International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

pp. 19-24, April

T-SHIELD: A Hybrid Embedded Tamper-Secure Architecture for Intelligent Measuring Instruments

Sharmila Devi J[1], Mohamed Saheerdeen H[2], Vasan S R[3], Mohamed Rifath J[4]

[1]Assistant Professor, Department of Instrumentation and Control Engineering, A.V.C. College of Engineering, Mayiladuthurai, Tamil Nadu, India

[2,3,4]Second Year Students, Department of Instrumentation and Control Engineering, A.V.C. College of Engineering, Mayiladuthurai, Tamil Nadu, India

Corresponding Author E-mail: sharmeejeyam@gmail.com

ABSTRACT: Tampering with electronic measuring instruments poses a serious threat to transactional integrity, regulatory compliance, and public trust, particularly in cost-sensitive deployments, such as retail weighing systems. Existing protection mechanisms rely on either passive mechanical seals or isolated software checks, both of which are inadequate against coordinated physical and firmware-level attacks. This study presents T-SHIELD, a hybrid tamper-secure embedded architecture that integrates physical integrity sensing, firmware trust enforcement, and lightweight anomaly evaluation into a unified protection layer. Unlike recent solutions that emphasise computationally intensive machine learning, the proposed framework employs deterministic statistical intelligence tailored to resource-constrained embedded platforms. Experimental validation on a digital-weighing prototype demonstrated high tamper-detection accuracy, minimal false alarms, and negligible performance overhead. The results indicate that T-SHIELD offers a practical, regulation-friendly, and scalable solution for next-generation intelligent measurement instruments.

Keywords: Embedded security, Tamper detection, Firmware integrity, Intelligent measuring instruments, Anomaly detection

1. Introduction

Electronic measuring instruments are central to commercial transactions, industrial automation, and the enforcement of statutory metrology. Despite improvements in sensing accuracy and digital interfaces, security vulnerabilities remain largely unaddressed, enabling unauthorised calibration changes, sensor bypassing, firmware replacement, and replay-based data manipulation. These vulnerabilities result in financial losses and erode confidence in automated measurement systems. Traditional tamper-prevention mechanisms, such as lead seals and enclosure locks, provide only symbolic protection and can be easily circumvented. Firmware-only security mechanisms, while effective against software modification, fail to detect physical intrusions that subtly alter sensor behavior without modifying the code [1,4,5]. Recent research has explored machine learning-based anomaly detection; however, such approaches introduce high computational overhead, limited clarifications, and regulatory challenges [3,9], particularly in legally certified devices. This study addresses the limitations by proposing T-SHIELD, a hybrid embedded security layer that emphasises balanced protection rather than algorithmic complexity. The architecture combines physical tamper sensing, firmware integrity validation, and lightweight anomaly scoring to deliver reliable protection while maintaining a deterministic behavior

suitable for certification and field deployment [2,6].

2. Related Work

Research on tamper resistance in embedded systems has traditionally focused on physical protection techniques, including breakable seals, conductive meshes, and enclosure-intrusion switches. Although effective in detecting gross physical access, these methods lack contextual awareness and frequently generate false alarms owing to environmental disturbances [1,5]. Firmware security has evolved through the adoption of secure boot mechanisms, cryptographic hash verification, and trusted execution environments (TEEs). These techniques ensure code authenticity but remain ineffective against analog tampering, sensor substitution, and calibration drift induced by mechanical manipulation [4,8]. Network-based intrusion detection and blockchain-backed audit trails have also been proposed; however, their dependence on continuous connectivity and computational resources limits their applicability in low-cost measuring devices [2,6,10].

Distinct prior approaches, T-SHIELD integrates physical, firmware, and data integrity mechanisms within a single embedded framework, emphasizing minimal intelligence and deterministic decision-making rather than continuous learning [3].

3. System Building

Figure 1(a) illustrates the physical integrity-sensing layer of the proposed T-SHIELD architecture. This layer is responsible for detecting unauthorized physical access and structural manipulation of measuring instruments. Micro-vibration sensors are deployed to capture abnormal mechanical disturbances caused by enclosure opening or component displacement, whereas continuity-based tamper meshes monitor seal integrity and detect breakage or short-circuit attempts. The signals from these sensors are interfaced with an embedded microcontroller, where they are continuously evaluated to identify deviations from the normal operational behavior. By providing early detection of physical tampering, this layer forms the first line of defense in the T-SHIELD security framework [4,8].

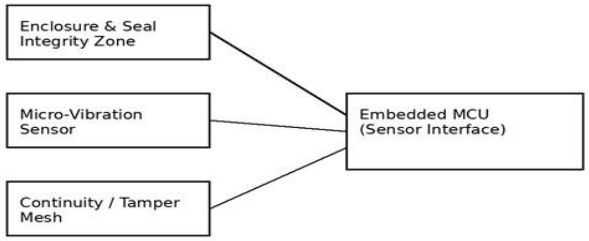

Figure 1(a): *Physical Integrity Sensing Layer of the T-SHIELD Architecture*

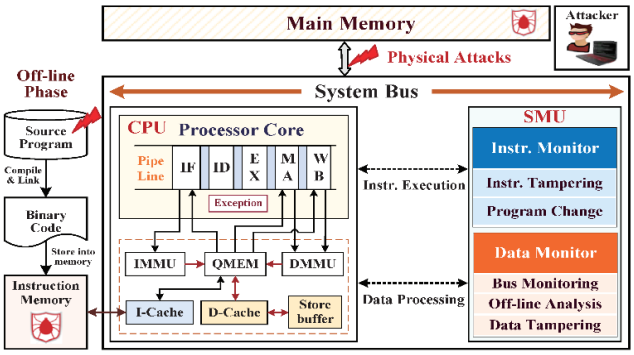

Figure 1(b): *Secure Firmware and Runtime Trust Enforcement Layer*

The complete integrated block diagram of the T-SHIELD framework is shown in Figure 1(c), which combines physical integrity sensing, secure firmware enforcement, lightweight anomaly evaluation, and trusted event logging. Layered integration ensures that both physical and digital tampering attempts are correlated and detected in a unified manner [2,7].

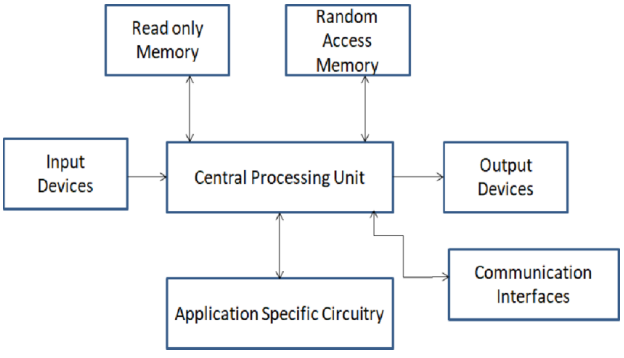

Figure 1(c): *Integrated T-SHIELD System block diagram*

4. Methodology

The proposed methodology relies on event-driven correlations rather than continuous model training. During factory calibration, the baseline signatures of the physical and operational behaviors were recorded, including the vibration envelopes, response timing, and calibration parameter stability. These baselines served as reference profiles during field operations. Incoming sensor data are continuously compared with stored baselines using deviation scoring. When deviations exceed the predefined thresholds across multiple sensing domains, a potential tampering event is flagged. To prevent false positives caused by transient environmental factors, a confirmation cycle was performed before logging or enforcing restrictions. This approach ensures robustness while maintaining the operational continuity. Importantly, the absence of adaptive retraining preserves deterministic behavior, which is essential for legal metrology compliance and post-event clarifications [3,9].

5. Results and Performance Evaluation

Experimental validation was conducted using a prototype digital weighing instrument subjected to controlled tampering scenarios, including enclosure opening, sensor displacement, and firmware modification. The performance metrics are listed in Table 1.

Table 1: *Tamper Detection Performance of T-SHIELD*

Tamper Condition	Detection Accuracy (%)	False Alarm Rate (%)	Detection Latency (ms)
Enclosure Intrusion	98.6	1.2	42
Sensor Manipulation	97.9	1.5	47
Firmware Alteration	100	0.0	35
Environmental Noise	–	1.8	–

The results in Table 1 indicate that T-SHIELD achieves consistently high detection accuracy across diverse tampering scenarios while maintaining a low false alarm rate. Firmware modification attempts were detected immediately during the secure boot process, confirming the effectiveness of cryptographic integrity enforcement [4,8].

Figure 2(a) shows the statistical baseline sensor response of the measuring instrument during normal operation. The distributions of the temperature and vibration readings exhibited stable, besides unimodal behavior, indicating consistent environmental and structural conditions in the absence of tampering. These baseline profiles were established during calibration and subsequently used as reference patterns for anomaly evaluation. The absence of abnormal skewness or abrupt distribution shifts confirms the suitability of these sensor signals for reliable tamper detection [1].

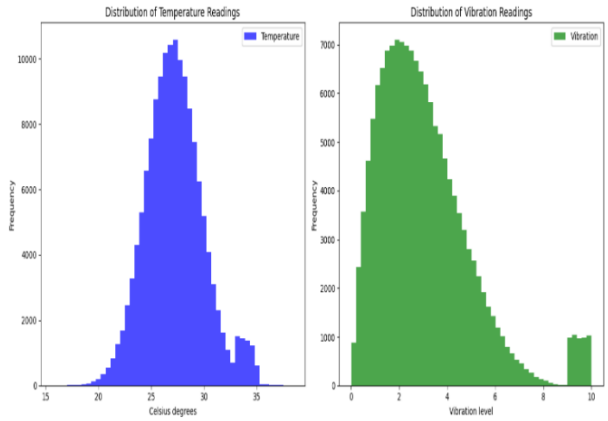

Figure 2(a): *Statistical Baseline Sensor Response during Normal Operation*

The effect of physical tampering on the system is shown in Fig. 2(b). A significant increase in the anomaly score is observed when enclosure intrusion or sensor displacement occurs, clearly

distinguishing tampered states from normal operating conditions [3,9].

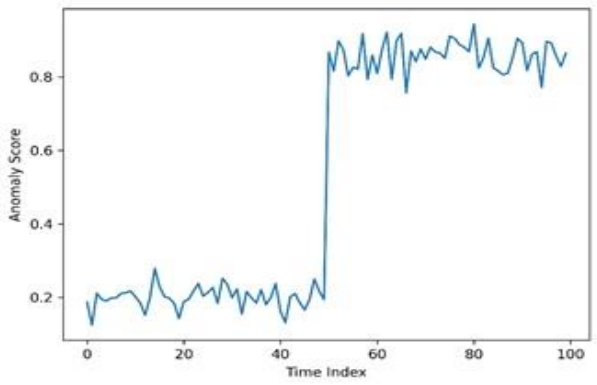

Figure 2(b): *Anomaly Score Variation under Physical Tampering*

Figure 2(c) illustrates the system response to firmware tampering during the secure boot and runtime phases. Under normal conditions, the firmware integrity status remains stable, indicating the successful verification of an authenticated firmware image. When a firmware modification attempt is introduced, the integrity status rapidly deviates from the baseline, reflecting a cryptographic hash mismatch that is detected by the trust enforcement layer. Following this detection, the system transitions to a restricted execution mode, preventing unauthorized firmware from operating. This response confirms that firmware tampering is detected immediately and reliably, ensuring the integrity of the measuring instrument before normal operation can resume [4,8].

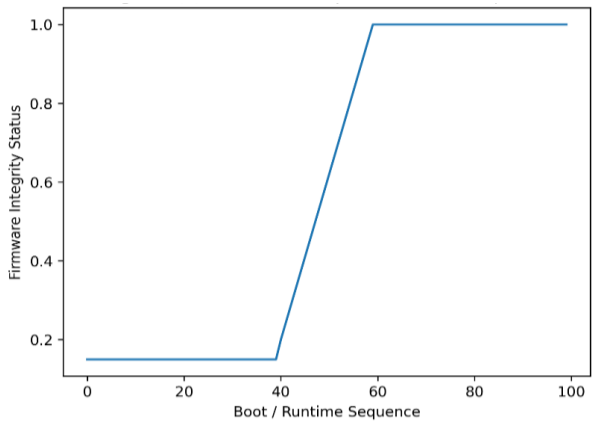

Figure 2(c): *Firmware Tamper Detection Response*

5.1 Comparative Evaluation with Existing Tamper-Protection Approaches

To clearly position the proposed framework within the current research landscape, a structured Comparative Evaluation of Tamper-Protection Approaches is shown in Table 2.

Table 2: Comparative Evaluation of Tamper-Protection Approaches

Evaluation Criteria	Mechanical Seals	Secure Boot Mechanisms	ML-Based Anomaly Detection	T-SHIELD (Proposed)
Protection Focus	Physical intrusion only	Firmware integrity	Behavioral anomaly patterns	Physical, Firmware and Behavioral
Computational Demand	Negligible	Low	High	Low–Moderate
Hardware Overhead	Very Low	Low	Moderate–High	Low
Power Requirement	None	Low	High	Low
Interpretability	High	High	Limited	High
Regulatory Compatibility	Moderate	High	Challenging	High

The comparison in Table 2 underscores the fundamental differences in scope and architectural philosophy among existing tamper-protection strategies. Traditional mechanical sealing mechanisms primarily address visible physical intrusion and offer limited protection beyond post-event inspection. While such approaches

introduce negligible computational and power overhead, they are incapable of detecting firmware manipulation or subtle sensor-level alterations [1].

Secure boot and firmware verification techniques strengthen software integrity by ensuring that only authenticated code is executed during device start up [4]. These mechanisms are computationally efficient and well-suited for embedded platforms; however, they remain restricted to the digital domain and do not account for physical tampering that may alter calibration parameters or sensing behavior without modifying firmware.

Machine learning-based anomaly detection has been proposed to capture complex deviations in operational patterns [3]. Although effective in adaptive environments, these methods require greater processing capability, additional memory allocation, and often periodic retraining. Such requirements may limit their practicality in low-power, legally certified measuring instruments where deterministic operation and clarity are critical.

The proposed T-SHIELD framework adopts a balanced approach by integrating physical integrity sensing and firmware validation with deterministic deviation analysis. By avoiding continuous learning models and instead relying on structured baseline comparisons, the architecture maintains a predictable computational demand while preserving interpretability. This combination enables comprehensive tamper detection without significantly increasing hardware cost or energy consumption, thereby supporting scalable deployment in commercial measurement systems.

6. Discussion

The results demonstrate that the security effectiveness of embedded measuring instruments is more strongly influenced by architectural integration than by algorithmic complexity. By correlating physical disturbances with firmware integrity checks, T-SHIELD detects attacks that would bypass isolated security mechanisms. The deterministic nature of the detection logic enhances the clarifications and supports regulatory acceptance. Furthermore, the minimal computational overhead ensures compatibility with low-power microcontrollers, making the proposed system economically viable for large-scale deployment. Compared to machine learning-heavy solutions, T-SHIELD offers superior predictability, lower power consumption, and simpler certification pathways [2,3,6].

6.1 Scalability and Deployment Considerations

Beyond laboratory validation, the practical adoption of tamper-detection mechanisms depends on scalability, economic feasibility, and regulatory acceptance. The proposed architecture was intentionally designed to operate within the constraints of low-cost embedded platforms commonly used in commercial measuring instruments. Since anomaly evaluation relies on baseline deviation scoring rather than computationally intensive inference models, the processing requirements remain modest and predictable. This makes the framework compatible with widely available microcontrollers without requiring hardware upgrades.

From a deployment perspective, several practical factors merit consideration. Environmental conditions may vary across installation sites, potentially influencing vibration profiles and sensor readings. To address this, baseline calibration can be performed during manufacturing or installation to ensure contextual adaptation. Long-term sensor aging and drift may also affect detection thresholds; therefore, periodic recalibration protocols can be incorporated within standard maintenance procedures.

Another aspect concerns firmware lifecycle management. Secure update mechanisms must be preserved throughout the operational lifetime of the instrument to prevent integrity bypass during maintenance cycles. However, because the proposed architecture does not depend on

continuous cloud connectivity or remote processing, it remains suitable for rural and offline deployments where network infrastructure is limited.

Overall, the architectural simplicity of T-SHIELD supports scalable integration across distributed commercial systems without imposing substantial additional infrastructure or operational costs. The deterministic nature of the decision logic further facilitates regulatory approval and post-event forensic analysis, strengthening its applicability in legally controlled measurement environments.

7. Conclusion

This study presents T-SHIELD, a hybrid embedded tamper-secure architecture designed for intelligent measuring instruments. The proposed framework integrates physical integrity sensing, firmware-level trust enforcement, and lightweight anomaly evaluation to address physical and digital tampering threats. The experimental results confirmed high detection accuracy, low false alarm rates, and minimal latency. This architecture provides a practical and regulation-friendly solution suitable for widespread deployment in commercial and industrial measuring systems [1,4,10].

References

1. Li, S.; Xu, L.; Zhao, S., Year: 2020, “Secure sensing and data integrity mechanisms for smart embedded systems”, Sensors, Vol: 20, No: 18, pp. 5124 – 5124.

2. Ammar, M.; Russello, G.; Crispo, B., Year: 2018, “Internet of Things: A survey on the security of IoT frameworks”, Journal of Information Security and Applications, Vol: 38, No: xx, pp. 8 – 27.

3. Kocabas, U.; Soyata, T., Year: 2021, “Lightweight anomaly detection for resource-constrained IoT devices”, Future Generation Computer Systems, Vol: 115, No: xx, pp. 321 – 334.

4. Gupta, R.; Shukla, S., Year: 2021, “Firmware security challenges and mitigation techniques in embedded systems”, Microprocessors and Microsystems, Vol: 82, No: xx, pp. 103910 – 103910.

5. Law, Y. W.; Doumen, J.; Hartel, P., Year: 2019, “Survey and benchmark of security mechanisms for wireless sensor networks”, Ad Hoc Networks, Vol: 93, No: xx, pp. 101916 – 101916.

6. Fremantle, P.; Scott, P., Year: 2017, “A survey of secure middleware for the Internet of Things”, PeerJ Computer Science, Vol: 3, No: xx, pp. e114 – e114.

7. Alrawais, A.; Alhothaily, A.; Hu, C.; Cheng, X., Year: 2017, “Fog computing for the Internet of Things: Security and privacy issues”, IEEE Internet of Things Journal, Vol: 4, No: 2, pp. 490 – 502.

8. Costin, A.; Zaddach, J.; Francillon, A.; Balzarotti, D., Year: 2014, “A large-scale analysis of the security of embedded firmware”, Proceedings of the USENIX Security Symposium, Vol: xx, No: xx, pp. 95 – 110.

9. Sedjelmaci, H.; Senouci, S.; Feham, M., Year: 2013, “An efficient intrusion detection framework in cluster-based wireless sensor networks”, Security and Communication Networks, Vol: 6, No: 10, pp. 1211 – 1224.

10. Granjal, J.; Monteiro, E.; Sá Silva, J., Year: 2015, “Security for the Internet of Things: A survey of existing protocols and open research issues”, IEEE Communications Surveys and Tutorials, Vol: 17, No: 3, pp. 1294 – 1312.