HIGHLY SECURE IOT SENSOR DATA LOGGING ON THE CARDANO BLOCKCHAIN

Abhra Adhikari[1], Muthuraj Ramu[1], Robin Thomas[1], Hongxu Su[2], and BharathRamesh[3]

[1]OliveIoT Innovations, Ottiyambakkam,Chennai, India
[2]Control and Simulation Lab, Dept of Electrical and Computer Engineering,National University of Singapore, Singapore
[3]International Centre for Neuromorphic Systems, The MARCS Institute,Western Sydney University, New South Wales, Australia

ABSTRACT

The tracking of sensor information has advanced significantly with the rise of the Internet ofThings (IoT) and cloud computing, replacing local storage and records. However, it faces challenges such as data leakage, compromised privacy, data tampering, and origin misrepresentation due to mutable data storage and central points of failure. Blockchain-based solutions have been proposed, but they often suffer from high costs, limited scalability, and vulnerability to data tampering in cloud-based processes. This paper introduces a novel approach using Extended Unspent Transaction Output (eUTXO) blockchains, which offer better scalability, lower transaction costs, higher throughput, enhanced privacy, along with a tamper-resistant log. Our framework overcomes limitations of traditional blockchain methods and central- ized cloud systems. By adopting this approach, IoT-based sensor tracking attains new levels of integrity and privacy. Comprehensive evaluations demonstrate the effectiveness and practicality of our system. The proposed framework addresses sensor tracking challenges and advances hardware-backed IoT solutions asthe next logical step.

KEYWORDS

Cardano Blockchain, IoT Integration, Industrial IoT (IIoT), Sensor Information Tracking.

1. INTRODUCTION

The tracking of sensor information has advanced significantly with the rise of the Internet of Things (IoT) and cloud computing, reshaping conventional data management practices by replacing local storage and manual records [1]. The advent of IoT technologies has ushered in a new era of interconnected devices and seamless data exchange, empowering industrial IoT (IIoT) to leverage real-time insights into automated processes [3]. Cloud computing has further facilitated centralized data storage and accessibility, offering scal- able solutions for handling vast amounts of sensor data. However, these advancements come with their own set of challenges. As sensor data flows through interconnected net- works and centralized cloud repositories, it becomes susceptible to various vulnerabilities [4]. Data leakage, compromised

David C. Wyld et al. (Eds): AISO, SIP, SOFTFM, NLDM, CRBL, BIOM, COMIT– 2024
pp. 83-89, 2024. - CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141507

privacy, data tampering, and origin misrepresentation are among the critical challenges stemming from the mutable nature of data storage and the presence of central points of failure [2]. Addressing these concerns is crucial to ensuring the integrity, security, and reliability of sensor information tracking in the era of IoT and cloud computing [5].

Blockchain-based solutions have been proposed as a means to address the challenges insensor information tracking and learning [6][7][8]. However, these solutions often encounter drawbacks, including high transaction costs, limited scalability, and susceptibility to data tampering when integrated with cloud-based processes [9]. To overcome these limitationsand achieve a more robust framework, we introduce a novel approach leveraging the unique capabilities of a blockchain, which is common for securing financial assets [10] but not sensors. In other words, our proposed solution establishes a decentralized network of cloud- based IoT nodes and sensors. This integration significantly enhances the security and reliability of sensor data tracking, ensuring the integrity of information as it traverses through interconnected devices and user interface systems reading the sensor information directly from the blockchain records.

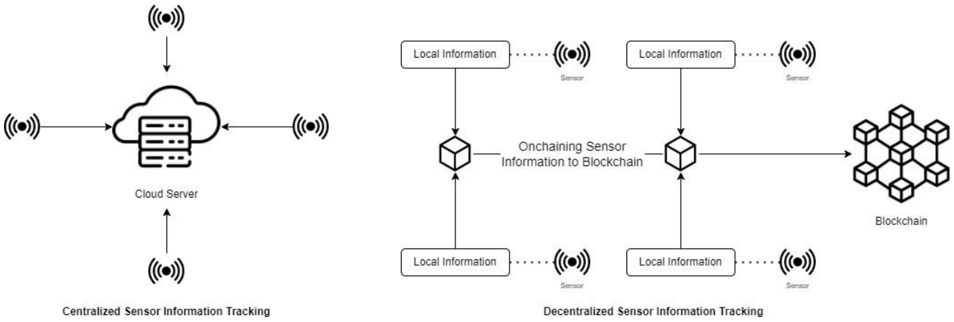
Cloud Server
Centralized Sensor Information Tracking
Local Information
Sensor
Local Information
Sensor
Onchaining Sensor Information to Blockchain
Blockchain
Local Information
Sensor
Local Information
Sensor
Decentralized Sensor Information Tracking

Fig. 1. Centralized vs Decentralized sensor information Tracking.

Implementing blockchain-based cloud IoT systems introduces unique challenges, partic-ularly in terms of speed and scalability. Blockchain platforms like Cardano, which operate on the Proof of Stake (PoS) decentralized consensus mechanism and utilize the Extended Unspent Transaction Output (eUTXO) model, offer a more favorable environment for data-intensive blockchain operations. These eUTXO platforms boast higher throughput, improved scalability, sustainability, power efficiency, and enhanced interoperability. Tothe best of our knowledge, our work is the first to introduce a comprehensive IoT sensor tracking on a eUTXO blockchain.

Figure 1 illustrates the clear distinction between a traditional centralized sensor track- ing system and the decentralized, secure, and efficient setup enabled by our integration with the Cardano blockchain. Our approach emphasizes the potential for broader appli- cations in IIoT scenarios, where trustworthy and scalable sensor information tracking is of utmost importance. The blockchain-based system enables secure and immutable data storage while mitigating data tampering risks, thereby ensuring trustworthy sensor infor- mation records.

Our main goal in this research is to showcase the deployment of a temperature sensor tracking arrangement integrated with the Cardano blockchain. Since this represents a proof-of-concept, the next work can eventually be substituted with hardware integrations for low power and high fidelity implementations. By leveraging the unique capabilities of the Cardano blockchain, which operates on the eUTXO model and utilizes the PoS decentralized consensus mechanism, we aim to exemplify a approach that ensures superior security, scalability, and efficiency compared to existing implementations of blockchain and IoT integrations for sensor use cases. Our proposed setup promises enhanced data integrity, mitigating the risks associated with centralized systems, and ensuring a tamper-resistant and decentralized record of sensor information.

2. DECENTRALIZED SENSOR INFORMATION TRACKING

The proposed system shown in Figure. 2 consists of three main parts: the Cardano blockchain network, an IoT system, and a user interface. The Cardano blockchain is the core of the framework, and it ensures that the sensor information is stored in an im- mutable and tamper-resistant ledger. The IoT system is carefully designed and calibrated to seamlessly integrate with sensor measurement points, allowing for accurate and real- time on-chaining of relevant sensor data. This strategic integration eliminates the need for centralized cloud-based computing processes by directly submitting sensor data to the blockchain. This eliminates the vulnerabilities associated with traditional on-chaining methods, making the data more secure against tampering or unauthorized changes. By reducing reliance on cloud-based data interpretation, this approach not only enhances security but also improves scalability and traceability, setting it apart from traditional sensor tracking methods.

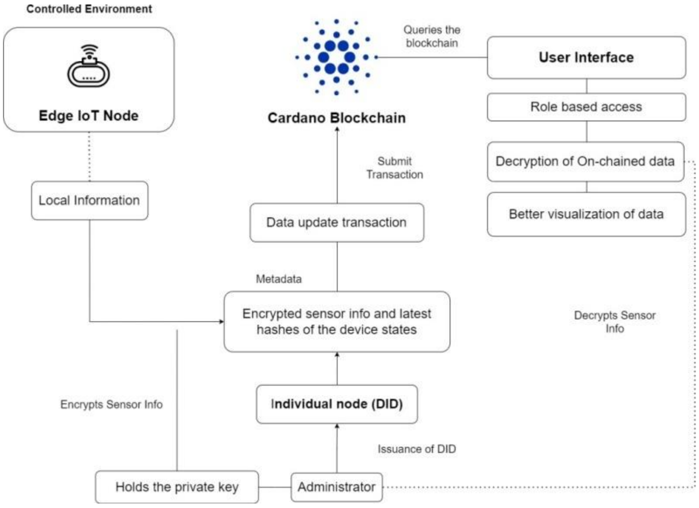

Fig. 2. Architecture of our decentralized framework for sensor information tracking.

Cardano integration enhances security and provides tamper-resistant environments for cryptographic operations. These modules ensure secure key storage, safeguard sensitive data through encryption, and implement secure boot processes, making it difficult for attackers to compromise the system or manipulate data. This physical layer of protection, along with the resistance to software exploits and unauthorized access, significantly fortifiesthe integrity and trustworthiness of the sensor data tracking process. This section outlines the methodology that incorporates these components, highlighting its innovative potentialin the field of secure and efficient sensor data management.

2.1. Cardano Blockchain Network

Cardano is a cutting-edge blockchain platform renowned for its research-driven development and innovative features. It utilizes a PoS consensus mechanism, Ouroboros, for efficiency, and is structured into settlement and computation layers for stability and flexibility. The Extended Unspent Transaction Output (EUTXO) model, utilized by Cardano, represents a distinct transaction approach in blockchain. It operates by managing unspent transaction outputs (UTXOs) associated with specific transactions, enhancing security by preventing double-spending. EUTXO simplifies validation, scalability, and privacy since transactions can be independently verified without a global state.

Cardano's eUTXO model establishes a secure and adaptable environment for manag- ing multiple processes seamlessly, ensuring uninterrupted system operations. By allowing each UTXO to be consumed only once and in its entirety, this framework enhances scal- ability, privacy, and simplifies transaction logic, streamlining transaction verification. An advantage unique to the eUTXO model is its ability to accurately anticipate required transaction fees prior to completion, a feature absent in account-based models. In con- trast, account-based blockchains like Ethereum lack determinism, leading to uncertainty regarding on-chain effects, potentially resulting in financial losses and unexpected costs. Through eUTXO, improved security, predictable transaction costs, and enhanced paral- lelization capabilities are achieved.

Leveraging Cardano's blockchain technology in implementing IoT for sensor tracking yields multiple benefits. Cardano's immutable ledger system efficiently manages device networks designed for sensor tracking, ensuring coherent monitoring of inter-device inter- actions. Given the susceptibility of the expansive IoT ecosystem to data breaches, safe- guarding personal privacy remains a prime concern. By harnessing Cardano's blockchain to store data exchanged between devices, an extra layer of security guards against malicious actors. This strategy prevents the compromise of the entire network due to a vulnerability in a single device. The tamper-proof ledgers not only document system modifications but also facilitate continuous trend analysis. Amid data exchange across devices, users can promptly detect any anomalous changes.

We transmitting the IoT data to a cloud database for subsequent computing operations. This technique conducts computing on-site where data is generated or utilized, facilitating the capturing and processing of IoT data at its source. The synergy between IoT andcloud computing enables swift real-time data analysis, ensuring untampered on-chaining of sensor information. Each Cloud-based IoT node is allocated an individual digital identity, realized through Cardano's NFTs, which maintains the node's state metadata. This unique identity expedites the rectification of compromised nodes and accelerates issue diagnosis. Comprising a compact single-board computer linked to one or multiple IoT sensors, the Cloud-based IoT system collects critical sensor data.

Calibration and configurations for the attached IoT sensors are hashed and stored within each node's digital identity. These identities are issued by administrators during setup, activating the nodes. Administrators possess private keys for identity issuance and initiation. Once operational, the IoT node stores sensor data in the cloud, subsequently computing and on-chaining the data based on its nature and deployment location.

While public data is on-chained without encryption, private sensor data undergoes AES256 encryption. This encrypted data, alongside the initialization vector, is on-chained. The on-chain process occurs through transaction metadata of the UTXO transactions. These transactions consume digital identity UTXOs and necessary UTXOs to cover trans- action costs as per Cardano protocol parameters. Transaction metadata also encompasses the hash of the cloud server and sensor state, swiftly identifying unauthorized changes or hacks, leading to node suspension or labeling as malicious. This approach swiftly isolates compromised devices and facilitates prompt, foolproof issue diagnosis and resolution.

3. EXPERIMENTAL RESULTS

The primary aim of this study was to assess the practical usability of the proposed system through the implementation of a temperature sensor. To achieve this, a K-Type Thermocouple was utilized and connected to a PC through an Analog to Digital Converter. The conceptual foundation of this endeavor was to enable the temperature sensor to record the average temperature every 5 minutes and store this data on the blockchain using a dedicated wallet hosted on a separate PC. The The PC not only acts as the wallet host but also directly interfaces with the temperature sensor, receiving raw data which is then used to calculate and maintain an ongoing average.

Subsequently, the wallet generates a transaction containing temperature readings, the current state of the wallet, and sensor metadata, all of which is stored within the local wallet. This transaction is facilitated through submission APIs [12] like Blockfrost, Koios, and potentially Mithril [13] in the future. The unique identity of the sensor is represented through an NFT, serving as a reference point for the corresponding transaction. The user interface directly extracts information from the blockchain, visually presenting the temperature data as a graph. Additionally, the PC can trigger alerts, such as sending SMS notifications to human agents in response to specific conditions.

To validate the framework, a controlled sensor environment was established within a local shrimp business. For this purpose, a PC with 8 GB of RAM was chosen as the single board computer, coupled with a temperature sensor boasting a range of -250 °C to 250 °C. The data collection process lasted approximately 4 hours, during which the mean temperature was consistently recorded every 5 minutes and securely stored on the blockchain. It is important to note that all on-chain data was made publicly available, but it was encrypted to maintain privacy.

The successful integration of the IIoT sensor into the Cardano blockchain was achieved by configuring and calibrating the sensor specifically for the supply chain environment. This involved enclosing the sensor in an IP 66-rated enclosure and seamlessly integrating it into the supply chain infrastructure. The device’s functionality was tested for an hour with 15-minute intervals for on-chain updates.

First, our data logging video[1] shows how the user connects to the PC via an SSH client and establishes the SSH shell to the PC. Once connected, there is a folder named data under the home directory that contains the live temperature measurement. These measurements are saved as text files within the data folder for on-chaining.

Firstly, an NFT is minted onto the Cloud-based IIoT temperature sensor node as a Digital Identifier (DID). Every IIoT node will have an NFT in it on the setup process as shown in this footnote[2]. The metadata information showcases a specific example of this NFT-based DID implementation. In this case, a unique NFT is associated with the Cloud-based IIoT temperature sensor node. This NFT is represented by a hash value, in this case, ”6912da87277cb7...a908ce3”. Within this NFT, essential details are recorded:

[1] Data logging demo video: https://tinyurl.com/429crre9

[2] DID Example (see metadata value): https://tinyurl.com/yecm3bbx

– Image: Represented by an IPFS (InterPlanetary File System) link, pointing to an image at ”ipfs://QmXX8DXa...vaa4wU.”
– MediaType: The media type of the linked image, identified as ”image/jpg.”
– Onchain_server_sha256: This is a SHA256 hash that serves as a reference point for the state of the IIoT temperature sensor node. It captures the current state of the node’s attributes and parameters, essentially serving as a snapshot of its configuration at a given time. In this example, the hash value is ”e2d8370e248...51ab4eb06e.”

We have integrated the sensor node to three popular Cardano wallets - Nami, Eternl and Gerowallet. This step is crucial to provide privacy features to dedicated clients without compromising their competitiveness. The type of data that needs encryption depends on the client. As a proof of concept, we showcase how the temperature data itself can be encrypted and decrypted using the wallet that contains the node NFT. The IIoT Node on-chained the data after encrypting it with AES256. The wallet containing the Admin Node ID is verified by a data signature and the decryption access is provided to the admin of the supply chain. A video demo can be viewed here[3].

4. CONCLUSION

In conclusion, this paper introduced a novel framework that merges eUTXO-backed sensor tracking with Cardano’s blockchain capabilities. This fusion addresses security, scalability, and efficiency challenges in sensor data management. The combination yields enhanced scalability, cost predictability, and robust security. Our practical implementation on a PC validates the concept’s viability. A transition to application-specific integrated cir- cuits illustrates our commitment to adaptability. This research highlights the strength of Cardano’s blockchain and eUTXO-backed integration, emphasizing the value of research- driven solutions. The framework not only advances sensor data tracking but also offers broader applications for a more secure and decentralized IoT ecosystem. As technology evolves, this work marks a pivotal stride toward unlocking the full potential of sensor data tracking via the Cardano blockchain and eUTXO-backed integration.

[3] Video Demo: https://tinyurl.com/3awk5unh

REFERENCES

[1] A. M. Rahmani, S. Bayramov, and B. Kiani Kalejahi, “Internet of things applications: opportunities and threats,” Wireless Personal Communications, vol. 122, no. 1, pp. 451–476, 2022.

[2] A. Makkar, T. W. Kim, A. K. Singh, J. Kang, and J. H. Park, “Secureiiot environment: Federated learning empowered approach for securing iiot from data breach,” IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6406–6414, 2022.

[3] S. Munirathinam, “Industry 4.0: Industrial internet of things (iiot),” in Advances in computers. Elsevier, 2020, vol. 117, pp. 129–164.

[4] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “A survey on the adoption of blockchain in iot: Challenges and solutions,” Blockchain: Research and Applications, vol. 2, no. 2, p. 100006, 2021.

[5] M. F. Elrawy, A. I. Awad, and H. F. Hamed, “Intrusion detection systems for iot-based smart environ- ments: a survey,” Journal of Cloud Computing, vol. 7, no. 1, pp. 1–20, 2018.

[6] A. J. Cabrera-Guti´errez, E. Castillo, A. Escobar-Molero, J. A. ´ Alvarez Bermejo, D. P. Morales, and

[7] L. Parrilla, "Integration of hardware security modules and permissioned blockchain in industrial iot networks," IEEE Access, vol. 10, pp. 114331–114345, 2022.

[8] E. Bandara, D. Tosh, P. Foytik, S. Shetty, N. Ranasinghe, and K. De Zoysa, "Tikiri—towards a lightweight blockchain for iot," Future Generation Computer Systems, vol. 119, pp. 154–165, 2021.

[9] C. Li, Q. Shen, C. Xiang, and B. Ramesh, "A trustless federated framework for decentralized and con- fidential deep learning," in 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain). IEEE, 2022, pp. 1–6.

[10] A. Hayat, V. Shahare, A. K. Sharma, and N. Arora, "Introduction to industry 4.0," in Blockchain and its Applications in Industry 4.0. Springer, 2023, pp. 29–59.

[11] I. Bentov, Y. Ji, F. Zhang, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-time cryptocur- rency exchange using trusted hardware," in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 1521–1538.

[12] Y. E. Oktian and S.-G. Lee, "Blockchain-based federated learning system: A survey on design choices," Sensors, vol. 23, no. 12, 2023.

[13] A. V. Pomogalova, A. A. Martyniuk, and K. E. Yesalov, "Key features and formation of transactions in the case of using utxo, eutxo and account based data storage models," in 2022 International Conference on Modern Network Technologies (MoNeTec). IEEE, 2022, pp. 1–7.

[14] P. Chaidos and A. Kiayias, "Mithril: Stake-based threshold multisignatures," Cryptology ePrint Archive, 2021.

[15] H. de Voogt, "Assessing atala prism as an implementation of ssi, viewed from the perspective of the general data protection regulation and its underlying ideals," Viewed from the Perspective of the General Data Protection Regulation and Its Underlying Ideals (February 19, 2022), 2022.