Blockchain for Data Integrity Against Timestamp Attacks in Digital Twin-Based EV Battery Monitoring

1st Mitra Pooyandeh
Center for ICT and Automotive Convergence
Kyungpook National University
Daegu, South Korea
m.pooyandeh@knu.ac.kr

2nd Dong Seog Han
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, South Korea
dshan@knu.ac.kr

***Abstract*—Ensuring data integrity in digital twin (DT) systems for EV battery monitoring is critical. Timestamp attacks, which reorder sensor data without altering content, threaten communication integrity. This paper proposes a conceptual blockchain-enhanced architecture to secure the communication layer between the BMS and its DT. By logging hashed data packets with network-verified timestamps on a permissioned blockchain, reliable detection of timestamp attacks is enabled. Conceptual evaluation shows 100\% detection with zero false positives and a modest overhead of 0.35 seconds per packet. These findings suggest blockchain integration can significantly enhance communication security and data integrity in real-time EV DT applications.**

***Index Terms*—Digital twin, Blockchain, timestamp attack, lithium-ion battery.**

I. Introduction

The rapid global adoption of electric vehicles (EVs) underscores the critical need for robust and reliable lithium-ion battery (LIB) management systems [1], [2], [3]. The digital twin (DT) technology has emerged as a transformative tool in the field of intelligent vehicles [4], especially for the management and monitoring of EV battery systems [5], [6]. By creating a real-time virtual replica of a physical battery system, digital twins enable predictive analytics such as accurate state of charge (SoC) estimation [7], fault detection, and life cycle management. These systems rely heavily on the timely and trustworthy transmission of sensor data from the EV's battery management system (BMS) to the cloud-based digital twin platform.

However, the effectiveness of DT relies heavily on the integrity and timeliness of data communication between the BMS and the DT platform. Conventional integrity checks (e.g., hashes or message authentication codes) ensure data content remains unaltered, but they do not guarantee sequential order. This leaves DT systems vulnerable to timestamp attacks [8], where adversaries manipulate the temporal sequence of packets without modifying their values. Such subtle attacks can degrade SoC estimation accuracy, mislead predictive models, and compromise overall system safety.

To address this challenge, this paper proposes a blockchain-enhanced architecture for securing communication in DT-based EV battery monitoring. Unlike lightweight cryptographic approaches that ensure authenticity only at the packet level, blockchain provides an immutable, verifiable ledger of packet order and timestamps. This property makes it particularly suited for detecting reordering attacks that exploit temporal consistency.

The key contributions of this work are as follows:

We define a threat model for timestamp attacks in EV battery monitoring and highlight its potential impact on DT performance.

We propose a blockchain-enhanced architecture that ensures both authenticity and sequential integrity of BMS-to-DT communication.

We provide a conceptual evaluation, demonstrating that the system achieves 100% detection of timestamp attacks with no false positives while maintaining near real-time responsiveness.

We compare blockchain with alternative approaches (digital signatures, MACs) and justify its adoption in this context.

The remainder of this paper is organized as follows: Section II reviews blockchain-based solutions relevant to energy systems, highlighting their potential for enhancing security and trust. Section III provides an overview of the proposed system. Section IV introduces the conceptual framework. Section V presents the conceptual implementation of the proposed system, demonstrating its feasibility and performance. Section VI discusses the key findings, evaluates the system's effectiveness, and considers potential limitations. Finally, Section VII concludes the paper and outlines future research directions.

II. Related Work

Faria *et al.* [9] proposed a blockchain-based framework to ensure transparency and traceability in the second-life LIB market by securely recording degradation and usage data from EV batteries. Their simulation demonstrates how blockchain integration can enhance trust, reduce testing costs, and promote the sustainable reuse of batteries in stationary

Identify applicable funding agency here. If none, delete this.

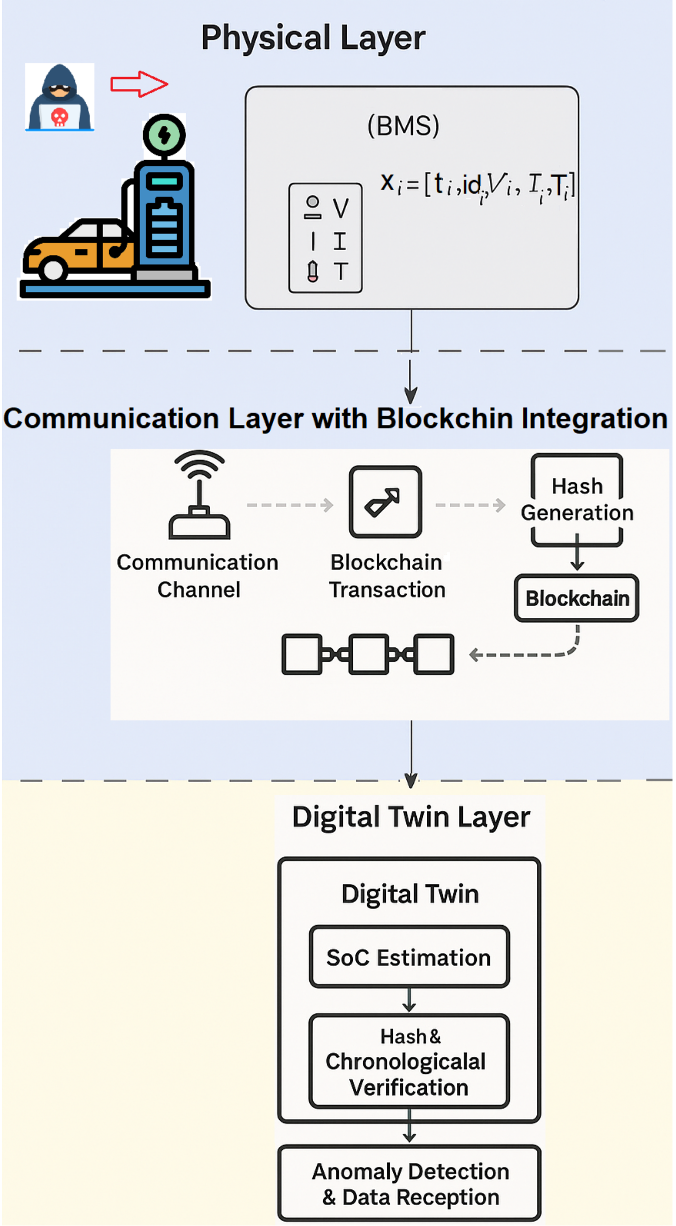
Physical Layer
(BMS)
$x_i=[t_i,id_i,V_i,I_i,T_i]$
V
I
T
Communication Layer with Blockchin Integration
Communication Channel
Blockchain Transaction
Hash Generation
Blockchain
Digital Twin Layer
Digital Twin
SoC Estimation
Hash& Chronologicalal Verification
Anomaly Detection & Data Reception

Fig. 1. Proposed hybrid architecture integrating a blockchain-enhanced digital twin system for EV battery monitoring. The system consists of three layers: (1) the physical layer, where the BMS collects sensor data; (2) the communication layer, where a permissioned blockchain ensures secure data transmission and timestamp validation; and (3) the digital twin layer, which verifies hash integrity and data sequence before performing SoC estimation. The architecture mitigates timestamp attacks by preserving data integrity and chronological consistency.

energy applications. Zhong *et al.* [10] proposed a blockchain-based energy market system for EVs that integrates an automated market maker (AMM) for dynamic pricing and a blockchain-oracle-powered estimator for real-time SoC. Their solution ensures cost-effective, transparent energy distribution and accurate SoC prediction, demonstrated through smart contract deployment and experimental validation on Ethereum. Liu *et al.* [11] propose a blockchain-based, interpretable deep learning framework— battery life prediction (BLP)-Transformer—for predicting electric vehicle battery life within the internet of vehicles (IoV). Their architecture ensures secure data transmission and storage via smart contracts, while offering accurate and explainable predictions of battery degradation using a feature-focused Transformer model. Florea [12] presented a blockchain-based battery management system for electric vehicles using the IOTA Tangle to enable decentralized battery monitoring, charging, and swapping. The implementation ensures secure, low-cost data exchange among EVs and stations, demonstrating feasibility through a prototype tested with LiPo batteries and Raspberry Pi hardware. Couraud *et al.* [13] proposed a blockchain-enabled real-time control framework for aggregating distributed residential batteries to participate in wholesale energy markets. Using a smart contract and model predictive control (MPC), their system enhances energy export reliability, boosts revenues by 35%, and increases self-consumption while ensuring grid stability under realistic conditions.

While conventional sequence number–based schemes combined with MAC or hash functions are effective in centralized or tightly synchronized systems, they rely on the assumption that sequence generation and packet forwarding entities are fully trusted. In distributed digital twin–based architectures, this assumption may not hold: intermediate gateways or aggregation nodes can be partially compromised, enabling an attacker to delay or reorder packets while preserving valid sequence numbers and cryptographic authentication. In such cases, syntactically correct packets may still introduce semantic timeline inconsistencies between the physical battery behavior and its digital twin representation. Moreover, maintaining a trusted global ordering across heterogeneous and distributed components becomes challenging when clock synchronization or sequence generation cannot be universally trusted. The proposed blockchain-enhanced architecture introduces an immutable, globally verifiable transaction ordering shared among stakeholders, enabling detection of timestamp and reordering attacks that may remain invisible to conventional sequence number–based mechanisms.

To the best of our knowledge, this work is among the first to investigate blockchain as a mechanism for timestamp integrity protection in EV digital twin systems.

III. System Overview

Electric vehicle battery monitoring systems increasingly rely on digital twins for real-time SoC estimation and performance management. However, they are vulnerable to timestamp attacks, where the timing of sensor data is maliciously altered to degrade system accuracy or mislead decision-making. Ensuring the integrity and authenticity of timestamped sensor data is therefore critical to reliable operation.

In this work, the attacker is assumed to have the capability to manipulate packet timing or ordering at intermediate communication layers while remaining compliant with protocol-level authentication checks. Specifically, the attacker delays, reorders, or selectively replays authenticated sensor packets, creating timeline inconsistencies that desynchronize the digital twin from the physical battery system without modifying packet contents. This threat model captures realistic scenarios in which protocol-level authentication remains intact, yet subtle temporal manipulation degrades SoC estimation accuracy, as analyzed in [8].

To address this threat, we propose a blockchain-enhanced system architecture that secures the digital twin pipeline against timestamp manipulation. The system integrates cryptographic validation and immutable logging to ensure that data is both authentic and chronologically consistent.

As depicted in Fig. 1, the system operates across three logical layers: (1) the physical layer, where the BMS collects sensor data with timestamps and unique identifiers; (2) the secure communication layer, where an edge node and permissioned blockchain infrastructure enforce tamper resistance and detect anomalies; and (3) the digital twin layer, which retrieves packets, verifies their hashes against blockchain records, and ensures the temporal order matches the blockchain ledger before performing SoC estimation. This layered design provides strong protection against timestamp attacks and enhances trust in EV battery monitoring. The following section presents the detailed architectural workflow, security mechanisms, and results from a conceptual evaluation designed to validate the system's feasibility and detection capabilities.

IV. Conceptual Framework for Blockchain-Enhanced Timestamp Integrity in EV Battery Digital Twins

This section outlines a conceptual framework for integrating blockchain into digital twin environments to enhance data integrity and mitigate timestamp attacks in EV battery monitoring. Rather than an implemented model, this framework illustrates logical structure, workflow, and evaluation considerations for future realization.

A. System Architecture Design

Building upon the three-layer structure introduced earlier, this subsection elaborates on the data flow and functional responsibilities across the system. At the physical layer, the BMS collects real-time sensor readings—voltage, current, and temperature—along with cycle identifiers and precise timestamps. These raw data packets are forwarded to the edge node for secure processing. The secure communication layer performs cryptographic operations and interacts with a permissioned blockchain network. Upon receiving each packet, the edge node computes a SHA-256 hash and assembles a transaction including metadata such as the timestamp and packet ID. Transactions are grouped into blocks and appended to the chain, forming a tamper-resistant audit log of all received data.

The digital twin layer ingests data only after verifying two conditions: (1) that the hash of each packet matches the corresponding blockchain record, and (2) that the timestamp sequence is consistent with the block order. If either condition fails, the packet is flagged as anomalous and excluded from the SoC estimation pipeline.

This layered and validated flow of information forms the foundation for detecting timestamp anomalies while maintaining high-fidelity digital twin performance.

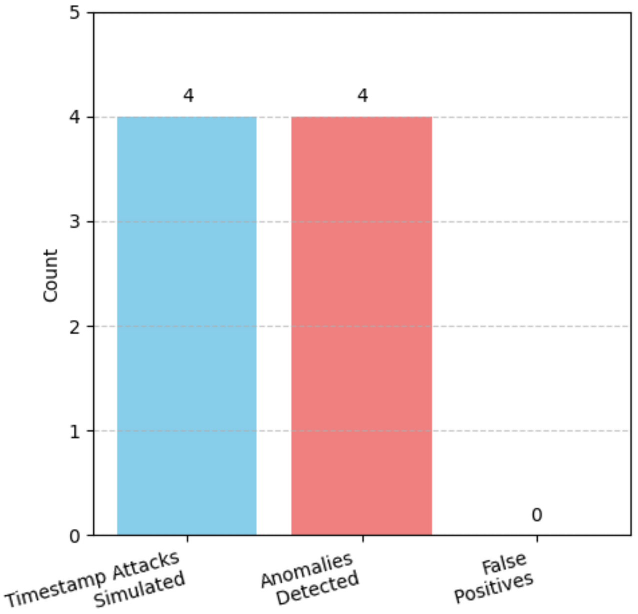

Fig. 2. Conceptual detection results: all four simulated timestamp attacks were identified with zero false positives.

B. Blockchain Mechanism for Data Integrity

The system is assumed to operate over an insecure communication channel between the BMS and the DT. The attacker has the following capabilities: *Packet reordering:* Deliberately changes the sequence of transmission. *Replay/injection:* Replays old packets or inserts malicious ones. The blockchain layer plays a central role in securing data integrity across the system. Through immutable logging, it permanently records the hashes and timestamps associated with each data packet, making any effective modification detectable. Cryptographic chaining ensures the sequential order of transactions and facilitates tamper detection, while the use of a permissioned ledger introduces distributed trust that eliminates the risk of unilateral data manipulation. This setup also provides robust protection against timestamp attacks by verifying both the authenticity and the temporal consistency of transmitted data.

1) Proposed Blockchain-Enhanced Architecture: The BMS generates a packet (ID, sensor values, timestamp). The edge node hashes the packet and submits a blockchain transaction containing the hash and timestamp. The blockchain network validates and immutably records the transaction. The DT accepts a packet only if:

- Its hash matches the blockchain record.
- Its timestamp order is consistent with block order.

Packets failing either condition are discarded and logged as anomalies.

2) Why Blockchain Instead of Lightweight Cryptography?: Lightweight schemes such as MACs or digital signatures can authenticate packet content efficiently. However, they cannot: (1) Provide a tamper-proof chronological record shared across multiple entities, (2) Guarantee non-repudiation and distributed trust, and (3)Enable post-event forensic analysis by reconstructing the full packet history.

Table I compares blockchain with alternative methods.

TABLE I
COMPARISON OF SECURITY MECHANISMS

Feature	**MAC/Signature**	**Blockchain**
Data authenticity	✓	✓
Timestamp integrity	✗	✓
Immutable audit trail	✗	✓
Multi-party trust	Limited	✓
Overhead	Low	Moderate

V. CONCEPTUAL EVALUATION

A conceptual evaluation of the proposed system was conducted to assess its effectiveness. This evaluation was performed in a simulated environment, where the data flow and blockchain logic were conceptually modeled using Python. Involving 20 transmitted data packets and 4 deliberate timestamp attacks, the blockchain mechanism successfully identified all anomalies with a 100% detection rate and no false positives. Additionally, all legitimate packets were validated correctly, resulting in 100% hash verification accuracy.

Performance estimates indicate a blockchain transaction overhead of approximately 0.35 seconds per data packet. The overall system response time for anomaly detection remains under 1 second. These performance estimates are derived from a simplified Python-based simulation that models the core cryptographic operations (hashing, block creation) and transaction submission to a conceptual lightweight blockchain ledger. The values reflect typical latencies observed in similar local or permissioned blockchain test environments, assuming optimized network conditions and a limited number of participating nodes. While a full-scale deployment on embedded hardware would require further empirical validation, these conceptual figures serve to demonstrate the potential for real-time or near-real-time operation. These results demonstrate that the proposed architecture holds strong potential for real-time or near-real-time deployment in electric vehicle battery monitoring applications.

A. Conceptual Results

This subsection details the outcomes of the Python-based conceptual simulation. The evaluation focused on two aspects: (1) anomaly detection capability against timestamp attacks, and (2) estimated performance overhead of the blockchain integration. Figures 2 and 3 summarize the results, showing detection accuracy, absence of false positives, and sub-second response times.

Fig. 2 and 3 provide a visual summary of the conceptual evaluation.

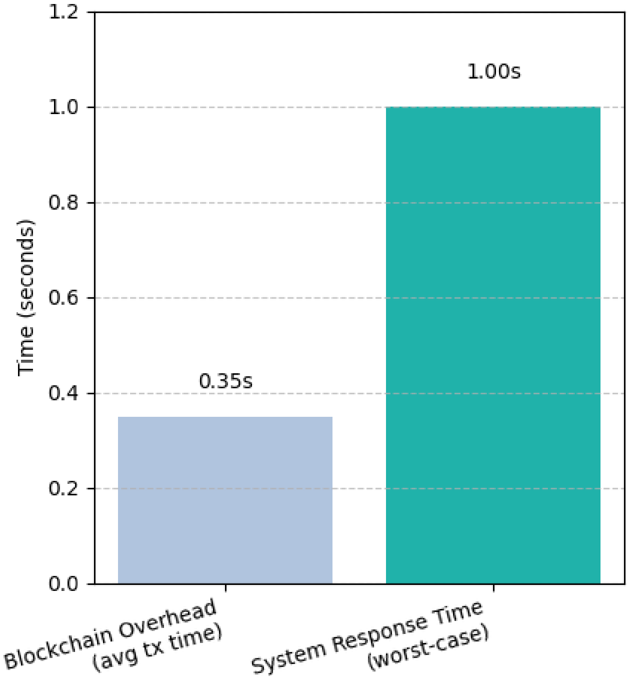

Fig. 3. Conceptual performance metrics: average blockchain overhead per transaction and worst-case anomaly response time.

Fig. 2 illustrates the conceptual attack and detection counts, presenting the system's effectiveness in identifying timestamp attacks. In this conceptual scenario, out of 4 timestamp attacks simulated by deliberately reordering data packet timestamps, the blockchain-based mechanism successfully identified 4 anomalies. This resulted in a 100% detection accuracy, demonstrating the proposed system's robust capability to pinpoint timestamp manipulations. Essentially, the evaluation also showed 0 false positives, indicating that legitimate data packets were never incorrectly flagged as anomalies. This high precision is a direct benefit of the cryptographic verification inherent in blockchain, where any deviation from the expected hash or sequential order is deterministically detected. This result underscores the blockchain's potential to provide a trustworthy and tamper-proof record of data sequence, which is essential for maintaining the integrity of time-series data in digital twin applications.

Fig. 3 presents the conceptual performance metrics, detailing the estimated overhead and responsiveness of the proposed blockchain integration. The blockchain overhead (average transaction time) was conceptually estimated at approximately 0.35 seconds per data packet. This metric represents the time taken to hash a data packet and commit its transaction to the blockchain ledger. Furthermore, the system response time (worst-case) for anomaly detection, from the moment a timestamp attack occurs to its identification and logging, was estimated to be under 1 second. These performance figures are derived from a simplified Python-based simulation that models the core cryptographic operations (hashing, block creation) and transaction submission to a conceptual lightweight blockchain ledger. The values reflect typical latencies observed in similar local or permissioned blockchain test environments, assuming optimized network conditions and a limited number of participating nodes. While a full-scale deployment on embedded hardware would require further empirical validation, these conceptual figures serve to demonstrate the potential for real-time or near-real-time operation. The relatively low overhead and rapid response time suggest that the proposed blockchain architecture is suitable for real-time applications in electric vehicle battery monitoring where data integrity is paramount.

B. Implementation Status

At present, the proposed blockchain-enhanced framework exists at the conceptual and simulation stage. The proof-of-concept evaluation was conducted using Python scripts that emulate packet transmission, hashing, and blockchain-like transaction logging, but no real blockchain deployment has yet been carried out.

Future implementation will focus on a full-scale prototype using real-world BMS datasets [14] and a permissioned blockchain platform such as Hyperledger Fabric. Planned development steps include:

- **Edge node prototype:** a lightweight module for real-time data hashing and transaction submission.
- **Blockchain integration:** configuration of a Hyperledger Fabric test network with low-latency consensus (e.g., Raft or PBFT) to maintain sub-second transaction finality.
- **Dataset validation:** applying the framework to real BMS datasets to test resilience against timestamp attacks under practical conditions.
- **Performance metrics:** measuring latency, throughput, detection accuracy, and computational overhead to verify system viability for deployment in EV battery monitoring.

This staged implementation plan bridges the gap between the current conceptual evaluation and a deployable system, ensuring that the framework can be validated in both simulated and real-world environments.

C. Preliminary Analysis and Performance Estimation

To complement the conceptual evaluation, we provide a brief analysis of the system's detection accuracy, computational complexity, and estimated performance.

In the simulated scenario with 20 data packets and 4 timestamp attacks, the system achieved 100% detection accuracy with zero false positives. This means all 4 attack packets were correctly identified as true positives (TP = 4), and none of the normal packets were incorrectly flagged as attacks (false positives FP = 0). Given that there are 20 total packets and 4 of them are attacks, the remaining 16 packets are normal and correctly classified as true negatives (TN = 16). Based on this, standard metrics can be calculated as follows:[1]

TABLE II
SUMMARY OF PRELIMINARY ANALYSIS AND PERFORMANCE ESTIMATION

Metric	Value
True Positives (TP)	4
True Negatives (TN)	16
False Positives (FP)	0
False Negatives (FN)	0
Precision	1.0
Recall	1.0
Accuracy	1.0
Blockchain Overhead (Avg. Transaction Time)	0.35 seconds
Worst-case System Response Time	$<$ 1 second
Theoretical Throughput	2.86 packets/sec

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} = \frac{4}{4+0} = 1.0 \tag{1}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} = \frac{4}{4+0} = 1.0 \tag{2}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{Total}} = \frac{4+16}{20} = 1.0 \tag{3}$$

A summary of these key metrics and other performance results is provided in Table II.

The blockchain-related operations include hashing, block creation, and anomaly verification. These have the following conceptual time complexity:

- **Hashing:** $\mathcal{O}(n)$ where n is the packet size
- **Block writing and chaining:** $\mathcal{O}(1)$ for the act of adding the block to the chain (e.g., updating pointers or hashes). Note that the process of forming a block (collecting transactions, computing Merkle root, proof-of-work or consensus) may have higher complexity depending on the number of transactions per block and the blockchain protocol, but this preliminary analysis focuses on the chaining step.
- **Timestamp anomaly check:** $\mathcal{O}(m)$ for m packets

Estimated performance metrics from the Python-based simulation are as follows:

- **Blockchain overhead (avg. transaction time):** 0.35 seconds
- **Worst-case system response time:** $<$ 1 second
- **Theoretical throughput:** 2.86 packets/sec

These estimates are based on a lightweight conceptual model assuming ideal local network conditions and a permissioned blockchain. While full-scale deployment may introduce additional overhead, the current results suggest feasibility for real-time or near-real-time operation in electric vehicle battery monitoring applications.

VI. DISCUSSION AND LIMITATION

The conceptual evaluation highlights the strong potential of the proposed blockchain-based system in securing digital twin data against timestamp attacks. The results indicate a 100% detection rate with zero false positives across all simulated timestamp attacks. This is a significant finding, as

[1] Here, TP = True Positives, TN = True Negatives, FP = False Positives, FN = False Negatives, representing correct and incorrect classifications of attack detection.

it demonstrates that blockchain's immutable, network-verified timestamping effectively mitigates the subtle reordering tactics characteristic of such attacks. By ensuring that only validated and sequentially consistent data are processed by the digital twin, the system preserves the integrity and accuracy of SoC estimation.

Furthermore, the performance metrics reinforce the system's practical feasibility. An average blockchain overhead of 0.35 seconds per packet and a worst-case system response time of under 1 second suggest that the architecture supports real-time EV battery monitoring without sacrificing responsiveness. These findings conceptually validate that integrating blockchain can enhance data integrity and trustworthiness without imposing substantial computational or communication delays.

However, these findings are derived from a conceptual implementation and limited-scale simulations. Real-world deployment may be affected by factors such as network latency, transaction throughput, and system scalability. Consequently, future work should focus on empirical validation under realistic operating conditions and investigate optimization strategies to further reduce latency and resource consumption.

Blockchain transaction confirmation latency, particularly in public networks, is a known limitation. In the proposed architecture, blockchain confirmation is intentionally excluded from the real-time monitoring and control loop. Instead, real-time SoC estimation relies on provisional ordering and local consistency checks, while the blockchain provides a tamper-resistant and auditable global ordering for attack detection and post-hoc validation. This architectural separation prevents attackers from exploiting transaction pending states to influence real-time digital twin behavior. Nevertheless, confirmation latency remains a system-level constraint and will be further investigated in future work.

VII. Conclusion

This paper proposed and conceptually evaluated a novel blockchain-based approach to mitigate timestamp attacks in DT-based LIB monitoring for Electric Vehicles. By leveraging blockchain's immutability and cryptographic chaining, our system aims to ensure the sequencial integrity of critical battery data.

The conceptual evaluation demonstrated 100% detection accuracy for timestamp attacks with no false positives, coupled with an acceptable average transaction overhead of 0.35 seconds and a rapid system response time of less than 1 second. This work confirms the conceptual viability of using blockchain to safeguard data integrity in time-sensitive cyber-physical systems, contributing to more reliable EV battery management. Future work will focus on validating the proposed architecture through real-world EV battery monitoring scenarios and experimental deployments.

Acknowledgment

This research was supported by the Core Research Institute Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (RS-2021-NR060127).

References

[1] A. Upadhyaya and C. Mahanta, ”An Overview of Battery Based Electric Vehicle Technologies With Emphasis on Energy Sources, Their Configuration Topologies and Management Strategies,” in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 2, pp. 1087-1111, Feb. 2024, doi: 10.1109/TITS.2023.3316191.

[2] M. S. Nazim, A. Chakma, M. I. Joha, , S. S. Alam, M. M. Rahman, M. K. S. Umam, and Y. M. Jang, ”Artificial intelligence for estimating State of Health and Remaining Useful Life of EV batteries: A systematic review,” The ICT Express, 2025.

[3] Z. Xie, and X. Song, ”A renewable-energy-driven energy-harvesting-based task scheduling and energy management framework,” ICT Express, 10(1), 39-45, 2024.

[4] M.A.L. Sarker, M.O.F. Sarker and D.S. Han, ”A survey on digital twin-assisted intelligent vehicle localization,” ICT Express, 2025.

[5] J. N. Njoku, E. C. Nkoro, R. M. Medina, C. I. Nwakanma, J. -M. Lee and D. -S. Kim, ”Leveraging Digital Twin Technology for Battery Management: A Case Study Review,” in IEEE Access, vol. 13, pp. 21382-21412, 2025, doi: 10.1109/ACCESS.2025.3531833.

[6] H. Lee, S. Jung, and J. Kim, ”Truthful electric vehicle charging via neural-architectural Myerson auction,” ICT Express, 7(2), 196-199, 2021.

[7] A. Caliwag, and W. Lim, ”Optimal least square vector autoregressive moving average for battery state of charge estimation and forecasting,” ICT Express, 7(4), 493-496, 2021.

[8] M. Pooyandeh and I. Sohn, ”A Time-Stamp Attack on Digital Twin-Based Lithium-ion Battery Monitoring for Electric Vehicles,” 2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Osaka, Japan, 2024, pp. 499-502, doi: 10.1109/ICAIIC60209.2024.10463501.

[9] F. L. Faria, A. K. de Oliveira, and R. Rüther, ”A sustainable blockchain-based framework to develop the Li-ion second-life batteries market,” Energy, 316, 134603, 2025.

[10] JJ. Zhong et al., ”Blockchain-Based EV Constant Function Pricer and Oraclized State of Charge Estimator,” in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 12, pp. 21769-21782, Dec. 2024, doi: 10.1109/TITS.2024.3469890.

[11] S. Liu, C. Wu, J. Huang, Y. Zhang, M. Ye and Y. Huang, ”Blockchain-Based Interpretable Electric Vehicle Battery Life Prediction in IoV,” in IEEE Internet of Things Journal, vol. 11, no. 4, pp. 7214-7227, 15 Feb.15, 2024, doi: 10.1109/JIOT.2023.3315483.

[12] B. C. Florea, ”Electric Vehicles Battery Management Network Using Blockchain IoT,” 2020 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj-Napoca, Romania, 2020, pp. 1-6, doi: 10.1109/AQTR49680.2020.9129916.

[13] B. Couraud, V. Robu, D. Flynn, M. Andoni, S. Norbu and H. Quinard, ”Real-Time Control of Distributed Batteries With Blockchain-Enabled Market Export Commitments,” in IEEE Transactions on Sustainable Energy, vol. 13, no. 1, pp. 579-591, Jan. 2022, doi: 10.1109/TSTE.2021.3121444.

[14] Chen Fei, October 13, 2022, ”Lithium-ion battery data set”, IEEE Dataport, doi: https://dx.doi.org/10.21227/fh1g-8k11.