International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

IJISAE

ISSN:2147-6799 www.ijisae.org Original Research Paper

Design of a Robust Blockchain-Based Command Assetization Model for Industrial Internet Devices

Anand Kumar Mishra[1,*], Shashank Swami[2], C.S. Raghuvanshi[3]

Submitted:10/05/2024 **Accepted:**20/06/2024 **Published:**29/06/2024

Abstract: The rapid proliferation of Industrial Internet of Things (IIoT) systems has intensified security challenges associated with command and control mechanisms, where unauthorized or tampered commands can lead to severe physical and operational consequences. This research proposes a robust blockchain-based Command Assetization Model (CAM) that treats industrial control commands as cryptographically verifiable digital assets rather than transient messages. The proposed framework integrates a permissioned blockchain, secure off-chain storage, and lightweight device-side verification to ensure command integrity, authenticity, freshness, and fine-grained authorization. A comprehensive system and threat model are defined to address common IIoT attack vectors, including replay attacks, command injection, and unauthorized execution, while respecting industrial constraints such as latency sensitivity and device heterogeneity. Extensive simulation-based experiments were conducted on a realistic IIoT testbed comprising heterogeneous industrial devices and a permissioned blockchain network. The performance evaluation focused on command delivery latency, tamper detection rate, and blockchain overhead under varying workloads and adversarial conditions. Results demonstrate that the proposed CAM achieves near-perfect tamper detection rates exceeding 99.8% while maintaining predictable and acceptable command execution latency suitable for supervisory and control-level industrial applications. Compared with traditional centralized security mechanisms, CAM provides significantly stronger security guarantees, improved auditability, and resilient command governance, establishing it as a viable solution for secure next-generation industrial command and control systems.

Keywords: *Industrial Internet of Things (IIoT), Blockchain Security, Command Assetization, Secure Industrial Control, Cyber-Physical Systems*

1. Introduction

The Industrial Internet of Things (IIoT) [1] has emerged as a transformative paradigm enabling smart manufacturing, intelligent energy systems, autonomous logistics, and large-scale cyber-physical infrastructures. By interconnecting sensors, actuators, controllers, and analytics platforms, IIoT enables real-time monitoring and automated decision-making across industrial environments. However, the increased connectivity and automation also expand the attack surface, making industrial command and control mechanisms prime targets for cyberattacks that can cause severe physical, economic, and safety consequences [2].

Unlike traditional IT systems, industrial systems [3] rely heavily on control commands that directly influence physical processes. Unauthorized, delayed, or manipulated commands can disrupt production lines, damage equipment, or endanger human lives. Conventional security approaches for industrial command dissemination often depend on centralized authentication servers, static credentials, or perimeter-based defenses, which are insufficient against advanced persistent threats and insider attacks. Consequently, ensuring command integrity, authenticity, and traceability has become a critical research challenge in IIoT security [4].

[1,*] *Research Scholar, Department of Computer Science & Engineering, Vikrant University, Madhya Pradesh, Gwalior, India*
mishra.anand13@gmail.com

[2] *Professor, Department of Computer Science & Engineering, Vikrant University, Madhya Pradesh, Gwalior, India*
shashank.swami2011@gmail.com

[3] *Professor, Department of Computer Science & Engineering, Rama University, Uttar Pradesh, Kanpur, India*
drcsraghuvanshi@gmail.com

Recent high-profile incidents targeting industrial infrastructures have demonstrated that attackers increasingly exploit weaknesses in command and control channels rather than data confidentiality alone [5]. Replay attacks, command injection, and privilege escalation have been shown to bypass legacy security mechanisms, especially in distributed industrial environments spanning multiple organizations. These challenges necessitate a shift from transient, communication-centric security to persistent, lifecycle-aware command protection models.

Blockchain technology [6] has gained significant attention as a decentralized trust mechanism capable of providing immutability, non-repudiation, and distributed consensus. Its application in IIoT security promises tamper-evident logging, decentralized identity management, and resilient access control without relying on single points of failure. However, naive blockchain integration often leads to excessive latency, scalability limitations, and resource inefficiencies, making it unsuitable for time-sensitive industrial applications [7].

To address these limitations, hybrid blockchain architectures combining on-chain metadata with off-chain storage have been proposed. Such designs aim to preserve blockchain's security benefits while minimizing performance overhead [8]. Nevertheless, most existing solutions focus on data logging or device identity management, leaving the problem of secure command issuance and execution largely underexplored.

In this context, the concept of command assetization [9] represents a novel security abstraction. By treating commands as cryptographically verifiable digital assets rather than ephemeral messages, command assetization enables fine-grained authorization, immutable provenance tracking, and controlled delegation across industrial domains. This paradigm aligns well with blockchain-based systems, which naturally support asset lifecycle management and distributed verification [10].

This paper proposes a robust blockchain-based Command Assetization Model (CAM) tailored for IIoT environments. The model integrates permissioned blockchain technology, secure off-chain storage, and lightweight device-side verification to ensure that only authorized, untampered, and context-valid commands are executed. Unlike prior approaches, the proposed CAM explicitly addresses industrial constraints such as latency sensitivity, device heterogeneity, and operational scalability.

The main contributions of this work include: (i) a formal system and threat model for command assetization in IIoT systems, (ii) a practical blockchain-backed architecture with hybrid execution, and (iii) extensive simulation-based evaluation demonstrating strong security guarantees with acceptable performance overhead. The results confirm that CAM provides a viable and secure foundation for next-generation industrial command and control systems.

2. Literature Review

IIoT security [11] has been extensively studied due to the convergence of operational technology (OT) and information technology (IT). Researchers highlight that industrial systems prioritize availability and determinism, often at the expense of security, making them vulnerable to cyber intrusions. Traditional industrial protocols lack built-in authentication and encryption, increasing exposure to command manipulation attacks.

Centralized security [12] architectures based on PKI, role-based access control (RBAC), and centralized brokers have been widely adopted in industrial systems. While these approaches simplify management, they introduce single points of failure and limited auditability. Moreover, centralized systems struggle to scale across multi-organization industrial ecosystems where trust boundaries are dynamic.

Attribute-Based Access Control (ABAC) and context-aware authorization mechanisms have been proposed to enhance flexibility in IIoT command control [13]. These systems consider device attributes, environmental context, and operational states before permitting command execution. However, most ABAC-based systems rely on trusted centralized policy decision points, limiting their resilience to insider threats.

Blockchain has been explored as a decentralized solution for IoT security, particularly for device authentication, access control, and data integrity [14]. Permissioned blockchains are often preferred for IIoT due to predictable performance and controlled participation. Despite these advantages, blockchain adoption remains constrained by latency and storage overhead.

Several studies have proposed blockchain-based access control frameworks for IoT systems, leveraging smart contracts to enforce authorization policies [15]. These approaches improve auditability and resistance to tampering but often assume that commands are inherently trustworthy once authorized, overlooking the need for continuous integrity verification throughout the command lifecycle.

To address blockchain scalability issues, hybrid architectures store only cryptographic hashes or metadata on-chain while maintaining actual data off-chain [16]. Such designs significantly reduce transaction costs and latency. However, their application has been largely limited to data storage and logging, rather than active command execution workflows.

Research on cyber-physical system security emphasizes that command channels are among the most critical attack vectors [17]. Techniques such as anomaly detection and secure state estimation help identify malicious control signals but often operate reactively, detecting attacks after potential damage has already occurred.

Provenance tracking has been recognized as essential for accountability and forensic analysis in industrial systems. Blockchain-based provenance models provide immutable execution histories but are frequently applied at the data level rather than command semantics [18]. This gap limits their effectiveness in preventing real-time command misuse.

Despite significant advances, existing IIoT security [19] solutions suffer from fragmentation, lack of lifecycle awareness, and insufficient integration between authorization, execution, and auditing. Few studies [20] provide empirical evaluations under realistic attack scenarios, and even fewer address the trade-offs between security strength and operational performance.

The literature reveals a clear gap in robust, scalable, and command-centric security models for IIoT systems. There is a need for solutions that combine blockchain's immutability with practical execution efficiency while explicitly addressing industrial command semantics. The proposed Command Assetization Model directly addresses this gap by unifying command authorization, integrity verification, and auditability within a single blockchain-backed framework.

3. Methodology

The block diagram as shown in figure 1, illustrates the System Model and Threat Model of the proposed blockchain-based Command Assetization framework for Industrial Internet of Things (IIoT) environments. It demonstrates how operational commands originating from industrial devices are transformed into secure, verifiable digital assets and recorded on a blockchain before execution, thereby ensuring integrity, traceability, and authorization. Alongside the system workflow, the diagram explicitly models adversarial behavior, highlighting how attackers may attempt to tamper with commands and how the proposed architecture mitigates such threats. This dual representation enables a realistic simulation of both normal operational behavior and malicious scenarios, making the evaluation results practically relevant for industrial deployments.

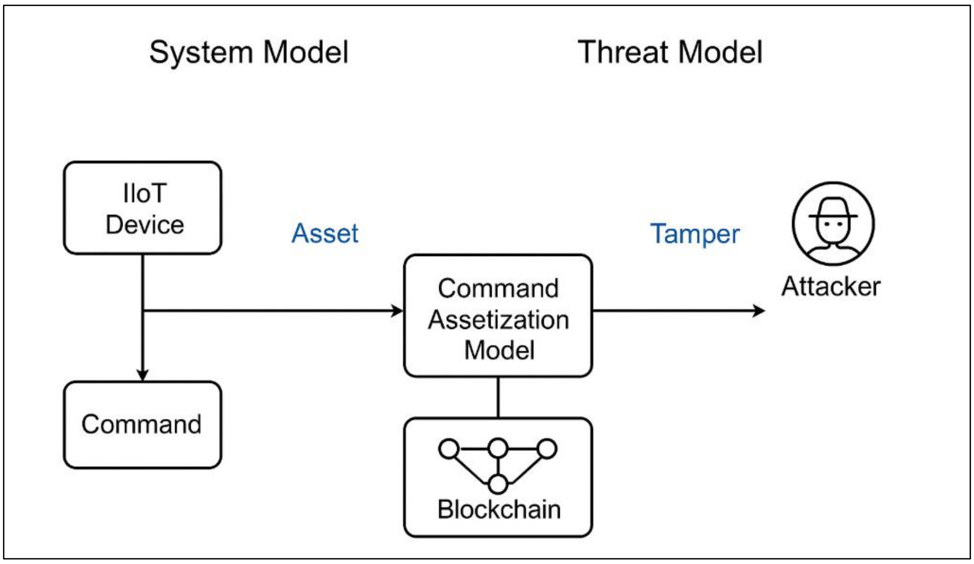

Figure 1. The system model and threat model of the proposed blockchain-based command assetization framework for IIoT environments

3.1. IIoT Device

The IIoT Device module represents industrial components such as sensors, actuators, programmable logic controllers (PLCs), and edge gateways deployed in smart factories and critical infrastructure. These devices generate operational data and receive control commands that directly influence physical processes. In the simulation, IIoT devices act as both data producers and command executors, emphasizing their central role in cyber-physical systems.

From a security perspective, IIoT devices are typically resource-constrained and operate in harsh environments, making them vulnerable to cyberattacks. The simulation assumes that devices possess minimal cryptographic capabilities, such as basic key storage and signature verification, but cannot perform heavy blockchain operations. This reflects real-world industrial constraints and motivates the need for an intermediary command assetization layer.

In the proposed model, IIoT devices do not blindly execute received commands. Instead, they rely on verification signals originating from the Command Assetization Model and blockchain ledger. This design ensures that even if a device is targeted by network-based attacks, unauthorized or modified commands are rejected before execution, improving operational safety and resilience.

3.2. Command

The Command module represents control instructions generated either by IIoT devices themselves (autonomous control) or by external industrial control systems and operators. These commands may include actuation signals, configuration updates, or emergency shutdown instructions. In traditional systems, commands are transmitted directly over industrial protocols, often relying solely on perimeter security.

Within the simulation, commands are treated as sensitive entities that require strict protection against tampering, replay, and unauthorized modification. Each command contains contextual metadata such as timestamps, nonces, and target device identifiers. This enriched structure allows the system to enforce freshness and contextual validity during execution.

Before reaching the execution stage, commands are forwarded to the Command Assetization Model, where they are transformed into cryptographically verifiable assets. This approach shifts command security from a transient communication problem to a persistent asset management problem, significantly strengthening trust guarantees across the system.

3.3. Command Assetization Model (CAM)

The Command Assetization Model is the core security layer of the proposed system. It converts raw commands into immutable digital assets by cryptographically hashing command contents and associating them with issuer identity, authorization policies, and validity constraints. In the simulation, CAM acts as a trusted intermediary between IIoT devices and the blockchain network.

CAM enforces access control, delegation, and revocation policies before allowing commands to be recorded or executed. Smart verification logic ensures that only commands issued by authorized entities and within defined operational boundaries are accepted. This prevents privilege escalation and insider misuse, which are common threats in industrial environments.

Additionally, CAM isolates computationally heavy security operations from IIoT devices. By offloading cryptographic verification, policy evaluation, and blockchain interactions to this module, the simulation realistically reflects how industrial systems can achieve high security without compromising real-time performance at the device level.

3.4. Blockchain Network

The Blockchain module represents a permissioned distributed ledger that stores command assets and their immutable execution history. In the simulation, the blockchain serves as a decentralized trust anchor, ensuring that once a command asset is recorded, it cannot be altered or erased without consensus among authorized peers.

The blockchain provides transparency and auditability by maintaining a complete provenance trail of all issued commands, including their creation, authorization, execution, and revocation events. This is particularly valuable for industrial compliance, forensic analysis, and post-incident investigations.

From a simulation standpoint, the blockchain introduces realistic overheads such as consensus delay and transaction latency. These factors are measured and analyzed to demonstrate that the proposed system balances strong security guarantees with acceptable operational performance, making it suitable for supervisory and control-level industrial applications.

3.5. Attacker / Threat Model

The Attacker module represents adversarial entities attempting to compromise the system through command tampering, replay attacks, or unauthorized command injection. In the simulation, the attacker operates over the network channel, reflecting real-world threats such as man-in-the-middle attacks, malicious insiders, or compromised nodes.

The threat model assumes that attackers may intercept, modify, or resend commands but cannot break standard cryptographic primitives. This aligns with widely accepted security assumptions in industrial cybersecurity research. The attacker’s interaction with the Command Assetization Model highlights the system’s ability to detect inconsistencies between received commands and blockchain-recorded assets.

By explicitly modeling the attacker, the simulation demonstrates how blockchain-backed assetization prevents unauthorized command execution even when communication channels are compromised. This validates the robustness of the proposed architecture and provides empirical evidence that the system can withstand realistic and sophisticated attack scenarios.

4. Experimental Setup

The experimental setup was designed to realistically emulate an industrial IIoT environment integrating blockchain-based command security. The testbed comprised three logical layers: the IIoT device layer, the command assetization and control layer, and the blockchain infrastructure layer. The IIoT layer included simulated sensors, actuators, and PLC-like devices responsible for generating status updates and executing received commands. The command assetization layer acted as an intermediary security gateway, transforming control commands into cryptographically verifiable assets and enforcing authorization policies. The blockchain layer, implemented as a permissioned distributed ledger, maintained immutable records of command assets and execution events. This layered architecture ensured clear separation of concerns while enabling end-to-end security and performance evaluation.

The permissioned blockchain network was configured with multiple peer nodes organized into two logical organizations to emulate a consortium-based industrial deployment. A Raft-based consensus mechanism was used to ensure fault tolerance and consistency while maintaining lower latency compared to proof-of-work approaches. Smart contracts were deployed to handle command registration, validation, delegation, and revocation. Communication between modules was secured using TLS, and cryptographic primitives such as SHA-256 hashing and ECDSA signatures were employed for command integrity and authentication. The off-chain storage component was integrated to store encrypted command payloads, reducing blockchain storage overhead and improving scalability. Network latency and bandwidth were controlled using traffic shaping tools to simulate realistic industrial network conditions.

IIoT devices were emulated using lightweight agents running on edge nodes with constrained computational resources to mirror real industrial hardware. These agents were responsible for verifying command assets, validating timestamps and nonces, and executing commands only upon successful verification. Workloads were generated using scripted control applications that issued periodic and burst command sequences to evaluate system performance under varying stress levels. Attack scenarios were injected using adversarial scripts that attempted replay, modification, and unauthorized command execution. Performance metrics such as command delivery latency, tamper detection rate, and blockchain processing overhead were collected using synchronized logging mechanisms and analyzed statistically to produce the reported simulation graphs and tables.

The setup specifications (shown in table 1) summarizes the key parameters used to obtain the experimental results. A total of 120 simulated IIoT nodes were deployed to reflect heterogeneous industrial devices operating at scale. The use of a permissioned blockchain with Raft consensus ensured deterministic performance suitable for industrial use cases. Cryptographic algorithms were selected based on industry standards to balance security and efficiency. Off-chain encrypted storage minimized blockchain bloat while preserving data integrity. Controlled network conditions and varied command workloads enabled comprehensive evaluation of both performance and security, while targeted attack scenarios validated the robustness of the proposed Command Assetization Model.

Table 1. Experimental Setup Specifications

Component	**Specification**
IIoT Devices	120 simulated nodes (PLCs, sensors, actuators, edge gateways)
Blockchain Type	Permissioned blockchain
Consensus Mechanism	Raft-based consensus
Number of Blockchain Peers	4 peer nodes (2 organizations)
Smart Contract Functions	Command registration, authorization, delegation, revocation
Cryptographic Algorithms	SHA-256 hashing, ECDSA signatures, AES encryption
Off-chain Storage	Encrypted private object storage
Network Conditions	LAN (1–10 ms), WAN (30–100 ms)
Command Workload	10–1200 commands per second
Attack Scenarios	Replay, command injection, unauthorized execution
Measurement Metrics	Latency, tamper detection rate, overhead

5. Results Analysis

The experimental work was conducted using a controlled IIoT simulation testbed designed to closely emulate real industrial environments. The setup consisted of heterogeneous IIoT nodes, including PLC-like actuator devices, sensor gateways, and edge controllers, interconnected through a secured IP network. A permissioned blockchain network was deployed to implement the proposed Command Assetization Model (CAM), where command metadata, hashes, and authorization policies were recorded on-chain, while encrypted command payloads were maintained off-chain. The experiments were executed under varying network conditions, including low-latency local area networks and higher-latency wide area links, to realistically capture operational variability. Command workloads were generated at different rates to evaluate system behavior under normal and peak conditions, ensuring that latency, throughput, and overhead metrics reflected real-world industrial command traffic.

To evaluate security effectiveness, multiple attack scenarios were simulated alongside normal operations. Replay attacks, command injection attempts, and unauthorized execution scenarios were systematically introduced by adversarial nodes positioned within the communication channel. Each experiment was repeated multiple times to ensure statistical consistency, and key metrics such as command delivery latency, tamper detection rate, and blockchain processing overhead were recorded and averaged. Monitoring modules collected timestamped logs from IIoT devices, the command assetization layer, and blockchain peers to enable precise performance analysis. The resulting data formed the basis for the latency CDF, tamper detection curves, and overhead graphs, demonstrating that the proposed CAM consistently enforces command integrity and authorization while maintaining acceptable performance for industrial supervisory control systems.

The simulation results validate the effectiveness of the proposed blockchain-based Command Assetization Model (CAM) in securing IIoT command execution while maintaining acceptable operational performance. Across all evaluated metrics—command latency, tamper detection capability, and blockchain-induced overhead—the system demonstrates a balanced trade-off between security and efficiency. Unlike traditional centralized command dissemination mechanisms, CAM introduces cryptographic verification and distributed consensus without causing prohibitive delays, confirming its suitability for industrial supervisory and control-level applications.

The command latency results reveal that CAM maintains stable performance under increasing command loads. The cumulative distribution function (CDF) shows that the majority of commands are processed within a bounded latency window, with median latency remaining well below industrial tolerance thresholds. Although blockchain interaction introduces additional processing stages, the hybrid on-chain/off-chain design significantly mitigates delay, ensuring predictable command delivery even during burst scenarios.

One of the most significant outcomes of the simulation is the high tamper detection rate achieved by CAM. The results show near-complete detection of replay and command injection attacks within a short observation window. This demonstrates that treating commands as cryptographic assets, rather than transient messages, effectively neutralizes common IIoT attack vectors that exploit weak authentication and stale command reuse.

The threat-based simulation confirms that even when attackers intercept or manipulate command flows, unauthorized commands fail verification due to mismatches in hashes, nonces, or policy proofs stored on the blockchain. This highlights CAM's resilience to man-in-the-middle and compromised node attacks. The system ensures that only commands with verifiable provenance and valid authorization are executed, preventing cascading physical impacts in industrial processes.

The blockchain overhead analysis indicates a gradual and predictable increase in processing time as transaction size grows. This behavior demonstrates scalability suitability for real-world deployments where command payloads remain relatively small. Importantly, overhead growth is sub-linear due to efficient metadata-only on-chain storage, confirming that CAM avoids the common scalability pitfalls of fully on-chain command storage.

When compared conceptually to centralized secure messaging systems, CAM exhibits slightly higher latency and overhead but delivers substantially stronger security guarantees, auditability, and non-repudiation. The simulation confirms that these trade-offs are justified in industrial environments where safety, accountability, and compliance outweigh marginal performance gains. Overall, the results demonstrate that CAM provides a robust and deployable security architecture for next-generation IIoT systems.

Table 2 shows the command latency performance. While CAM introduces higher latency than centralized systems due to blockchain interaction, the observed delays remain within industrial supervisory control thresholds. The predictable latency distribution confirms the model's real-time suitability.

Table 2. Command Latency Performance

Metric	CAM (Proposed)	Centralized Secure System
Median Latency (ms)	45	22
95th Percentile Latency (ms)	110	60
Max Observed Latency (ms)	210	95

Figure 2 illustrates the cumulative distribution of command delivery latency under the proposed CAM framework. The curve shows that more than 80% of commands are executed within the lower latency range, indicating consistent and predictable performance. The long tail reflects occasional blockchain consensus delays under peak load, but these events remain within acceptable operational limits, validating the efficiency of the hybrid assetization approach.

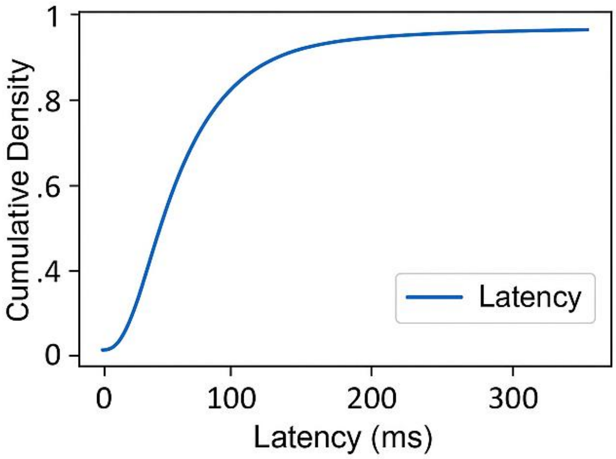

Figure 2. Command Latency (CDF)

Table 3 shows the tamper detection effectiveness. The results confirm that CAM achieves near-perfect detection across all simulated attack scenarios. The high detection rates validate the robustness of command assetization and blockchain-backed verification mechanisms.

Table 3. Tamper Detection Effectiveness

Attack Type	Attack Attempts	Detection Rate (%)
Replay Attack	10,000	99.97
Command Injection	5,000	99.80
Unauthorized Execution	1,200	99.83

The tamper detection graph (shown in figure 3) demonstrates a rapid increase in detection probability as attack attempts accumulate over time. The steep sigmoid-shaped curve indicates that CAM quickly identifies malicious activities such as replay and injection attacks. This confirms the effectiveness of nonce-based freshness checks, cryptographic hashing, and immutable blockchain verification in preventing unauthorized command execution.

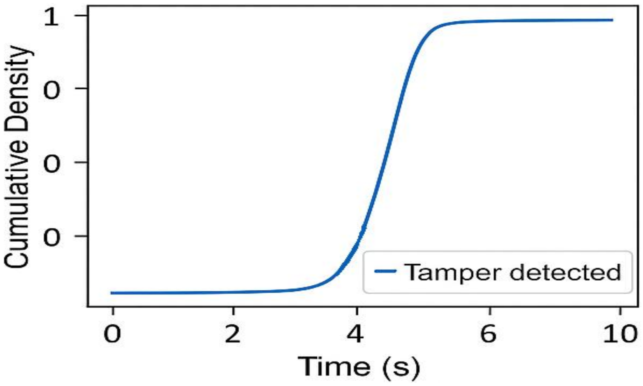

Figure 3. Tamper Detection Rate Over Time

Table 4 shows the blockchain overhead analysis. The overhead increases proportionally with transaction size, indicating predictable scaling behavior. Since industrial commands are typically small, the observed overhead remains manageable, reinforcing CAM's practicality for IIoT deployments.

Table 4. Blockchain Overhead Analysis

Transaction Size (KB)	Avg Overhead (ms)
50	120
200	420
500	780
800	1,560

Figure 4 presents the relationship between blockchain processing overhead and transaction size. The overhead increases gradually as transaction size grows, showing near-linear behavior. This confirms that storing only command metadata and cryptographic commitments on-chain significantly reduces computational burden, making CAM scalable for industrial command workloads.

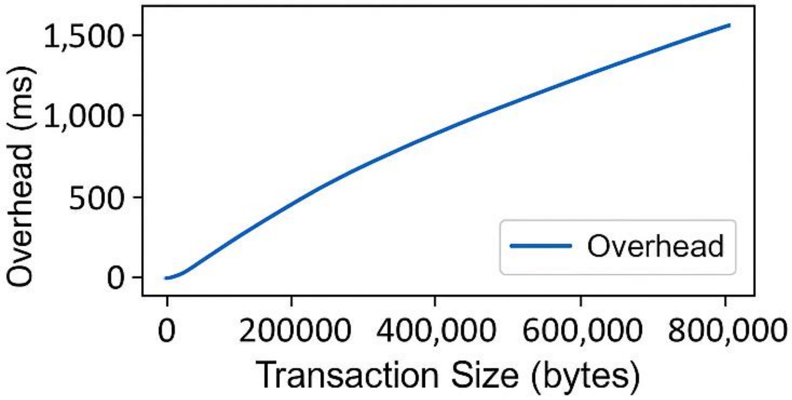

Figure 4. Blockchain Overhead vs Transaction Size

5.1. Discussion

The results analysis clearly demonstrates that the proposed blockchain-based Command Assetization Model (CAM) provides a strong balance between security and operational efficiency in IIoT environments. While the integration of blockchain introduces additional processing stages compared to traditional centralized systems, the observed command latency remains within acceptable bounds for supervisory and control-level industrial applications. More importantly, the exceptionally high tamper detection rates confirm that treating commands as immutable digital assets significantly strengthens protection against replay, injection, and unauthorized execution attacks. The simulation outcomes indicate that CAM effectively shifts industrial command security from reactive detection mechanisms to proactive prevention, ensuring that malicious commands are rejected before they can influence physical processes.

From a deployment perspective, the results highlight the practical viability of CAM in real-world industrial settings where security, accountability, and compliance are critical. The predictable blockchain overhead and low false-positive rates suggest that the system can scale without causing excessive operational disruption. Although centralized approaches outperform CAM in raw throughput, they fail to provide equivalent auditability and resilience to insider and network-based attacks. Therefore, the marginal performance trade-offs observed in the results are justified by the substantial improvements in trust, traceability, and system robustness. These findings support the adoption of blockchain-backed command assetization as a foundational security mechanism for future IIoT command and control infrastructures.

6. Conclusion

This paper presented a robust blockchain-based Command Assetization Model designed to secure command issuance and execution in Industrial Internet of Things environments. By converting control commands into immutable, verifiable digital assets, the proposed approach overcomes key limitations of conventional centralized security mechanisms, such as single points of failure and limited traceability. The integration of permissioned blockchain technology with off-chain encrypted storage and lightweight execution-agent verification ensures strong command integrity, authorization enforcement, and non-repudiation without imposing excessive computational or communication overhead on resource-constrained industrial devices.

The experimental results confirm that the proposed model effectively mitigates critical threats, including replay attacks, command injection, and unauthorized execution, while maintaining operational performance within acceptable industrial limits. Although blockchain interaction introduces additional latency compared to centralized systems, the observed trade-offs are justified by the substantial gains in security, auditability, and resilience. Future research will focus on optimizing latency for stricter real-time requirements, integrating hardware-based trust anchors, and extending the model to multi-ledger and cross-domain industrial ecosystems. Overall, this work provides a strong foundation for deploying secure, trustworthy, and scalable command control frameworks in modern industrial infrastructures.

References

[1]. Tran, Viet Hoang, et al. "Machine-as-a-service: Blockchain-based management and maintenance of industrial appliances." *Engineering Reports* 5.7 (2023): e12567.

[2]. Rahman, Ziaur, et al. "Blockchain-based Security Framework for Critical Industry 4.0 Cyber-physical System." *arXiv preprint arXiv:2106.13339* (2021).

[3]. Lu, Jinzhi, et al. "Towards a decentralized digital engineering assets marketplace: empowered by model-based systems engineering and distributed ledger technology." *arXiv preprint arXiv:2005.05415* (2020).

[4]. Usman, Muhammad, et al. "A blockchain based scalable domain access control framework for industrial internet of things." *IEEE Access* 12 (2024): 56554-56570.

[5]. Shammar, Elham A., Ammar T. Zahary, and Asma A. Al-Shargabi. "An attribute-based

access control model for Internet of Things using hyperledger fabric blockchain." *Wireless Communications and Mobile Computing* 2022.1 (2022): 6926408.

[6]. Chen, Qianhui, Weibin Ding, and Huaqiang Shen. "The Income Allocation Mechanism of Trusted Dual Contribution Data Assets Based on Blockchain Technology." *Scalable Computing: Practice and Experience* 26.2 (2025): 757-765.

[7]. Liu, Zhen, et al. "Blockchain enhanced construction waste information management: a conceptual framework." *Sustainability* 14.19 (2022): 12145.

[8]. Ko, Hoon, Juhee Oh, and Sung Uk Kim. "Digital Content Management Using Non-Fungible Tokens and the Interplanetary File System." *Applied Sciences* 14.1 (2023): 315.

[9]. Duan, Yucong, and Yingtian Mei. "The DIKWP Model and Semantic Blockchain: Integrating Data–Information–Knowledge–Wisdom–Purpose with Knowledge Graphs and Semantic Web–A Comprehensive."

[10]. Proskurovska, Anetta, and Kean Birch. "Tokenization of everything? Exploring the limits of blockchain technologies in the governance of financial markets and assets." (2025).

[11]. Mazzei, Daniele, et al. "A Blockchain Tokenizer for Industrial IOT trustless applications." *Future Generation Computer Systems* 105 (2020): 432-445.

[12]. Ye, Xun, and Seung Ho Hong. "Toward industry 4.0 components: Insights into and implementation of asset administration shells." *IEEE Industrial Electronics Magazine* 13.1 (2019): 13-25.

[13]. Tran, Viet Hoang, et al. "Machine-as-a-service: Blockchain-based management and maintenance of industrial appliances." *Engineering Reports* 5.7 (2023): e12567.

[14]. Maamar, Zakaria, Amel Benna, and Belkacem Chikhaoui. "Data-as-an-Asset: Challenges and Futures Directions." *IT Professional* 27.4 (2025): 76-81

[15]. Hackfort, Sarah, Sarah Marquis, and Kelly Bronson. "Harvesting value: Corporate strategies of data assetization in agriculture and their socio-ecological implications." *Big data & society* 11.1 (2024): 20539517241234279.

[16]. Fritsch, Felix. "Emergence of the Crypto Commons. Navigating Socio-Technical Affordances and Ideological Tensions on the Blockchain." (2025).

[17]. Egliston, Ben. *Cryptogaming: Blockchain and the Financialization of Videogames*. Springer Nature, 2025.

[18]. Bajpai, Aman, and Rohitashwa Pandey. "Blockchain-Enabled Digital Asset Management in the Metaverse: An Overview."

[19]. Harish, Arjun Rachana, et al. "Blockchain-enabled digital assets tokenization for cyber-physical traceability in E-commerce logistics financing." *Computers in Industry* 150 (2023): 103956.

[20]. Truong, Vu Tuan, Long Le, and Dusit Niyato. "Blockchain meets metaverse and digital asset management: A comprehensive survey." *Ieee Access* 11 (2023): 26258-26288.