EcoIntegrity: AI-Augmented Blockchain Framework for Carbon Footprint Tracking and Incentives in IoT

Liyuan Liu[1] and Meng Han[2(✉)]

[1] Saint Joseph's University, Philadelphia, PA 19131, USA
lliu@sju.edu
[2] Zhejiang University, Hangzhou 310027, Zhejiang, China
mhan@zju.edu.cn

Abstract. The accelerating demands for environmental sustainability necessitate the development of robust systems capable of meticulous carbon footprint tracking. This paper introduces "EcoIntegrity," an AI-augmented blockchain framework tailored for IoT environments to ensure transparent and accurate carbon footprint monitoring. Our comprehensive approach involves a three-phase solution that combines advanced AI algorithms, immutable blockchain technology, and an equitable incentive mechanism. The first phase harnesses IoT devices for data acquisition, emphasizing the need for precise and reliable data collection. This sets the foundation for the second phase, where AI, particularly recurrent neural networks and Local Outlier Factor algorithms, come into play. These algorithms are adept at predicting anomalous activities and emissions, thereby bolstering data integrity. The subsequent phase leverages the blockchain's secure ledger system to store the verified data, thereby fortifying the framework against potential breaches and ensuring data immutability. Furthermore, recognizing the collaborative nature of IoT networks in environmental monitoring, the framework integrates the Shapley value from cooperative game theory. This ensures a fair distribution of incentives among the IoT devices, encouraging accurate data reporting and collaboration. Our results demonstrate that "EcoIntegrity" not only streamlines carbon tracking but also significantly contributes to sustainable environmental management. Our proposed framework pioneers an intelligent framework for IoT-based carbon monitoring advances AI applications for integrity assurance, promotes blockchain for secure data storage, and fosters fairness through strategic reward distribution. The practical implications of our work extend to improved environmental reporting, regulatory adherence, and the promotion of sustainable practices within IoT networks.

Keywords: carbon footprint · artificial intelligence · blockchain · IoT · incentive mechanism

X. Li et al. (Eds.): SmartGift 2024, LNICST 600, pp. 159–181, 2025.
https://doi.org/10.1007/978-3-031-78806-2_10

1 Introduction

As global awareness of sustainability issues intensifies, the significance of carbon footprint tracking has escalated, drawing widespread attention across various sectors. This growing concern is underpinned by alarming environmental data: according to the Global Carbon Project, global CO2 emissions soared to approximately 36.4 gigatonnes in 2021, underscoring the critical need for effective monitoring and reduction strategies [1]. These emissions not only degrade the quality of human life but also contribute to overarching global problems, particularly climate change. In this context, the Intergovernmental Panel on Climate Change (IPCC) stresses the necessity of curtailing CO2 emissions to limit global warming to 1.5°C, highlighting the vital role of carbon footprint tracking in evaluating progress towards these climatic objectives [2]. The repercussions of climate change pose a threat to all life on Earth, propelling individuals and organizations alike to assume responsibility for environmental stewardship. Numerous corporations, for instance, are adopting ambitious sustainability targets, such as Microsoft's commitment to achieving carbon negativity by 2030 [3]. Precise carbon footprint measurement is crucial for these entities to assess and disclose their advancements accurately.

Beyond corporate initiatives, consumer attitudes are also shifting. A Nielsen report in 2020 revealed that 73% of global consumers are willing to alter their consumption patterns to lessen environmental impacts, underscoring the demand for transparent carbon footprint tracking [4]. In tandem with these societal changes, governmental bodies are instituting regulations to aid in carbon management. The European Union's Emissions Trading System (EU ETS), for example, plays a fundamental role in regulating emissions from key industrial sectors [5]. Moreover, carbon footprint tracking serves as a tool for enhancing energy efficiency. The industrial sector in the United States, accounting for 32% of the nation's total energy consumption in 2020, stands to benefit from such data-driven strategies [6]. Additionally, urban centers are leveraging smart technologies for carbon management. Copenhagen's goal to achieve carbon neutrality by 2025 exemplifies the use of carbon footprint data in steering urban development policies [7].

The Internet of Things (IoT) is a rapidly growing technology widely used in various fields, including smart homes, smart grids, and smart cities. Its widespread use has led to innovative applications, such as tracking and monitoring carbon footprints in different sectors. Research by Chakravarthi et al. [8] and Faize et al. [9] shows that smart grids can use IoT sensors and smart meters to monitor electricity use in real-time. This information is essential for calculating the carbon footprint from energy use, especially when it involves high carbon-emitting sources. Studies by Kokare et al. [10] and Ionescu et al. [11] focus on monitoring and controlling power consumption in real-time, highlighting the increasing range of IoT applications in energy management. Recent developments include IoT devices that can report carbon emissions directly. For instance, Hamidu et al. [12] developed a low-cost IoT sensor for monitoring greenhouse gases in industrial areas, emphasizing the accuracy and importance of IoT

in environmental protection. However, there are concerns about the reliability of these IoT-based carbon tracking systems. Security issues, like those exposed by the Mirai malware attack that infected networked IoT devices and created a controllable network of bots [13], show the vulnerabilities in IoT. Additionally, smart grids, which rely heavily on IoT technologies, have faced data breaches. In the energy sector, there have been cases of smart meters or energy consumption data being manipulated for inaccurate billing. The concerns surrounding data security and privacy in IoT devices have highlighted potential integrity issues in their use for tracking and monitoring carbon footprints in real-world scenarios. Moreover, when multiple IoT devices collaborate to monitor a single piece of equipment, the complexity increases. Therefore, it becomes crucial to design an effective incentive mechanism that encourages collaborative work among these diverse devices. This approach not only ensures the accurate collection of data but also fosters a cooperative environment among various IoT components involved in carbon footprint tracking. According to the integrity challenges we faced, we proposed the research questions below:

- How can advanced anomaly detection algorithms be integrated into IoT systems to enhance the integrity of carbon footprint tracking and monitoring?
- What are the most secure database architectures or technologies suitable for mitigating risks of hacking and data breaches in IoT networks focused on environmental monitoring?
- In the context of collaborative IoT systems working on unified tasks, what incentive models, based on principles of fairness and efficiency, can be effectively implemented to ensure fair reward distribution among participating devices?

Therefore, in this study, we have developed "EcoIntegrity," an AI-augmented blockchain framework with integrated incentive mechanisms for tracking and monitoring carbon footprints in IoT environments. This framework is specifically designed to address the research questions we have proposed. EcoIntegrity presents a groundbreaking AI-augmented blockchain framework, revolutionizing carbon footprint tracking in the IoT landscape. This paper explores EcoIntegrity's multifaceted approach to automate carbon reporting. The framework commences by utilizing IoT devices for comprehensive data collection, focusing on historical and behavioral aspects essential for accurate carbon footprint analysis. The next phase involves the deployment of AI algorithms for meticulous data scrutiny, targeting fraud detection to uphold reporting integrity. Subsequently, EcoIntegrity incorporates blockchain technology to securely record verified carbon data, enhancing transparency and trust in the process. Another novel aspect of EcoIntegrity is its incentive mechanism, employing the Shapley value method to equitably reward the collaborative efforts of IoT devices. This strategy aims to foster honest and precise data reporting. By integrating these advanced technologies, EcoIntegrity not only optimizes carbon footprint tracking but also signifies a significant stride towards sustainable environmental practices. Our main contribution can be concluded below:

- We developed EcoIntegrity, a three-phase intelligent framework designed to ensure the integrity of IoT-based carbon footprint tracking and monitoring. This framework uniquely integrates AI algorithms, blockchain technology, and an incentive mechanism, providing a comprehensive solution for environmental data integrity.
- Our approach utilizes recurrent neural networks and Local Outlier Factor (LoF) algorithms for the advanced prediction of anomalous activities and carbon emission prediction. This application of AI enhances the system's ability to detect and address data integrity issues effectively.
- We employ blockchain technology for the secure storage of carbon emission and energy consumption data. This not only ensures the safety and reliability of the data but also enhances transparency and traceability within the framework.
- Addressing the collaborative nature of IoT devices in environmental monitoring, we implement the Shapley value-a concept from game theory-to distribute rewards fairly among participating devices. This ensures equitable compensation based on each device's contribution to the task.
- Lastly, the real-world benefits of the EcoIntegrity framework are substantial. It offers a scalable, secure, and efficient solution for carbon footprint tracking, potentially leading to more accurate environmental reporting, enhanced regulatory compliance, and fostering a culture of sustainability and accountability in IoT networks.

The structure of the remainder of this paper is as follows: Sect. 2 presents the related works pertinent to this study. Section 3 details the three phases of the EcoIntegrity framework, elaborating on its design and functionality. Section 5 describes the experimental setup and discusses the results obtained from applying the EcoIntegrity framework. Finally, Sect. 6 concludes the paper, addressing its limitations and outlining potential directions for future research.

2 Related Works

2.1 Advanced Anomaly Detection and Prediction in IoT for Sustainability

This section delves into advanced anomaly detection techniques within the IoT framework, emphasizing their significance for sustainability. Numerous researchers have been developing various algorithms, including those for anomaly detection in IoT, aimed at enhancing sustainability. For instance, Gomez et al. [14] introduced a deep learning-based framework to combat the increasing threat of cyberattacks in industrial sectors, which threaten sustainability efforts. By creating precise anomaly detectors for industrial systems and implementing them in a water treatment facility, they achieved notable recall and precision rates, surpassing previous methods in identifying cyberattacks that affect sustainability. Mohamudally et al. [15] tackled the complexities of implementing Anomaly Detection Engines (ADE) within IoT networks. They assessed various

time series models for instantaneous anomaly detection to boost predictive maintenance and cybersecurity, ultimately favoring unsupervised machine learning as the most flexible and effective approach for IoT analytics. Singh et al. [16] proposed an adaptive machine learning framework utilizing Principal Component Analysis (PCA) for anomaly detection in the Oil and Gas industry. This method significantly reduced carbon emissions by accurately forecasting and analyzing shutdown events, aiding in achieving climate goals by improving system reliability and operational efficiency. Malik et al. [17] investigated an IoT-based system for the remote monitoring and control of photovoltaic (PV) installations. They underscored the integration of AI for anomaly detection and optimization to boost energy efficiency and reduce carbon emissions in the renewable energy sector.

Focusing on specific models for anomaly detection, supervised learning models such as Decision Trees, Support Vector Machines (SVM), and Neural Networks are commonly used. These models require labeled data to learn and predict anomalies. Alloghani [18] reviewed supervised deep learning techniques in IoT security, particularly assessing their effectiveness in intrusion detection within smart environments like agriculture, homes, and cities. Due to the occasional scarcity of labeled data, unsupervised models are also employed in anomaly detection within IoT. These include Clustering (e.g., K-Means, DBSCAN) and PCA, suitable for identifying outliers in data without labeled instances. For example, Habeeb et al. [19] developed a clustering-based algorithm named Streaming Sliding Window Local Outlier Factor Coreset Clustering Algorithms (SSWLOFCC) for anomaly detection in IoT technology. Deep neural networks and recurrent neural networks are effective for analyzing spatial data and time-series data, common in IoT devices, for predicting and detecting anomalies. Baojao et al. [20] reviewed threat detection algorithms in IoT, focusing on three models: Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU). Also, some researchers employed Generative Adversarial Networks (GANs) models to identify the anomalies in IoT devices. For example, Ullah et al. [21] developed a framework that utilizes conditional GANs (cGANs) to detect anomalies in IoT networks by generating realistic distributions for given feature sets to address data imbalance issues. This approach used a single class cGAN (ocGAN) to learn minority data classes and a binary class cGAN (bcGAN) for binary balance dataset augmentation, showing improved performance in anomaly detection metrics across several IoT datasets.

In reviewing the literature on anomaly detection within IoT systems, it becomes clear that there is a gap in the application of hybrid algorithms for enhancing the integrity of carbon footprint records in IoT devices. While considerable work has been done in applying artificial intelligence and machine learning for anomaly detection, the specific use of hybrid algorithms to improve the accuracy of carbon footprint data has not been extensively explored. This gap suggests an opportunity for developing a hybrid model that combines the strengths of multiple algorithms to better monitor and verify carbon emission data from IoT devices. Addressing this gap is crucial for improving

sustainability efforts and ensuring the accuracy of environmental impact assessments in the IoT domain, which in turn could lead to more effective carbon management strategies.

2.2 Blockchain for IoT Security

In the context of utilizing IoT devices for carbon footprint tracking, as mentioned in some studies [22], the issue of data security within these devices is a persistent challenge. IoT devices are known to collect a vast array of sensitive personal data critical for monitoring carbon footprints. A prime real-world application is smart energy meters, widely used in homes and businesses, which play a key role in monitoring energy consumption and carbon footprint. However, their data security is a pressing issue. Research from Oregon State University revealed that these devices could be hacked to cause power grid instability [23], underscoring the risk of sensitive data exposure that could reveal personal habits and occupancy.

Addressing IoT security challenges, current research increasingly explores the integration of blockchain technology into IoT devices. Blockchain, known for its decentralization, transparency, and immutability, offers a robust solution to enhance data security within IoT ecosystems. Such integration aims to preserve data integrity, providing a secure and transparent framework for data storage and management amidst evolving threats. Yu et al. [24] investigated blockchain's potential to resolve IoT security and privacy concerns, proposing a framework that combines blockchain with IoT to ensure data security and enable features like authentication and decentralized transactions, showcasing blockchain's applicability through practical instances. Tahir et al. [25] developed a blockchain-empowered IoT network tailored for healthcare, introducing a lightweight framework for authentication and authorization that employs random numbers and joint conditional probability to secure IoT device connections. Zhang et al. [26] proposed a blockchain-based security architecture for IoT, aimed at establishing a mutual trust environment among devices to facilitate reliable data exchange, addressing the critical need for a secure communication infrastructure within IoT networks. Moreover, blockchain's application extends to carbon footprint data tracking within IoT. Luo et al. [27] explored IoT's role in the food sector, particularly in reducing carbon emissions through enhanced supply chain transparency, notably in high-impact areas like meat production. Liu et al. [28] introduced a novel framework that combines carbon footprint calculation with blockchain technology, utilizing blockchain as a tool for transparent and secure carbon emission management. Niya et al. [29] presented a distributed system, powered by IoT and blockchain, for automated water and air quality monitoring, employing blockchain to securely store sensor data, thus ensuring the integrity of environmental monitoring data.

While the integration of blockchain technology into IoT devices has been increasingly explored to enhance data security and integrity, the specific focus on employing blockchain to ensure the integrity of carbon footprint tracking in IoT devices presents a notable research gap. This gap is particularly evident

when considering the potential for combining blockchain with game theory algorithms and AI to bolster the accuracy and reliability of carbon footprint data. Such an approach would not only address security vulnerabilities but also significantly contribute to the transparency and accuracy of carbon emissions tracking. This innovative combination could provide a robust framework for environmental monitoring and sustainability efforts, offering a new dimension to IoT applications in carbon footprint management.

2.3 Incentive Models in Collaborative IoT Systems

Collaborative IoT systems are pivotal in the realm of carbon footprint tracking, leveraging the interconnectedness of devices to offer a multifaceted view of emissions data. For instance, in smart cities, IoT sensors across transportation, residential, and industrial sectors can collectively monitor and analyze emissions, providing a holistic understanding of the city's environmental impact [30]. Similarly, in agriculture, the collaboration between IoT devices monitoring soil conditions, crop health, and equipment usage can optimize farming practices, reducing unnecessary resource consumption and associated carbon emissions [31–33]. This collaborative approach not only enhances the accuracy of carbon footprint assessments but also fosters targeted and effective sustainability measures, illustrating the critical role of inter-device cooperation in environmental conservation efforts.

However, in collaborative IoT systems aimed at environmental monitoring, ensuring consistent participation is challenging due to diverse stakeholders and technological variability. Incentives are essential here to motivate participants to share data [34], aligning individual contributions with collective environmental objectives and overcoming collaboration barriers, thereby enhancing the system's efficacy in carbon footprint reduction efforts. Several studies have developed incentive mechanisms within collaborative IoT systems to promote fairness and integrity in data sharing, ensuring that contributions are both recognized and secure. Lim et al. [35] proposed a federated learning-based approach with a hierarchical incentive mechanism to address incentive mismatches in mobile crowdsensing, facilitating collaborative machine learning among IoT devices without compromising data privacy. Ferreira et al. [36] developed a collaborative approach using IoT for parking control in cities, employing Bluetooth Low Energy (BLE) beacons and a reward mechanism to incentivize user participation. Yu et al. [37] introduced intelligent algorithms incorporating learning-enabled incentives and coalitional games to encourage resource sharing among IoT devices in 5G networks. Cheng et al. [38] presented a reverse auction-based incentive mechanism integrated with blockchain to motivate IoT managers to collaborate, aiming to minimize and stabilize incentive costs while ensuring privacy. Liu et al. [39,40] introduced a blockchain-based system for verifying education, employment, and skill information, employing a two-stage process with a game-based incentive mechanism to ensure accuracy and participation.

Yin et al. [41] introduced a collaborative sensing model for IoV, utilizing bidding and blockchain for enhanced participation and secure data exchange.

Collaborative IoT systems employ monetary and non-monetary incentives, leveraging game theory algorithms such as Vickrey-Clarke-Groves (VCG) [42], Stackelberg games, second-price auctions, and Shapley values to promote fair and secure data sharing. The VCG mechanism is often applied to maximize social welfare by encouraging truthful bidding [43], while Stackelberg games model the strategic interaction between leaders and followers in the system [44]. Second-price auctions are used to determine the optimal pricing strategy without overcharging [45], and Shapley values are employed to fairly distribute rewards among contributors based on their individual contributions to the collaborative effort [34]. These algorithms play a crucial role in aligning individual incentives with the collective goals of the IoT ecosystem, ensuring equitable participation and contribution.

The integration of IoT in environmental monitoring, especially in carbon footprint tracking, has progressed but faces a significant gap in data integrity and reliability. Current systems often miss a cohesive strategy that merges advanced analytics, secure data handling, and incentives for active engagement and accurate data collection. EcoIntegrity tackles this issue with an innovative framework that blends AI and blockchain, enhanced by a well-designed incentive scheme. AI, with a focus on deep learning and LoF algorithms, bolsters anomaly detection and data integrity, while blockchain provides data security and transparency. EcoIntegrity also introduces a fair incentive model using game theory's Shapley value, addressing the need for cooperative IoT environments in sustainability efforts. EcoIntegrity represents a major step forward in creating scalable, secure IoT systems for carbon tracking, enhancing reporting accuracy, and promoting sustainability within IoT networks.

3 Introduction to EcoIntegrity

The EcoIntegrity framework is structured around three distinct phases, each meticulously crafted to ensure fairness and integrity in monitoring carbon footprints using IoT devices. As illustrated in Fig. 1, the framework begins with the phase of data collection and anomaly detection, followed by the phase where data is stored securely using Blockchain and smart contracts. The final phase involves the distribution of rewards based on incentives, completing the comprehensive approach to environmental monitoring.

Phase 1: The initial stage of the EcoIntegrity framework is devoted to the meticulous acquisition and analysis of carbon emission data from IoT devices. Aimed at constructing an extensive and varied dataset, this phase intricately reflects the operational behaviors and environmental impact of these devices. The strategy for data collection is comprehensive, incorporating an array of sensors and techniques that extend from direct emission measurements to indirect evaluations based on usage patterns and energy consumption. Following data collection, the EcoIntegrity framework employs LOF algorithms to discern anomalies within the dataset-data points that markedly diverge from established patterns. Such outliers may reveal operational inefficiencies, like heightened energy usage

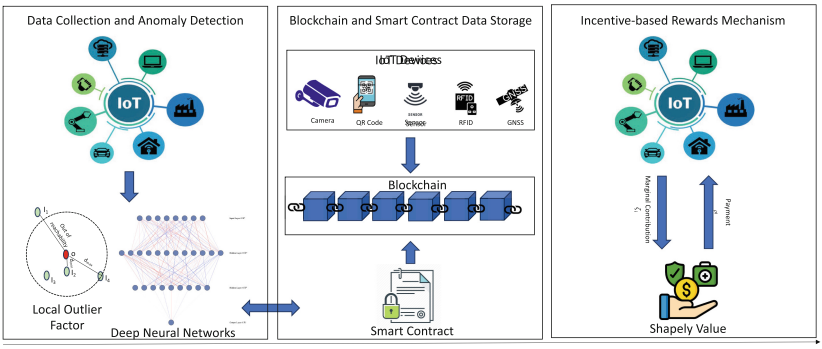


Fig. 1. Overview of EcoIntegrity

or irregular usage patterns, or suggest possible device malfunctions that could erroneously elevate reported emissions. In tandem, RNNs, such as LSTM, recognized for their proficiency in processing sequential and time-series data, are utilized for behavior analysis of IoT devices. LSTM is particularly effective for predicting future emissions based on historical patterns, thereby contributing to a deeper understanding of device behavior over time. This dual-analytic approach serves not only to identify irregularities in emission reporting but also to bolster the cybersecurity aspects of the framework. Through the continuous analysis of data, LSTM aids in detecting signs of security compromises or unauthorized intrusions, enhancing the protective measures of the system, and ensuring the integrity of the data collection phase.

Phase 2: In the transition to the second phase, the EcoIntegrity framework shifts its focus from the initial collection of data to its strategic management and storage, leveraging the core attributes of blockchain technology: decentralization, transparency, and immutability. This phase is fundamentally about securing the integrity and accessibility of the carbon emission data and the insights gleaned during the anomaly detection stage. The decentralized nature of blockchain eliminates central points of failure, thereby enhancing the resilience and reliability of the data storage system. The transparency inherent in blockchain technology allows for every transaction and data entry to be visible to all participants in the network, subject to privacy controls. The immutability of blockchain ensures that once data or a transaction has been recorded, it cannot be altered retroactively. Smart contracts play a pivotal role in this phase, acting as self-executing contracts with the terms of the agreement directly written into lines of code. These contracts autonomously enforce and execute the predefined rules and operations, such as data storage protocols and access permissions. In the context of EcoIntegrity, smart contracts are used to store not only the raw and analyzed emission data but also the algorithms and parameters defining baseline behaviors and operational norms. This codification into the blockchain ensures that the methodologies used for emission monitoring and anomaly detection are transparent, consistent, and tamper-proof. IoT devices first register with

the central authority, undergoing authentication via asymmetric cryptography to ensure secure communication. Following registration, devices either directly report carbon emissions using onboard sensors or estimate emissions based on operational data. This emission information is then encrypted using the device's private key for authenticity. For secure and private storage on the blockchain, emission data is hashed and accompanied by a zero-knowledge proof (ZKP), allowing devices to prove data validity without revealing the actual data. This process ensures that emission reporting and storage are both secure and privacy-preserving, leveraging cryptographic techniques to maintain data integrity and confidentiality within the blockchain-based EcoIntegrity framework.

Phase 3: EcoIntegrity's final phase embodies the essence of the platform's commitment to environmental integrity by leveraging the Shapley value, a sophisticated concept from cooperative game theory, to establish a transparent and equitable reward mechanism. This meticulous approach evaluates the contributions of IoT devices towards reducing the carbon footprint, taking into account not only direct emission reductions but also efficiency improvements and the implementation of sustainable operational practices. Each device's contribution is quantitatively assessed, ensuring that rewards are allocated in a manner that accurately reflects the device's impact on environmental sustainability. The integrity of the EcoIntegrity system is further upheld by the transparent application of the Shapley value, which ensures that the reward distribution is not only fair but also based on a clear and logical assessment of each device's marginal contribution to the collective goal of carbon footprint reduction. This methodical approach to reward allocation underlines the system's dedication to fairness, encouraging broader adoption of sustainable practices among IoT device operators. By integrating the Shapley value, EcoIntegrity not only incentivizes eco-friendly behavior but also establishes a framework where the integrity of contributions and rewards is paramount. This fosters trust among participants, ensuring that the system remains robust, transparent, and focused on its core mission of promoting environmental sustainability through technological innovation.

4 Formulation of EcoIntegrity

In the foundational phase of the EcoIntegrity framework, the dataset D is constructed from data points d_i, where $i = 1, 2, \ldots, n$, and n represents the total number of data points collected from IoT devices. Each data point d_i can be represented as a tuple containing emissions data, usage patterns, and power consumption metrics, denoted as $d_i = (e_i, u_i, p_i)$. The data collection integrates a range of sensors S and methodologies M, leading to a comprehensive dataset:

$$D = \bigcup_{j=1}^{s} S_j \cup \bigcup_{k=1}^{m} M_k$$

where s is the number of sensors and m is the number of methodologies employed. Upon aggregation, the dataset D undergoes analysis through LoF algorithms and

LSTM models. The LoF algorithm identifies anomalies by calculating the local density deviation of a given data point d_i with respect to its neighbors. The anomaly score, $A(d_i)$, for each data point is given by:

$$A(d_i) = \text{LoF}(d_i, \text{Neighbors}(d_i))$$

where $\text{Neighbors}(d_i)$ represents the neighboring data points of d_i. Parallelly, LSTM models are employed to uncover complex patterns within the dataset D. The function f_{LSTM} represents the LSTM model that maps input data points to an output space that highlights intricate patterns and correlations:

$$f_{LSTM} : d_i \mapsto o_i$$

where o_i represents the output indicating patterns, correlations, or features identified by the LSTM model from data point d_i. This dual-layered analytical approach ensures a robust examination of the IoT devices' emissions data, enhancing the framework's ability to detect deviations and potential cybersecurity threats within the dataset D. The LOF-LSTM model within EcoIntegrity, outlined in Algorithm 1, serves dual functions: it detects anomalies in IoT carbon emissions data and predicts irregular activities. Initially, LOF identifies outliers by assessing local density variations, highlighting potential inefficiencies. Then, the LSTM component, proficient in handling time-series data, predicts future anomalies by learning from both standard and atypical patterns. This combination enhances EcoIntegrity's ability to proactively manage environmental impacts, improving the sustainability of IoT devices.

Transitioning into Phase 2, the EcoIntegrity framework shifts its focus towards the strategic management and secure storage of carbon emission data, leveraging the inherent strengths of blockchain technology such as decentralization, transparency, and immutability. This phase is characterized by a series of key formalizations, each building upon the last to create a robust and secure data management system. At the heart of Phase 2 lies the seamless integration of blockchain technology, signified by:

- A blockchain $B = \{b_1, b_2, \ldots, b_n\}$, with each block b_i serving as a repository for a set of transactions T_i.
- Transactions $t \in T_i$, each encapsulating vital emission data or insights, are meticulously structured as $t = \{\text{data}, \text{signature}, \text{timestamp}\}$, ensuring clarity and traceability.

Building on the foundation of blockchain integration, the framework enhances $\text{Visibility}(t) \forall t \in T_i$ within each block $b_i \in B$, promoting unparalleled transparency and accessibility to all network participants. A cornerstone of blockchain technology, immutability, is rigorously enforced through:

$$\text{Hash}(b_i) = \text{Hash}(\text{PrevHash}(b_{i-1}) + \text{Hash}(T_i) + \text{Nonce}), \tag{1}$$

ensuring that once data is recorded, it becomes an immutable part of the blockchain. Further fortifying Phase 2 are smart contracts, denoted as SC, which

Algorithm 1. Advanced Integrated LOF-LSTM Model for Anomaly Detection and Carbon Emission Prediction

Input: Time-series dataset $D = \{d_1, d_2, \ldots, d_n\}$, where $d_i = (e_i, u_i, p_i)$ represents emissions, usage, and power data
Output: Anomaly scores $\text{LOF}_k(d_i)$ and LSTM-based insights
procedure EnhancedLOF(D, k)
  for $i = 1$ to n **do**
    Compute k-distance: $d_k(d_i) = \min\{d(d_i, d_j) | d_j \in N_k(d_i) \setminus \{d_i\}\}$
    for each $d_j \in N_k(d_i)$ **do**
      Compute reachability distance: $rd_k(d_i, d_j) = \max\{d_k(d_j), d(d_i, d_j)\}$
    end for
    Compute LRD: $\text{LRD}_k(d_i) = \left(\frac{1}{|N_k(d_i)|} \sum_{d_j \in N_k(d_i)} rd_k(d_i, d_j)\right)^{-1}$
    Compute LOF score: $\text{LOF}_k(d_i) = \frac{1}{|N_k(d_i)|} \sum_{d_j \in N_k(d_i)} \frac{\text{LRD}_k(d_j)}{\text{LRD}_k(d_i)}$
  end for
end procedure
procedure AdvancedLSTM(D)
  Initialize LSTM parameters Θ
  for each time step $t = 1$ to T **do**
    Compute the forget gate: $f_t = \sigma(W_f \cdot [h_{t-1}, d_t] + b_f)$
    Compute the input gate: $i_t = \sigma(W_i \cdot [h_{t-1}, d_t] + b_i)$
    Compute the cell candidate: $\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, d_t] + b_C)$
    Compute the cell state: $C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$
    Compute the output gate: $o_t = \sigma(W_o \cdot [h_{t-1}, d_t] + b_o)$
    Compute the new hidden state: $h_t = o_t * \tanh(C_t)$
  end for
  return Hidden states h_t and cell states C_t as LSTM-based insights for each time step
end procedure
Combine insights from EnhancedLOF and AdvancedLSTM for a comprehensive environmental impact analysis

act as self-executing contracts with predefined rules and operations, encapsulating data storage protocols and access permissions within immutable lines of code. A pivotal aspect of Phase 2 involves:

$$\text{DeviceKeyPair} = (\text{PublicKey}, \text{PrivateKey}), \tag{2}$$

facilitating secure communication and authentication of IoT devices within the framework.

$$\text{Signature} = \text{Sign}(\text{PrivateKey}, \text{Data}), \tag{3}$$

ensuring the authenticity and integrity of the transmitted data. To round off Phase 2, the framework employs advanced cryptographic techniques to ensure data privacy and security, including:

$$\text{EncryptedData} = \text{Encrypt}(\text{PublicKey}, \text{Data}) \tag{4}$$

These interconnected formalizations coalesce to ensure that Phase 2 of the EcoIntegrity framework not only adheres to the principles of blockchain technology but also advances the framework's mission to secure the integrity and confidentiality of carbon emission data through sophisticated cryptographic techniques.

In the final phase of the EcoIntegrity framework, the essence of the platform's commitment to environmental integrity is captured through the application of the Shapley value, a concept derived from cooperative game theory. This phase is characterized by the following formulation: Given a set of IoT devices $N = \{1, 2, \ldots, n\}$ and a characteristic function $v : 2^N \to \mathbb{R}$ that assigns a total value to each coalition of devices, the Shapley value for device i is given by:

$$\psi_i(M) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(n - |S| - 1)!}{n!} (M(S \cup \{i\}) - M(S)) \tag{5}$$

where:

- S is a subset of N not containing device i.
- $|S|$ denotes the number of devices in subset S.
- $M(S \cup \{i\}) - M(S)$ represents the incremental contribution of device i to the monitoring and tracking effectiveness of the coalition S.

This formulation ensures that the reward for each IoT device is proportional to its marginal contribution to the collective goal of reducing the carbon footprint, considering both direct emission reductions and efficiency improvements.

The effectiveness of each IoT device in monitoring and tracking carbon footprint is quantitatively evaluated based on a blend of emission data accuracy, operational efficiency, and adherence to data reporting standards, formalized as:

$$M_i = \alpha A_i + \beta(1 - O_i) + \gamma R_i \tag{6}$$

where:

- M_i is the monitoring effectiveness score of device i.
- A_i quantifies the accuracy of the emission data captured by device i.
- O_i is the operational downtime rate of device i, with $1 - O_i$ indicating operational efficiency.
- R_i denotes the device's adherence to reporting standards and frequency for device i.
- α, β, γ are weighting coefficients that signify the relative importance of each aspect in the overall effectiveness.

The integration of the Shapley value ensures that the EcoIntegrity framework not only incentivizes eco-friendly behavior but also establishes a fair and transparent system for rewarding contributions, thereby fostering trust and encouraging the broader adoption of sustainable practices. Algorithm 2 illustrates how the Shapley Value algorithm strengthens EcoIntegrity by ensuring each IoT device's contributions to carbon tracking are assessed fairly and transparently. It deters

data manipulation by evaluating each device's impact in different network setups, thus enhancing collective data reliability. This method fosters trust and cooperation within the IoT ecosystem by quantitatively acknowledging contributions to improved monitoring, aligning with the framework's goal of precise environmental data oversight.

Algorithm 2. Shapley Value Calculation for IoT Payments

Input: Set $N = \{1, \ldots, n\}$, Effectiveness M
Output: Shapley ψ_i for each $i \in N$
procedure ShapleyValues(N, M)
  for $i \in N$ **do**
    $\psi_i \leftarrow 0$
    for all $S \subseteq N \setminus \{i\}$ **do**
      $MC \leftarrow M(S \cup \{i\}) - M(S)$
      $\psi_i \leftarrow \psi_i + \frac{|S|! \cdot (n-|S|-1)!}{n!} \cdot MC$
    end for
  end for
  return $\{\psi_i\}_{i=1}^{n}$
end procedure

We present a mathematical proof to demonstrate that the Shapley value serves as an effective incentive mechanism ensuring fairness and integrity in the context of IoT devices monitoring and tracking carbon footprints. The Shapley value is defined by four key properties, as outlined below [34]:

Property 1 (Efficiency). Efficiency in Shapley value allocation ensures that the total effectiveness is fully distributed:

$$\sum_{i \in N} \psi_i = M(N)$$

Property 2 (Symmetry). It ensures equal rewards for equal contributions. If $M(S \cup \{i\}) = M(S \cup \{j\})$ for any $S \subseteq N \setminus \{i, j\}$, then $\psi_i = \psi_j$.

Property 3 (Dummy Player). A device i with no marginal contributions ($M(S \cup \{i\}) = M(S)$ for all $S \subseteq N \setminus \{i\}$) receives $\psi_i = 0$, ensuring integrity by not rewarding non-contributory devices.

Property 4 (Additivity). For any two effectiveness functions M_1 and M_2, the Shapley value satisfies $\psi_i(M_1 + M_2) = \psi_i(M_1) + \psi_i(M_2)$ for all $i \in N$. This property ensures that the Shapley value behaves consistently across different monitoring scenarios or combined effectiveness measures, reinforcing the integrity of the incentive mechanism.

Theorem 1. *Shapley values ψ_i ensure fairness and integrity in distributing rewards among IoT devices in N based on their contributions to the network's effectiveness M.*

Proof. The properties of efficiency, symmetry, dummy player, and additivity ensure that rewards are distributed fairly and in proportion to the actual contributions, maintaining fairness and integrity in the reward system.

5 Experiments and Results

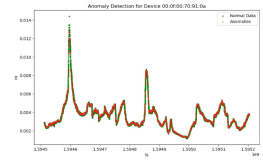
5.1 Anomaly Detection and Carbon Emission Prediction

For Phase 1, our experimental design aims to demonstrate the advantages of the hybrid model, particularly in enhancing anomaly detection and the performance of carbon emission predictions through the integration of LOF algorithms.

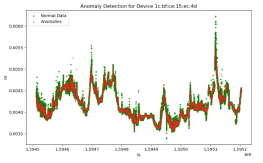
Dataset Description: The dataset utilized is the publicly available Environmental Sensor Telemetry Dataset, sourced from Kaggle.com [46]. The dataset under examination was generated by an intricate network of three identical, custom-engineered sensor arrays, each linked to a Raspberry Pi device. These arrays, embodying the essence of IoT technology, were strategically positioned across diverse environmental settings to capture a broad spectrum of data. Specifically, the deployment locations included an area characterized by stable, cooler, and more humid conditions, a second locale subject to highly fluctuating temperature and humidity levels, and a third setting known for its consistently warmer and drier atmosphere. The IoT devices, were distinguishable by three unique devices and meticulously recorded seven distinct types of sensor data, encompassing temperature, humidity, carbon monoxide (CO), liquid petroleum gas (LPG), smoke, light, and motion metrics. The comprehensive dataset, spanning a week from July 12, 2020, to July 19, 2020, encompasses a total of 405,184 data entries. Each data record was meticulously timestamped and transmitted as a single MQTT message payload, adhering to the ISO-standardized Message Queuing Telemetry Transport (MQTT) network protocol.

Experiments Design and Discussion: In our first experiment of Phase 1, we embarked on a detailed investigation of environmental sensor data, leveraging the LOF algorithm to identify anomalies across three IoT devices. In our analysis, the LOF algorithm was meticulously configured with specific parameters to optimize its performance for detecting anomalies within the IoT sensor data. The parameter "$n_{neighbors}$" set at 20, was chosen to define the number of neighboring points considered when calculating the local density deviation of a given data point, thus balancing sensitivity to local anomalies against the broader data context. Additionally, the "contamination" parameter was set to 0.1, indicating an estimated proportion of outliers in the data, guiding the LOF algorithm in thresholding anomaly scores. This careful parameterization of the LOF model was pivotal in tailoring the anomaly detection process to the nuanced characteristics of the environmental sensor dataset, ensuring both precision and reliability in identifying data points that deviated significantly from established patterns.

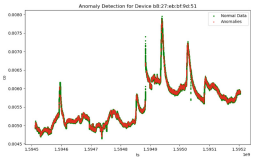
Figures 2a, 2b, and 2c show the anomalies and normal activities for each IoT device, delineating normal data points in green, symbolizing standard environmental readings, and anomalies in red, highlighting deviations from the norm.



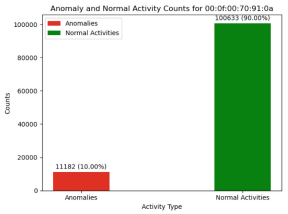
(a) Anomaly Detection for Device 1



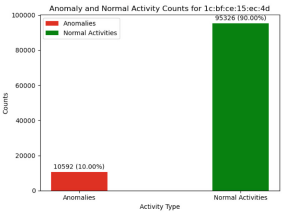
(b) Anomaly Detection for Device 2



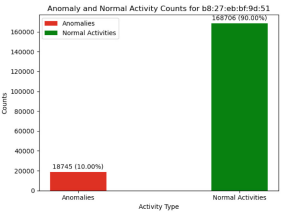
(c) Anomaly Detection for Device 3



(d) Anomaly and Normal Activity Counts for Device 1



(e) Anomaly and Normal Activity Counts for Device 2



(f) Anomaly and Normal Activity Counts for Device 3

Fig. 2. Anomaly detection results and activity counts for three devices (Color figure online)

These visualizations provided an intuitive understanding of the data's distribution and the LOF algorithm's effectiveness in isolating outliers. From these figures, we found that Device 1, situated in stable, cooler, and more humid conditions, shows distinct peaks where anomalies were detected. Device 2, exposed to highly variable temperatures and humidity, presents a more frequent occurrence of anomalies, reflecting the unstable environmental conditions. Device b8:27:eb:bf:9d:51, operating in warmer and drier conditions, shows fewer anomalies than Device 3, indicating more stable conditions but still with noticeable deviations at specific instances. Figures 2d, 2e, and 2f show the count of normal and anomalous readings captured over the experimental period. Each device shows a consistent pattern where approximately 90% of the data is classified as normal and 10% as anomalies. This consistency underlines the LOF algorithm's ability to discern and maintain a proportionate detection rate across varying environments. The findings suggest that the LOF algorithm is effectively identifying deviations in sensor data that could potentially skew the accuracy of subsequent CO emission predictions.

To verify the hybrid model is better than using LSTM to predict the carbon emission directly, we conducted our second experiment in Phase 1. Our experimental design was meticulously crafted to assess the performance of an LSTM neural network in predicting CO emissions from IoT devices, both before and after the application of the LOF anomaly detection. The dataset was normalized using MinMaxScaler to scale the features, including humidity, light, LPG, motion, smoke, temperature, and CO levels, to a uniform range between 0 and

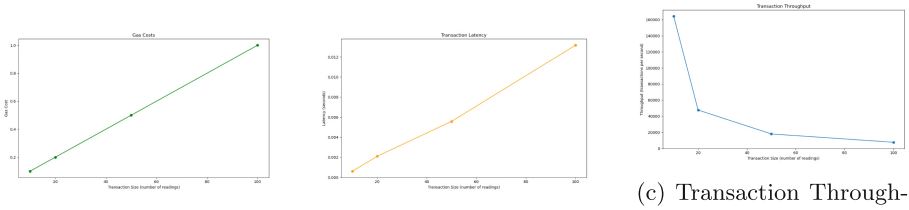
1, enhancing the model's ability to learn from the data effectively. For the LSTM architecture, we employed a sequential model with two LSTM layers, each consisting of 50 units. The first LSTM layer was designed to return sequences, setting the stage for the second LSTM layer to capture long-term dependencies. This design choice was pivotal in recognizing patterns over sequences of 10-time steps, reflective of the temporal nature of environmental data. The model was compiled with the Adam optimizer and mean squared error loss function, indicative of the emphasis on minimizing prediction errors. Figure 4a illustrates the comparative analysis of Root Mean Square Error (RMSE) values for three distinct IoT devices before and after the application of the LOF for anomaly detection. Prior to implementing LOF, the RMSE values for the devices were significantly higher, indicating a less accurate model for CO emissions prediction. Specifically, Device 1 exhibited an RMSE of 4.56, Device 2 was at 5.54, and Device 3 showed a value of 2.66, reflecting considerable prediction error. Post-LOF application, a substantial decrease in RMSE values across all devices was observed, suggesting a notable enhancement in the predictive accuracy of the LSTM model. This substantial reduction in RMSE underscores the effectiveness of integrating LOF as a preprocessing step to eliminate outliers that can potentially skew the predictive performance of machine learning models.

5.2 Blockchain and Smart Contract Data Storage

In this Phase, the dataset we used is simulated. We use Python to simulate a local blockchain environment. The object of the first experiment in this Phase is to evaluate the efficiency of blockchain storage for IoT carbon footprint data and the integrity of the data once it's stored on the blockchain. For our simulation, we deployed a custom class representing the smart contract and another encapsulating the blockchain's functionality. We simulated IoT devices transmitting data in varying sizes, ranging from 10 to 100 individual readings per transaction, to mimic the variable loads expected in a real-world scenario. Each "transaction" consisted of randomly generated data representing carbon emissions readings. The LOF was configured with 20 neighbors and a contamination factor of 0.1 to filter out anomalies before storage, representing pre-validation efforts. We tracked the latency from data transmission to confirmation on the blockchain, the transaction throughput to determine the system's capacity, and the simulated gas costs for each transaction to estimate operational expenses.

Figure 3a depicts a linear increase in gas costs with the transaction size, indicating that as the volume of data in a single transaction increases, so does the cost of processing that transaction. This is expected in blockchain networks where larger data payloads require more computational resources to validate and record. Figure 3b shows an upward trend in transaction latency as the size of the transaction grows. This suggests that larger transactions take longer to be confirmed on the blockchain, which is consistent with the need for more extensive validation processes that come with increased data size. Figure 3c presents a decrease in transaction throughput as the transaction size increases. This inverse

relationship highlights the trade-off between data granularity and system performance; while larger packets of data provide more detailed information per transaction, they also slow down the overall rate at which the system can process transactions. These findings collectively provide valuable insights into the scalability and cost-effectiveness of blockchain solutions for IoT environmental data management. They underscore the need for optimizing the balance between transaction size, cost, and latency to ensure a sustainable and efficient blockchain framework for large-scale IoT data integration.



(a) Gas Costs (b) Transaction Latency (c) Transaction Throughput

Fig. 3. Blockchain performance metrics: Gas costs, latency, and throughput

5.3 Shapley Value-Based Rewards Distribution

In this phase, the experiment is meticulously crafted to demonstrate the equity of the Shapley Value mechanism. The core objective is to validate Shapley Value as an equitable incentive model that motivates IoT devices to contribute effectively to carbon footprint monitoring within our proposed framework. The initial experiment is structured to evaluate the monitoring efficacy of three distinct IoT devices, each with unique operational characteristics. The devices were chosen based on their diverse performance metrics to simulate real-world scenarios. This experimental setup allows us to explore the nuances of how the Shapley Value can serve as a fair and incentivizing tool for IoT devices engaged in environmental sustainability efforts. The effectiveness score for each device, denoted as M_i, is calculated using the formula:

$$M_i = \alpha A_i + \beta(1 - O_i) + \gamma R_i$$

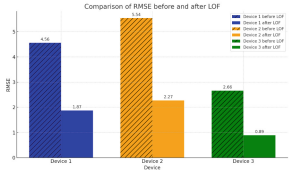
where A_i represents the accuracy of emission data, O_i denotes operational downtime, and R_i signifies adherence to reporting standards. The coefficients α, β, and γ are set to 1, indicating equal importance of all factors. The devices were characterized as follows to reflect realistic operational conditions:

– **Device 1:** Exhibited high accuracy ($A_i \approx 1.0$), minimal downtime ($O_i \approx 0$), and strong adherence to reporting standards ($R_i \approx 1.0$), making it highly effective in environmental monitoring.

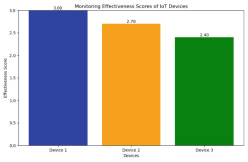
- **Device 2:** Demonstrated moderate levels across all parameters ($A_i, 1 - O_i, R_i \approx 0.9$), indicating average effectiveness.
- **Device 3:** Showed lower accuracy ($A_i \approx 0.8$), higher downtime ($O_i \approx 0.2$), and reduced adherence to reporting standards ($R_i \approx 0.8$), marking it as the least effective among the three.

This structured approach allows for a comprehensive comparison of the devices' capabilities in monitoring environmental data, which is visually represented through effectiveness scores in the results section. Figure 4b illustrates the monitoring effectiveness scores for these three distinct IoT devices. Device 1's highest effectiveness score of 3.0 can be attributed to its high data accuracy, almost negligible downtime, and strong adherence to reporting standards. These characteristics render Device 1 exceptionally reliable and efficient in environmental monitoring tasks, underlining its suitability for scenarios where precision and continuous operation are critical. Device 2 with an effectiveness score of 2.7, presents a case of balanced operational parameters. Its moderate accuracy, downtime, and adherence to reporting standards (all parameters approximately 0.9) suggest that the effectiveness score is slightly lower than Device 1. Device 3, which scored 2.4 is the lowest among the three devices. Secondly, we explored the allocation of a fixed budget across three IoT devices engaged in carbon footprint tracking, employing three distinct distribution methods: Shapley Value, Equal Distribution, and Random Distribution. The Shapley Value method allocates the budget based on each device's marginal contribution to the collective effort, ensuring a fair distribution that acknowledges individual contributions. Equal Distribution, in contrast, divides the budget equally among all devices, disregarding their individual contributions. The Random Distribution method introduces an element of unpredictability by allocating the budget in random proportions to each device, without consideration for their contributions, ensuring only that the total allocation does not exceed the predefined budget. The experiment's objective was to compare these methods in terms of how they distribute limited resources among participating entities, illustrating the implications of each method on fairness, efficiency, and incentive mechanisms within a collaborative IoT environment. The total budget for this experiment was set at 8.1 units, chosen to demonstrate the allocation dynamics under a constrained resource scenario. Figure 4c displays the budget allocation across three distribution methods. Under the Shapley Value method, the distribution appears fair, reflecting the marginal contributions of each device with allocations of 3.00, 2.70, and 2.40 respectively. This aligns with the principle of Shapley Value, which ensures that each player (device) is rewarded according to their contribution to the total effectiveness. Equal Distribution method allocates an identical budget of 2.70 to each device, disregarding their individual contributions. This approach, while simple, does not account for the differences in the devices' performances or their contributions to monitoring effectiveness. Random Distribution introduces an element of variability, allocating budgets of 2.66, 2.33, and 3.11 to the devices. This method, as indicated by the name, does not follow a predictable

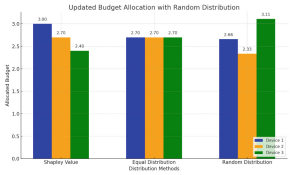
pattern and can result in allocations that may not correspond to the devices' effectiveness or contributions.



(a) RMSEs Before and After LOF



(b) Effectiveness Scores



(c) Reward Distribution

Fig. 4. Experiments Results among Three Random Devices

6 Conclusion

In our research, we introduce "EcoIntegrity," an AI-enhanced blockchain framework tailored for tracking the carbon footprint within an IoT ecosystem. This innovative framework unfolds in three distinct but cohesive phases, each designed to harness the capabilities of IoT devices for reliable and accurate carbon footprint monitoring. The first phase leverages artificial intelligence, utilizing LoF algorithms and recurrent neural networks to detect anomalous behavior in IoT device activity. Concurrently, LSTM is applied to predict behavioral patterns of IoT devices, such as carbon emissions, ensuring a proactive approach to environmental impact assessment. In the second phase, we integrate blockchain technology and smart contracts to ensure that the recorded carbon footprint data are preserved in an immutable, transparent, and secure ledger. This phase is pivotal in maintaining the credibility of the data by preventing alterations and providing a clear audit trail. The final phase focuses on incentivization. Recognizing the necessity for IoT devices to engage in carbon footprint reporting actively, we incorporate an incentive mechanism. Here, the Shapley Value, a concept derived from game theory, is utilized to ensure equitable and integrity-driven distribution of rewards. This approach not only stimulates participation but also upholds fairness and integrity in the recognition of each device's contribution to the network. "EcoIntegrity" stands out as a robust application that empowers IoT devices to track their environmental impact, embodying principles of truthfulness and integrity throughout the process.

One limitation of our current research lies in the utilization of simulated and public data for the experimental phases. While simulations provide valuable insights and a controlled environment to test our hypotheses, they cannot fully replicate the intricacies and unpredictable nature of real-world data. Consequently, the findings and efficacy of the "EcoIntegrity" framework, as they stand, are provisional and subject to the variances that actual IoT device data

would present. To bridge this gap, future work will involve deploying our framework in a real-world setting, where data from physical IoT devices will be used to further validate and refine our model. This progression will allow us to confront practical challenges, adapt to real-time data complexities, and evaluate the framework's performance in a live environment, ultimately enhancing its reliability and applicability.

Funding. This research was funded by the National Key Research and Development Program of China under Grant No. 2023YFB2704400.

References

1. Codur, A.-M., Harris, J.M., Feriz, M.B.: Forests and climate: Economics and policy issues
2. Intergovernmental Panel on Climate Change. Climate change 2021: The physical science basis (2021). https://www.ipcc.ch/report/ar6/wg1/
3. Microsoft. Microsoft's sustainability commitment (2021). https://www.microsoft.com/en-us/sustainability
4. Nielsen: Sustainable shoppers buy the change they wish to see in the world. Nielsen Insights (2020). https://www.nielsen.com/insights
5. Ellerman, A.D., Marcantonini, C., Zaklan, A.: The European union emissions trading system: ten years and counting. Rev. Environ. Econ. Policy (2016)
6. International Energy Agency. Global energy review 2020 (2020). https://www.iea.org/reports/global-energy-review-2020
7. Pedersen, J.L., Bey, N., Friis Gerholt, S., Rohde, R.: The road towards carbon neutrality in the different Nordic countries. Nordic Council of Ministers (2020)
8. Chakravarthi, P.K., Yuvaraj, D., Venkataramanan, V.: Iot-based smart energy meter for smart grids. In: 6th International Conference on Devices, Circuits and Systems (ICDCS). IEEE vol. 2022, pp. 360–363 (2022)
9. Faize, Y., Crenne, J., Hanusse, N., Jego, C.: An energy efficient and scalable node architecture for sensor network. In: 19th IEEE International New Circuits and Systems Conference (NEWCAS), vol. 2021, pp. 1–4. IEEE (2021)
10. M. P. Kokare and S. Pawar, "Energy monitoring system in electric grids: the role of advanced intelligent and iot for future electric grid," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*. IEEE, 2020, pp. 1–4
11. Ionescu, L., Mazare, A., Ionescu, N., Lita, A.: Energy consumption monitoring using private blockchain network based on ethereum smart contracts. In: IEEE 28th International Symposium for Design and Technology in Electronic Packaging (SIITME), vol. 2022, pp. 132–135. IEEE (2022)
12. Hamidu, I., Afotey, B., Ayatul-Lahi, Z.: Design and development of a low-cost sensor IoT computing device for greenhouse gas Momitor from selected industry locations. Scalable Comput. Pract. Experien. **23**(4), 363–376 (2022)
13. Kambourakis, G., Kolias, C., Stavrou, A.: The MIRAI botnet and the IoT zombie armies. In: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pp. 267–272. IEEE (2017)
14. Gómez, Á.L.P., Maimó, L.F., Celdrán, A.H., Clemente, F.J.G.: Susan: a deep learning based anomaly detection framework for sustainable industry. Sustain. Comput. Inform. Syst. **37**, 100842 (2023)

15. Mohamudally, N., Peermamode-Mohaboob, M.: Building an anomaly detection engine (ADE) for IoT smart applications. Procedia Comput. Sci. **134**, 10–17 (2018)
16. Singh, A., Miller, S., Brinkley, M.: Lowering carbon foot-print by increasing operational efficiency using adaptive machine learning. In: SPE Annual Technical Conference and Exhibition? SPE, p. D031S057R005 (2022)
17. Malik, A., Haque, A., Kurukuru, V.B.: IoT-based monitoring and management for photovoltaic system. In: Fault Analysis and its Impact on Grid-connected Photovoltaic Systems Performance, pp. 291–318 (2022)
18. Alloghani, M.A.: Anomaly detection of energy consumption in cloud computing and buildings using artificial intelligence as a tool of sustainability: a systematic review of current trends, applications, and challenges. In: Artificial Intelligence and Sustainability, pp. 177–210 (2023)
19. Ariyaluran Habeeb, R.A., et al.: Clustering-based real-time anomaly detection—a breakthrough in big data technologies. Trans. Emerging Telecommun. Technol. **33**(8), e3647 (2022)
20. Bajao, N.A., Sarucam, J.-A.: Threats detection in the internet of things using convolutional neural networks, long short-term memory, and gated recurrent units. Mesopotamian J. Cybersecur. **2023**, 22–29 (2023)
21. Ullah, I., Mahmoud, Q.H.: A framework for anomaly detection in IoT networks using conditional generative adversarial networks. IEEE Access **9**, 165 907-165 931 (2021)
22. Popli, S., Jha, R.K., Jain, S.: A survey on energy efficient narrowband internet of things (nbiot): architecture, application and challenges. IEEE Access **7**, 16 739-16 776 (2018)
23. Alanazi, F., Kim, J., Cotilla-Sanchez, E.: Load oscillating attacks of smart grids: vulnerability analysis. IEEE Access (2023)
24. Yu, Y., Li, Y., Tian, J., Liu, J.: Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wirel. Commun. **25**, 12–18 (2018)
25. Tahir, M., Sardaraz, M., Muhammad, S., Khan, M.S.: A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. Sustainability **12**, 6960 (2020)
26. Zhang, H., Lang, W., Liu, C., Zhang, B.: A blockchain-based security approach architecture for the internet of things. In: 2020 IEEE 4th Information Technology, Networking. Electronic and Automation Control Conference (ITNEC), vol. 1, pp. 310–313 (2020)
27. Luo, Z., et al.: Application of the IoT in the food supply chain: from the perspective of carbon mitigation. Environ. Sci. Technol. **56**(15), 10 567-10 576 (2022)
28. Liu, K.-H., Chang, S.-F., Huang, W.-H., Lu, I.-C.: The framework of the integration of carbon footprint and blockchain: using blockchain as a carbon emission management tool. In: Hu, A.H., Matsumoto, M., Kuo, T.C., Smith, S. (eds.) Technologies and Eco-innovation towards Sustainability I, pp. 15–22. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1181-9_2
29. Niya, S.R., Jha, S.S., Bocek, T., Stiller, B.: Design and implementation of an automated and decentralized pollution monitoring system with blockchains, smart contracts, and Lorawan. In: NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, pp. 1–4 (2018)
30. Alsamhi, S., Ma, O., Ansari, M.S., Almalki, F.A.: Survey on collaborative smart drones and internet of things for improving smartness of smart cities. IEEE Access **7**, 128 125-128 152 (2019)

31. Mahalakshmi, J., Kuppusamy, K., Kaleeswari, C., Maheswari, P.: IoT sensor-based smart agricultural system. In: Subramanian, B., Chen, S.-S., Reddy, K.R. (eds.) Emerging Technologies for Agriculture and Environment. LNMIE, pp. 39–52. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-7968-0_4
32. Elijah, O., Rahman, T.A., Orikumhi, I., Leow, C., Hindia, M.N.: An overview of internet of things (IoT) and data analytics in agriculture: benefits and challenges. IEEE Internet Things J. **5**, 3758–3773 (2018)
33. Liu, L., Han, M.: Weatherpon: a weather and machine learning-based coupon recommendation mechanism in digital marketing. In: 2023 IEEE 3rd International Conference on Software Engineering and Artificial Intelligence (SEAI), pp. 28–32. IEEE (2023)
34. Liu, L., Kong, Y., Li, G., Han, M.: Fairshare: an incentive-based fairness-aware data sharing framework for federated learning. In: Yang, H., et al. (eds.) ICIRA 2023. LNCS, vol. 14268, pp. 115–126. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-6486-4_10
35. Lim, W.Y.B., et al.: Hierarchical incentive mechanism design for federated machine learning in mobile networks. IEEE Internet Things J. **7**, 9575–9588 (2020)
36. Ferreira, J., Martins, A.: Ad hoc IoT approach for monitoring parking control process, pp. 113–121, (2017)
37. Yu, L., Li, Z., Liu, J., Zhou, R.: Resources sharing in 5g networks: learning-enabled incentives and coalitional games. IEEE Syst. J. **15**, 226–237 (2021)
38. Cheng, G., Deng, S., Xiang, Z., Chen, Y., Yin, J.: An auction-based incentive mechanism with blockchain for IoT collaboration. In: 2020 IEEE International Conference on Web Services (ICWS), pp. 17–26 (2020)
39. Liu, L., Han, M., Zhou, Y., Parizi, R.M., Korayem, M.: Blockchain-based certification for education, employment, and skill with incentive mechanism. In: Choo, K.-K.R., Dehghantanha, A., Parizi, R.M. (eds.) Blockchain Cybersecurity, Trust and Privacy. AIS, vol. 79, pp. 269–290. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-38181-3_14
40. Liu, L., Han, M., Zhou, Y., Parizi, R.: E 2 c-chain: a two-stage incentive education employment and skill certification blockchain. In: 2019 IEEE International Conference on Blockchain (Blockchain), pp. 140–147. IEEE (2019)
41. Yin, B., Wu, Y., Hu, T., Dong, J., Jiang, Z.: An efficient collaboration and incentive mechanism for internet of vehicles (IoV) with secured information exchange based on blockchains. IEEE Internet Things J. **7**, 1582–1593 (2020)
42. Liu, L., Ma, Z., Zhou, Y., Fan, M., Han, M.: Trust in ESG reporting: the intelligent Veri-green solution for incentivized verification. Blockchain: Res. Appl. 100189 (2024)
43. Nix, R., Kantarciouglu, M.: Incentive compatible privacy-preserving distributed classification. IEEE Trans. Dependable Secure Comput. **9**(4), 451–462 (2011)
44. Zeng, R., Zeng, C., Wang, X., Li, B., Chu, X.: Incentive mechanisms in federated learning and a game-theoretical approach. IEEE Network **36**(6), 229–235 (2022)
45. Cheng, G., Deng, S., Xiang, Z., Chen, Y., Yin, J.: An auction-based incentive mechanism with blockchain for IoT collaboration. In: 2020 IEEE International Conference on Web Services (ICWS), pp. 17–26. IEEE (2020)
46. Stafford, G.: Environmental sensor data 132k. kaggle dataset (2023). https://www.kaggle.com/datasets/garystafford/environmental-sensor-data-132k