A Framework for Metrological Assurance and Standardization of IoT Sensors to Mitigate Cybersecurity Risks

Akmaljon Mamatov[1], Khusniddin Sotvoldiev[1], Umidjon Rustamov[1], Anvarjon Boymirzaev[1], Jamshidbek Obidov[1], Kakhramon Ergashov[1], Elmurod Alikhonov[1], Abdukakhor Topvoldiev[1], Ibrokhimjon Khasanov[1] and Tayr Moydunov[2]

[1]*Department of Metrology and Standardization, Fergana State Technical University, Fergana Str. 86, 150100 Fergana, Uzbekistan*

[2]*Osh Technological University, Nasirdin Isanov Str. 81, 723503 Osh, Kyrgyzstan*

akmaljon9790011@gmail.com, sotvoldiyevxusniddin82@gmail.com, rustamov-83@inbox.ru, anvarjon.ferpi@gmail.com, jamshidobidov19@gmail.com, muxammadboras@gmail.com, saroylik0112@gmail.com, topvoldiyevabduqaxor95@gmail.com, ibroximjon.xasanov@fstu.uz, tayr.moydunov@mail.ru

Keywords: Internet of Things, Cybersecurity, Metrology, Standardization, Risk Management.

Abstract: The rapid expansion of the Internet of Things (IoT) has introduced critical vulnerabilities at the sensor layer, as conventional cybersecurity measures often fail to address data integrity at its source, creating significant risks in modern cyber-physical systems. This research addresses the urgent need for a verifiable method to ensure the trustworthiness of sensor data. The primary aim of this paper is to propose and validate a novel framework for the metrological assurance of IoT sensors, designed to mitigate cybersecurity risks by treating data manipulations as quantifiable measurement anomalies. The proposed framework integrates two foundational technologies: Digital Calibration Certificates (DCC) to establish a trusted metrological baseline and Distributed Ledger Technology (DLT) to ensure its immutable traceability. A mathematical model is developed to formalize attack vectors and introduce the Dynamic Trust Corridor (DTC) criterion for real-time verification. The core result is the development of the Metrological Trust Index (MTI), a continuous metric for data trustworthiness. Through numerical simulation of an industrial sensor, the framework demonstrated a 98.7% detection rate for bias injection attacks and a 94.1% rate for subtle drift manipulation attacks, significantly outperforming traditional methods. Theoretically, this work establishes a new paradigm for IoT security rooted in the principles of measurement science. Practically, the framework provides a concrete, auditable pathway for manufacturers and operators to comply with emerging regulatory standards such as the EU Cyber Resilience Act (CRA), enhancing the overall resilience of critical IoT ecosystems.

1 INTRODUCTION

1.1 The Crisis of Trust in IoT Ecosystems

The Internet of Things (IoT) has evolved into a ubiquitous technological backbone, interconnecting billions of devices that form the sensory layer of modern cyber-physical systems (CPS). From smart grids and industrial automation to autonomous vehicles and connected healthcare, these systems depend on a continuous stream of data to monitor, control, and optimize physical processes. At the heart of this ecosystem lies the sensor, which acts as the crucial interface between the physical and digital worlds. Consequently, the integrity of the entire system hinges on the trustworthiness of the data these sensors produce. However, this foundational layer is increasingly targeted by sophisticated cyber-attacks, including data spoofing, bias injection, and replay attacks, which can corrupt data at its source and lead to catastrophic system failures, financial losses, or even threats to human safety. These risks are consistent with recent studies on IoT sensor-layer security, cyber-risk management, secure IoT implementation, vulnerability modeling, and holistic cyber-risk assessment [1]-[5].

While indispensable, conventional cybersecurity frameworks and standards, such as the NIST Cybersecurity Framework or the ISO/IEC 27001 series, primarily focus on securing IT infrastructure,

network communications, and data access control. They employ robust mechanisms like encryption and authentication to protect data in transit and at rest. However, these frameworks often overlook a fundamental vulnerability: the integrity of the physical-layer data itself. They implicitly trust that the data generated by the sensor is authentic prior to its transmission. This gap means that an adversary who can compromise the sensor or manipulate its local environment can generate false-yet-perfectly-encrypted data, rendering traditional security measures ineffective.

1.2 A New Paradigm: Cybersecurity through Metrology

To address this critical gap, this paper proposes a paradigm shift: leveraging the principles of metrology as a direct tool for cybersecurity. Metrology, the science of measurement, provides a formal basis for understanding a sensor's performance, including its uncertainty, stability, and drift over time. We argue that this metrological fingerprint can be used to validate the trustworthiness of sensor data in real-time. The central thesis of our work is that: an unauthorized modification of a sensor's data stream constitutes a detectable deviation from its calibrated metrological behavior. By continuously verifying data against a trusted metrological baseline, it becomes possible to identify anomalies that are indicative of a cyber-attack.

1.3 Contribution and Paper Structure

The primary contribution of this work is the development of a comprehensive, quantitative framework for metrological assurance that formalizes this paradigm. Specifically, this paper:

1) Establishes an architecture that uses Digital Calibration Certificates (DCC) and Distributed Ledger Technology (DLT) to create an immutable and auditable record of a sensor's metrological identity.
2) Develops a mathematical model that formalizes cyber-attacks as specific types of metrological anomalies.
3) Introduces a quantitative metric, the Metrological Trust Index (MTI), for the real-time detection of these anomalies.
4) Validates the framework's effectiveness through simulation, demonstrating its superior performance compared to conventional methods.

The remainder of this paper is organized as follows: Section 2 reviews the foundational technologies. Section 3 details the mathematical modeling of the framework. Section 4 presents the system architecture and implementation algorithm. Section 5 describes the experimental validation. Finally, Section 6 provides concluding remarks and outlines future research directions.

2 FOUNDATIONAL TECHNOLOGIES FOR TRUSTED DATA

The proposed framework is built upon two cornerstone technologies that, when combined, create a robust foundation for trusted sensor data: Digital Calibration Certificates (DCC) to establish a verifiable metrological baseline, and Distributed Ledger Technology (DLT) to ensure the integrity and accessibility of that baseline.

2.1 The Digital Calibration Certificate (DCC) as a Trust Anchor

A Digital Calibration Certificate is a machine-readable, cryptographically secured document that contains all relevant information about a sensor's calibration and metrological characteristics. The reliability of the calibration laboratory and traceability process is aligned with ISO/IEC 17025 requirements [6]. Unlike traditional paper-based or PDF certificates, a DCC is designed for automated processing and integration into digital workflows. As conceptualized in recent metrological research, the DCC acts as a "metrological passport" for a sensor, providing a standardized format for its identity and performance properties. Similar approaches to securing metrological chains, digital metrology for IoT, and sensor-network metrology have been discussed in previous studies [7]-[9].

For the purpose of cybersecurity, a DCC must contain specific fields that allow for the dynamic assessment of data integrity. We propose a structure that includes not only standard calibration data but also parameters essential for modeling the sensor's behavior over time. A cryptographic signature from a trusted calibration laboratory ensures the authenticity and integrity of the certificate, making it a reliable "trust anchor" for all subsequent measurements. The key fields of such a security-oriented DCC are outlined in Table 1.

Table 1: Key fields of the proposed DCC for cybersecurity applications.

Field Name	Data Type	Description
Sensor_ID	String (UUID)	A unique, immutable identifier for the physical sensor device.
Calibration_Date	ISO 8601	The timestamp of the last valid calibration event.
Issuing_Lab_ID	String	Identifier of the accredited laboratory that performed the calibration.
Measurement_Range	Float	The lower and upper limits of the sensor's operational range.
Uncertainty_Budget	Float	The combined standard uncertainty (u_c) at the time of calibration, as per GUM.
Drift_Coefficient	Float	The expected temporal drift rate (λ) of the sensor's output over time.
Coverage_Factor	Float	The coverage factor (k) used to calculate the expanded uncertainty.
DCC_Signature	String (Hex)	A digital signature (e.g., ECDSA) from the issuing lab to ensure authenticity.
Previous_DCC_Hash	String (Hex)	The cryptographic hash of the previous DCC, creating a verifiable chain.

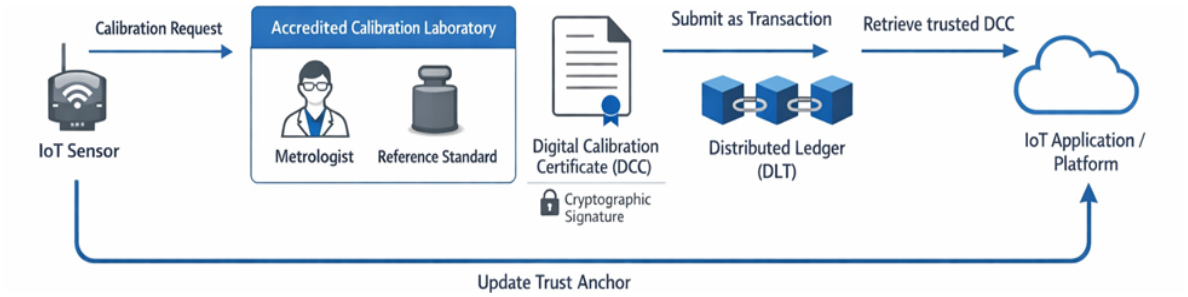

Figure 1: Conceptual architecture of the Digital Calibration Certificate (DCC) lifecycle on a distributed ledger.

2.2 Distributed Ledger Technology (DLT) for Immutable Traceability

While a DCC provides a trusted snapshot of a sensor's state, its value is diminished if the certificate itself can be lost, altered, or substituted. To mitigate this risk, our framework utilizes Distributed Ledger Technology (DLT), such as a blockchain, as a secure repository for storing and managing DCCs.

The inherent properties of DLT—decentralization, cryptographic security, and immutability—make it an ideal solution for maintaining a tamper-proof audit trail of a sensor's entire metrological history. As illustrated in Figure 1, the DCC lifecycle begins with sensor calibration at an accredited laboratory, where a digitally signed certificate is generated. The certificate is then submitted to the distributed ledger as a transaction, validated by the network, and permanently recorded in a new block linked to previous records. IoT applications can subsequently query the ledger to retrieve the latest trusted DCC, enabling real-time verification of sensor calibration status and ensuring complete traceability throughout the sensor lifecycle. Each time a sensor is recalibrated, a new DCC is issued and cryptographically linked to the previous certificate through the Previous_DCC_Hash field, creating an uninterrupted chain of metrological traceability.

3 MATHEMATICAL MODELING OF METROLOGICAL INTEGRITY

This section presents the mathematical core of the framework, translating the conceptual model into a formal, quantitative methodology for anomaly detection. We establish a baseline model for a sensor's behavior, formalize attack vectors as quantifiable deviations, and introduce a real-time index for measuring data trustworthiness.

3.1 Baseline Metrological Model

According to the principles established in the Guide to the Expression of Uncertainty in Measurement (GUM) [10]. Based on the data retrieved from the Digital Calibration Certificate (DCC), the measurement Y at time t for a physical quantity X is modeled as:

$$Y(t) = X(t) + \delta_{sys} + \epsilon_{rand}(t) + \delta_{drift}(t). \quad (1)$$

where δ_{sys} is the systematic error corrected during calibration, $\epsilon_{rand}(t)$ is the random noise modeled as a Gaussian process $\mathcal{N}(0,\sigma^2)$, and $\delta_{drift}(t)$ represents the temporal instability of the sensor. The drift is modeled linearly as:

$$\delta_{\text{drift}}(t) = \lambda \cdot (t - t_{\text{calib}}), \quad (2)$$

where λ is the drift coefficient and t_{calib} is the timestamp of the last calibration. The combined standard uncertainty u_c at the time of calibration is calculated as the root-sum-square of Type A and Type B components:

$$u_c = \sqrt{u_A^2 + u_B^2}\,. \quad (3)$$

The expanded uncertainty U, which defines the initial confidence interval, is given by:

$$U = k \cdot u_c, \quad (4)$$

where k ισ the coverage factor (typically $k = 2$ for a 95% confidence level).

3.2 Formalization of Metrological Attack Vectors

We categorize cyber-attacks by their mathematical impact on the measurement equation. This allows the framework to detect various attack types through a unified metrological lens:

- Bias Injection Attack: An adversary introduces a malicious offset B:

$$Y_{\text{attack}}(t) = Y(t) + B. \quad (5)$$

- Scaling Attack (Spoofing): The output is scaled by a malicious factor S:

$$Y_{\text{attack}}(t) = Y(t) \cdot (1 + S) \quad (6)$$

- Drift Manipulation Attack: The attacker introduces a false drift λ_{atk} to mimic natural aging but at a different rate:

$$Y_{\text{attack}}(t) = Y(t) + \lambda_{atk} \cdot (t - t_{\text{attack}}). \quad (7)$$

- Data Replay Attack: The current measurement is replaced by a previous trusted value $Y(t - \Delta t)$:

$$Y_{\text{attack}}(t) = Y(t - \Delta t). \quad (8)$$

3.3 The Dynamic Trust Corridor (DTC) Criterion

The core detection mechanism is the Dynamic Trust Corridor (DTC). Unlike static thresholds, the DTC accounts for the increasing uncertainty over time. First, we define the predicted measurement Y_{pred} at time t based on the last trusted state:

$$Y_{\text{pred}}(t) = Y_{\text{last}} + \lambda \cdot (t - t_{\text{last}}). \quad (9)$$

As time elapses since calibration, the uncertainty regarding the sensor's state increases. The uncertainty due to drift u_λ is modeled assuming a uniform distribution:

$$u_\lambda(t) = \frac{\lambda \cdot (t - t_{\text{calib}})}{\sqrt{3}}\,. \quad (10)$$

The dynamic standard uncertainty $u_{dyn}(t)$ and the resulting expanded uncertainty $U_{dyn}(t)$ are:

$$u_{\text{dyn}}(t) = \sqrt{u_c^2 + u_\lambda(t)^2} \quad (11)$$

$$U_{\text{dyn}}(t) = k \cdot u_{\text{dyn}}(t)\,. \quad (12)$$

The DTC is defined by its Lower Boundary (LB) and Upper Boundary (UB):

$$LB(t) = Y_{\text{pred}}(t) - U_{\text{dyn}}(t). \quad (13)$$

$$UB(t) = Y_{\text{pred}}(t) + U_{\text{dyn}}(t). \quad (14)$$

A measurement $Y_{meas}(t)$ is flagged as an anomaly if it breaches these boundaries:

$$\text{Anomaly} = \begin{cases} 1 & \text{ιφ } Y_{\text{meas}}(t) \notin [LB(t), UB(t)] \\ 0 & \text{οτηερωισε}\,. \end{cases} \quad (15)$$

Figure 2 illustrates the Dynamic Trust Corridor (DTC) for a simulated temperature sensor. The shaded region represents the permissible measurement interval bounded by the lower and upper limits, LB(t) and UB(t) (Eqs. 13–14), which gradually widens over time to account for sensor drift. Under normal operating conditions, the sensor measurements remain within the corridor, whereas measurements that exceed these limits are classified as metrological anomalies, indicating possible sensor malfunction or cyber-intervention. The simulation was performed using $\lambda = 0.05$ units/month, $u_c = 0.1$, and a coverage factor $k = 2$ (95% confidence level).

3.4 The Metrological Trust Index (MTI)

To provide a continuous assessment of data integrity, we introduce the Metrological Trust Index (MTI). We define the normalized deviation $\xi(t)$ as:

$$\xi(t) = \frac{|Y_{\text{meas}}(t) - Y_{\text{pred}}(t)|}{U_{\text{dyn}}(t)}\,. \quad (16)$$

The MTI is then calculated as:

$$MTI(t) = \max(0, 1 - \xi(t)). \quad (17)$$

Figure 3 demonstrates the response of the proposed Metrological Trust Index (MTI) to a simulated bias injection attack initiated four months after calibration. The upper plot shows the deviation of the measured sensor signal from the predicted

reference response, while the lower plot illustrates the corresponding MTI values. Before the attack, the MTI remains close to 1, indicating complete confidence in the measurement. Immediately after the attack, the index drops to 0, reflecting that the measurement exceeds the allowable uncertainty limits defined by the metrological model. The simulation was conducted using $\lambda = 0.05$ units/month, $u_c = 0.1$, $k = 2$, and an attack magnitude of $B = 3\sigma$. These results demonstrate the capability of the proposed MTI to provide real-time detection of abnormal sensor behavior and to support trustworthy decision-making in IoT monitoring systems.

4 FRAMEWORK ARCHITECTURE AND IMPLEMENTATION

To translate the mathematical models into a functional system, this section outlines a multi-layered architecture and a step-by-step algorithm for real-time metrological verification.

4.1 The 4-Layer Metrological Assurance Architecture

We propose a modular four-layer architecture that separates sensing, metrological verification, secure data management, and application services, thereby ensuring scalability, interoperability, and secure operation. Figure 4 presents the proposed metrological assurance architecture and the corresponding data flow between its components. Real-time sensor measurements acquired by the Physical Sensor Layer are transmitted to the Metrological Assurance Layer, where the Dynamic Trust Corridor (DTC) and Metrological Trust Index (MTI) are computed using the associated Digital Calibration Certificate (DCC). The verified data and calibration records are then securely linked through the Distributed Ledger Layer, which provides immutable storage and auditability. Finally, the Application/Risk Management Layer converts the metrological trust information into operational decisions for monitoring, control, and cyber-physical risk management.

The architecture consists of four interconnected layers::

1) Physical Sensor Layer. Contains the IoT devices. Each device is assigned a unique hardware-bound ID linked to its DCC. Secure standardization of IoT sensor networks is also relevant for IEEE P1451.0-based sensor architectures [11].
2) Metrological Assurance Layer (Edge). The core computational engine. It retrieves the DCC, receives real-time data, and executes the DTC and MTI calculations.
3) Distributed Ledger Layer (DLT). Acts as the immutable database for DCCs and an audit log for high-risk anomalies detected by the Edge layer.
4) Application/Risk Management Layer. Translates the MTI into operational decisions (e.g., shutting down a compromised valve or ignoring a suspicious temperature reading).

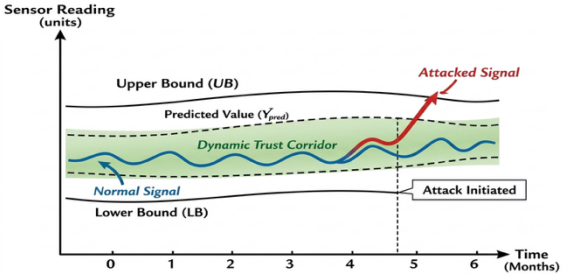

Figure 2: Dynamic Trust Corridor (DTC) for simulated sensor measurements.

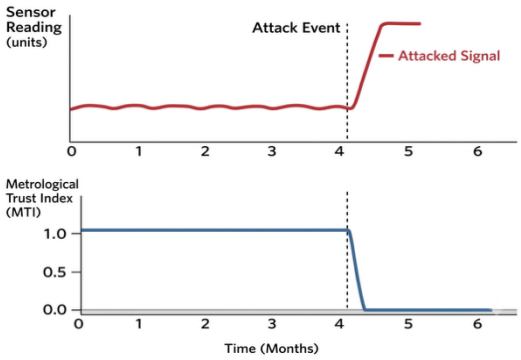

Figure 3: Response of the Metrological Trust Index (MTI) to a simulated bias injection attack.

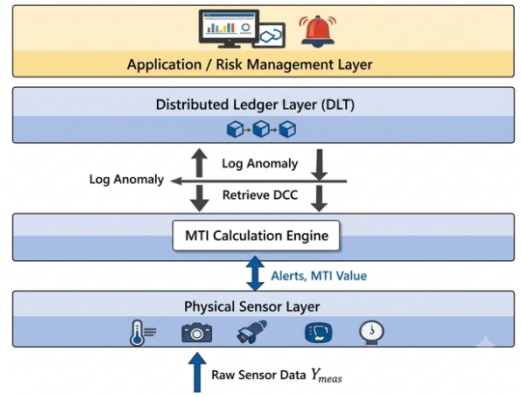

Figure 4: Four-layer architecture of the proposed metrological assurance framework.

Table 2: Algorithm for continuous metrological verification (edge-layer implementation).

Step	Operation	Description
1	Initialize	Retrieve Sensor ID and fetch latest DCC from DLT.
2	Model Update	Calculate $U_{dyn}(t)$ and $Y_{pred}(t)$ using Formulas (9) and (12).
3	Data Acquisition	Receive $Y_{meas}(t)$ from the physical sensor layer.
4	MTI Calculation	Compute instantaneous $MTI(t)$ using Formula (17).
5	Window Filtering	Update $\overline{MTI}(t)$ and $P_{alert}(t)$ using Formulas (18) and (19).
6	Decision	If $P_{alert} >$ Threshold, flag data as compromised and log to DLT.
7	Iterate	Repeat for the next sampling interval.

4.2 Algorithm for Continuous Verification

The operational logic of the Metrological Assurance Layer is governed by an iterative algorithm. To enhance robustness against transient sensor noise, we implement a windowed averaging approach for the Trust Index. Let N be the observation window size. The windowed Metrological Trust Index $\overline{MTI}$ is defined as:

$$\overline{\mathrm{MTI}}(t) = \frac{1}{N}\sum_{i=0}^{N-1} w_i \cdot \mathrm{MTI}(t-i). \quad (18)$$

where w_i are weighting coefficients. An alert is triggered based on the deviation of the windowed index from the unity. We define the Alert Probability P_{alert} as a sigmoid function of the trust deficit:

$$P_{alert}(t) = \frac{1}{1+e^{-\alpha(\tau-\overline{\mathrm{MTI}}(t))}}. \quad (19)$$

where τ is a sensitivity threshold and α is a scaling factor. The system also calculates a Global Risk Score R_G for the IoT node, integrating the metrological state with the asset's criticality C:

$$R_G(t) = C \cdot \left(1 - \overline{\mathrm{MTI}}(t)\right). \quad (20)$$

Finally, to quantify the overall reliability of the sensor network, we introduce the Metrological Reliability Index R_{met} for a network of M sensors:

$$R_{met} = \prod_{j=1}^{M} \overline{\mathrm{MTI}}_j . \quad (21)$$

The edge-layer procedure for continuous metrological verification is summarized in Table 2.

4.3 Alignment with Regulatory Standards

The proposed framework provides a technical pathway for compliance with emerging regulations such as the EU Cyber Resilience Act (CRA) and the NIS2 Directive [12]. Specifically, it satisfies the requirements for "Security by Design" and "Continuous Vulnerability Monitoring" by providing a quantifiable evidence base for data integrity. By integrating metrological traceability (via DCC) with cybersecurity (via MTI), manufacturers can demonstrate that their IoT devices possess the necessary resilience against sensor-layer manipulations, which are currently a significant gap in baseline security controls.

4.4 Alignment with Regulatory Standards

The proposed framework provides a technical pathway for compliance with emerging regulations such as the EU Cyber Resilience Act (CRA) and the NIS2 Directive [12]. Specifically, it satisfies the requirements for "Security by Design" and "Continuous Vulnerability Monitoring" by providing a quantifiable evidence base for data integrity. By integrating metrological traceability (via DCC) with cybersecurity (via MTI), manufacturers can demonstrate that their IoT devices possess the necessary resilience against sensor-layer manipulations, which are currently a significant gap in baseline security controls.

5 EXPERIMENTAL VALIDATION

Numerical simulation is widely used in engineering studies to validate complex technical models before physical implementation [13]. To evaluate the effectiveness of the proposed framework, we conducted a series of numerical simulations modeling a critical IoT sensor in an industrial environment (Smart Factory).

5.1 Simulation Setup

The testbed simulates a high-precision temperature sensor “characterized by a drift coefficient $\lambda = 0.05$

units/month and an initial calibration uncertainty u_c = 0.1". Two attack scenarios were simulated: a sudden bias injection (Formula 5) and a subtle drift manipulation (Formula 7). The simulation covered a period of 6 months post-calibration to observe the expansion of the Dynamic Trust Corridor.To strengthen the comparative evaluation, an additional baseline was implemented: the Cumulative Sum (CUSUM) control chart, a widely adopted statistical process control method for drift and shift detection [14], [15]. The CUSUM algorithm accumulates deviations from the expected mean and triggers an alarm when the cumulative sum exceeds a predefined threshold h. For fair comparison, the CUSUM parameters were tuned on the same training data (allowable slack k_cusum = 0.5σ, decision threshold h = 5σ), using the same 6-month simulation scenario.

5.2 Evaluation Metrics

The performance of the proposed detection algorithm was evaluated using four widely adopted statistical metrics. Prediction accuracy was assessed using the Root Mean Square Error (RMSE), which measures the average deviation between the predicted and measured sensor values. The effectiveness of anomaly detection was evaluated using the Detection Rate (DR), representing the proportion of correctly identified attacks, the False Positive Rate (FPR), indicating the frequency of false alarms, and the overall Accuracy (ACC), reflecting the proportion of correctly classified normal and anomalous observations. Here, true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) denote the standard outcomes of binary classification used to quantify the detection performance.

5.3 Results and Discussion

To further validate the superiority of the MTI-Framework, it was compared against the CUSUM (Cumulative Sum) control chart, a well-established statistical method for process monitoring. While CUSUM improved upon STM for drift detection (DR = 78.4%), the MTI-Framework achieved a significantly higher detection rate (94.1%) for the same subtle drift scenario.

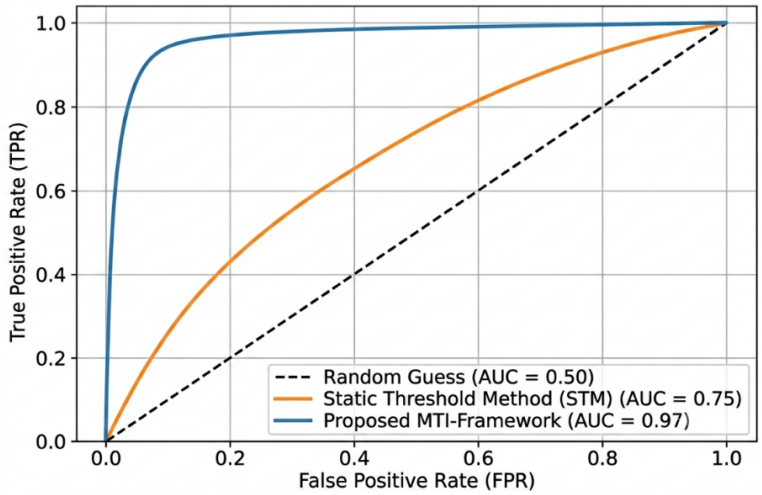

Figure 5: Receiver Operating Characteristic (ROC) curve comparing attack detection performance of the proposed MTI-Framework (AUC = 0.97), the Static Threshold Method (STM, AUC = 0.75), the CUSUM baseline (AUC = 0.89), and a Random Guess classifier (AUC = 0.50).

Table 3: Comparative analysis of detection performance: MTI-Framework vs. STM and CUSUM baselines (simulation: temperature sensor, λ = 0.05 units/month, 6-month post-calibration period).

Metric	STM	CUSUM	MTI-Framework (Proposed)
Detection Rate / DR (Bias)	84.2%	91.3%	98.7%
Detection Rate / DR (Drift)	61.5%	78.4%	94.1%
False Positive Rate / FPR	4.8%	3.1%	1.2%
Overall Accuracy / ACC	79.4%	88.6%	97.5%
AUC (ROC)	0.75	0.89	0.97

This superiority is attributed to the MTI's use of a dynamic uncertainty corridor (DTC) calibrated to the sensor's individual metrological profile stored in the DCC, rather than relying on generic population statistics. The ROC analysis (Fig. 5) confirms this advantage, with the MTI-Framework achieving an AUC of 0.97 versus 0.89 for CUSUM and 0.75 for STM.The proposed MTI-based framework was compared against a traditional Static Threshold Method (STM), where alarms are triggered only when values exceed fixed operational limits. The results of the comparative analysis are summarized in Table 3. The data indicates that the MTI-Framework significantly outperforms the STM, particularly in detecting "Drift Manipulation" attacks. These subtle attacks often remain within static thresholds for extended periods, but are immediately identified by the MTI as they deviate from the expected metrological drift pattern stored in the DCC.

Simulation: bias injection and drift manipulation scenarios on a temperature sensor ($\lambda = 0.05$ units/month, $u\_c = 0.1$). TPR = True Positive Rate; FPR = False Positive Rate. A higher AUC indicates superior discrimination ability. The integration of the windowed filtering (Formula 18) effectively reduced the FPR by smoothing out transient stochastic noise (ϵ_{rand}), ensuring that security alerts are only triggered by persistent metrological anomalies. This demonstrates that the framework is not only accurate but also robust for real-world industrial deployments where sensor noise is prevalent.

6 CONCLUSIONS

This paper addresses the critical challenge of ensuring data integrity in the Internet of Things by proposing a unified framework that bridges the gap between metrology and cybersecurity. By formalizing the concept of “metrological attacks” and leveraging the Digital Calibration Certificate (DCC) as a trust anchor, we have demonstrated that physical-layer data integrity can be rigorously quantified and verified. Furthermore, the architectural integration of Distributed Ledger Technology ensures the immutability of the metrological chain, satisfying the stringent traceability requirements of Industry 4.0 standards. Practically, this framework provides a viable technological roadmap for compliance with emerging regulations, such as the EU Cyber Resilience Act, offering manufacturers a verifiable method to demonstrate "Security by Design."

7 FUTURE WORK

Future research will focus on two main directions. First, the proposed Metrological Trust Index (MTI) algorithm will be implemented and evaluated on resource-constrained edge devices, such as Cortex-M microcontrollers, to assess its computational efficiency, memory requirements, and real-time performance. Second, machine learning (ML) techniques will be integrated to model non-linear sensor drift more accurately, enabling adaptive refinement of the Dynamic Trust Corridor (DTC) under complex and dynamically changing environmental conditions. These developments are expected to further improve the scalability, robustness, and practical applicability of the proposed metrological assurance framework for Industrial IoT systems.

REFERENCES

[1] T. Gundu, “Internet of Things: Sensor Layer Security Risk Mitigation Framework,” in 2023 Int. Conf. Electr. Comput. Energy Technol. (ICECET), Cape Town, South Africa, 2023, [Online]. Available: https://doi.org/10.1109/ICECET58911.2023.10389252.

[2] M. A. Almaiah and R. B. Sulaiman, “Cyber Risk Management in the Internet of Things: Frameworks, Models, and Best Practices,” J. Sens. Actuator Netw., vol. 13, no. 1, 2024.

[3] B. T. Geetha, D. Bhuva, and A. Bhuva, “Fortifying IoT: A Cybersecurity Model for Secure Implementation,” in 2024 Int. Conf. Intell. Comput. Inf. Ind. (IC3I), 2024, [Online]. Available: https://doi.org/10.1109/IC3I61595.2024.10829198.

[4] M. Bhole, W. Kästner, and T. Sauter, “Towards Unveiling Vulnerabilities and Securing IoT Devices: An Ontology-Based Approach,” in 2024 IEEE 29th Int. Conf. Emerg. Technol. Factory Autom. (ETFA), 2024, [Online]. Available: https://doi.org/10.1109/ETFA61755.2024.10710882.

[5] K. Kandasamy, S. Srinivas, and K. Achuthan, “IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process,” EURASIP J. Inf. Secur., vol. 2020, no. 1, 2020, [Online]. Available: https://doi.org/10.1186/S13635-020-00111-0.

[6] ISO/IEC 17025:2017, “General requirements for the competence of testing and calibration laboratories,” International Organization for Standardization, Geneva, Switzerland, 2017.

[7] H. Aranha, M. Masi, and T. Pavleska, “Securing the metrological chain in IoT environments: An architectural framework,” in 2021 IEEE Int. Workshop Metrol. Ind. 4.0 IoT, Rome, Italy, 2021, pp. 1-6, [Online]. Available: https://doi.org/10.1109/METROIND4.0IOT51437.2021.9488526.

[8] T. Mustapaa et al., "Digital Metrology for the Internet of Things," in 2020 Global Internet Things Summit (GIoTS), Dublin, Ireland, 2020, pp. 1-6, [Online]. Available: https://doi.org/10.1109/GIOTS49054.2020.9119603.

[9] S. Eichstädt, M. Gruber, and A. P. Vedurmudi, "Integrating metrological principles into the Internet of Things: A digital maturity model for sensor network metrology," Techn. Messen, vol. 90, no. 1, pp. 12-24, 2023, [Online]. Available: https://doi.org/10.1515/teme-2023-0103.

[10] JCGM 100:2008, "Evaluation of measurement data - Guide to the expression of uncertainty in measurement (GUM)," Joint Committee for Guides in Metrology, 2008.

[11] K. Zhou, J. Wu, and K. B. Lee, "Security for IEEE P1451.0-Based IoT Sensor Networks," in IECON 2021 - 47th Annu. Conf. IEEE Ind. Electron. Soc., Toronto, ON, Canada, 2021, [Online]. Available: https://doi.org/10.1109/IECON48115.2021.9589277.

[12] A. J. Jara, I. C. Martinez, and J. S. Sanchez, "CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2," in 2024 IEEE Int. Smart Cities Conf. (ISC2), 2024, [Online]. Available: https://doi.org/10.1109/SCFC62024.2024.10698057.

[13] E. Madaliev et al., "Numerical study of axisymmetrical transsonic impact based on the SST turbulence model," BIO Web Conf., vol. 145, p. 03034, Jan. 2024, [Online]. Available: https://doi.org/10.1051/bioconf/202414503034.

[14] S. W. Roberts, "Control Chart Tests Based on Geometric Moving Averages," Technometrics, vol. 1, no. 3, pp. 239-250, 1959.

[15] E. S. Page, "Continuous inspection schemes," Biometrika, vol. 41, no. 1/2, pp. 100-115, 1954, [Online]. Available: https://doi.org/10.2307/2333009.