Securing Blue Carbon Accounting: A Cryptographic Framework for Coastal Ecosystem Monitoring

Heider A. M. Wahsheh
Department of Information Systems-College of Computer Science and Information Technology,
King Faisal University, Ahsa 31982, Saudi Arabia

***Abstract*—Blue carbon ecosystems have significant long-term carbon sequestration capacity, making them an important nature-based solution for climate change mitigation. However, monitoring and accounting processes are increasingly dependent on distributed IoT sensors, satellite remote sensing, and cloud-based analytics platforms. This growing digitalization exposes the blue carbon data lifecycle to risks such as tampering, unauthorized access, and loss of data provenance. A compliance-aware cryptographic framework is presented to secure blue carbon accounting throughout the end-to-end process, from in situ measurement to carbon credit verification. In contrast with generic IoT–blockchain architectures, the framework binds sensing devices to national Public Key Infrastructure (PKI) identities and produces audit-ready cryptographic evidence aligned with Monitoring, Reporting, and Verification (MRV) workflows. The design employs the Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure authenticity and non-repudiation, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) encryption for confidentiality, a hash-chained log for ordered integrity, and Secure Multiparty Computation (SMC) for privacy-preserving validation. Experimental results under simulated attacks (n = 50) demonstrate a 100% detection rate across the evaluated tampering scenarios, while maintaining an average IoT-layer cryptographic latency below 10 ms and a blockchain throughput of 145 transactions per second, exceeding the requirements for continuous ecosystem monitoring. These findings indicate that strong lifecycle-wide cryptographic guarantees can be achieved without imposing prohibitive computational overhead.**

Keywords*—Blue carbon accounting; environmental cybersecurity; blockchain security; Public Key Infrastructure (PKI); elliptic curve cryptography; secure multiparty computation; IoT security; data integrity; carbon credit verification; MRV

I. Introduction

Mangroves, seagrasses, and salt marshes, or Blue Carbon Ecosystems (BCE) have more powerful capabilities to support climate function, and store carbon, than most terrestrial forests. They also help sustain biodiversity, coastal protection, and nearby communities [1]. In Saudi Arabia, BCE preservation and restoration has recently begun to be evaluated within the Saudi Green Initiative (SGI) and the National Red Sea Sustainability Strategy as well as the Middle East Green Initiative (MGI) [2–3]. However, due to the expansion of blue carbon monitoring and the expected large-scale implementation of the Internet of Things (IoT), as well as the use of satellites and cloud-based remote sensing for data collecting and processing, the data lifecycle raises issues such as data tampering, unauthorized access, and loss of data provenance [4]. These issues threaten the scientific integrity, and the trust of carbon markets and their verification systems, in addition to the reputational issues associated with cloud technology. Although some existing technological solutions based on cryptography and blockchain offer some level of protection, they do not have a fully developed, end-to-end, compliance-based security framework for blue carbon accounting [5].

In response to this issue, we propose a lightweight framework that ensures authenticity, confidentiality, integrity, and traceability for all stages of the BCE data lifecycle. This is made possible by incorporating elliptic curve cryptography with the Saudi national Public Key Infrastructure (PKI) (i.e., National Center for Digital Certification (NCDC) and the Saudi Root Certification Authority (Saudi Root CA)). More specifically, this research aims to answer the following question: How to architect blue carbon accounting that is secure, scalable and compliance preserving with respect to the constraints of distributed IoT in order to provide authenticity, confidentiality, integrity, non-repudiation and audibility? In contrast to standard IoT-blockchain systems that provide only tamper-evident logs, the framework we propose adds a compliance-aware trust layer that associates a PKI-credentialed, certificate-based identity with each sensing device. It also enables the generation of audit-compliant cryptographic data that is suited to the Monitoring, Reporting, and Verification (MRV) certification process and enables privacy-preserving, multi-stakeholder validation through secure multi-party computation (SMC).

A. Motivation

Climate action urgency and rapidly growing voluntary and compliance carbon markets create a need for secure and verified blue carbon data infrastructures. Without adequate digital safeguards, incomplete, fraudulent, or low-quality data may undermine ecosystem monitoring and distort carbon credit valuation. In high-stakes environmental markets, data quality is not merely technical. It is the foundation of economic credibility and regulatory legitimacy. From a governance perspective, blue carbon accounting is more firmly integrated into MRV systems requiring data transparency, auditability, and reproducibility. The measurements produced from IoT sensors and remote sensing systems must be capable of being justified formally as evidence for certification and registration processes. Most current monitoring systems focus on the ecological accuracy of data but do not sufficiently account for systemic cybersecurity risks that come from decentralized data collection and several party data-verification. A purpose-built, cryptography-based system will offer a primary means of technical trust for the system. With the appropriate safeguards, blue carbon systems

can enhance their resiliency to cyber-attacks at every stage of measurement, transmission, aggregation, and verification, and at the same time, maintain scientific credibility and the integrity of the marketplace.

B. National Infrastructure and Legal Alignment

The national PKI ecosystem in Saudi Arabia provides a solid foundation for digital trust. The secure digital certificates and signature services are managed by the NCDC, and Saudi Root CA under the international and national requirements, and the NCDC and Saudi Root CA are the primary trust anchors [2,3,6]. This PKI framework, with the addition of legally-recognized digital signatures, device-identifiable verification, and standardized certificate lifecycle management, will support blue carbon accounting mechanisms. Although the oversight of regulations remains the responsibility of the nation-state, such integration supports greater interoperability between governmental and privatized entities. It also enhances the trust of international players impacting carbon credit validation. If the workflow of environmental monitoring and national digital trust systems are integrated, blue carbon accounting will not only be a technical measurement process, but also a legally defensible and policy-compliant digital ecosystem. Besides the national requirements, integrating blue carbon accounting with a state-controlled PKI system provides the legally defensible digital ecosystem that allows for the recognition of digital evidence of a state-controlled PKI system in the international carbon markets. As digital submissions become more prevalent in voluntary carbon registries and climate finance systems, datasets that are digitally signed and backed by certificates will help assure the origin and integrity of the data. This alignment of data integrity with the growing digital framework in carbon markets will reduce disputes, support direct and transparent audits by third parties, and provide the infrastructure for international interoperability with certification systems within carbon markets.

C. Background: ECC and PKI

Using Elliptic Curve Cryptography (ECC) in IoT-based environmental monitoring systems is beneficial because it offers extensive safety features with significantly low computation costs relative to standard public-key systems. The Elliptic Curve Digital Signature Algorithm (ECDSA) offers authentication and non-repudiation and Public Key Infrastructures (PKIs) offer secure key management and verification. These components are part of the proposed framework's foundation. ECC is efficient in terms of computation, as it offers equivalent security to traditional Rivest–Shamir–Adleman (RSA)-based schemes but with significantly less key sizes. This is especially critical to remote coastal IoT systems for low computation time, memory, and especially low power usage. This high efficiency is essential for monitoring blue carbon, as the dispersed sensors are located in remote areas with a low energy budget and a high intermittent connectivity. In a Public Key Infrastructure (PKI) all digital certificates are issued to authorized devices, associating the device's identity with valid, corresponding digital keys. This allows measurements taken by the sensing device to become attributed to legitimate operators. This also allows the environmental observation reports to be verified by any organization, without having to trust the observations.

Alongside institutionally governed certificate management and ECC-based signatures, the framework builds a scalable trust model to offer regulatory accountability and secure data provenance across the entire blue carbon accounting process [6,7].

D. Contributions

This paper aims to achieve the following: 1) identify the marketplace for blue carbon accounting and the related IoT, cloud, and satellite-based monitoring frameworks, and outline a corresponding threat model; 2) outline a data lifecycle cryptographic approach using the combination of ECDSA, AES-GCM, hash-chained logs, and Secure Multiparty Computation (SMC); 3) construct a proof-of-concept prototype using actual datasets from coastal ecosystems for functionality and resilience testing; and 4) relate the framework to the Saudi sustainability initiatives (SGI, MGI, National Red Sea Strategy) and to regulatory carbon credit frameworks (Verra, Gold Standard).

E. Paper Structure

The subsequent sections of this paper are laid out as follows: Section II discusses the existing literature concerning blue carbon monitoring and relevant cryptographic advancements. Section III explains the threat model and corresponding security requirements, while Section IV describes the proposed framework. Section V outlines the prototype implementation, and Section VI presents the security and performance evaluation. Finally, Section VII concludes the paper and discusses limitations and future research directions.

II. Related Work

Environmental monitoring and blue carbon accounting intersect remote sensing, marine ecology, IoT, and applied cryptography. While new approaches focusing on carbon stock measurement are being developed, the field of securing these solutions is still in its infancy. As a result, no existing approaches provide end-to-end security solutions for blue carbon accounting.

A. Blue Carbon Measurement Techniques

Surveys in the field and biomass monitoring are still the most common ways of evaluating blue carbon ecosystems, and are extremely labor-intensive and only viable on a small scale. Evaluating remote sensing for the purposes of monitoring large expanses of mangroves and seagrass meadows has been successfully conducted with multi- and hyperspectral imaging technologies [8]. For example, the Habitat classification and change detection [9] is a proven technique with the use of Sentinel-2 and Landsat satellites. However, there is a need for ground truth data to bridge the gap between biomass estimates from satellite and field [10]. As field surveys, remote sensing, and AI-driven habitat classification to closing this gap, hybrid approaches are necessary.

B. Environmental Data Management Security

The rapid proliferation of IoT-based monitoring systems has made the protection of environmental data more urgent. Some protocols for monitoring water quality, air quality, and wildlife have incorporated security measures, including encryption and authentication, and secure log [11]. Other recent works have

added blockchain and digital signature technologies for improved provenance and integrity security [11-12]. Still, these techniques remain mostly generic and do not address the specialized security, compliance, and verification needs of systems for blue carbon accounting.

C. The Use of Blockchain and Cryptography in Other Ecological Applications

The primary reason for the use of blockchain technologies in the field of ecology and environmental sciences is due to the secure, immutable, and decentralized record-keeping and validation. Use cases include credit for carbon offset trading systems, transparent sustainability reporting, and ecosystem data sharing networks [13]. The use of some cryptographic techniques, such as digital signatures and zero-knowledge proofs, enhances the accountability of these systems.

D. Marine Cybersecurity and AI-Enabled Conservation

There is also some literature on the dual use of cryptography and artificial intelligence in the protection of the marine environment. The integrity of the datasets from coral reef research has, for example, implemented the use of watermarking [12]. Meanwhile, AI-focused methods were created for the management of marine litter in the Gulf of Aqaba [14]. Most recently, studies have shown the utility of AI for assessing the health of coral reefs with the aim of sustainable conservation [15-18]. These instances illustrate the nascent intersection of AI, cryptography, and marine ecosystem monitoring, providing vital cross-cutting building blocks for developing reliable and safe blue carbon accounting methodologies. While there is a body of work demonstrating the intersection of cryptography, AI, and marine ecosystem monitoring, no work comprehensively addresses the security of the blue carbon accounting workflows. Most work prioritizes ecological monitoring of the work without the security aspect or applies a one-size-fits-all cryptographic mechanism that is not designed for blue carbon needs. This underscores the necessity for IoT monitoring, cryptographic security, and adherence to the global carbon credit standard to be delivered in a cohesive manner. In Table I, a cross-architectural feature level comparison is made among generic IoT security architectures, blockchain-based environmental monitoring systems, and the proposed compliance-aware framework. The focus of the described analysis is on the end-to-end cryptographic protection, integration with a country's Public Key Infrastructure (PKI) system, compliance, and the use of privacy-preserving analytics.

TABLE I. COMPARATIVE ANALYSIS OF SECURITY AND COMPLIANCE FEATURES ACROSS ENVIRONMENTAL MONITORING ARCHITECTURES

Feature	Generic IoT Security	Blockchain-based Monitoring	Proposed Framework
End-to-End Lifecycle Protection	Partial	Partial	✓
National PKI Integration	✗	✗	✓
Compliance-Aware Design	✗	✗	✓
SMC Integration	Rare	Limited	✓

The current limitations of most IoT security solutions, including those that address only communication without data lifecycle guarantees, are detailed in Table I. Also, blockchain monitoring systems, while boasting monitoring immutability, do not typically include national PKI and do not factor in design for certifying architecturally. The proposed framework, however, incorporates lifecycle cross-SMC and compliance design to create a framework that fuses regulatory and technical cybersecurity gaps with paradigms of the European Union (EU) carbon market regulations. These limitations inspire the advanced threat modeling and compliance-driven cryptographic design that follows.

III. THREAT MODEL AND SECURITY REQUIREMENTS

The integration of IoT sensors, remote sensing systems, and cloud systems for the monitoring of blue carbon creates diverse and numerous cyber security threats. Due to the distributed nature of these systems and reliance of multiple stakeholders, they are susceptible to both external and internal threats. For these reasons, a precise threat model is crucial for defining the boundaries of adversarial actions, and those boundaries, along with stated security requirements, define the range of actions that the system can take to defend itself.

A. Formal System Model

The blue carbon accounting system is described formally as the tuple $\mathcal{M}$ = (D, E, N, L, A), with D referring to distributed sensing devices (IoT nodes and satellite feeds), E to edge aggregation nodes, N to cloud environmental data processing and analytics services, L to the distributed ledger system ensuring evidentiary record integrity via mechanisms of (crypto-) verifiable record, and A to the data custodians and certification authorities auditors for compliance and verifications. The data path D → E → N → L is followed, and A performs the verifications and compliance evaluations.

The adversary $\mathcal{A}$ is modelled as operating under a probabilistic polynomial time (PPT) and can be categorized as: 1) external passive adversary, 2) external active adversary, 3) malicious insider, and 4) resource exhaustion adversary. Security is examined in the system's life-cycle focusing on the system's authentication, confidentiality, integrity, non-repudiation, provenance, and auditability. The system's lifecycles, while under standard distributed system deployment and cryptographic hardness assumptions, provide mechanisms to guarantee the intended security objectives.

This formal abstraction provides a foundation on which security requirements can be analyzed and adversarial resilience can be evaluated in the following sections. Assuming adversaries operate within the bounds of a probabilistic polynomial time model (PPT) and do not attack the cryptographic primitives like the ECDLP or AES-256. From a physical point of view, the study does not consider compromised hardware IoT devices. However, it considers network, replay, and insider attacks. The national public key infrastructure (PKI) system, including the governance and trust of certificate issuance and revocation, is assumed to have proper governance. For secure multi-party computation (SMC), the honest-but-curious model is applied. It is assumed that the system remains secure against up to (t–1) colluding participants, which means that no coalition smaller than the defined threshold can compromise the aggregate data's privacy. This is consistent with

the SMC security definitions and is a realistic expectation in multi-party collaboration environments.

B. Threat Model

In the blue carbon accounting pipeline, different types of attacks can occur. First, there are adversaries who may artificially inflate or deflate the rate of carbon sequestration by manipulating data from satellite sensors or remote sensing [19]. Second, if the cloud backend or IoT gateways are accessed by an unauthorized person (i.e. hacker), sensitive ecological data, such as the location of ecosystems or biomass (which may be of commercial or political interest), may be revealed.

Replay attacks involving valid but outdated data may obscure ongoing ecosystem degradation. Ecosystem degradation may also be especially insidious when it comes to insider threats, which occur when employees are authorized to manipulate device logs for their own economic or strategic gain relating to carbon markets. Lastly, denial-of-service attacks may cause communication or cloud endpoint attacks to postpone or prevent important reporting, which may be detrimental to the monitoring of conservation efforts and the policies that respond to those efforts [20].

C. Security Requirements

To protect the system from these threats, certain security properties are essential. Every point in the data pipeline must preserve data provenance in order to guard against data alterations that go undetected during transmission or during data storage. Authenticity and non-repudiation make it possible to connect each measurement to a verifiable source. It is also important to ensure that the data source, especially for sensitive ecological locations, is safeguarded with strict confidentiality. Last but not least, integrity and traceability must be maintained through audit trails, which will allow regulators and auditors to recreate the complete historical record of measurements. For any cryptographically secured blue carbon accounting framework to be pragmatically deployed, it must be aligned with internationally accepted carbon crediting frameworks, e.g. the Verra Verified Carbon Standard (VCS) and the Gold Standard.

D. Security Assumptions

The security of the proposed method is predicated on certain accepted hardness assumptions. For instance, the security of ECDSA relies on the computational intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP), while the security of AES-GCM is based on the security of AES-256 at standard block cipher security levels. The hash-chaining method operates on the assumption of collision resistance of the hash function in use, and SMC protocols operate with a model of honest-but-curious participants (unless this is stated otherwise). All these assumptions are in tandem with accepted practices in cryptography and national PKI systems.

IV. Proposed Cryptographic Framework

The proposed framework, which integrates ultra-lightweight cryptographic primitives in IoT devices, edge nodes, and cloud-based validation systems, offers the entire blue carbon accounting pipeline lifecycle cryptographic protection. The proposed solution offers a three-phase workflow: the collection of carbon-related measurements using in-field sensors, drones, and satellite feeds; processing of the data in encrypted form during aggregation and analytical computation; and lastly, the validation of the compliance and integrity of data which are validated by auditors and certification bodies through privacy public cryptography protection mechanisms.

The architecture is intended to be cost-effective and computationally lean to allow integration into economically limited monitoring devices and to comply with the requirements of the carbon credit mechanism. A fundamental design feature is the conversion of blue carbon MRV data into crypto-evidence of provenance that is able to stand up in court and be verified. This is done by integrating the identities of PKI-backed devices with compliance workflow devices.

A. Digital Signatures with ECDSA

Non-repudiation and authentication are guaranteed by the use of the Elliptic Curve Digital Signature Algorithm (ECDSA). Prior to sending, each sensing device makes a digital signature of its measurements, thereby enabling verification of data origin, and preventing a downstream node from disputing the reported measurement [7]. Because of their relatively smaller key size, ECC-based signatures are most appropriate for IoT-based blue carbon monitoring deployments.

B. Encryption with AES-GCM

Privacy requirements are satisfied by the use of Galois/Counter Mode (AES-GCM), which is the Advanced Encryption Standard (AES) and a mode that combines Authentication and Encryption [7]. This ensures that only authorized users can access sensitive information related to the environment such as locations and estimates of carbon stocks. AES-GCM is ideal for real-time data transmission across distributed coastal monitoring networks as it is both suitable and computationally sound [12].

C. Hash-Chained Logs for Immutability

To protect the integrity of the historical record, the measurements are arranged in a hash-chained log, in which each new record contains a cryptographic hash of the previously stored value, creating a sequential structure that is both tamper-evident and sequentially. If earlier measurements are altered, the chain will be broken, and the alteration will be easily detectable. This allows record integrity to be verified independently and without the use of trust [7,12]. At the Device and Edge layer, the hash chain acts as a lightweight and sequential integrity mechanism in order to detect tampering locally, in-transit (to the ledger) through a mechanism of prior commitment to the ledger. At the inter-organizational level, the blockchain-based logging system is tamper-evident and provides a time-stamped audit trail to all the actors involved. In this multi-layered design, hash chaining preserves the integrity of the local record in resource-constrained environments, and the distributed ledger system provides cross-stakeholder accountability and long-term auditability.

D. Secure Multiparty Computation (SMC)

The computation of blue carbon accounts involves numerous actors, including government officials, scientists, and certifying agencies. To create a collaborative framework for validation of raw measurements without disclosure of sensitive data, Secure

Multiparty Computation (SMC) protocols are employed. SMC enables participants to compute combined carbon metrics while keeping individual entries confidential.

Assumed within the threat model of honest-but-curious behavior, participants follow the protocol but may try to gain insights from the protocol's intermediate outputs. The SMC method used here is sufficiently protective of privacy during intermediate aggregation, allowing regulations and certifying authorities to perform compliance checks with proof-of-compliance, certain verifiable computations [21].

E. Workflow from Collection to Verification

The collection to verification workflow description of the total process is as follows. Before transmission, sensors encrypt and digitally sign their measurements. Edge nodes perform first-level aggregation and forward the protected data to the distributed ledger, where data is protected through hash-chained structures and consensus mechanisms. Immutable data is available to auditors, who may be authorized to perform some SMC-based aggregated methods, and certifying authorities, who perform privacy-preserving validation. This results in multi-layered workflows of authenticity, integrity, and non-repudiation, coupled with the traceability and auditability of the entire data lifecycle.

F. Alignment with National and International Standards

The architecture is compliant with the National Center for Digital Certification (NCDC) and the Saudi Root CA to satisfy the digital trust environment of Saudi Arabia. Internationally, it complies with the needs of carbon credit standards such as Verra Verified Carbon Standard (VCS) and Gold Standard [2-3]. The framework allows cryptographic proofs to be included in certification submissions and, therefore, can be readily incorporated into carbon markets and policy.

V. Implementation

A prototype implementing the cryptographic framework has been constructed to assess the practicality of the method regarding integration with blue carbon accounting pipelines. The prototype implementation combines IoT devices with cryptographic libraries and a cloud back end to replicate, as closely as possible, real-life scenarios in environmental monitoring.

A. Hardware and Software Environment

The code for cryptography and system control was implemented in Python 3.11. With regard to ECDSA and AES-GCM, the PyCryptodome library was used as the web service interface among the IoT devices, edge nodes, and cloud servers. A flask was used. The prototype was tested in a cloud environment that was virtualized using Ubuntu 22.04 Long-Term Support (LTS). For IoT nodes, LoRaWAN-enabled Raspberry Pi 4 Model B devices were used to simulate end-to-end secure, low-range, long-use communication. Table II summarizes the hardware and software environment related to the proposed framework.

The layout shown in Table II illustrates a tiered deployment architecture in which functions such as sensing, cryptographic processing, ledger logging, and privacy-preserving computation are kept separate. Modularity retains secure and scalable data collection and transmission, even when integrated with different types of coastal monitoring devices.

TABLE II. System Components and Experimental Deployment Environment

Component	Specification / Tool	Role in System
IoT Node	Raspberry Pi 4, LoRaWAN	Secure in situ data collection
Sensors	Normalized Difference Vegetation Index (NDVI) probe, salinity probe	Vegetation & water quality monitoring
Cryptography	PyCryptodome (ECDSA, AES-GCM)	Signing & encryption
Web API	Flask (Python)	Data exchange interface
Cloud Backend	Amazon Web Services (AWS), Amazon Elastic Compute Cloud (EC2), Ubuntu 22.04, AWS Key Management Service (KMS)	Storage & key management
Ledger	Hyperledger Fabric	Immutable record logging
Privacy Module	Multi-Party Computation in Python (MPyC) framework	SMC

B. Cryptographic Integration

Each IoT node was configured to sign its data packets and encrypt them (using ECDSA and AES-GCM, respectively) before transmission. Packet aggregation occurs at edge nodes, which then transmit the packets to the backend, where logging is provided by Hyperledger Fabric, which is immutable and auditable. For validation by multiple stakeholders, SMC of the aggregated values was done without disclosure of the raw measurements to the participating parties, using the MPyC framework.

C. Benchmarking Methodology

Our measurements focused on three main areas of interest:

- Cryptographic overhead — the signing, encryption and secure multiparty SMC per data packet, and the resulting latency.
- Network latency — the round-trip time from the IoT nodes to the cloud verification services.
- Blockchain throughput — the number of transactions per second in the simulated environmental logging workload. Benchmarking results are shown in Table III.

TABLE III. Performance Benchmarking of Prototype Under Controlled Testing Conditions

Metric	Result	Test Conditions
Avg. ECDSA Signing Time	7.4 ms	256-bit key, Raspberry Pi 4 IoT node, averaged over multiple runs
AES-GCM Encryption Time	2.1 ms	1 KB data packet, AES-256, IoT device layer
SMC Latency	11 ms	Aggregation phase at edge node
Blockchain Throughput	145 TPS	Hyperledger Fabric testbed under simulated environmental logging workload

The results from Table III show that when deployed on low-power IoT nodes, ECDSA and AES-GCM operations cause negligible computational delays. Hyperledger Fabric offers a

real-time (close to) append-only ledger system that facilitates rapid transaction logging while being subjected to simulated workload scenarios. Even though SMC entails an extra layer of processing, its delay is still tolerably low for operational use when it comes to privacy-preserving streaming analytics.

VI. Evaluation

The assessment of the proposed framework has been done in three parts: validation of security, evaluation of the performance, and evaluation of the auditor/operator components. Results of the evaluation and analyses are shown in an organized way and in conjunction with some tables.

A. Security Validation

The evaluation of the model was done with respect to some surrogate attack vectors that came from the specified adversary model, which includes the evaluation of model manipulation, replay attacks, unauthorized access, insider attacks, and denial of service. A set of controlled simulations was done to measure the effectiveness of the defense mechanisms that were employed. The summary of all of the security evaluations and assessments is in Table IV.

TABLE IV. Security Evaluation Results Under Simulated Attack Conditions

Attack Scenario	Defense Mechanism	Outcome
Data Tampering	ECDSA digital signatures	100% detection (n = 50 simulated tampering attempts)
Replay Attack	Timestamp + hash-chained log	Successful prevention under replay simulation
Unauthorized Access	AES-GCM encryption	No unauthorized disclosure observed
Insider Manipulation	Immutable ledger logs	Attempted modifications flagged and traceable
Denial of Service (DoS) on IoT Nodes	Redundancy + edge buffering	Delayed reporting without data loss

The attack scenarios included in Table IV show the attack scenarios included against the proposed mechanisms are ECDSA documented altered packets with AES-GCM hindering access to protected data, the replay attack was documented by a hash-chained log, and the creation of unmodifiable logs placed the insider modifications, and edge buffering mechanisms decreased the impact of denial-of-service (DOS) attacks and operationally without loss of data. All of these results show us that the attack scenarios included against the proposed mechanisms are of a layered and comprehensive nature and thus provide complete lifecycle protection against the layered attack scenarios.

B. Performance Analysis

The performance of the system was assessed against the simulated deployment of the system in order to evaluate the operational feasibility. The results show that the above-mentioned proofs of the proposed mechanisms provide a dominant system that provides a clear and easy environment for the data packets that are typical for the environment, blockchain throughput provides the ability to log almost in real-time, and SMC provides a system that is operationally acceptable within the provided range of dominant systems. The performance metrics for the operational scenario provide a summary of the performance metrics measured.

TABLE V. Summary of Operational Performance Metrics

Parameter	Measured Value	Observation
Avg. End-to-End Latency	62 ms	Suitable for near real-time monitoring
Packet Loss under Load	<1%	Stable under simulated network stress
Blockchain Synchronization Delay	<5 s	Observed under periodic logging intervals without throughput degradation

Table V shows that the system has an end-to-end latency of 62 ms, and under simulated conditions loss of packets is negligible. The delay caused by blockchain sync is within the operational limits acceptable for sync monitoring to near real-time. These findings reiterate the fact that the integration of ledger technology does not lead to a considerable performance reduction. The total energy impact also remained within the operational limits practicable for solar-assisted and hybrid-powered deployments to the coasts. Regarding the quantitative evaluation of the deployed cryptographic primitives, latency measurement was done to assess the impact of the computation of signature generation, encryption, and SMC at the levels of IoT and edge.

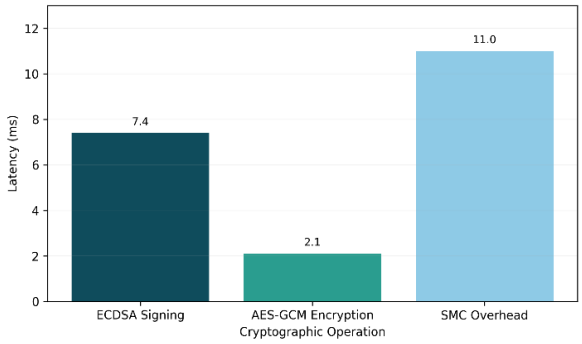

Fig. 1. Measured latency of deployed cryptographic primitives, demonstrating lightweight computational overhead at IoT and edge levels.

As illustrated in Fig. 1, the measured latency of the deployed cryptographic primitives demonstrates lightweight computational overhead at both the IoT and edge layers. AES-GCM encryption shows the smallest delay of 2.1 ms and ECDSA signing takes 7.4 ms per transaction, which is still within an acceptable bound performance for IoT devices that have constrained resources. The increased latency of SMC is 11 ms and is mainly limited to the aggregation phases and not so much to the continuous packet transmission, limiting its impact on the operation overall. This shows us that strong cryptographic guarantees can be integrated without the computational overhead becoming prohibitive, enabling real-time blue carbon monitoring deployments to remain practical.

To examine whether the added blockchain had an impact on performance, the throughput of the Hyperledger Fabric backend was recorded and compared, as shown in Fig. 2, to the minimum operational requirements for uninterrupted logging of the environmental data.

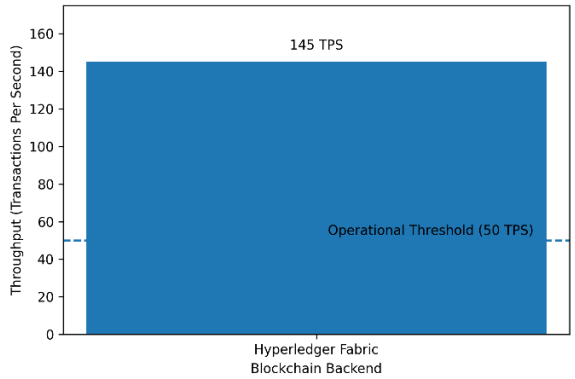

Fig. 2. The performance of Blockchain throughput concerning the minimal operational transaction necessities for the scalable monitoring of the environment.

The observed throughput of 145 transactions per second (TPS) provides a performance headroom of 2.9× relative to the minimum operational threshold for continuous environmental logging, which is 50 TPS. Under the given deployment conditions, the system, combined with hierarchical edge aggregation and batching of sensor measurements, enables proportional scaling of distributed IoT nodes without reaching the capacity of the ledger. The design also separates the cryptographic computation at the device level from the consensus at the ledger, thus allowing for both vertical and horizontal expansion of the monitoring clusters. All of this suggests the framework is capable of scaling to large coastal monitoring deployments in a controlled manner without reducing the performance expectations. A simple snapshot in scaling can be achieved by estimating ledger throughput with the equation $TPS_{req} = (n \times r) / b$, where n is the number of sensors, r is the average number of packets per second produced by each sensor, and b is the edge layer batching. With an observed throughput of $TPS_{obs} = 145$ and an estimated operational average of 50 TPS, the framework is designed to maintain proportional scalability in relation to the number of distributed IoT nodes, especially with hierarchical edge aggregation and periodic ledger commitment.

C. Feedback from Operators and Auditors

Starting from the framework, a pilot usability and validation assessment was conducted to understand the propositional framework from operational and auditing perspectives. Feedback was also gathered through structured workflow simulations as they relate to the assessment and operational transparency of logging, as well as the readiness of certification. Feedback was summarized and presented in Table VI.

TABLE VI. SUMMARY OF AUDITOR AND OPERATOR FEEDBACK (PILOT STUDY)

Stakeholder	Key Observation	Practical Impact
Field Operator	Automated signing and encryption reduced manual intervention	Increased operational efficiency
Auditor	Immutable logs provided verifiable evidence trails	Strengthened certification confidence
Policy Analyst	Alignment with SGI/MGI and international carbon standards	Facilitated regulatory integration

The five simulated audits and four system operators were part of the pilot evaluation structured session to validate workflow systems. System operators were able to provide feedback on the testing environment, but the test environment was simulated.

VII. CONCLUSION AND FUTURE WORK

This paper proposes an architecture that incorporates compliance and cryptography to protect blue carbon accounting pipelines in vast and hybrid Internet of Things and Cloud-based construction environments. Protection encompasses the monitoring lifecycle of Authenticity, Integrity, Confidentiality, and Traceability by compliance with ECDSA Digital Signature Standards, the Advanced Encryption Standard with Galois/Counter Mode (AES-GCM), hash-chained logging, secure multiparty computation, and compatibility with national Public Key Infrastructures (PKI). The processing that results from the cryptography has shown to be negligible. The combined signing and encryption latency at the IoT layer remained below 10 ms, and the blockchain backend sustained a throughput of 145 transactions per second. The results of closed tests for tampering and replay scenarios demonstrate that the implementation of a closed test for retention and replay scenarios is a viable option. The findings of these tests indicate that enforcing the monitoring lifecycle can be achieved without compromising operational performance. The assessments were performed in a controlled environment of the prototype system. There is the possibility of complicated post-maintenance operation in distributed key and certificate management, which may increase the complexity of ongoing operation and maintenance. The SMC component takes an honest-but-curious approach, which may not appropriately capture adversarial collaborative scenarios in the real world. Future research will focus on post-quantum migration strategies combined with the real-time detection of anomalies to capture sensor behavioral anomalies. A step-wise migration strategy is proposed whereby Post-Quantum Cryptography (PQC) signatures will be at the edge/cloud attestation layers, and elliptic curve cryptography (ECC) will remain on constrained devices until a sufficient hardware upgrade is available. Hybrid certificate schemes may allow backward compatibility with existing PKI validation systems.

REFERENCES

[1] S. Farahmand, N. Hilmi, and C. M. Duarte, "The rise and flows of blue carbon credits advance global climate and biodiversity goals," *npj Ocean Sustainability*, vol. 4, no. 1, art. no. 39, 2025.

[2] R. Alajmi, "Green growth is a pathway to sustainable development: An empirical study of Saudi Green Initiative," *J. Econ. Admin. Sci.*, vol. 31, no. 148, pp. 115–129, 2025.

[3] A. F. M. Maniruzzaman and K. Al-Saleem, "Renewable energy and energy justice in the Middle East: International human rights, environmental and climate change law and policy perspectives," *J. World Energy Law Bus.*, vol. 18, no. 1, art. no. jwae021, 2025.

[4] O. G. Ndubuisi and F. I. S. P. O. N., *Improving Advanced Research Methods for Climate Change and Environmental Sustainability*. 2025.

[5] P. K. Goel and S. P. Yadav, "Cloud security protocols for protecting carbon monitoring systems," in *Advanced Systems for Monitoring Carbon Sequestration*. Hershey, PA: IGI Global, 2025, pp. 127–148.

[6] National Center for Digital Certification (NCDC), "National Center for Digital Certification (NCDC)," GOV.SA, Available: https://my.gov.sa/ar/content/13990, Accessed: Sept. 2, 2025.

[7] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology," Available: https://www.nist.gov/, Accessed: Sept. 1, 2025.

[8] L. Zhao, X. Fan, and S. Xiao, "Remote-sensing indicators and methods for coastal-ecosystem health assessment: A review of progress, challenges, and future directions," *Water*, vol. 17, no. 13, art. no. 1971, 2025.

[9] C. Zarzuelo Romero, A. López-Ruiz, M. Bermúdez, M. Ortega-Sánchez, and I. Caballero, "Monitoring intertidal ecosystems: Assessing spatio–temporal variability with Sentinel-2 and Landsat 8," *Int. J. Appl. Earth Obs. Geoinf.*, vol. 128, art. no. 104676, 2025.

[10] P. J. Kashyap, K. Bora, S. Das Podder, A. Amakawa, A. Paul, and C. R. Saikia, "Mangrove monitoring using geospatial technologies incorporating field inventory: A review," in *Revealing Ecosystem Services Through Geospatial Technologies: Beyond the Surface*. Cham: Springer, 2025, pp. 123–138.

[11] M. Al-Khalidi, R. Al-Zaidi, T. Ali, S. Khan, and A. K. Bashir, "AI-optimized elliptic curve with certificate-less digital signature for zero trust maritime security," *Ad Hoc Netw.*, vol. 166, art. no. 103669, 2025.

[12] H. Wahsheh and M. Wahsha, "Digital safeguards for coral reefs with cryptographic watermarking in marine research," in *Proc. Int. Conf. Computing Systems & Intelligent Applications (ComSIA)*. Cham: Springer, 2025, pp. 685–696.

[13] S. Noliya, A. Gupta, and V. Kumar, "E-waste management through blockchain technology: Supply chain led environmental sustainability," *EDPACS*, pp. 1–11, 2025.

[14] M. Wahsha, H. Wahsheh, and T. Al-Najjar, "Enhancing marine litter management in the Gulf of Aqaba through AI," in *Proc. Int. Conf. Information, Communication and Computing Technology (ICICCT)*. Cham: Springer, 2024, pp. 56–67.

[15] M. Wahsha and H. Wahsheh, "Deploying AI for health monitoring of Diadema sea urchins: Toward sustainable marine ecosystems," in *Proc. Int. Conf. Inventive Communication and Computational Technologies (ICICCT)*. Singapore: Springer, 2024, pp. 651–660.

[16] A. Mandal and A. R. Ghosh, "AI-driven surveillance of the health and disease status of ocean organisms: A review," *Aquaculture Int.*, vol. 32, no. 1, pp. 887–898, 2024.

[17] M. Wahsha and H. Wahsheh, "From data to action toward sustainable marine conservation: AI-based coral health assessment," in *Proc. Int. Conf. Computing and Communication Networks (ICCCN)*. Singapore: Springer, 2024, pp. 213–222.

[18] T. Miller, I. Durlik, E. Kostecka, S. Sokołowska, P. Kozlovska, and R. Zwolak, "Artificial intelligence in maritime cybersecurity: A systematic review of AI-driven threat detection and risk mitigation strategies," *Electronics*, vol. 14, no. 9, art. no. 1844, 2025.

[19] G. S. Pujar, A. Taori, A. Chakraborty, and T. Mitran, "Sensing climate change through earth observations: Perspectives at global and national level," in *Digital Agriculture: A Solution for Sustainable Food and Nutritional Security*. Cham: Springer, 2024, pp. 225–280.

[20] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions," *Sensors*, vol. 25, no. 1, art. no. 213, 2025.

[21] G. Premi, A. Mishra, A. Kaur, J. R. Sahoo, P. Aggarwal, and S. Mathur, "Secure multi-party computation for privacy preservation in collaborative networks," in *Proc. 2025 Int. Conf. Automation and Computation (AUTOCOM)*, 2025, pp. 637–642.