International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

AMTA-Sec: An Adaptive Multi-Layer Trust Architecture For Attack-Resilient Distributed Blue Carbon MRV Systems

Vaishali Hirlekar[1,2], Balajee Maram[2] and Ayush Hirlekar[3]

[1]Computer Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India.
[2]Computer Science and Engineering, SR University, Warangal, Telangana, India.
[3]Computer Science and Engineering, SIES Graduate School of Technology, Navi Mumbai,Maharashtra, India.
*Corresponding author(s). E-mail(s): vaishali.hirlekar@sakec.ac.in; Contributing authors: balajee.maram@sru.edu.in; ayushvhiot123@gst.sies.edu.in

Abstract
Blue carbon ecosystems such as mangroves, tidal marshes, and seagrass mead-ows are among the most effective natural carbon sinks and play a significant role in climate change mitigation. Distributed IoT telemetry, edge computing, machine learning, and blockchain-enabled carbon registries are now increasingly being used in modern Monitoring, Reporting, and Verification (MRV) systems to facilitate automated environmental monitoring and carbon credit verifica-tion. In contrast to centralized MRV systems, large scale distributed MRVs systems pose significant cybersecurity threats, such as telemetry spoofing, replay attacks, malicious edge compromises, validator collusion, trust poisoning, and adversarial manipulation of machine learning based soil organic carbon (SOC) estimation models. This paper introduces Adaptive Multi-Layer Trust Architec-ture (AMTA-Sec) to solve these problems, which aims to ensure the reliability and security of distributed blue carbon MRV systems against attacks. This framework highlights dynamic trust computation, edge-level anomaly detection, blockchain-assisted integrity verification, secure machine learning model protec-tion, and distributed trust orchestration across the sensing, edge, cloud and ledger layers. The experimental results showed that the proposed architecture is scalable and cyber-resilient by achieving an accuracy of 93.6 % for malicious telemetry detection, 91.2% for model poisoning detection, 100% for edge integrity violation detection and a reduction of 37% in blockchain write overhead across various scenarios of cyberattacks.

Keywords: Cyber-resilient MRV, Blockchain Security, Distributed Trust Management, Environmental Cyber-Physical Systems, Adversarial Machine Learning, Carbon Credit Fraud Detection, Edge Security, Attack-Aware Architecture

1 Introduction

The importance of blue carbon systems such as mangroves, tidal marshes, and seagrass meadows in the long-term sequestration of carbon and in reducing greenhouse gas build up in the atmosphere has resulted in their emerging as key natural climate solu-tions [1, 2]. Many carbon storage projects are dependent upon Monitoring, Reporting and Verification (MRV) systems to validate carbon storage and control carbon credit issuance for the climate programs that operate on a voluntary or compliance basis [3]. The modern MRV infrastructures are rapidly transforming to distributed digital ecosystems that combine Internet of Things (IoT) telemetry, edge computing, machine learning, cloud analytics and blockchain-based registries for real-time monitoring of the environment and carbon accounting [4, 5]. For practical coastal deployment, the sensing nodes are spread over geographically separated mangrove forests, estuarine wetlands, and tidal ecosystems, where there is no easy way to monitor the nodes continuously. These sensing devices are always sampling soil organic carbon (SOC), salinity, biomass, and tidal data that get aggregated by edge gateways and orchestrated in the

cloud to be used for carbon estimation and verification [6].
Distributed MRV infrastructure is still very vulnerable to cyber threats although technological developments have occurred. It is possible for an attacker to physically interfere with the sensing devices installed at remote coastal locations, alter calibration parameters, introduce bogus telemetry streams or compromise edge gateways used to process the local environmental data [7]. These types of malicious activity could lead to inflated estimates of SOCs causing bogus carbon credits to be generated and compromising the integrity and credibility of environmental sustainability programs [8].
The main application of blockchain-based environmental monitoring systems, shown by recent studies, is the immutable recording of transactions once the environ-mental data has already been put into the validation process [9] and [10]. But the immutability of blockchain doesn't ensure the authenticity of the upstream sensing layer and machine learning inference and the distributed orchestration layer. Existing systems rarely include integrated adaptive trust computation, secure model valida-tion, adversarial telemetry filtering, or attack-aware orchestration mechanisms, which can detect malicious entities in sensing, edge, cloud and blockchain systems [11].
In addition, as machine learning models are embedded in environmental MRV systems, they create new attack surfaces such as adversarial perturbation, poisoning attacks or manipulated inference behavior [12]. Distributed training sets can be com-promised by injected fake environmental telemetry or by gradual tampering with the model outputs that can affect carbon estimation processes without immediate detec-tion.Distributed training sets can be tainted with fake environmental telemetry or gradually tampered with model outputs that can impact carbon estimation processes without immediate detection.[13–15]

To overcome these issues, this research work introduces Attack Resilient Dis-tributed Blue Carbon MRV System with Adaptive Multi-Layer Trust Architec-ture (AMTA-Sec). The proposed framework encompasses dynamic trust computa-tion, secure federated machine learning validation, edge-level anomaly detection, blockchain-assisted integrity verification and attack-aware orchestration across sens-ing, edge, cloud and ledger layers. It consistently monitors the behavior of nodes, integrity check results, and evidence of anomalies to identify and isolate malicious entities as they happen.
The main features of this work are highlighted as follows:

- Design of a secure blue carbon monitoring framework with an attack awareness distributed design.
- The development of a dynamic trust computation mechanism in the sensing layer, edge, cloud, machine learning layer and blockchain layer.
- Areas of current research include integrating secure federated model validation to safeguard SOC estimation from adversarial attacks.Current research includes integration of secure federated model validation to protect SOC estimation from adversarial attack.
- Blockchain-based Forensic Traceability for Carbon Credit Verification: Tamper-resistant tracking and verification of carbon credits.Forensic Traceability with Blockchain for Carbon Credit Verification: Tamper-proof tracking and verification of carbon credits.
- valuation under realistic cyber attack scenarios: spoofing of telemetry data, replay attacks, compromise of the edges, manipulation of the validators, and model poisoning attacks.

2 Related Work and Threat Landscape

The recent progress of distributed environmental Monitoring, Reporting, and Verifica-tion (MRV) systems has brought about the integration of both IoT telemetry and edge computing, machine learning and blockchain technologies into carbon monitoring sys-tems. The technologies strengthen scalability, transparency and automation of carbon credit verification ecosystems. Distributed MRV systems still have many challenges with regard to cyber security, including different sensing environments, physically exposed deployments, and decentralized trust management.

The use of blockchain for MRV has been extensively considered for enhancing traceability and transparency in carbon accounting systems. The authors of [16, 17] proposed a green blockchain-based architecture for the IoT systems to address the security challenges associated with the hazardous material supply chain by using decentralized validation and tamper-resistant transaction management in distributed monitoring systems. Likewise, works on blockchain-based environmental monitoring solutions for sustainability applications where trust, transparency, and immutability of auditing are crucial requirements have also been explored [18, 19].

There have been several studies that have investigated the IoT-based environmen-tal sensing architecture for ecological monitoring and climate applications. Most of the systems used involve

spatially distributed sensors to monitor environmental variables like soil organic carbon (SOC), salinity, biomass indices, and changes in the tide level. Nevertheless, the sensing devices which are deployed in remote coastal environments are often under resource constraints and no physical protection, which make them be susceptible to the telemetry spoofing, replaying attacks, adjusting the firmware and calibration manipulation [20, 21].

The significance of edge computing in minimizing latency and boosting localized environmental analytics has also been highlighted by recent study. Edge-assisted archi-tectures enable telemetry preprocessing at the edge of the sensing environments and reduce cloud communication overhead and enable real-time environmental validation [22, 23]. However, the presence of a large number of compromised edge gateways is a significant threat as they can spoof the results of telemetry aggregation, modify the inference output or insert a spoofed hash in the path to the blockchain node anchoring. The models of machine learning have been more and more introduced for predictive SOC estimation, carbon flux analysis and ecological forecasting in the MRV systems. However, Adversarial Machine Learning Attacks raise new cybersecurity concerns in Distributed Environmental Infrastructure. For example, they can add poisoned teleme-try streams to a training data set or alter the way the model predicts using adversarial perturbations [24, 25]. In the current state of the art, MRV architectures do not include secure federated validation, ensemble trust verification or adversarial anomaly filtering mechanisms that would protect environmental prediction models [26].

Immune to editing of transaction records and the ability to audit transactions transparently, blockchain-based carbon registries also enhance forensic traceability [27]. But the immutability of blockchain doesn't ensure authenticity of the upstream sensing and computation layers. However, without adaptive trust evaluation mech-anisms, carbon verification processes can be compromised by validator collusion, fraudulent endorsement, or trust poisoning attacks.

For the cyber-physical and IoT environments, several distributed trust manage-ment models have been proposed. Dynamic trust computation frameworks are based on assessing node reliability in terms of behavioral consistency, anomaly evidence and past interaction patterns [28–30]. These approaches show the significance of adaptive trust orchestration in identifying malicious entities in the distributed sys-tems comprising heterogeneous systems. Most current trust frameworks, however, are not tailor-made for environmentally-distributed MRV ecosystems which include edge-assisted telemetry processing and blockchain-based carbon verification.

Table I summarizes major attack surfaces within distributed blue carbon MRV infrastructures.

These challenges highlight the necessity for a cyber-resilient MRV architecture capable of dynamically validating trust, protecting machine learning models, detecting malicious telemetry, and preserving secure environmental verification workflows.

Table 1 Major Attack Surfaces within Distributed Blue Carbon MRV Infrastructures

Layer	Potential Attack
Sensor Layer	Telemetry spoofing, replay attacks, calibration manipulation Edge Layer Malware injection, unauthorized access, hash manipulation Cloud Layer Trust poisoning, privilege escalation Blockchain Layer Validator collusion, fraudulent endorsement ML Layer Model poisoning, adversarial perturbation

3 Proposed AMTA-Sec Framework

The proposed AMTA-Sec framework models the distributed blue carbon MRV infrastructure as a cyber-physical trust network composed of sensing devices, edge gateways, cloud orchestration clusters, secure machine learning validation modules, and blockchain validators. The distributed system is represented as:

$$G = \{V, E\}, \quad (1)$$

where:

$$M = \{Si, Ej, Ck, Lm, Mp\}, \quad (2)$$

represent sensing nodes, edge gateways, cloud orchestration nodes, blockchain val-idators, and secure machine learning modules respectively. Each node maintains a dynamic trust score:

$$v(t)[0, 1] \quad (3)$$

which continuously evolves according to behavioral consistency, anomaly evidence, model integrity validation, and attack detection outcomes.

3.1 Sensing Layer

Distributed IoT sensors deployed across mangrove ecosystems continuously col-lect environmental telemetry including SOC values, salinity measurements, biomass indices, tidal variations, and hydrological parameters. Since sensing devices operate in physically exposed environments, they remain vulnerable to spoofing attacks, replay attacks, and calibration manipulation. To mitigate these threats, AMTA-Sec performs cross-sensor anomaly correlation and historical consistency analysis.

Sensor trust is computed using:

$$\tau_{Sj}(t) = \alpha_1 A_i(t) + \alpha_2 H_i(t) + \alpha_3 C_i(t) \quad (4)$$

where: Ai(t) represents anomaly conformity, Hi(t) represents historical reliability, Ci(t) represents calibration integrity. Sensors exhibiting abnormal environmental deviations experience trust degradation and temporary isolation.

3.2 Edge Processing and Integrity Validation Layer

Edge gateways deployed near coastal monitoring stations perform localized teleme-try aggregation, preliminary SOC estimation, anomaly detection, and batch integrity verification. Each edge node continuously validates telemetry batches using SHA-256 hash fingerprinting and behavioral resource monitoring. Compromised edge nodes are detected through: • Unexpected batch hash modifications • Sudden CPU utilization spikes • Abnormal communication frequency • Unauthorized firmware behavior Edge trust is computed as:

$$\tau_{Ej}(t) = \beta_1 U_j(t) + \beta_2 R_j(t) + \beta_3 I_j(t) \quad (5)$$

where: Uj(t) represents uptime consistency, Rj(t) represents resource stability, Ij(t) represents integrity validation.

3.3 Secure Machine Learning Protection Layer

Unlike conventional MRV systems, the proposed AMTA-Sec framework incorporates a dedicated secure machine learning validation layer to protect SOC estimation models against poisoning and adversarial attacks. The framework employs multiple security mechanisms:

3.3.1 Federated Model Validation

SOC models are trained using distributed environmental datasets collected from geo-graphically separated sensing clusters. Model updates are validated across multiple edge gateways before global synchronization.

3.3.2 Adversarial Input Filtering

Telemetry streams undergo adversarial consistency verification prior to model infer-ence. Sudden ecological inconsistencies, impossible tidal transitions, and statistically abnormal SOC fluctuations are rejected before model execution.

3.3.3 Model Integrity Verification

All machine learning models are hash-anchored within the blockchain layer to ensure model authenticity and prevent unauthorized model replacement.

3.3.4 Ensemble Trust Verification

Multiple SOC prediction models operate simultaneously across distributed edge clus-ters. Significant prediction deviations trigger anomaly alerts and retraining validation. The secure model trust update mechanism is represented as:

$$\tau_M(t+1) = \lambda \tau_M(t) + (1-\lambda) B_m(t) - \mu A_m(t) \quad (6)$$

where: Bm(t) denotes benign model behavior, Am(t) represents adversarial anomaly evidence.

3.4 Cloud Orchestration Layer

The cloud layer performs distributed trust aggregation, cross-site SOC valida-tion, transaction batching, and global environmental analytics. Cloud orchestration continuously evaluates:

- Cross-cluster telemetry consistency
- Distributed anomaly correlation
- Model inference reliability
- Multi-layer trust aggregation

Suspicious telemetry batches are quarantined before blockchain anchoring.

3.5 Blockchain Validation Layer

The blockchain layer employs a permissioned Hyperledger Fabric architecture to ensure tamper-

resistant carbon credit issuance and immutable forensic auditability. Validator trust is continuously evaluated according to:

- Consensus consistency
- Endorsement reliability
- Historical behavioral integrity
- Transaction approval deviation

The global trust score is computed as:

$$\tau_{global} = \omega_S\tau_S + \omega_E\tau_E + \omega_C\tau_C + \omega_L\tau_L + \omega_M\tau_M \quad (7)$$

where:

- τ_{global} represents the overall global trust score of the framework,
  - τ_S denotes the sensor trust score,
  - τ_E denotes the edge trust score,
  - τ_C represents the communication trust score,
  - τ_L indicates the blockchain ledger trust score,
  - τ_M represents the machine learning model trust score,
  - $\omega_S, \omega_E, \omega_C, \omega_L$, and ω_M are the weighting coefficients assigned to each trust component such that:

$$\omega_S + \omega_E + \omega_C + \omega_L + \omega_M = 1$$

Carbon credits are issued only when: $tau_{global} > \theta$ where θ represents the minimum acceptable trust threshold.

4 Secure Model Implementation And Protection Strategy

The proposed framework of AMTA-Sec takes an innovative approach by introducing an additional approach for defending the SOC estimation models against adversarial attacks and poisoning attempts focused on the protection of secure machine learning. In practical blue carbon monitoring applications, adversaries could try to trick the SOC prediction algorithm by adding fake environmental telemetry to training data sets. Slowly, these poisoning attacks can lead to a biased estimate of SOC and give rise to fake carbon credit values that are not discovered on the spot.

A proposed framework includes distributed and secure model validation within the edge and cloud orchestration layers to reduce these risks.

A. Federated Secure Model Training Distributed telemetry data from geographically-distributed mangrove sensing clusters is used to train SOC estimation models. The idea is to train local partial SOC models at the edge and only to for-ward validated model parameters to centralized servers. This approach provides a more streamlined exposure of unaltered telemetry, reduce the risk of central poisoning, greater privacy and environmental data protection and distributed trust validation.

B. Adversarial Detection Pipeline Environmental consistency validation is per-formed before the telemetry are fed into the SOC prediction engine - Temporal tidal verification, Salinity transition analysis, Biomass consistency correlation, Historical SOC deviation monitoring. Failure of ecological consistency threshold is rejected prior to model inference.

C. Model Integrity Anchoring Each version of the SOC that is validated is cryptographically hashed and linked to the blockchain layer.Each SUCCESSFULLY validated SOC version is cryptographically hashed and tied to the blockchain layer. This enables - Model authenticity verification wherein Unwanted model replacement is prevented. Immutable forensic reconstruction Model lifecycle management for Trust.

D. Ensemble Trust Validation, The framework is based on distributed ensemble SOC prediction on multiple edge clusters. When one prediction model is drastically different from the other models, the model's trust score is automatically lowered by the system. Model trust is updated regularly with the following:

$$\tau_M(t+1) = \lambda\tau_M(t) + (1-\lambda)B_m(t) - \mu A_m(t) \quad (8)$$

where hostile evidence dynamically affects degradation of trust.

E. Validator Reputation Management Blockchain validators are dynamically eval-uated using endorsement consistency and consensus behavior analysis. Validators exhibiting abnormal transaction approval behavior are automatically excluded from consensus participation. Table II summarizes the attack detection and mitigation mechanisms.

Table 2 Attack Detection and Mitigation Mechanisms

Attack	Detection Mechanism	Mitigation
Sensor spoofing	Environmental anomaly correlation	Trust degradation
Replay attack	Timestamp mismatch	Transaction rejection
Edge compromise	Hash integrity validation	Node isolation
Model poisoning	Ensemble inconsistency	Model quarantine
Validator collusion	Consensus deviation analysis	Validator exclusion

Algorithm 1 AMTA-Sec Secure Model Implementation and Protection Strategy

Require: Distributed telemetry streams T_i, sensing nodes S_i, edge gateways E_j, SOC models M_p
Ensure: Secure SOC prediction and trustworthy carbon verification Initialize global trust score τ_{global}
Initialize model trust $\tau_M(t)$ Initialize blockchain ledger L **for** each sensing node S_i **do**
Collect telemetry:
$T_i = \{SOC_i, Sal_i, Bio_i, Tide_i\}$
Compute sensing trust:
$\tau_{Si}(t) = \alpha_1 A_i(t) + \alpha_2 H_i(t) + \alpha_3 C_i(t)$
if $\tau_{Si}(t) < \theta_S$ **then**
Reject telemetry stream
Isolate compromised sensing node
else
Forward validated telemetry to edge gateway
end if end for
for each edge gateway E_j **do**
Perform temporal tidal verification Perform salinity transition analysis Perform biomass consistency correlation
Perform historical SOC deviation monitoring Compute edge trust:
$\tau_{Ej}(t) = \beta_1 U_j(t) + \beta_2 R_j(t) + \beta_3 I_j(t)$
if hash inconsistency OR abnormal behavior detected **then**
Quarantine telemetry batch Reduce $\tau_{Ej}(t)$
else
Train local SOC prediction model Generate local model parameters W_j
end if end for
Perform federated aggregation of validated model parameters
for each model update **do**
Execute ensemble SOC prediction validation
if prediction deviation exceeds anomaly threshold **then**
Trigger adversarial poisoning alert Mark model as suspicious
Increase adversarial evidence $A_m(t)$
else
Increase benign behavior score $B_m(t)$
end if

Update model trust:
$\tau_M(t+1) = \lambda\tau_M(t) + (1-\lambda)B_m(t) - \mu A_m(t)$

Generate SHA-256 fingerprint of validated SOC model Anchor model hash into blockchain ledger
Compute global trust score:
$\tau global = \omega S\tau S + \omega E\tau E + \omega C\tau C + \omega L\tau L + \omega M\,\tau M$
if $\tau_{global} \geq \theta$ **then**
Approve carbon credit issuance
Commit verified transaction to blockchain
else
Reject carbon credit transaction Trigger forensic investigation
end if
Return secure SOC estimation model and verified MRV transaction

5 Security and Performance Evaluation

5.1 Cyberattack Detection Accuracy

A prototype implementation of the proposed AMTA-Sec framework has been deployed in distributed edge-cloudblockchain environment with simulated blue carbon teleme-try datasets. The cyber resilience of the proposed architecture was assessed by running multiple cyberattack scenarios, such as telemetry spoofing, replay attacks, model poisoning, edge compromise and validator manipulation. The proposed AMTA-Sec framework was tested with various types of adverse attacks such as telemetry spoofing attacks, replay attacks, edge tampering attacks, validator manipulation attacks, and machine learning poisoning attacks. The attack-aware trust orchestration engine con-tinuously monitored the anomaly behavior, integrity validation results and consistency of consensus across distributed MRV layers, to detect malicious entities.

Figure 1 demonstrates the cyberattack detection performance of the proposed framework. The highest detection accuracy was observed for edge tampering attacks because the cryptographic SHA-256 integrity validation immediately detected unau-thorized batch modifications. Model poisoning attacks exhibited slightly lower detec-tion accuracy due to gradual adversarial perturbation patterns designed to evade immediate anomaly detection.

5.2 Secure SOC Model Protection Evaluation

Estimation models for SOC were tested with growing amounts of model poisoning to assess their resilience to adversarial model poisoning. The performance of the conven-tional centralized models deteriorated quickly as the prediction accuracy was tested

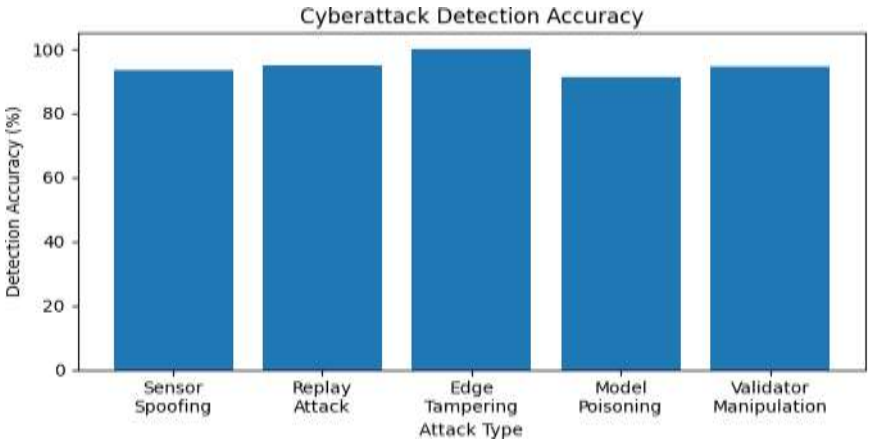

Fig. 1 Cyberattack detection accuracy of the proposed AMTA-Sec framework under multiple adver-sarial scenarios.

and validated in a federated manner, trust was validated in the ensemble model, and adversarial telemetry filtering prevented the rapid decay in prediction accuracy of the conventional centralized models.

As illustrated in Figure 2, the stability of the conventional MRV systems decreases with the increasing intensity of poisoning. On the other hand, the proposed AMTA-Sec architecture allows

for maintaining the prediction accuracy while being adversarial even in the presence of adversarial updates by separating out suspicious model updates and conducting distributed trust validation prior to synchronization.

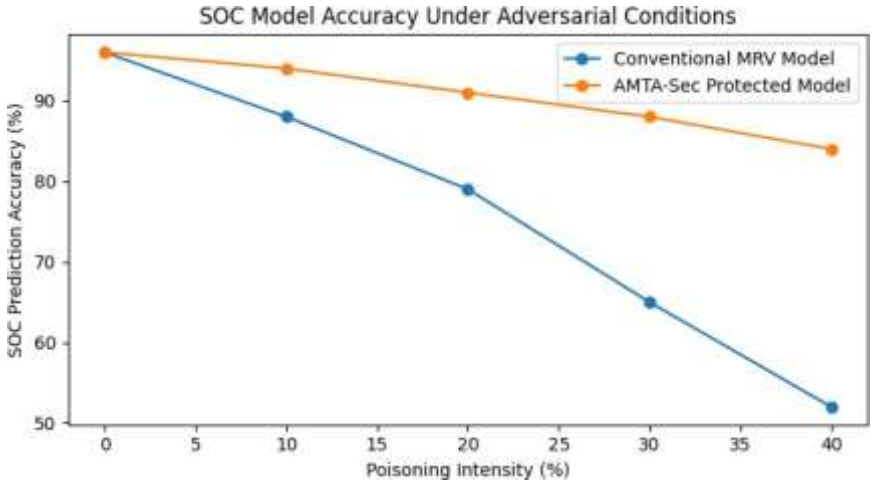

Fig. 2 SOC Model Accuracy Under Adversarial Conditions

This section will assess the latency and Blockchain Overhead.This portion eval-uates Latency and Blockchain Overhead. The proposed framework minimizes the computational burden of clouds by preprocessing the data on the edge and by aggregat-ing telemetry data in distributed manner. Additionally, Blockchain batch optimization reduced transaction overhead and maintained immutable auditability.

The average processing latency of conventional centralized MRV system and the proposed AMTA-Sec system are compared in figure 3. The edge-assisted trust orches-tration strategy achieved an average latency of 0.96 seconds, with no compromise to the secure environmental validation and real-time anomaly detection.

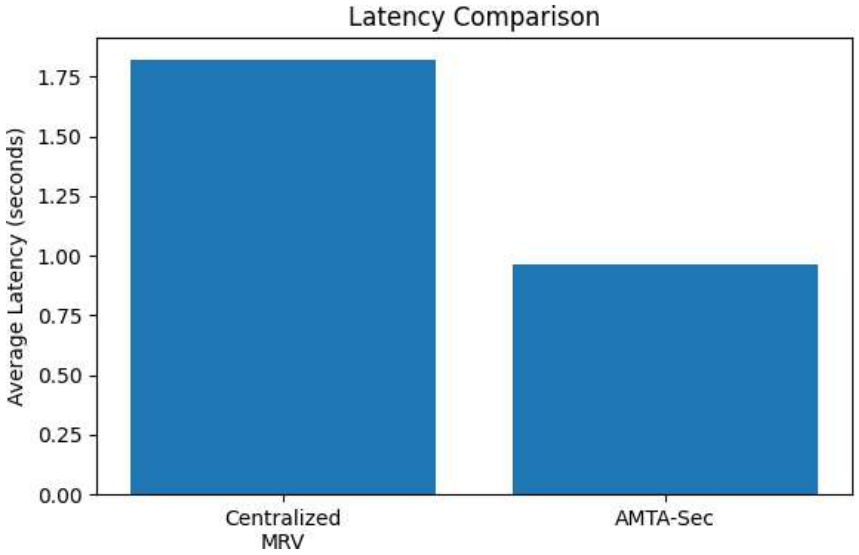

Fig. 3 Latency Comparison

6 Results and Discussion

This paper introduced an Adaptive Multi-Layer Trust Architecture (AMTA-Sec) for an attack-resilient distributed blue carbon MRV system. The proposed architecture extends the traditional MRV approach that leverages blockchain for managing the immutable ledger with additional components of distributed trust orchestration, secure machine learning protection, edge integrity verification, and

adversarial attack detec-tion at the sensing layer, edge layer, cloud layer, and blockchain layer. The proposed framework was experimentally analyzed under various cyber attack scenarios such as telemetry spoofing, replay attacks, edge tampering, model poisoning, and valida-tor manipulation. Experimental evaluation showed that the unifying of dynamic trust orchestration and anomaly correlation, federated model validation, and blockchain-assisted integrity verification enabled strong attack detection capabilities under all adversarial conditions. The framework managed to detect the sensor spoofing attack with a detection accuracy of 93.6%, 95.1% for replay attack detection accuracy, 94.4% for validator manipulation detection accuracy and 91.2% for adversarial model poi-soning attacks. The performance was highest in the case of edge tampering attack, where the distributed edge gateways are equipped with cryptographic integrity vali-dation mechanisms based on SHA-256.The best performance was achieved in the edge tampering attack where the distributed edge gateways are provided with the cryp-tographic integrity validation mechanisms based on SHA-256. For each of the SOC estimation models, the models were tested with respect to increasingly intense poi-soning levels of adversarial machine learning attacks. In experimental results it was shown that the model accuracy of the conventional centralized MRV models dropped significantly as the poisoning intensity increased from 0% to 40%, from 96% to 52%. The proposed AMTA-Sec protected model, on the other hand, showed a much higher stability and resilience and its prediction accuracy was preserved at 84% under 40% poisoning intensity, as verified on a federated level, by means of an ensemble and trust verifier, as well as adversarial telemetry filtering. Finally, the performance eval-uation indicated that the edge-assisted telemetry preprocessing and distributed trust orchestration greatly enhanced the operational efficiency. The proposed architecture achieved an average processing latency of 0.96 seconds in a conventional centralized MRV system, which was 1.82 seconds, while maintaining a secure environment that was validated, immutable, and capable of detecting anomalies in real time.

7 Conclusion

The paper suggested an Adaptive Multi-Layer Trust Architecture (AMTA-Sec) for securing Distributed blue carbon Monitoring, Reporting, and Verification (MRV) infrastructure in response to Cyber threats since their occurrence is dynamic. The framework brings together dynamic trust orchestration, secure federated machine learning validation, edge integrity verification, anomaly-aware telemetry analysis, and blockchain-assisted forensic traceability in sensing, edge, cloud, and ledger worlds.

The proposed architecture is different from the existing blockchain-based MRV sys-tems that are mostly about managing immutable transactions, as it adds attack-aware security mechanisms that can detect and counteract malicious actions at multiple dis-tributed layers. The framework enhances the authenticity of environmental telemetry, ensures that the SOC estimation models are not easily manipulated and increases the reliability of verification workflows for distributed carbon credits.

The proposed AMTA-Sec architecture further illustrates how trust-aware orches-tration and secure ML protection should be integrated in distributed cyber-physical systems in environmentally distributed systems. The framework combines feder-ated validation, cryptographic integrity verification, and adaptive anomaly detection, thereby providing superior operational resilience without compromising the scalable and timely environmental monitoring functions.

Furthermore, blockchain-based model anchoring and immutable audit logging enhance forensic traceability to ensure secure reconstruction of compromised teleme-try flows, malicious node activity and distributed attack propagation paths. These features are very relevant to geographically dispersed coastal ecosystems in which physical oversight or centralized trust assumptions are not feasible.

The proposed framework provides a secure and scalable base for next-generation environmental MRV infrastructures that will enable the development of trustwor-thy, transparent and tamper-resistant carbon accounting ecosystem. The plan for future research is to integrate Zero Trust Environmental Orchestration, AI-based Intrusion Prediction, Quantum-resistant Blockchain validation, Federated Anomaly Intelligence Sharing and Self-healing Distributed Trust Architectures to further bolster Cybersecurity resiliency in Distributed Environmental Monitoring Systems.

8 Funding Declaration:

No funding was received for conducting this study.

References

[1] T. P. Abiodun, N. I. Nwulu and P. O. Olukanmi, "Application of Blockchain Technology in Carbon Trading Market: A Systematic Review," IEEE Access, vol. 13, pp. 5446-5470, 2025,

doi: 10.1109/ACCESS.2024.3523672.
[2] M. Yan et al., "Blockchain for Transacting Energy and Carbon Allowance in Networked Microgrids," in IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 4702-4714, Nov. 2021, doi: 10.1109/TSG.2021.3109103.
[3] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-Enabled Secure Energy Trading With Verifiable Fairness in Industrial Internet of Things," in IEEE Trans-actions on Industrial Informatics, vol. 16, no. 10, pp. 6564-6574, Oct. 2020, doi: 10.1109/TII.2020.2974537.
[4] Z. Chen, M. Zhang, H. Zhang and Y. Liu, "Mapping Mangrove Using a Red-Edge Mangrove Index (REMI) Based on Sentinel-2 Multispectral Images," in IEEE Transactions on Geoscience and Remote Sensing, vol. 61, pp. 1-11, 2023, Art no. 4409511, doi: 10.1109/TGRS.2023.3323741.
[5] L. Bergamasco, S. Saha, F. Bovolo and L. Bruzzone, "Unsupervised Change Detection Using Convolutional-Autoencoder Multiresolution Features," in IEEE Transactions on Geoscience and Remote Sensing, vol. 60, pp. 1-19, 2022, Art no. 4408119, doi: 10.1109/TGRS.2022.3140404.
[6] M. E. Malerba, M. D. P. Costa, D. A. Friess, "Remote sensing for cost-effective blue carbon accounting," *Earth-Science Reviews*, vol. 238, p. 104337, 2023, doi: 10.1016/j.earscirev.2023.104337.
[7] D. Datta, M. Dey, P. K. Ghosh, S. Neogy, and A. K. Roy, "Coupling multi-sensory earth observation datasets, in-situ measurements, and machine learn-ing algorithms for total blue C stock estimation of an estuarine mangrove forest," *Forest Ecology and Management*, vol. 546, p. 121345, 2023, doi: 10.1016/j.foreco.2023.121345.
[8] Q. Li, J. Shi, K. Ni, R. Wang, C. Zhang, N. Yang, Y. Yang, Y. Shen, R. Guo, and Z. Liao, "A highly credible and efficient real-time carbon MRV + O system for delicacy management of distributed carbon abatement behaviors," *Applied Energy*, vol. 355, p. 122265, 2024, doi: 10.1016/j.apenergy.2023.122265.
[9] Y. Gao, X. Qiu, L. Xu, P. Zhang, A. Xu and X. Yan, "Blockchain-Based Car-bon Footprint Verification System: An Efficient Solution with Anti-Malicious Propagation," 2025 IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA), Shenyang, China, 2025, pp. 795-802, doi: 10.1109/ISPA67752.2025.00107.
[10] M. Oudani, A. Sebbar, K. Zkik, I. El Harraki, and A. Belhadi, "Green blockchain based IoT for secured supply chain of hazardous materials," *Computers and Industrial Engineering*, vol. 175, p. 108814, 2023, doi: 10.1016/j.cie.2022.108814.
[11] A. V. Hirlekar, "A decentralized blue-carbon MRV system and tokenized carbon credit marketplace with gasless transactions, IoT telemetry, and ML-driven SOC estimation," in *Proc. 6th International Conference on IoT Based Control Net-works and Intelligent Systems (ICICNIS)*, Bengaluru, India, 2025, pp. 882–889, doi: 10.1109/ICICNIS66685.2025.11315559.
[12] V. Hirlekar and B. Maram, "Blue Carbon Management and Carbon Credit Markets: A Review of Ecological, Technological, and Digital Frameworks," 2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC), Pathum Thani, Thailand, 2026, pp. 1496-1502, doi: 10.1109/ICAUC68182.2026.11441059.
[13] E. B. Ewane, P. P. Selvam, R. AlMealla, M. S. Watt, P. S. P. Arachchige, B. Bomfim, W. S. W. M. Jaafar, S. Salehian, T. Ali, N. Manickam, M. M. Abdullah, S. Westover, and M. Mohan, "Mangrove-based carbon mar-ket projects: What stakeholders need to address during pre-feasibility assess-ment," Journal of Environmental Management, vol. 374, p. 124074, 2025, doi: 10.1016/j.jenvman.2025.124074.
[14] T. Kuwae, A. Watanabe, S. Yoshihara, F. Suehiro, and Y. Sugimura, "Imple-mentation of blue carbon offset crediting for seagrass meadows, macroalgal beds, and macroalgae farming in Japan,"Marine Policy, vol. 138, p. 104996, 2022, doi: 10.1016/j.marpol.2022.104996.
[15] K. Alsafadi, A. K. Srivastava, K. Halder, F. Wang, S. Yang, and W. Cao, "A machine learning framework for modeling and upscaling mangrove carbon pro-ductivity (ML-MCP)," Agricultural and Forest Meteorology, vol. 375, p. 110821, 2025, doi: 10.1016/j.agrformet.2025.110821.
[16] M. E. Malerba, M. D. P. Costa, D. A. Friess, L. Schuster, M. A. Young, D. Lagomasino, O. Serrano, S. M. Hickey, P. H. York, M. Rasheed, J. S. Lefcheck, B. Radford, T. B. Atwood, D. Ierodiaconou, and P. Macreadie, "Remote sensing for cost-effective blue carbon accounting," Earth-Science Reviews, vol. 238, p. 104337, 2023, doi: 10.1016/j.earscirev.2023.104337.
[17] A. D. Roy, P. S. P. Arachchige, M. S. Watt, A. Kale, Remote sensing-based mangrove

blue carbon assessment in the Asia-Pacific: A systematic review," Science of The Total Environment, vol. 938, p. 173270, 2024, doi: 10.1016/j.scitotenv.2024.173270.

[18] A. S. M. Muñoz, Á. I. G. Alvis, and I. F. B. Mart´ınez, "A random forest model to predict soil organic carbon storage in mangroves from Southern Colombian Pacific coast," Estuarine, Coastal and Shelf Science, vol. 299, p. 108674, 2024, doi: 10.1016/j.ecss.2024.108674.

[19] T. L. Maxwell, T. Hengl, L. L. Parente, R. Minarik, T. A. Worthington, P. Bunting, L. S. Smart, M. D. Spalding, and E. Landis, "Global mangrove soil organic carbon stocks dataset at 30 m resolution for the year 2020 based on spa-tiotemporal predictive machine learning," Data in Brief, vol. 50, p. 109621, 2023, doi: 10.1016/j.dib.2023.109621.

[20] J. F. Montenegro, M. Mohan, E. B. Ewane, "Mangrove-based carbon market projects: Current trends and future perspectives," Forest Policy and Economics, vol. 181, p. 103658, 2025, doi: 10.1016/j.forpol.2025.103658.

[21] L. Vanderheyden, N. Gayot, and G. Van den Broeck, "What monitoring, report-ing, and verification (MRV) systems can reduce costs and enhance scalability of carbon farming?," Journal of Environmental Management, vol. 401, p. 128885, 2026, doi: 10.1016/j.jenvman.2026.128885.

[22] W. Hughes, T. Magnusson, A. Russo, and G. Schneider, "Cheap and secure metatransactions on the blockchain using hash-based authorisation and preferred batchers," Blockchain: Research and Applications, vol. 4, no. 2, p. 100125, 2023, doi: 10.1016/j.bcra.2022.10012 5.

[23] E. Barros, P. Misságia, O. Oliveira, W. Feroni, M. Missagia, V. Tesolini, R. Feroni, and T. Xavier, "Conceptual approach and fundamental aspects for a low-carbon energy matrix," Latin American Journal of Energy Research, vol. 12, pp. 57–72, 2025, doi: 10.21712/lajer.2025.v12.n4.p57-72.

[24] M. Dahl, P. Lavery, I. Mazarrasa, J. Samper-Villarreal, F. Adame, S. Crooks, C. Duarte, D. Friess, D. Krause-Jensen, C. Leiva-Dueñas, C. Lovelock, P. Macreadie, P. Masqu´e, M. Mateo, and O. Serrano, "Recommendations for strengthening blue carbon science," One Earth, vol. 8, p. 101175, 2025, doi: 10.1016/j.oneear.2025.101175.

[25] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social Internet of Things systems," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 6, pp. 684–696, Nov.–Dec. 2016, doi: 10.1109/TDSC.2015.2420552.

[26] L. Wang, Y. Li, and L. Zuo, "Trust management for IoT devices based on federated learning and blockchain," 2024, doi: 10.21203/rs.3.rs-4568992/v1.

[27] M. Yan et al., "Blockchain for Transacting Energy and Carbon Allowance in Networked Microgrids," in IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 4702-4714, Nov. 2021, doi: 10.1109/TSG.2021.3109103.

[28] M. Li, D. Hu, C. Lal, M. Conti and Z. Zhang, "Blockchain-Enabled Secure Energy Trading With Verifiable Fairness in Industrial Internet of Things," in IEEE Trans-actions on Industrial Informatics, vol. 16, no. 10, pp. 6564-6574, Oct. 2020, doi: 10.1109/TII.2020.2974537.

[29] Z. Chen, M. Zhang, H. Zhang and Y. Liu, "Mapping Mangrove Using a Red-Edge Mangrove Index (REMI) Based on Sentinel-2 Multispectral Images," in IEEE Transactions on Geoscience and Remote Sensing, vol. 61, pp. 1-11, 2023, Art no. 4409511, doi: 10.1109/TGRS.2023.3323741.

[30] L. Bergamasco, S. Saha, F. Bovolo and L. Bruzzone, "Unsupervised Change Detection Using Convolutional-Autoencoder Multiresolution Features," in IEEE Transactions on Geoscience and Remote Sensing, vol. 60, pp. 1-19, 2022, Art no. 4408119, doi: 10.1109/TGRS.2022.3140404.