A Conceptual Model for Sensor-Driven, Blockchain-Secured Evidence Containers in Forensic Investigations

Adarsh V P
Assistant Professor, Department of Digital and Cyber Forensic Science, AJK College of Arts and Science,Coimbatore,India.
adarshvp@ajkcas.com

Abstract

Maintaining the integrity of forensic evidence is important in criminal investigations and judicial proceedings. The traditional methods used for detection of tampering, like the seals and security bags, are vulnerable to some kind of failure and can even be bypassed. This creates a risk to the chain of custody. This paper presents a conceptual model of a sensor driven, blockchain-based forensic evidence container designed to provide real-time tamper detection with immutable digital logging using blockchain technology. The system uses multiple sensors, interconnected by sensor fusion and a microcontroller. The events recorded by the sensor are transmitted using the MQTT protocol and are recorded on the Ethereum testnet, where the immutability of the blockchain guarantees the transparency and non-repudiation of evidence transfer. The proposed framework is expected to increase the evidentiary value by creating a verifiable audit trail and immediate alerts against any attempt to tamper or any unauthorized access. Future work is to convert this concept to a complete, functional prototype integrating all hardware and software components in a rugged physical container. This includes finalizing the placement and mounting of sensors, implementing power management systems, developing production quality firmware, creating a user interface for authorized personnel and extensive field testing.

Keywords

Blockchain forensics, Chain of custody, Tamper detection, IoT-enabled evidence management, Forensic integrity, Smart evidence containers, Sensor Fusion

1. Introduction

Chain of custody (CoC) refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence[1]. In the present, the chain of custody (CoC) is maintained by keeping a logbook with records of the names of agencies that handle the evidence, which is a time-consuming and complicated method and often prone to tampering with evidence[2]. These weaknesses can lead to gaps in documentation, manual handling errors, loss of traceability, and the total dismissal of evidence in court proceedings, thus compromising the integrity and reliability of evidence. **D'Anna et al. (2023)** had clearly discussed the major problems in the traditional chain of custody mechanisms such as inadequate packaging and sealing leading to contamination of evidence, the loss or disappearance of recovered evidence and the digitalization of chain of custody. The purpose is to adapt paper based chain of custody documentation to digitization, mainly using one of the secure and traceable IT systems like the HORIZON laboratory information management system which is used in the United States, which uses unique container codes and electronic signatures for certified control [3]. **Badiye A et al.(2023)** in their paper mentioned some limitations in the current CoC mechanism such as risk associated with multiple transfers, consequence of broken chain and the need for constant physical possession [4]. To overcome this problem in the traditional chain of custody, various researchers proposed blockchain based chain of custody which was found to be a potential replacement for the current paper based chain of custody. **Bonomi et al. (2018)** proposed a solution, B-CoC, which is designed to enforce integrity which ensures the evidence has not been altered or tampered by using the features of blockchain technology[5]. CustodyBlock (CB) is another

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_6

model proposed by **Alruwaili et al. (2021)** which uses private blockchain protocol and smart contracts to monitor the control, transfer, analysis, and preservation of digital evidence[6].
Another area that led us to develop this topic is that smart packaging has been widely used in other domains for a very long time. **Osadchy, S (2024)** demonstrated how modern technologies are transforming traditional packaging in the pharmaceutical industry. Sensors such as temperature and humidity sensors and RFID are integrated into packaging that allows tracking, reads and updates the temperature and humidity at different transportation stages. NFC and BLE modules are used to obtain and share storage conditions to a smartphone or to cloud providing a real-time access[7]. **Chen et al., (2020)** had discussed the use of smart packaging systems in the food industry to monitor the internal and external changes to create a visual summary of the complete temperature profile of a product by recording both time and temperature effects on food products. Sensor-enabled RFID tags can detect changes in food properties like pH, conductivity, and gases through added sensing elements[8]. **Shunmugathammal M et al. (2024)** provides a comprehensive overview of the Shipping Container with Environmental Monitoring and Location Tracking system. This work involves the integration of advanced sensors and communication technologies such as fire sensors, water sensors, GPS modules, accelerometers, microcontrollers, LoRa transmitters, receivers, and display which work together to provide a continuous surveillance of the container's environment and location throughout its journey. [9]

So in conclusion, Blockchain based CoC has already been proposed in forensics and IoT and sensors are already used in logistics, supply chains, pharmaceuticals, and food safety for monitoring shock, temperature, humidity, contamination, and movement. But no existing work is found where it integrates sensors and blockchain inside a physical evidence container. **Batista et al. (2023)** in their paper confirm that blockchain chain of custody research is completely based on digital evidence and physical evidence remains an open research problem[10]. Current studies only upload metadata about physical evidence to blockchain. The blockchain knows about the evidence, but it does not know what is happening to the evidence. Even with heavy use of IoT and sensor enabled containers in other industries such as logistics, pharma, cold chain and food safety, forensics has not adopted or adapted to this technology. No model continuously monitors physical evidence conditions in transit such as the environment conditions, tampering, unauthorized access, shock events and records them in the blockchain. The proposed model applies proven technologies from logistics or pharma to the forensic domain.

2. Methodology

This study is presented as a conceptual architecture and does not include a physical prototype or actual performance data. The proposed model is a layered architecture with four distinct but integrated layers, each responsible for specific system functions.

1. Sensor Layer - for physical monitoring and data acquisition
2. Processing Layer - for data processing, decision logic and control
3. Communication Layer - for secure data transmission and network management
4. Blockchain Layer - for logging and distributed consensus mechanism.

This modular design helps in maintainability, scalability, and flexibility for future modifications.

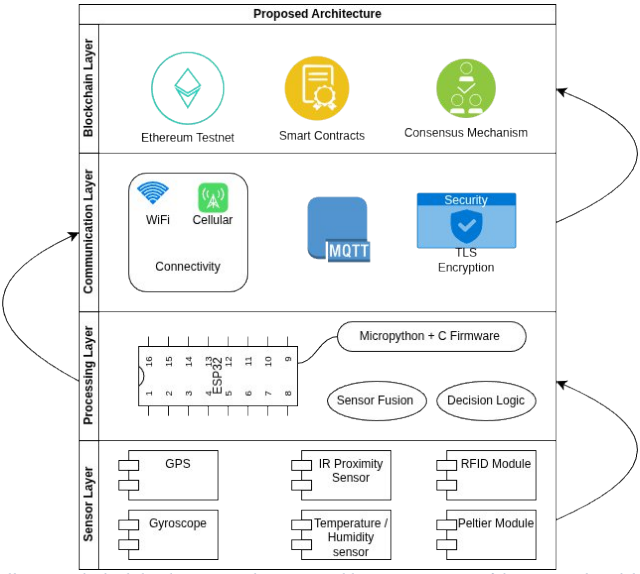


Figure 1. This figure illustrates the high-level system architecture and layer interactions of the proposed model which depicts the arrangement of various sections of the container which includes: Sensor layer, Processing layer, Communication layer and Blockchain layer respectively.

2.1 The Sensor Layer

The sensor layer contains multiple sensor types that work together to provide continuous monitoring collectively of physical evidence containers across different threat vectors.

Table 1: This table shows the sensors, purpose, limitations of each sensor and mitigation steps

Sensor	Purpose	Limitations	Mitigation
GPS/GNSS Module	To detect unauthorized route deviations, verify evidence transportation paths, movement outside authorized geographic zones, to detect speed anomalies and provide location details for all events.	Reduced accuracy in indoor environments and urban canyons, No signal in underground facilities or shielded areas and these modules are vulnerable to GPS jamming and spoofing attacks.	Multi-sensor fusion with accelerometer and gyroscope to detect movement when GPS is unavailable. Also to generate alert when GPS signal is lost unexpectedly
Infrared (IR) Proximity Sensor	The purpose is to detect opening of the lid, unauthorized access and any breach attempts made towards the container.	Vulnerable to IR blocking or shielding. May produce false positives in high-ambient light. Line-of-sight requirement	Multiple IR sensors at different positions; cross-validation with other sensors (gyroscope, proximity sensor)

RFID Reader Module	To verify authorized personnel before accessing the evidence, detect unauthorized access attempts and to log all access attempts with handler credentials.	Limited read range requires close proximity. Vulnerable to RFID cloning if weak authentication is used. Requires handlers to possess valid RFID credentials	Strong cryptographic authentication; integration with biometric systems for future enhancement; alert on repeated failed authentication attempts
Gyroscope	To detect improper handling, sudden impact and drops, inversion of the container and excessive vibration.	Requires calibration to establish baseline. Drift over extended periods. Sensitive to environmental vibration	Periodic recalibration; sensor fusion with accelerometer for drift correction; intelligent thresholding to distinguish normal transport vibration from tampering
Proximity Sensor	To Detect forced entry attempts, magnetic manipulation, and unauthorized proximity to container seals	Sensitive to environmental electromagnetic interference. May produce false positives in electrically noisy environments. Limited range	Adjustable sensitivity thresholds; multi-sensor validation before alert generation; shielding of sensor electronics
Temperature and Humidity Sensors	To ensure evidence preservation requirements are met and to detect environmental anomalies	Reduce the accuracy after long term use	Periodic calibration and auto compensation techniques can be used.

Table 2: This table shows the other modules that can be added to the existing model.

Module	**Purpose**	**Limitations**	**Mitigations**
Peltier module	For cold chain evidences and for samples that must avoid evaporation	High power consumption and high heat dissipation on the hot side	Use of heat sink and cooling fan with proper ventilation for the heat to dissipate.
Camera Module	For visualising the internal of the evidence container during transit. Also it captures the photo of the person who opens and closes the container	May produce noisy, low quality images in low light and motion blur during transit	Use sensors with larger pixel size, IR illumination, or image-denoising algorithms.

2.2 Processing Layer

The processing layer is responsible for executing data acquisition from sensors, fusion algorithms, decision logic, local storage, and managing the communication. The microcontroller proposed for this project is an

ESP32 and was selected based on the following requirements for a forensic chain of custody system as shown in table 3.

Table 3: This table shows the requirements for a microcontroller for this proposed model

Multi-sensor Interface Capability	Must support 6+ sensors simultaneously (GPS, RFID, gyroscope, proximity, IR, temperature/humidity)
Wireless Connectivity	Built-in WiFi and Bluetooth for data transmission to blockchain gateway
Computational Power	Sufficient processing for sensor fusion algorithms, cryptographic operations, and real-time event detection
Power Efficiency	Low power consumption with sleep modes for extended battery operation (target: 7+ days)
Security Features	Hardware encryption, secure boot capability for forensic evidence integrity
Memory	Adequate RAM for multi-tasking and Flash for data buffering during offline periods
Development Ecosystem	Mature libraries, community support, and forensic application precedents
Cost-Effectiveness	Scalable deployment cost (around 300 - 1000 Rs per unit for MCU)
Real-time Performance	Ability to handle time-critical tamper detection
Update Capability	Over-the-air (OTA) firmware updates for security patches

Table 4 : This table shows the comparative analysis of ESP32 with other microcontrollers [11].

Criterion	ESP32	Arduino Uno/Mega	Raspberry Pi Pico	STM32F4	Weight
Processing Power	Dual-core 240MHz	Single 16MHz	Dual-core 133MHz	Single 168MHz	HIGH
Built-in Wireless	WiFi + BT/BLE	None	None	None	CRITICAL
RAM	520 KB	8 KB (Mega: 8KB)	264 KB	192 KB	HIGH
Flash Storage	4 MB (expandable)	256 KB	2 MB	1 MB	MEDIUM
GPIO Pins	34	54 (Mega)	26	82	MEDIUM
Power (Active)	~160-260 mA	~50 mA	~50 mA	~100 mA	HIGH
Deep Sleep	<10 μA	~15 mA	~0.8 mA	~2 μA	CRITICAL

Cryptographic HW	AES, SHA, RSA	None	None	AES, RNG	HIGH
Secure Boot	Yes	No	No	Yes	CRITICAL
OTA Updates	Native WiFi	Complex	Possible	Complex	MEDIUM
Development Ease	Excellent	Excellent	Very Good	Good	MEDIUM
Community Support	Very Large	Largest	Growing	Large	LOW

Based on the comparative analysis in Table 4, the ESP32 was identified to be the optimal primary microcontroller as it has integrated Wireless Connectivity. Provides Hardware-accelerated cryptographic operations (AES-128/256, SHA-2, RSA) and secure boot options. Arduino does not provide hardware security entirely, while STM32 offers comparable security but without integrated wireless. The dual-core architecture (240 MHz each) provides enough processing for Sensor data acquisition and fusion algorithms and Wireless communication, cryptographic operations, event detection. 520 KB SRAM enables Multi-sensor data buffering during offline periods up to 2 hours at 1Hz sampling, MicroPython runtime environment which is approximately 150KB, Cryptographic operation working memory, Local event logging before blockchain synchronization. Arduino provides 8KB which is insufficient for multi-sensor systems. While active power consumption is higher than Arduino, the ESP32's deep sleep mode enables duty-cycled operation [12].

Table 5: This table shows the limitations of other available microcontrollers

Arduino Uno/Mega	Raspberry Pi Pico	STM32F4
Insufficient RAM (8KB vs 520KB required) No hardware security features Requires expensive external WiFi shields 16MHz clock insufficient for cryptographic operations	Strong alternative with good processing power (264 MIPS) but lacks integrated wireless (requires Pico W variant at higher cost) No hardware cryptographic acceleration No secure boot implementation Limited forensic application precedent	Competitive alternative with excellent security features But No integrated wireless (requires external modules) Higher cost when wireless capability is added. A steeper learning curve reduces development speed. More complex OTA update implementation. Would be preferred for applications without wireless requirements

The ESP32 provides the only platform combining all critical requirements security, wireless, processing power, and memory in a single, cost-effective package specifically suited for IoT-enabled forensic applications. It is also important to note that while the ESP32 was chosen, Raspberry Pi Microcontroller Unit (MCU) or STM32F4 will be used in future research due to its flexibility, expandable memory, and speed, regardless of being significantly more expensive

2.3 Firmware

A hybrid architecture will be selected, combining MicroPython for application logic with C modules for performance-critical operations.

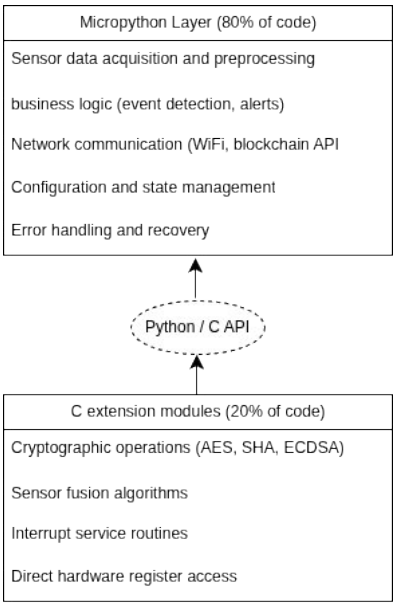


Figure 2. The firmware that is going to be used in the proposed architecture. The figure shows a hybrid setup where 80% of the code is written in micropython and 20% of the code will be in C

2.4 Communication Layer

The communication layer manages secure data transmission between the evidence container and blockchain network. For the proposed model MQTT protocol can be implemented because of its wide use in IoT devices. It is lightweight and has low bandwidth which is good for limited connectivity scenarios. Quality of Service (QoS) levels in MQTT protocol guarantees the reliability of message delivery. The sensors don't push transactions, they don't understand the blocks, they don't sign anything, and they don't wait for confirmations. They simply publish data to the MQTT broker.

2.4.1 MQTT Configuration:

Protocol: MQTT v5.0
Broker: Mosquitto or cloud-based (AWS IoT, Azure IoT Hub)
Port: 8883 (MQTT over TLS)
Transport: TLS 1.3

Topic Structure:

```
evidence/{container_id}/events        # Event publications
evidence/{container_id}/status        # Status updates
evidence/{container_id}/alerts        # Critical alerts
evidence/{container_id}/commands      # Remote commands (optional)
```

QoS Levels:
QoS 0: Periodic status updates (best effort)
QoS 1: Standard event logging (at least once)
QoS 2: Critical events and authentication (exactly once)

Keep-Alive: 60 seconds
Clean Session: False (maintain session across disconnections)

2.4.2 Sample Message Format (JSON):

Figure 3. shows the sample json format that can be used in the communication layer.

2.4.3 TLS Encryption

All the messages from sensor to broker and broker to subscriber travels through a fully encrypted tunnel. There are no plaintext anywhere and no downgrade attacks to older TLS versions. There are the two authenticated encryption ciphers TLS 1.3 relies on. AES-256-GCM which is hardware accelerated on most CPUs and is extremely fast and secure. ChaCha20-Poly1305 which is faster on low-power IoT devices lacking AES hardware but provides the same security level. To prevent rogue sensors, spoofed devices, or unauthorized gateways from injecting data, sensors must provide a valid client certificate.

Mutual TLS (mTLS) with client certificates ensures both sensors and the broker authenticate each other before any exchange of data is performed. Session keys are shared via Elliptic Curve Diffie Hellman Ephemeral (ECDHE), providing perfect forward secrecy so that even if long-term keys are compromised later, previously captured MQTT traffic remains unreadable.

2.4.4 Network Connectivity

Primary connectivity proposed for the framework is WiFi (802.11 b/g/n). It automatically connects to known networks, Priority list of evidence facility, police station, and secure public networks and has WPA2/WPA3 authentication. Secondary connectivity can be Cellular which is via an external module. 4G LTE or 5G connectivity for mobile scenarios. Can be used as a backup when WiFi is unavailable.

For offline Operation local event buffering during network unavailability can be implemented and automatically synchronized when connectivity is restored.

2.5 Blockchain Layer

The blockchain layer provides immutable, distributed, and transparent logging of all evidence handling events. Ethereum testnet will be for development and testing of the blockchain layer. Ethereum testnets are networks used by protocol developers or smart contract developers to test both protocol upgrades as well as potential smart contracts in a production-like environment before deployment to Mainnet [13].

The proposed blockchain layer for this architecture is sepolia testnet which utilizes the Ethereum Sepolia testnet for development and testing. The purpose of using sepolia testnet is to validate proof of concept without costs. The consensus mechanism is proof of stake. The block creation time for sepolia is approximately 12 seconds. Also there are faucets available which provide free test ETH for transaction fees. For production deployment, other blockchain options such as Ethereum Mainnet, Layer-2 Solutions such as Polygon or Arbitrum, Permissioned Blockchain (Hyperledger Fabric, Quorum) and Hybrid
Approaches are considered

3. Smart Contract Architecture

The proposed system employs 2 smart contracts for different functions. The following Solidity code snippet (figure 4(a-d)) shows the conceptual design of the smart contracts used in the proposed framework. These snippets represent the logical structure rather than a deployed implementation.

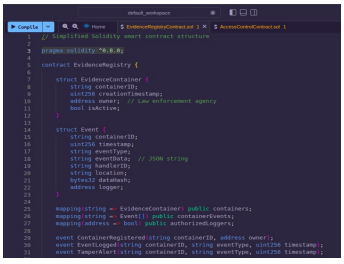


Figure 4 (a)

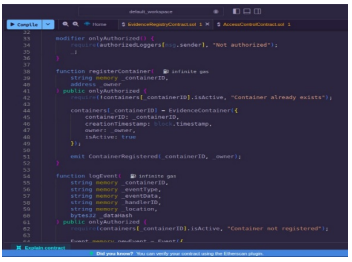
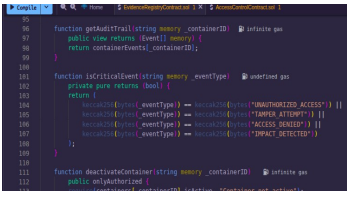
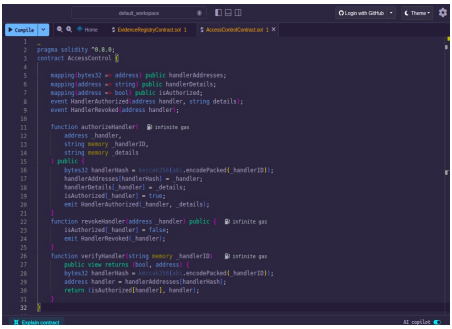


Figure 4 (b)

Figure 4(a-d). Solidity based Evidence Registry Smart Contract architecture



3.1 Access Control Contract:



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract AccessControl {

    mapping(bytes32 => address) public handlerAddresses;
    mapping(address => string) public handlerDetails;
    mapping(address => bool) public isAuthorized;
    event HandlerAuthorized(address handler, string details);
    event HandlerRevoked(address handler);

    function authorizeHandler(
        address _handler,
        string memory _handlerID,
        string memory _details
    ) public {
        bytes32 handlerHash = keccak256(abi.encodePacked(_handlerID));
        handlerAddresses[handlerHash] = _handler;
        handlerDetails[_handler] = _details;
        isAuthorized[_handler] = true;
        emit HandlerAuthorized(_handler, _details);
    }
    function revokeHandler(address _handler) public {
        isAuthorized[_handler] = false;
        emit HandlerRevoked(_handler);
    }
    function verifyHandler(string memory _handlerID)
        public view returns (bool, address) {
        bytes32 handlerHash = keccak256(abi.encodePacked(_handlerID));
        address handler = handlerAddresses[handlerHash];
        return (isAuthorized[handler], handler);
    }
}
```

Figure 5. Solidity based Smart Contract for access control

3.3 Data Flow: Sensor to Blockchain

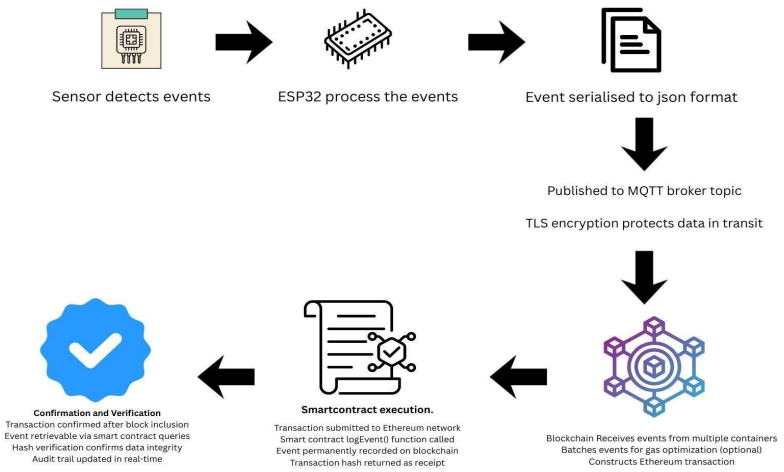


Figure 6. Shows the Complete Transaction Flow from sensor layer to blockchain layer

3.4 Conceptual Evaluation and Validation

The proposed system is a conceptual architecture and therefore the assessment is focused on theoretical validation, scenario based analysis, and estimation of feasibility rather than actual hardware measurements. This form of validation is standard for early-stage forensic technology research where field deployment and prototype fabrication require specialized environments and institutional approvals.

3.5 Threat Coverage Analysis

To assess the effectiveness of the proposed architecture, a threat coverage mapping was performed.

Table 6. Summarizes how each major forensic evidence threat is handled by system components.

Threat Category	Typical Cause	System Component(s)	Mitigation Mechanism
Unauthorized Access	Handler impersonation, unlogged access	RFID authentication, proximity sensor, IR sensor	Access attempts logged; lid opening without authentication recorded as tamper event
Container Tampering	Breaking seals, opening in transit	IR lid sensor, magnetic/proximity sensor, camera module	Immediate alert generated, event logged on blockchain
Environmental Damage	Heat, humidity, moisture	Temperature/Humidity sensors	Deviation triggers anomaly event with timestamp
Mishandling or Shock	Dropping, shaking, inversion	Gyroscope + accelerometer	Abnormal motion classified and logged
Route Deviations	Unauthorized detours	GPS/GNSS	Route mismatch triggers alert; recorded on-chain
Log Manipulation	Altered records, missing entries	Blockchain layer	Immutable, distributed event logging prevents retroactive editing
Network Failure	Connectivity loss	Local encrypted buffering	Data preserved and synchronized when network restores

3.6 Scenario-Based Validation

Since the system is conceptual, scenario based validation is used to demonstrate how the system operates. The following scenarios show how the system responds to real world forensic risks.

Scenario 1 - Unauthorized Lid Opening During Transit

IR proximity sensor detects lid displacement. RFID module confirms no authorized credential was presented. The MCU classifies the event as a critical tamper event.

MQTT transmits events with QoS 2 (exactly once). Blockchain smart contract records the timestamp, the container ID, “unauthorized access” event type and sensor signature. A tamper event is permanently stored, independently verifiable, and cryptographically bound to the evidence chain-of-custody.

Scenario 2 - Environmental Deviation of Biological Sample

The temperature sensor detects a rise above threshold (e.g., more than 8°C). The MCU cross checks with a humidity sensor to confirm the actual disturbances in the environment. Event published with QoS 1. The blockchain logs the deviation event. Environmental preservation violations become auditable and attributable, supporting admissibility challenges and accountability.

Scenario 3 - Route Deviation During Inter-Agency Transport
The GPS module detects deviation which is greater than 200 m from expected route path. The MCU verifies movement is not due to indoor signal loss using IMU data. Alert transmitted over MQTT. The event was added to the blockchain. Investigators gain visibility on evidence mishandling or diversion attempts.

Scenario 4 - Network Downtime in Remote Field Area
No WiFi/Cellular connectivity detected. The events are buffered locally in encrypted flash. Once reconnected, MCU publishes all stored events with preserved timestamps. Smart contract logs events in chronological order. Integrity maintained despite connectivity constraints.

3.7 Architectural Feasibility Assessment

The feasibility of the proposed design is supported by technologies already proven in various other fields such as cold-chain logistics, pharmaceuticals, and supply-chain monitoring. Key points for feasibility include Sensor technologies which are widely available, inexpensive, and field-tested in hostile environments. The ESP32-class MCU is capable of multi-sensor fusion, cryptographic operations, and wireless connectivity. MQTT protocol is the most widely used IoT protocol with good performance in low-bandwidth or unstable networks.

Blockchain logging is industry proven for immutable audit trails. Low throughput chain of custody events are not that expensive to record. When it comes to power management, existing IoT devices show multi day battery life which is feasible with duty cycled sensing. So collectively, these factors indicate that the proposed architecture is technically possible to implement with components which are commercially available.

3.8 Comparative Conceptual Evaluation

The system was compared in a conceptual way against traditional chain of custody methods and existing blockchain based CoC models.

Table 7: Comparison Table of Existing methods to proposed method

Criterion	Traditional CoC	Blockchain only CoC	Proposed System
Tamper Detection	Manual, often delayed	Not supported	Real-time sensor-driven
Environmental Monitoring	Rare or manual	Not supported	Continuous monitoring
Unauthorized Access Logging	Handwritten logs	Digital logs only	Sensor + RFID validation
Physical-Digital Linking	Weak	Partial	Strong (sensor to blockchain)
Data Integrity	High risk of manipulation	Immutable	Immutable + sensor data

Route Tracking	Manual	Not integrated	GPS based
Real-Time Alerts	No	No	Yes

The proposed model provides an approach that links physical conditions directly to an immutable chain-of-custody records, which solves the gap mentioned in previous literature.

3.9 Validation Summary

Although there is no physical prototype present, the combination of threat coverage, scenario based analysis, feasibility justification and comparison with traditional and blockchain based chain of custody provides strong evidence that the proposed architecture is useful, and addresses a recognized forensic need. These forms of conceptual validation agree with early stage research in digital forensics, IoT security, and blockchain based system design.

4. Discussion and Conclusion

The proposed model bridges the physical-digital gap with the use of Multi-sensor monitoring which creates a comprehensive physical security layer while blockchain provides digital integrity assurance. Since all actions are permanently recorded in the blockchain, it provides a strong deterrence against tampering of evidence intentionally or procedural violations. The framework enables immediate detection and response compared to the traditional methods. Since the framework adopts the permissioned blockchain architecture, prosecutors, defense attorneys, forensic analysts, and courts can access identical evidence handling records, promoting trust, facilitating discovery processes, reducing disputes, and supporting judicial efficiency. However apart from its advantages, there are some important limitations that must be looked into. Higher production cost. Long distance transports may cause battery depletion. So power-independent solutions like traditional seals remain more reliable for indefinite storage periods. Also Individual sensors have their own limitations which we already discussed in table 1. While multi-sensor fusion mitigates these limitations, perfect detection remains impossible. Network connectivity is another issue since the framework uses blockchain technology, which makes the model vulnerable to signal jamming, or natural coverage gaps which can affect real time alerts. And finally as a conceptual framework which is currently at the proof of concept stage, the system is not ready for implementation. It requires extensive field testing, long-term reliability data, established maintenance protocols, and vendor ecosystem. Practical deployment requires additional development and validation.

Future work is to convert this concept to a complete, functional prototype integrating all hardware and software components in a rugged physical container. This includes finalizing the placement and mounting of sensors, implementing power management systems, developing production quality firmware, creating a user interface for authorized personnel and extensive field testing.

Abbreviations

MQTT - Message Queuing Telemetry Transport
CoC - Chain of Custody
GPS - Global Positioning System
GNS - Global Navigation System
RFID - Radio Frequency Identification
MCU - Microcontroller Unit
OTA - Over The Air
TLS - Transport Layer Security
ETH - Ether

References

1. Longley, R. What Is Chain of Custody? Definition and Examples. ThoughtCo. 2022. Available online: https://www.thoughtco.com/chain-of-custody-4589132 (accessed on 29 December 2022).

2. Patil, H., Kohli, R.K., Puri, S. et al. Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. Egypt J Forensic Sci 14, 12 (2024). https://doi.org/10.1186/s41935-023-00383-w

3. D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data. Healthcare (Basel, Switzerland), 11(5), 634. https://doi.org/10.3390/healthcare11050634

4. Badiye A, Kapoor N, Menezes RG. Chain of Custody. [Updated 2023 Feb 13]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK551677/

5. Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-coc: A blockchain-based chain of custody for evidences management in digital forensics. arXiv preprint arXiv:1807.10359.

6. Alruwaili, F. F. (2021). CustodyBlock: A Distributed Chain of Custody Evidence Framework. *Information*, *12*(2), 88. https://doi.org/10.3390/info12020088

7. Osadchy, S. (2024, 11 28). SMART PACKAGING OF PHARMACEUTICAL PRODUCTS. Management, navigation and communication systems. Collection of scientific works, 4(78), 4. https://doi.org/10.26906/SUNZ.2024.4.119

8. Chen, S., Brahma, S., Mackay, J., Cao, C., & Aliakbarian, B. (2020). The role of smart packaging system in food supply chain. Journal of food science, 85(3), 517-525.

9. M. Shunmugathammal, S. S. Subramoniam, N. Bharathy and G. K, "The Smart Shipping Container with Environmental Monitoring and Location Tracking System," 2024 International Conference on Advances in Computing, Communication and Materials (ICACCM), Dehradun, India, 2024, pp. 1-4, doi:10.1109/ICACCM61117.2024.11058988.

10. Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M., & Miranda, F. P. d. (2023). Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. Journal of Risk and Financial Management, 16(8), 360. https://doi.org/10.3390/jrfm16080360

11. Gping. (2025, October 9). *ESP32 vs STM32 vs RP2040 vs Arduino — Ultimate MCU Comparison & How to Choose*. Bettlink. Retrieved December 12, 2025, from https://www.bettlink.com/blog/esp32-vs-stm32-vs-rp2040-vs-arduino-guide

12. Nick. (n.d.). The ESP32 Chip explained: Advantages and Applications. DeepSea Developments. Retrieved December 13, 2025, from https://www.deepseadev.com/en/blog/esp32-chip-explained-and-advantages/

13. Networks | ethereum.org. (2025, October 22). Ethereum.org. Retrieved December 9, 2025, from https://ethereum.org/developers/docs/networks/