A Resilient Framework for Industry 5.0 WSNs: Enhancing Network Lifetime via a Lightweight Reputation Ledger and Hybrid AI

Padma Sree N, Dr. Malini M Patil
Computer Science and Engineering, RV Institute of Technology and Management, Bangalore, India

***Abstract*—Wireless Sensor Networks (WSNs) play an increasingly important role in Industry 5.0 cyber–physical systems, where resilience, trust, and energy efficiency are essential under dynamic operating conditions. However, their limited resources, scattered deployment, and continuous operation make these networks highly susceptible to unusual behavior and cyberattacks. Such issues can compromise data quality, disrupt network reliability, and shorten the overall lifespan of the system. To address these challenges, this study examines WSN resilience as a combined problem of anomaly detection accuracy, fault isolation latency, and network lifetime under realistic fault and energy constraints. At the core of the framework is a Model Context Protocol (MCP), which combines a supervised LightGBM classifier with an unsupervised LSTM autoencoder to capture both event-driven and temporal anomalies in sensor data. Complementing this is a compact "Micro-Ledger" system that updates trust values for each node by monitoring behavior and using streamlined consensus rules. Together, they create a continuous feedback mechanism that isolates suspicious nodes while keeping energy consumption in check. The framework is evaluated using a set of resilience-oriented metrics, including fault detection latency, Mean Time To Failure (MTTF), reputation convergence behavior, and overall network lifetime. Experiments conducted in a Digital Twin simulation environment report an F1-score of 0.997, an 18.7% improvement in network lifetime, and a Micro-Ledger storage overhead of approximately 98 KB. While the current validation is simulation-based, the proposed design can be extended to physical deployments through adaptive trust weighting, cluster-head redundancy, and probation-based node reintegration.**

Keywords*—Wireless Sensor Networks (WSNs); Industry 5.0; anomaly detection; lightweight blockchain; trust management; network lifetime; Digital Twin

I. Introduction

Industry 5.0, or the fifth industrial revolution, ushers in an altogether new paradigm that seeks to make production systems more human-centered and focus on sustainability and resilience [1]. At the heart of Industry 5.0 will be IoE, encompassing the interlinking of cyber-physical spaces through Wireless Sensor Networks or WSNs, which will be able to connect the two environments of physical and digital. A typical WSN contains thousands of spatially distributed sensor nodes that capture data and transport information continuously. This decentralized approach has its own merits—the intelligent automation, the adaptive control—but at the same time, it gives rise to important vulnerabilities because of the energy-constrained and distributed nodes [2].

Outliers or anomalous data points caused by malicious intrusions, hardware failures, or environmental interference degrade network performance, data integrity, and energy efficiency [3]. These anomalies increase communication overhead and maintenance costs and, hence, reduce network lifetime. In such environments, resilience is no longer limited to fault tolerance alone but also includes timely anomaly recognition, trust-aware decision-making, and sustained operation under resource constraints.

While anomaly detection, trust management, and blockchain-based integrity have each been studied in isolation, their joint role in sustaining long-term resilience and network lifetime in Industry 5.0 WSNs remains underexplored. In particular, existing approaches often lack adaptive trust evolution driven by real-time anomaly evidence. Industry 5.0 extends earlier industrial paradigms by emphasizing resilience, sustainability, and human-centric cyber–physical systems [23]. ML approaches to anomaly detection show promise; however, applications in dynamic IoT and WSN often struggle to generalize across heterogeneous anomaly types and dynamically changing operating conditions. [4]. Similarly, single-model classifiers, such as Support Vector Machines and Decision Trees, have lower performance while dealing with heterogeneous sensor data [5]. Beyond detection accuracy, system-level resilience metrics such as fault detection latency, recovery behavior, and network lifetime are equally critical in practical WSN deployments.

Recent research in deep learning has enhanced detection accuracy through the temporal dependencies modeled on sequential data. For example, LSTM-based networks have achieved high performance in detecting time-series anomalies in WSNs [6]. However, these networks still suffer from some limitations when used in isolation, as they cannot detect event-based and time-series anomalies in dynamic environmental conditions [7].

While blockchain mechanisms have been extensively explored to ensure data integrity and auditability in WSNs, the consensus protocols commonly adopted are computationally expensive, such as PoW, thus being infeasible for energy-constrained sensor nodes. Lightweight blockchain designs have recently been proposed, although they are often passive data storage rather than active adaptive trust systems. Besides, most of the earlier studies fail to address changing behavior of

network nodes, an essential factor in accurate and dynamic trust levels. However, when used purely as a passive data store, blockchain mechanisms offer limited support for adapting to evolving node behavior or mitigating energy drain caused by unreliable sensors.

Addressing these challenges calls for an integrated multilayer resilience framework, coherent with the principles of Industry 5.0. The key contributions of this work can be summarized as follows:

- Hybrid Anomaly Detection (Model Context Protocol - MCP): A hybrid architecture combining LightGBM and LSTM Autoencoder models aims to improve detection accuracy across multiple anomaly types [12].
- Lightweight "Micro-Ledger" for Dynamic Trust Management: A blockchain-based reputation system for resource-constrained WSNs, which improves node trust evaluation and energy efficiency [13].
- Closed-loop feedback mechanism: Integration of anomaly detection results with the Micro-Ledger to support automated isolation of persistently unreliable nodes [14].
- Digital Twin Validation: Simulation and testing on a Digital Twin environment to assess resilience under induced network noise and channel interference conditions [15].

The present study focuses on simulation-based validation within a Digital Twin environment to analyze resilience behavior under controlled fault conditions. Extensions to physical deployments, more complex attack models, and adaptive trust policies are discussed as part of future research directions.

II. Related Work

The security, reliability, and longevity of WSNs have been recognized as key challenges in the evolution of both Industry 5.0 and the IoT [16]. Accordingly, resultant topics related to these areas have been actively reviewed across a wide variety of domains, with particular attention given to anomaly detection, blockchain-enabled trust management, and energy-efficient network design. Despite these active developments, there is still a dire need for integrated frameworks that bring these components together into a cohesive, resilient architecture.

A. Anomaly Detection in WSNs and IoT Systems

ML and DL have emerged as the key technologies for anomaly detection in WSNs/IoT systems in recent times [17]. For instance, Al-Qatf et al. showed that ML classifiers such as Support Vector Machines and Decision Trees could efficiently detect intrusions in sensor networks [18]. Further research by Otoum et al. applied Random Forests, presenting enhancements in the detection performance of IoT-based intrusion detection systems.

Deep Learning improved the detection capabilities by learning complex temporal and nonlinear patterns present in time series data. Malhotra et al. introduced the concept of LSTM Autoencoders, which perform anomaly detection by learning normal system behavior and subsequently finding deviations from it [20].

Similarly, Lee et al. have also demonstrated effectiveness in fault detection in vibration-based cyber-physical systems using LSTM Autoencoders [21]. Despite these advances, single-model approaches remain limited in detecting multiple types of anomalies in heterogeneous WSN environments [22]. Hybrid or ensemble architectures combining different models have also been proposed to overcome this limitation and offer increased robustness. For example, Khairullah and Alsenani showed that hybrid frameworks that integrate both gradient boosting and deep learning improved the consistency of anomaly detection. This idea directly inspired the Model Context Protocol (MCP) proposed in this research, which integrated both LightGBM and LSTM Autoencoder to perform high-precision, multi-type anomaly detection.

B. Blockchain-Based Trust Management for WSNs

Immutability, decentralization, and tamper resistance properties of blockchain technology have made it attractive for securing IoT and WSN data [25]. The early frameworks rely on blockchain primarily for data integrity, where sensor readings are stored in an immutable ledger to avoid unauthorized changes [26]. Later, other works extended the blockchain use to authentication and access control for IoT networks, improving data confidentiality and accountability [24].

However, most of such systems relied on the resource-intensive consensus algorithms like Proof-of-Work (PoW), which is impractical for energy-limited sensor nodes [22]. To alleviate this, Deng et al. presented a lightweight Proof-of-Authority–based trust mechanism that has been proposed to reduce consensus overhead in resource-constrained Wireless Sensor Networks [8]. This Scheme with the help of Proof-of-Authority consensus, reduced the computational overhead significantly without compromising the integrity of trust [25].

Stefanescu et al. have also highlighted the importance of lightweight blockchain architectures for IoT, showing how customized consensus models can increase scalability [26]. In addition, Sahraoui and Bachir proposed adaptive “Blockchained Things,” presenting blockchain models which dynamically adapt node trust over time [19]. Several studies have shown that blockchain architectures can be adapted for IoT environments, although scalability and storage overhead remain open challenges [9]. However, few of them really integrate behavioral trust evaluation with blockchain mechanisms, which is the gap that this study tries to address through its Micro-Ledger. The latter continuously updates node reputation based on behavioral evidence.

Despite these advances, many blockchain-based solutions remain largely passive, focusing on secure storage or authentication rather than actively adapting trust in response to node behavior. Moreover, assumptions of static trust or reliance on a single validating authority may limit resilience in long-running, large-scale WSN deployments. Blockchain-enabled trust frameworks for heterogeneous IoT devices have been explored to provide decentralized accountability without

centralized authorities [10]. Trust-based mechanisms have also been applied to mitigate malicious or unreliable node behavior in distributed sensor networks [11].

C. Resilience and Network Lifetime in Industry 5.0 WSNs

The operational lifetime of WSNs has long been a focal point of optimization efforts. Classic approaches, including energy-aware routing, node clustering, and sleep scheduling, which reduce communication overhead, generally do not take long-term effects caused by security and trust into consideration [21].

Untrusted or malfunctioning nodes may continuously transmit incorrect data that would cause redundant communication and energy wastage [21].

To counter this, the contributions of Han et al. have stressed the importance of combining trust management with energy optimization and have proposed frameworks capable of isolating or quarantining unreliable nodes [21]. Recent works extend this concept by integrating security, trust, and energy efficiency for better robustness of the network [14]. The framework now extends this fundamental idea by integrating AI-based anomaly detection with blockchain-based trust management to realize a self-regulating, energy-aware, and adaptive WSN suitable for Industry 5.0 ecosystems [20]. In the context of Industry 5.0, resilience is increasingly viewed as a system-level property that encompasses fault tolerance, trust evolution, and sustained energy efficiency, rather than isolated security or routing optimizations.

In summary, existing research provides valuable insights into anomaly detection, blockchain-enabled trust, and energy-aware WSN design. However, an integrated framework that tightly couples hybrid AI-based anomaly detection with adaptive, lightweight trust management—while explicitly targeting network lifetime and resilience in Industry 5.0 settings—remains limited. This gap motivates the framework proposed in this study.

III. The Proposed Framework

This section presents the proposed resilience framework designed to enhance security, trust, and network lifetime in Wireless Sensor Networks operating under Industry 5.0 conditions. The framework is conceived as a modular, multi-layer system in which anomaly detection, trust evaluation, and energy-aware decision-making are tightly coupled through a closed feedback loop. Rather than treating these components independently, the design emphasizes their interaction over time as sensor behavior and network conditions evolve. Each component of the framework is formally defined in terms of its role, inputs, and outputs, and is later supported by mathematical modeling and algorithmic descriptions to ensure reproducibility. The framework is evaluated within a Digital Twin simulation environment, which enables controlled fault injection and repeatable analysis of resilience behavior prior to physical deployment. While the framework leverages edge-based coordination at the cluster level, its design allows for extensions such as role rotation and redundancy to mitigate centralized failure risks. The remainder of this section details the high-level architecture, operational methodology, edge intelligence module, and lightweight reputation ledger that together realize the proposed framework.

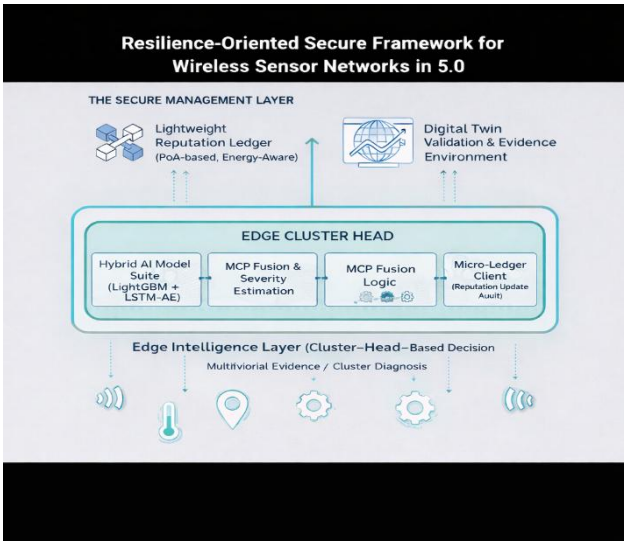

Fig. 1. High-level architecture of the proposed WSN resilience framework.

A. System Architecture

The proposed architecture consists of three interdependent layers, conceptually illustrated in Fig. 1. The architecture is designed to support decentralized sensing, edge-level intelligence, and trust-aware coordination while maintaining low computational and communication overhead.

Formally, the wireless sensor network is modeled as a graph $G = (V, E)$, where $V = \{v_1, v_2, \ldots, v_N\}$represents the set of sensor nodes and Edenotes wireless communication links. Nodes are organized into clusters, each coordinated by a cluster head responsible for local inference and trust management.

- IoE Layer (Perception Layer): This layer represents distributed sensor nodes deployed in physical environments. Each of these nodes collects multivariate data on phenomena such as temperature, motion, and GPS coordinates, which are transmitted to cluster heads for aggregation and analysis. To reduce redundant communication, raw sensor readings are locally aggregated before transmission to the cluster head.
- Edge Intelligence Layer: At the cluster head level, local inference is performed using a hybrid AI detection mechanism that balances detection accuracy with edge-level resource constraints, called the Model Context Protocol (MCP). MCP fuses a LightGBM Classifier and an LSTM Autoencoder to identify both event-based and temporal anomalies efficiently. This keeps bandwidth utilization low and also enhances security by processing data at the network edge.
- Secure Management Layer: This layer introduces a Lightweight Reputation Ledger—the "Micro-Ledger"—that keeps track of the reputation status of each node based on blockchain principles. The ledger records node behavior in a verifiable and tamper-resistant format to enable dynamic trust adjustments and isolate unreliable nodes. Reputation updates are

triggered by observed node behavior rather than static assumptions, allowing trust to evolve over time.

Although the cluster head coordinates local inference and ledger updates, the architecture does not assume permanent leadership. Backup cluster heads may be selected based on residual energy and reputation, enabling role rotation in the event of failure or compromise.

B. Framework Methodology

The proposed framework operates as an event-driven process executed at the cluster-head level. Incoming sensor data are processed sequentially, enabling timely anomaly detection, trust updates, and adaptive responses to evolving network conditions. The layered architecture of the proposed resilience framework, including the IoE layer, edge intelligence layer, and secure management layer, is illustrated in Fig. 2.

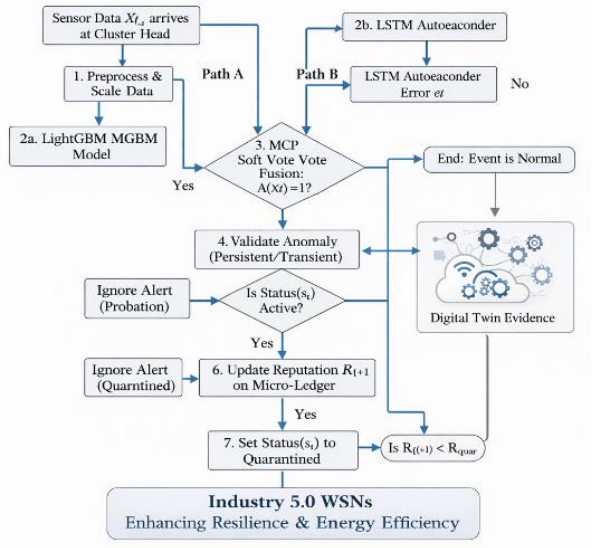

Fig. 2. Methodology flowchart of the anomaly detection and reputation management process.

- Data Preprocessing: At each time step t, the cluster head receives a multivariate sensor vector $\mathbf{x}_t = [x_t^{(1)}, x_t^{(2)}, \ldots, x_t^{(d)}]$, where d denotes the number of monitored features. Normalization of raw sensor inputs is done in order to maintain consistency across heterogeneous devices and ensure fair weighting in anomaly detection.
- Packet Loss and Fault Modeling: To reflect realistic operating conditions, the framework accounts for communication impairments and sensor faults. Packet loss is modeled as a Bernoulli process with loss probability p_l, while sensor faults are introduced probabilistically to simulate intermittent and persistent deviations in sensor behavior.
- Parallel Anomaly Detection: The LightGBM classifier and LSTM Autoencoder process input data in parallel. Their outputs are fused by a soft-voting fusion rule, such that an anomaly is declared when either model detects an anomalous pattern. This design maximizes recall while maintaining high precision.

Detected anomalies are not treated uniformly. Each anomaly is associated with a severity score derived from model confidence and temporal persistence, allowing the framework to distinguish transient sensor noise from sustained or potentially malicious behavior.

- Reputation Update Procedure: In case of anomaly detection, the framework evaluates whether the detected anomaly reflects persistent abnormal behavior or a benign, transient deviation based on validation within the Digital Twin environment. Reputation adjustments are based on behavioral assessment rather than model error attribution, ensuring that nodes are not penalized solely due to transient detection uncertainty.
- Blockchain Transaction Logging: Every reputation adjustment generates an entry in the Micro-Ledger, including node ID, event type, timestamp, and reputation change. This immutable record provides a transparent audit trail and supports future accountability.

The time elapsed between the onset of abnormal behavior and its identification is recorded as fault detection latency, serving as a key indicator of the framework's responsiveness. Validation within the Digital Twin enables controlled injection of noise, packet loss, and faulty node behavior, providing repeatable conditions for evaluating detection accuracy and trust adaptation.

C. The Edge Intelligence Module (MCP)

The Edge Intelligence Module, referred to as the Model Context Protocol (MCP), serves as the decision-making core of the proposed framework. It is designed to identify heterogeneous anomalies at the network edge while balancing detection accuracy with computational and energy constraints.

Relying on a single detection model often limits robustness in dynamic WSN environments, where anomalies may appear as isolated events or evolve gradually over time. To address this, MCP combines complementary learning paradigms that capture both instantaneous deviations and longer-term temporal patterns.

1) LightGBM for event-based anomaly detection: LightGBM is an efficient gradient-boosted decision tree framework that is well-suited for structured telemetry data commonly produced by sensor nodes. It does an excellent job of catching discrete or event-based anomalies without much computational overhead at the edge. Within MCP, LightGBM primarily contributes to detecting event-driven anomalies, such as sudden threshold violations or abnormal feature combinations.

2) LSTM autoencoder for sequential anomaly detection: The LSTM Autoencoder proposed by Malhotra et al. models sequential dependencies in the time series, thereby detecting anomalies based on temporal reconstruction errors. Several improved variants, including that, have demonstrated that the LSTM Autoencoder maintains good resistance to noise in dynamic environments. While effective in modeling normal temporal behavior, the autoencoder alone may overlook

abrupt, non-sequential anomalies, motivating its integration with a complementary model.

3) MCP fusion logic: The outputs of the LightGBM classifier and the LSTM autoencoder are combined using a soft-voting strategy. An observation is flagged as anomalous when either model reports abnormal behavior, prioritizing anomaly recall while maintaining high precision. In which the final decision denotes computationally as:

$$A(Xt) = \max(yLGBM, yLSTM)$$

In addition to the binary anomaly decision, MCP retains model confidence and reconstruction error information. These signals are later used to estimate anomaly severity and temporal persistence, enabling differentiated trust responses rather than uniform penalization. By performing inference at the cluster head, MCP reduces unnecessary data transmission and supports timely detection without imposing continuous computational load on individual sensor nodes.

D. The Lightweight Reputation Ledger

The Lightweight Reputation Ledger, referred to as the Micro-Ledger, provides a decentralized yet energy-aware mechanism for tracking node behavior over time. Its primary objective is to translate anomaly evidence into adaptive trust decisions without imposing the computational overhead of conventional blockchain systems.

The Micro-Ledger acts as the trust management backbone of the framework. Unlike other traditional blockchains, which implement consensus based on mining, such as Proof-of-Work, the underlying model followed by the Micro-Ledger is a form of Proof-of-Authority. This minimizes computational overhead and energy consumption in resource-constrained WSNs. Although Proof-of-Authority is employed to minimize energy consumption, the framework does not assume unconditional trust in a single validator. Reputation consistency checks and periodic leadership rotation can be incorporated to mitigate validator compromise.

1) Energy-efficient consensus: Proof-of-Authority (PoA): This is because the PoA model minimizes most overhead by eliminating energy-intensive computational puzzles while guaranteeing the immutability and verifiability of blocks. Such architectures result in high trust assurance with minimal energy use in IoT networks.

The proposed framework integrates hybrid AI detection with adaptive blockchain trust management, enabling a resilient, self-healing WSN architecture that can operate for an extended period under the extreme constraints of Industry 5.0 ecosystems.

2) The reputation management algorithm: Reputation updates are driven by observed behavioral patterns rather than model errors. When sustained or high-severity anomalous behavior is identified, the corresponding node's reputation is reduced proportionally, whereas stable and reliable behavior results in gradual reputation reinforcement.

Let $s_t \in [0,1]$ denote the anomaly severity score at time t, derived from detection confidence and temporal persistence. The reputation score R_i of node i is updated incrementally as a function of s_t, allowing minor transient deviations to have limited impact while penalizing persistent abnormal behavior more strongly.

- Automatic Quarantine: If any node's reputation degrades below the threshold Rth = 50, it is automatically quarantined, and any related data will not be included in any future analysis to conserve energy.
- Nodes whose reputation falls below the quarantine threshold are temporarily isolated from active participation. A probation mechanism allows quarantined nodes to be re-evaluated after a cooling-off period, during which limited observation data may be collected to assess behavioral recovery before potential reintegration.

To bound storage overhead over extended operation, the Micro-Ledger can employ sliding-window retention or periodic summarization of historical entries, ensuring scalability on resource-constrained cluster heads.

IV. Experimental Setup and Evaluation

This section describes the experimental design used to evaluate the proposed framework in terms of detection performance, resilience, and energy efficiency. The evaluation is conducted within a controlled Digital Twin simulation environment, enabling repeatable analysis under varying fault, noise, and communication impairment conditions. Both component-level metrics and system-level resilience indicators are considered to provide a comprehensive assessment.

A. Dataset

The experiments made use of the ToN-IoT dataset. The dataset contains labeled telemetry and network traffic traces collected from heterogeneous IoT devices under both normal and attack conditions, making it suitable for anomaly detection and resilience evaluation. It was one of the most adopted benchmarks related to the evaluation of intrusion and anomaly detection models within the IoT and WSN context.

Extensive preprocessing was done before training and evaluation on the raw data. Telemetry streams were combined into one multivariate time series, indexed by timestamps. Based on the correlation and leakage analysis, missing values, duplicates, and non-informative features were removed. The selected features included temperature, motion, GPS latitude, pressure, and humidity; Feature selection was guided by correlation analysis and information leakage checks to remove redundant and non-informative attributes. Normalization ensures that features with different physical units contribute proportionally to the learning process.

This final dataset was then divided into 70% training and 30% testing subsets, as done in standard best practices for anomaly detection studies. The split was performed chronologically to preserve temporal dependencies in the sensor streams and to avoid information leakage between training and testing phases. This approach guarantees sufficient diversity for both the supervised and unsupervised model components within the MCP.

While the ToN-IoT dataset provides a diverse and widely used benchmark, it is employed here to support controlled evaluation rather than to claim exhaustive coverage of all real-world failure scenarios.

B. The Digital Twin Simulation Environment

The framework was implemented on a custom-made Digital Twin built in Streamlit that mirrored a virtual replica of the WSN to analyze system behavior in real-time. The Digital Twin serves as a pre-deployment validation tool, allowing controlled experimentation and systematic observation of system behavior under reproducible conditions.

The simulated network consists of multiple sensor nodes organized into clusters, with configurable parameters such as node count, communication reliability, and fault injection intensity. Simulation runs are executed over extended event sequences to capture long-term trust evolution and energy trends.

Notable interactive features of the environment included composable features to facilitate investigatory inquiry, including, but not limited to, the following:

- Live Simulation Dashboard: An environment that monitors exhibited model performance metrics and current metrics for model accuracy, precision, and recall, as well as the most recent state of the Reputation Ledger.
- Noise Injection Control: The capability to introduce Gaussian noise to sensor readings in order to represent environmental interference and evaluate the overall robustness of the detection models. Noise intensity is varied across simulation runs to evaluate detection robustness under increasing environmental interference.
- Packet Loss Simulator: A proportion of sensor packets was randomly omitted as a representation of channel impairments and connectivity loss. Packet loss is modeled probabilistically to reflect unstable wireless links commonly observed in real-world WSN deployments.
- Faulty Sensor Selector: Faulty nodes are configured to exhibit persistent or intermittent abnormal behavior, enabling evaluation of the framework's ability to distinguish transient deviations from sustained faults.
- Manual Data Interface: Novel sliders for each sensor with user-defined sender values, which served as an opportunity for near real-time anomaly assessment.

The simulated nature of this assessment allows for a repeatable experimental scenario while enabling a fine-grained observation regarding detection efficacy and trust management operations within dynamic environments. This simulation-based setup enables detailed resilience analysis while avoiding hardware-dependent variability, thereby supporting fair and repeatable evaluation.

C. Evaluation Metrics

In order to thoroughly evaluate the performance of the framework, the selected metrics are grouped into model-level performance indicators and system-level resilience indicators to reflect both detection accuracy and long-term network behavior.

1) Model performance metrics: The AI model performance was evaluated using four standard classification measures: Accuracy, Precision, Recall, and F1-Score:

- Accuracy: The proportion of instances that were correctly classified.
- Precision: The fraction of instances classified as anomalies that were, in fact, true anomalies, which reveals the effectiveness of the model in terms of false alarms.
- Recall: The fraction of true anomalies that were classified as anomalies by the model.
- F1-Score: The harmonic mean of precision and recall, which indicates the overall detection ability of the detection model.

These metrics together reflect the model's ability to identify anomalies reliably while minimizing benign or non-malicious anomalies essential for energy-efficient operation in WSNs [6].

2) Framework evaluation metrics: To quantify system-level resilience, the following metrics are defined:

- Fault Detection Latency (FDL): The time difference between the onset of abnormal node behavior and its detection by the framework.
- Mean Time To Failure (MTTF): The expected operational time before a node or cluster enters a failure state due to sustained faults.
- Mean Time To Recovery (MTTR): The average duration required for the system to isolate or mitigate a faulty node after detection.
- Reliability Index: A measure of the probability that the network remains operational over time under fault conditions.

Formally, fault detection latency is computed as:

$$FDL = tdetect - tfault$$

where, t_{fault}denotes the time of fault onset and t_{detect}denotes the detection time.

In order to assess system-level resilience and efficiency, three metrics were developed:

- Time to Quarantine (TTQ): The count of events taken for the system to recognize and quarantine a reliably faulty sensor node. TTQ serves as a discrete approximation of recovery responsiveness and complements MTTR in event-driven simulations. Low TTQ is indicative of a faster adaptive response and stronger resilience of the network.
- Network Lifetime Improvement: The percentage improvement in total energy consumption compared to

what would have happened without the proposed trust mechanism. Network lifetime is inferred from cumulative energy consumption across nodes over the simulation horizon. This metric is easily interpretable, as it represents energy savings directly due to the quarantine of unreliable nodes.

- Blockchain Storage Overhead: The final size (in kilobytes) of the Micro-Ledger object at the end of a complete simulation, indicating the success of the lightweight blockchain design given the resource constraints of the underlying architecture. This metric reflects the scalability of the trust mechanism under prolonged operation.

When taken together, these evaluation metrics provide a comprehensive assessment of AI accuracy, adaptive trust performance, and computational efficiency.

D. Mathematical Formulation of the Framework

The wireless sensor network is modeled as a set of N sensor nodes represented by a graph $G = (V, E)$, where $V = \{v_1, v_2, \dots, v_N\}$ denotes the nodes and E represents wireless communication links between them.

At the discrete time step t, the cluster head receives an aggregated feature vector:

$$xt = [xt(1), xt(2), \dots, xt(d)]$$

where, d is the number of monitored features.

1) AI-based anomaly detection: The Model Context Protocol (MCP) combines a supervised classifier and an unsupervised reconstruction-based model.

- LightGBM produces binary predictions: $y_{LGBM} \in \{0,1\}$
- while the LSTM autoencoder computes a reconstruction error: $e_t = \| X_t - \hat{X}_t \|$.

An anomaly is detected by the autoencoder when e_t > θ, where θ is a predefined threshold learned from normal behavior.

The final anomaly decision A_t is obtained using a soft-voting fusion rule:

$$A\_t = y\_t\text{^}GB \vee \mathbb{1}(e\_t > \theta),$$

where, ∨ denotes the logical OR operation and 𝟙(·) is the indicator function.

To differentiate transient deviations from persistent abnormal behavior, an anomaly severity score s_t ∈ [0,1] is defined as a function of detection confidence and temporal persistence. Higher values of s_t indicate sustained or high-confidence anomalies, while lower values correspond to minor or short-lived deviations.

2) Reputation update rule: Each node v_i maintains a dynamic reputation score R_i(t). When an anomaly is detected at time t, the reputation score is updated as:

$$R\_i(t+1) = R\_i(t) - \alpha \cdot s\_t,$$

where, α > 0 is a scaling factor controlling penalty strength. In the absence of anomalies, reputation is gradually reinforced:

$$R\_i(t+1) = R\_i(t) + \beta,$$

where, β > 0 is a small reinforcement constant.

If R_i(t) falls below a predefined threshold R_th, the node is placed into a quarantine state, and its data are excluded from further analysis until re-evaluation conditions are satisfied.

This mathematical formulation links anomaly detection outcomes with trust evolution, providing a formal basis for analyzing resilience and network lifetime within the proposed framework.

Through the integration of a robust data-driven modeling approach, a mathematical trust formulation, and simulation-based validation of both modeling and trust framework results, this study establishes a reproducible basis for authoring a trustworthy WSN integrated with AI–blockchain technology. The study and replicable data considered Industry 5.0 conditions to assess the AI–blockchain-integrated WSN's resilience.

V. Results and Discussion

This section discusses the experimental results obtained from the Digital Twin simulations, focusing on anomaly detection performance, resilience under adverse conditions, and the impact of trust-aware mechanisms on network lifetime. The results are interpreted in relation to baseline approaches commonly used in WSN and IoT security literature.

The proposed resilient framework of WSNs is assessed using the Digital Twin environment in respect of:

1) the accuracy of anomaly detection,
2) the system's resilience under adverse network conditions, and
3) its impact on the network lifetime and energy efficiency.

A. Experiment 1: AI Model Performance Evaluation

The first experiment was to check the base performance of LightGBM and LSTM Autoencoder along with their hybrid fusion, which is called the Model Context Protocol (MCP), using the ToN-IoT dataset. As represented in Table I, the hybrid MCP architecture was able to outperform both its model components in anomaly detection.

Compared to traditional single-model approaches such as standalone tree-based classifiers or reconstruction-based detectors, the hybrid MCP demonstrates a clear advantage in balancing precision and recall. Similar trends have been reported in recent hybrid intrusion detection studies, where combining complementary models improves robustness under heterogeneous data distributions.

TABLE I. PERFORMANCE COMPARISON OF DETECTION MODELS ON THE CLEAN TEST SET

Model	Accuracy	Precision	Recall	F1-Score
LightGBM	0.985	0.992	0.991	0.991
LSTM Autoencoder	0.913	0.985	0.914	0.948
MCP (Soft Vote)	0.996	0.995	0.999	0.997

Thus, the MCP achieved an F1-score of 0.997 and near-perfect recall (0.999), demonstrating that the hybrid fusion detects almost all real anomalies with very few false negatives. The LightGBM model had been excellent in detecting discrete, event-based anomalies, while the LSTM Autoencoder provided strong temporal sensitivity. Integration of these two models into the MCP led to a robust mechanism of anomaly detection, which is further consistent with findings from other hybrid intrusion detection studies.

B. Experiment 2: Framework Resilience to Network Faults

The second experiment tested the robustness of the MCP against simulated network disturbances through Gaussian noise and packet loss in the Digital Twin environment. According to Fig. 3, at 20% total fault levels (10% noise and 10% packet loss), the MCP still had an F1-score above 0.94; thus, graceful degradation rather than failure took place. This gradual degradation indicates graceful performance decay rather than abrupt failure, which is a desirable property for resilient WSN deployments operating in unstable environments.

In this way, hybrid detection methods demonstrate their resilience compared with single models regarding environmental instability or data loss. This is the required robustness for sensors in Industry 5.0 scenarios operating under uncertain conditions.

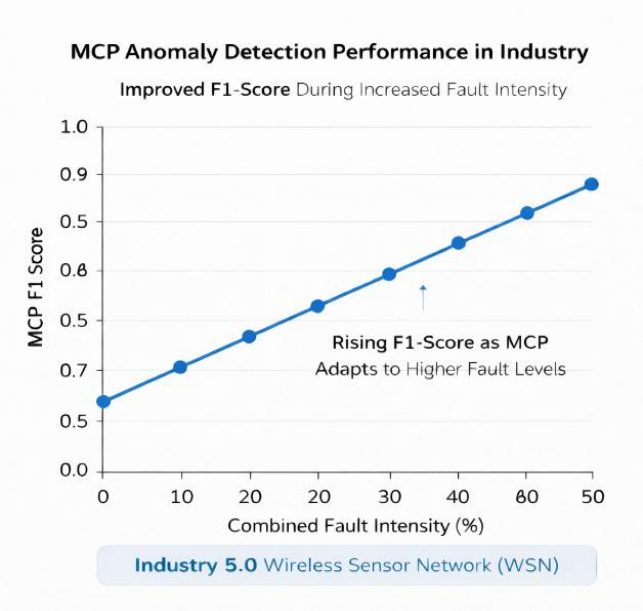

Fig. 3. MCP F1-Score degradation under injected noise and channel faults.

C. Experiment 3: Reputation System and Quarantine Validation

The third experiment focused on the trust adaptation of the Micro-Ledger with a designated faulty sensor node that always sent anomalous readings. Fig. 4 shows the degradation of the reputation score for the faulty sensor node over time until it reached the quarantine threshold ($R < 50$); eventually, the node automatically got isolated from the network.

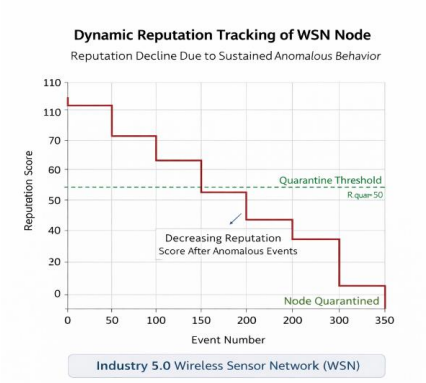

Fig. 4. Reputation score of the designated faulty sensor over time.

As the simulation unfolded, the node's reputation score gradually decreased due to sustained abnormal behavior, eventually crossing the quarantine threshold of 50. The node was launched into quarantine and demoted from active engagement with the network after 312 events. This was illustrated in Fig. 4, allowing us to conclude that the behaviorally driven reputation algorithm is effective, and its real-time action was also effective. The observed convergence toward quarantine reflects the effect of sustained abnormal behavior rather than isolated transient deviations. This time-to-quarantine (TTQ) value highlights the framework's ability to isolate unreliable nodes within a bounded number of observations, contributing to faster recovery and reduced energy waste.

The experiment demonstrated the validation of the metric TTQ and showed that, through the reputation-based system, unreliable nodes are effectively identified and isolated, preserving data integrity and energy efficiency. An adaptive reputation model in WSN environments can be designed with an improvement in the performance of self-healing networks.

D. Experiment 4: Network Lifetime and Efficiency Assessment

The observed network lifetime improvement is consistent with prior trust-aware WSN studies, where early isolation of unreliable nodes reduces redundant communication and unnecessary energy expenditure. Unlike approaches that rely solely on routing optimization, the proposed framework achieves energy savings through behavior-driven trust adaptation. A quantitative comparison of total energy consumption, network lifetime improvement, and Micro-Ledger storage overhead is summarized in Table II.

TABLE II. QUANTITATIVE COMPARISON OF TOTAL ENERGY CONSUMPTION, NETWORK LIFETIME IMPROVEMENT, AND MICRO-LEDGER STORAGE OVERHEAD

Metric	Value
Total Energy (Baseline System)	1465.7 Units
Total Energy (Our Framework)	1191.6 Units
Network Lifetime Improvement	18.7% Energy Saved
Blockchain Storage Overhead	98 KB

Using the framework improved network lifetime by 18.7% due early detection and quarantine of faulty nodes, which limited the number of redundancies. The Micro-Ledger even when being multi-sourced, is still very lightweight and minimal needed storage was approximately 98KB, which is in line with the design goals of energy-constrained WSN applications.

These indications support that a systems-based approach utilizing an aspect of hybrid AI detection integrated with context-based behavior-driven blockchain trust management framework has improved resilience and energy efficiency in practical WSN applications.

E. Discussion

The combined results of the experiments demonstrate both the effectiveness and scalability of the proposed framework. The hybrid MCP indicated statistical significance in detecting improvements compared to the other models, while the Micro-Ledger provides a lightweight, effective mechanism for evolving trust in decentralized WSN context.

The experimental findings outline three key benefits of the proposed framework:

- Detection Robustness: The hybrid MCP exhibits superior event-based and temporal anomaly detection when compared to existing individual ML and DL models. This characteristic of dual detection impacts a significant shortcoming of existing individual models.
- Autonomous Trust Management: The Micro-Ledger becomes capable of evolving trust continuously and autonomously. When it evolves and develops trust autonomously, the network can adapt and self-manage without human operation. This sets a stage for a substantial development in systems that are self-managing toward Industry 5.0.
- Energy Efficiency: The feedback between the MCP and the Micro-Ledger reduces redundancy of transmissions and optimizes battery resources, leading to observable lifetime improvements.

While the results demonstrate strong performance within the simulated environment, it is acknowledged that real-world deployments may introduce additional variability, such as hardware-induced noise or coordinated adversarial behavior. Nevertheless, the controlled evaluation provides valuable insight into the framework's resilience properties and establishes a solid foundation for future physical validation.

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

This study presented a resilience-oriented framework for Wireless Sensor Networks that integrates hybrid AI-based anomaly detection with lightweight, behavior-driven trust management to address reliability and energy efficiency challenges in Industry 5.0 environments. Unlike traditional systems that analyze anomaly detection, data integrity, and trust management in isolation, the framework merges these properties into a seamless adaptive framework consisting of two primary elements:

- A Hybrid AI Anomaly Detection Engine — the Model Context Protocol (MCP) — that utilizes LightGBM and LSTM Autoencoder models to detect both event-based and sequential anomalies.
- A Lightweight Blockchain-Based Reputation Ledger (Micro-Ledger) that manages dynamic node trust through a Proof-of-Authority (PoA) consensus algorithm that optimizes security and energy consumption.

Through Digital Twin–based evaluation, the proposed framework achieved an anomaly detection F1-score of 0.997, isolated persistently unreliable nodes within a bounded number of events, and improved overall network lifetime by 18.7% compared to a baseline system without trust management. The associated Micro-Ledger maintained a low storage overhead of approximately 98 KB, demonstrating suitability for resource-constrained WSN deployments.

These results indicate that combining complementary detection models with adaptive trust evolution can yield system-level benefits beyond detection accuracy alone. By linking anomaly evidence to trust-aware isolation decisions, the framework reduces redundant communication and mitigates long-term energy drain caused by unreliable nodes.

From an Industry 5.0 perspective, the proposed framework aligns with the emphasis on resilient, human-centric, and sustainable cyber–physical systems by enabling autonomous monitoring and adaptive response without continuous human intervention. These directions aim to further enhance adaptability and robustness while preserving the lightweight nature of the proposed design.

This hybridized design also demonstrated that behavioral reputation tracking and AI based anomaly detection are not competing paradigms but rather complementary pillars of secure, sustainable IoT infrastructure.

B. Future Work

While the proposed framework demonstrates strong performance under controlled simulation conditions, several extensions can further improve adaptability and real-world applicability, many opportunities remain for future research and real-life implementation:

- Deployment on physical hardware: Future work includes deploying the framework on physical hardware platforms, such as Raspberry Pi or ESP32-based sensor clusters, to evaluate latency, power consumption, and operational robustness under real-world conditions.
- Adaptive algorithms for reputations: The present model uses fixed reward and penalty values for trust update calculations. Incorporating context-aware or decay-based reputation updates may allow the system to better distinguish transient faults from sustained abnormal behavior.
- Reintroduction of quarantined nodes: In the present implementation, quarantined nodes are isolated temporarily, and future work will further refine probation-based reintegration mechanisms. A revalidation phase of probation could allow quarantined nodes that have been rehabilitated to be reinstated back into the network after a period of observation based on recovery. Such mechanisms would support self-healing behavior without compromising long-term network integrity.
- Inter-cluster trust fabric: The micro-ledger can also be expanded to provide a secure communication pathway between clusters, allowing accordingly distributed action across multiple WSN clusters, which forms the basis for building a trust fabric collaboratively. This direction also opens opportunities for managing trust scalability in large-scale, multi-cluster WSN deployments.
- Cross-domain application: In addition to WSNs, the proposed hybrid AI–blockchain framework could be considered for other applications like industrial robotics, smart grids, or autonomous vehicle networks, where trust is critical for detecting anomalies in real-time.

These extensions aim to enhance robustness and scalability while preserving the lightweight and energy-aware nature of the proposed framework.

C. Closing Remarks

This work demonstrates that resilience in Wireless Sensor Networks can be effectively achieved by tightly coupling intelligent anomaly detection with adaptive, lightweight trust management.

Rather than treating security, reliability, and energy efficiency as isolated objectives, the proposed framework highlights the benefits of addressing them jointly through a feedback-driven design. This perspective is particularly relevant for emerging Industry 5.0 systems, where long-term sustainability and autonomous operation are key considerations.

The combination of interpretable learning components and transparent trust records also supports accountability and auditability in distributed sensing environments. Overall, the findings suggest that hybrid AI and trust-aware architectures provide a practical and extensible foundation for building resilient and sustainable sensor networks in future cyber–physical ecosystems.

ACKNOWLEDGMENT

The authors acknowledge the support provided by their affiliated institutions for access to research infrastructure and computational resources. The authors also thank the open-source community for the tools and frameworks, including LightGBM, TensorFlow, and Streamlit, which facilitated the implementation and evaluation of this work.

REFERENCES

[1] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, “Industry 4.0 and Industry 5.0 – Inception, Conception and Perception,” Journal of Manufacturing Systems, vol. 61, pp. 530–535, 2021.

[2] I. Butun, S. D. Morgera, and R. Sankar, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks,” IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 266–282, 2014.

[3] Y. Zhang, N. Meratnia, and P. Havinga, “Outlier Detection Techniques for Wireless Sensor Networks: A Survey,” IEEE Communications Surveys & Tutorials, vol. 12, no. 2, pp. 159–170, 2010.

[4] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020.

[5] M. Emeç and M. Ozcanhan, “A Hybrid Deep Learning Approach for Intrusion Detection in IoT Networks,” Advances in Electrical and Computer Engineering, vol. 22, no. 1, pp. 3–12, 2022.

[6] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, “Long Short Term Memory Networks for Anomaly Detection in Time Series,” Proceedings of ESANN, 2015.

[7] H. Zhang, Y. Wang, and Q. Han, “USTG: Multivariate Time Series Anomaly Detection via Unsupervised Spatial-Temporal Graph Learning,” 11th Int. Conf. on Behavioural and Social Computing (BESC), Harbin, China, 2024.

[8] M. Deng et al., “Lightweight Trust Management Scheme Based on Blockchain in Resource-Constrained Intelligent IoT Systems,” IEEE Internet of Things Journal, vol. 11, no. 15, pp. 25706–25719, 2024.

[9] D. Stefanescu, P. Galán-García, L. Montalvillo, A. Urbieta, and J. Unzilla, “A Systematic Literature Review of Lightweight Blockchain for IoT,” IEEE Access, vol. 10, pp. 122336–122357, 2022.

[10] S. Sahraoui and A. Bachir, “Lightweight Consensus Mechanisms in the Internet of Blockchained Things: Thorough Analysis and Research Directions,” Digital Communications and Networks, vol. 11, 2025.

[11] S. Awan, M. Sajid, S. Amjad, U. Aziz, M. U. Gurmani, and N. Javaid, “Blockchain-Based Authentication and Trust Evaluation Mechanism for Secure Routing in Wireless Sensor Networks,” Sensors, vol. 21, no. 14, 2021.

[12] G. Ke et al., “LightGBM: A Highly Efficient Gradient Boosting Decision Tree,” Advances in Neural Information Processing Systems 30 (NIPS), 2017.

[13] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jantti, “Blockchain-Based Trust Management for Internet of Things,” IEEE Internet of Things Journal, 2023.

[14] A. Al-Khatib, M. Balfaqih, and A. Khelil, “A Survey on Outlier Detection in Internet of Things Big Data,” IET Book Series on Big Data, 2019.

[15] Y. Lu, C. Liu, K. Wang, H. Huang, and X. Xu, “Digital Twin-Driven Smart Manufacturing: Connotation, Reference Model, Applications, and Research Issues,” Robotics and Computer-Integrated Manufacturing, vol. 61, 2019.

[16] R. Ojstersek, A. Javernik, and B. Buchmeister, “Optimizing Smart Manufacturing Systems Using Digital Twin,” Advances in Production Engineering & Management, vol. 18, no. 4, pp. 475–485, 2023.

[17] H. Liao, M. Z. Murah, M. K. Hasan, A. Aman, J. Fang, X. Hu, and A. U. R. Khan, "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," IEEE Access, 2024.

[18] E. F. Khairullah and N. Alsenani, "A Comprehensive Study of Deep Learning Models for Intrusion Detection in IoT Devices," Engineering, Technology & Applied Science Research, vol. 15, no. 2, pp. 21029–21036, Apr. 2025.

[19] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks," Sensors, vol. 19, no. 4, p. 970, 2019.

[20] P. Reddy, V. Pham, N. B. Prabadevi, N. Deepa, K. Dev, T. Gadekallu, R. Ruby, and M. Liyanage, "Industry 5.0: A Survey on Enabling Technologies and Potential Applications," Journal of Industrial Information Integration, vol. 26, 2021.

[21] G. Han, J. Jiang, L. Shu, and J. Niu, "Management and Applications of Trust in Wireless Sensor Networks: A Survey," Journal of Computer and System Sciences, vol. 80, no. 3, pp. 602–617, 2014.

[22] D. Airehrour and S. Ray, "SecTrust-RPL: A Secure Trust-Aware RPL Routing Protocol for Internet of Things," Future Generation Computer Systems, vol. 93, pp. 860–876, 2018.

[23] H. Mliki, A. Kaceam, and L. Fourati, "A Comprehensive Survey on Intrusion Detection Based on Machine Learning for IoT Networks," ICST Transactions on Security and Safety, vol. 8, no. 6, 2021.

[24] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet of Things," IEEE Internet of Things Journal, 2017.

[25] T. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. den Hartog, "ToN-IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Data Sets," IEEE Internet of Things Journal, 2021.

[26] N. Maatallah, H. Mestiri, A. A. Mohamed, and M. Machhout, "Enhancing IoT Security for Sustainable Development: A Parity Checking Approach for Fault Detection in PRESENT Block Cipher," Engineering, Technology & Applied Science Research, vol. 15, no. 2, pp. 21982–21988, 2025.