMSU), Owerri, Nigeria, in 2010, and the Master of Science (M.Sc.) degree in biochemistry from the Federal University of Technology Owerri (FUTO), Owerri, in 2020. She is currently pursuing the Ph.D. degree in IT convergence engineering with the Kumoh National Institute of Technology, Gumi, South Korea.

She has extensive experience in interdisciplinary research. Her scholarly contributions include several articles published in reputable peer-reviewed journals and international conferences. Her research interests center on the intersection of environmental-IT security and biotechnology, specifically focusing on explainable AI (XAI), blockchain-enabled carbon trading systems, water quality monitoring, and trustworthy IoT frameworks for sustainable environmental management.

Ms. Ajakwe is a member of the Nigerian Society of Biochemistry and Molecular Biology.

Simeon Okechukwu Ajakwe (Senior Member, IEEE) received the Diploma degree in computer science from the Institute of Management Technology, Enugu, Nigeria, in 2004, the Bachelor of Science degree in computer science from Imo State University, Owerri, Nigeria, in 2009, the Master of Science (M.Sc.) degree (Hons.) in information technology from the Federal University of Technology, Owerri, Imo, Nigeria, in 2016, and the Ph.D. degree (Hons.) in IT-convergence engineering from the Kumoh National Institute of Technology, Gumi, South Korea, in 2023.

He is a Chartered Information Technology Professional (Citp) with many years of IT-related industrial and academic experience. He is also a Post-Doctoral Research Fellow with the ICT Convergence Research Center (ICT-CRC), Kumoh National Institute of Technology. He has published several articles and conference papers. His research interests include AI for aerial mobility, trustworthy AI, vehicular networks, the Internet of Medical Things, and information system security.

Dr. Ajakwe is a member of the Association of Computing Machinery (ACM), Computer Professionals of Nigeria (CPN), and the Nigerian Internet Society (NIS). He received several awards, such as the Best Ph.D. Thesis Award, the Best Paper Award, and the Research Excellence Award. He served as an editor, guest editor, and reviewer for reputable peer-reviewed journals.

Dong-Seong Kim (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2003.

He worked as a full-time Researcher at ERCACI, Seoul National University, from 1994 to 2003. From March 2003 to February 2005, he worked as a Post-Doctoral Researcher at the Wireless Network Laboratory, School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, USA. From 2007 to 2009, he was a Visiting Professor at the Department of Computer Science, University of California at Davis, Davis, CA, USA. He is currently the Director with the KIT Convergence Research Institute and the ICT Convergence Research Center (ITRC and NRF Advanced Research Center Program) supported by the Korean Government, Kumoh National Institute of Technology, Gumi, South Korea. His current main research interests are real-time IoT and smart platforms, industrial wireless control networks, networked embedded systems, and fieldbus.

Prof. Kim is a Senior Member of ACM.