



SMART-CONTRACT-BASED AUTHENTICATION AND DATA INTEGRITY FRAMEWORK FOR RESOURCE-CONSTRAINED IOT DEVICES

Xusainov Farhod Saidmurodovich

University of Information Technologies and Management, Master's Student

Abstract: *The rapid expansion of Internet of Things (IoT) ecosystems has increased the need for lightweight, transparent and verifiable security mechanisms. Resource-constrained IoT devices often operate with limited memory, processing power and energy capacity, while they exchange sensitive telemetry and control data in real time. This paper proposes a smart-contract-based authentication and data integrity framework that combines device identifiers, edge gateway pre-validation, cryptographic hashes, off-chain storage and an immutable blockchain audit ledger. The framework is designed to reduce dependence on a centralized server, verify device legitimacy before data exchange and provide evidence-based auditability of IoT security events. An algorithmic model, mathematical representation and analytical evaluation are presented. The results indicate that the proposed approach can improve authentication transparency, data integrity control and audit completeness while keeping blockchain load manageable through hybrid on-chain/off-chain storage.*

Keywords: *Internet of Things, blockchain, smart contract, device authentication, data integrity, edge gateway, off-chain storage, cybersecurity, audit ledger.*

INTRODUCTION

Internet of Things ecosystems are increasingly used in smart homes, smart cities, industrial automation, healthcare monitoring, logistics and energy systems. In such environments, sensors, actuators, microcontrollers, gateways, cloud platforms and user applications interact as a single cyber-physical system. The practical value of IoT depends not only on connectivity, but also on the trustworthiness of device identity, data integrity and control commands.

Conventional centralized security mechanisms are not always sufficient for large-scale IoT ecosystems. A central server may become a single point of failure, while the number of connected devices increases authentication complexity and audit workload. In addition, low-cost IoT devices frequently have limited hardware resources and cannot run heavyweight security protocols without affecting performance.

Blockchain technology offers a promising complementary mechanism for IoT security because it supports decentralized trust, immutable event records, cryptographic verification and transparent audit trails. However, storing every IoT data packet directly on a blockchain is inefficient. Therefore, this paper focuses on a hybrid framework in which smart contracts manage identity and access decisions, hashes are recorded on-chain, and large telemetry data are stored off-chain. The aim is to provide a practical balance between security, scalability and resource efficiency.

2. Related Work and Research Gap



Existing IoT security approaches usually rely on device passwords, certificates, encrypted communication channels, centralized access control and cloud-based monitoring. These mechanisms are useful, but they may become difficult to audit when a system contains thousands of heterogeneous devices. Moreover, if the central authentication server is compromised, the trust model of the whole ecosystem can be affected.

Blockchain-based IoT security studies propose decentralized identity management, transaction traceability, smart-contract-based access control and tamper-resistant logs. Nevertheless, several research gaps remain. First, many models do not clearly separate lightweight device tasks from heavier blockchain operations. Second, on-chain storage of raw IoT data increases cost and latency. Third, existing models often discuss authentication and data integrity separately, while a real IoT ecosystem requires a unified workflow from device registration to audit verification.

The research gap addressed in this paper is the lack of a compact framework that integrates edge gateway pre-validation, smart-contract-based authentication, hash-based integrity verification and off-chain storage for resource-constrained IoT devices. The proposed framework treats authentication, data integrity and auditability as interconnected security functions.

3. Proposed Smart-Contract-Based Framework

The proposed framework is named Smart-Contract Authentication and Integrity Framework for IoT (SC-AIF-IoT). It consists of four core components: IoT devices, edge gateway, blockchain smart contract and off-chain storage. IoT devices generate signed telemetry. The edge gateway performs preliminary validation and calculates the hash value of received data. The smart contract manages device registration, access policy and event recording. Large sensor datasets are stored off-chain, while their hash values and metadata are stored on the blockchain ledger.



Figure 1. Smart-contract-based authentication and integrity architecture for IoT devices.

In the framework, each device is assigned a decentralized identifier (DID) and a key pair. During registration, the device sends its identifier, public key and firmware metadata to the edge gateway. The gateway checks the request and forwards approved metadata to the smart contract. After registration, the device can transmit telemetry only if the smart contract confirms its status and access role. If the device is revoked or its signature is invalid, the request is rejected before it reaches the application layer.

4. Algorithmic Process

The authentication and integrity checking process is implemented as a sequence of lightweight and verifiable steps. The IoT device performs only basic signing and data transmission, while the edge gateway and blockchain layer perform validation, policy checking and audit recording. This distribution is important because many IoT nodes are resource-constrained and cannot process complex consensus operations directly.



Figure 2. Algorithmic flow of smart-contract-based IoT device authentication.

5. Mathematical Model

Let each IoT device be denoted as D_i . During registration, a decentralized device identifier is created as:

$$DID_i = H(PK_i || SN_i || t_{reg}), \quad (1)$$

where PK_i is the public key of the device, SN_i is the device serial number, t_{reg} is the registration time and $H(.)$ is a cryptographic hash function. The transmitted telemetry message is represented as:

$$M_i = \{DID_i, X_i, t_i, n_i, Sig_i\}, \quad (2)$$

where X_i is the sensor payload, t_i is the timestamp, n_i is a nonce and Sig_i is the digital signature. The integrity proof recorded in the blockchain ledger is calculated as:



$$h_i = H(DID_i || X_i || t_i || n_i). \quad (3)$$

The verification decision can be expressed as:

$$V_i = 1, \text{ if } \text{Verify}(PK_i, \text{Sig}_i, M_i) = \text{true and } H(DID_i || X_i || t_i || n_i) = h_i; \text{ otherwise } V_i = 0. \quad (4)$$

For analytical evaluation, the operational trust score is calculated using authentication success A_i , integrity confirmation I_i , access role validity R_i and normalized latency L_i :

$$T_i = \alpha A_i + \beta I_i + \gamma R_i - \delta L_i, \quad (5)$$

where α , β , γ and δ are weight coefficients selected according to the security policy of the IoT system. A higher T_i value indicates a more trusted device interaction, while a low value triggers additional verification or revocation.

6. Analytical Evaluation and Discussion

A scenario-based analytical evaluation was prepared to compare three security approaches: centralized authentication, blockchain without off-chain optimization and the proposed SC-AIF-IoT framework. The comparison focuses on authentication transparency, integrity verification, audit completeness, latency control and blockchain load. The values are normalized scores from 0 to 1 and are used to demonstrate expected methodological behavior rather than final deployment measurements.

Table 1. Analytical comparison of IoT security approaches

Approach	Authentication transparency	Integrity verification	Audit completeness	Latency control	Blockchain load
Centralized authentication	0.64	0.58	0.52	0.82	0.00
Blockchain without off-chain optimization	0.86	0.88	0.91	0.55	0.89
Proposed SC-AIF-IoT framework	0.90	0.92	0.94	0.76	0.41

The comparison shows that centralized authentication provides acceptable latency but lacks immutable auditability and decentralized trust. A pure blockchain approach improves transparency and integrity, but it creates high blockchain load and may increase transaction latency. The proposed framework provides a balanced result by recording only cryptographic proofs and security metadata on-chain, while storing large telemetry data off-chain. This design is more suitable for resource-constrained IoT environments because it does not require every device to interact directly with the blockchain layer.

The main practical advantage of the proposed framework is that a security event can be verified after it occurs. If a device sends suspicious data, the system can compare the payload hash with the immutable ledger record. If the hashes do not match, the data are rejected and the event is recorded. This supports forensic analysis, accountability and compliance-oriented monitoring in smart infrastructure.

7. Scientific Novelty and Practical Value



The scientific novelty of the study is the integration of device authentication, hash-based data integrity and immutable audit mechanisms into a single smart-contract-based IoT security framework. Unlike models that treat blockchain only as a storage layer, the proposed approach uses smart contracts as an active security control mechanism for registration, access policy and revocation.

The second novelty is the hybrid on-chain/off-chain architecture. Instead of storing raw IoT data directly in the blockchain, the framework records hashes, timestamps and metadata on-chain while keeping large payloads in off-chain storage. This reduces blockchain load and makes the solution more realistic for IoT systems with frequent telemetry exchange.

The practical value of the framework lies in its applicability to smart homes, smart city systems, industrial monitoring, healthcare IoT, logistics and energy infrastructure. It can support device registration, trusted data exchange, unauthorized request rejection, event auditing and post-incident verification.

8. Conclusion

This paper proposed a smart-contract-based authentication and data integrity framework for resource-constrained IoT devices. The framework combines decentralized device identifiers, edge gateway pre-validation, smart-contract-based access control, cryptographic hashes, off-chain storage and immutable audit records. The proposed architecture is designed to reduce dependence on a centralized trust server while keeping blockchain operations manageable.

The mathematical model defines device identifiers, telemetry messages, integrity proofs and verification decisions. The analytical comparison shows that the proposed hybrid framework can improve authentication transparency, integrity verification and audit completeness compared with a centralized model, while reducing blockchain load compared with a purely on-chain approach.

Future work should implement the framework on a permissioned blockchain platform such as Hyperledger Fabric, integrate it with real IoT devices and evaluate latency, throughput, energy consumption and security resistance under practical attack scenarios.

REFERENCES:

1. Rashidovich BG, Ugli NBU, Ugli NBB AI dan foydalanib, piyodalar o'tish joylarida to'xtash yoki yurishda davom etish haqida real vaqt rejimida maslahat bera oladigan murakkab qaror qabul qilish tizimini yaratmoqda //Universum: texnik fanlar. – 2026. – T. 6. – №. 1 (142). – S. 50-54.
2. Ugli NBU, Baxtiyorovna NS ilg'or biometrik autentifikatsiya tizimi: ALGORITMIK MODELLAR, XAVFSIZLIK TAHDILARI VA MULTIMODAL BAHOLASH RAMALARINI CHUKUR O'RGANISH //Universum: texnicheskie. – 2026. – T. 6. – №. 1 (142). – S. 64-68.



3. Ugli N. B. U., Ugli A. T. K. ADAPTIVE MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEMS: A HUMAN-CENTERED ANALYSIS OF DESIGN, EVALUATION, AND SECURITY CHALLENGES //Universum: технические науки. – 2026. – Т. 6. – №. 1 (142). – С. 69-72.
4. ugli Norboev B. U. et al. Artificial Intelligence in Education and the Digital Preconditions of Tertiary Expansion in Uzbekistan: ARDL Evidence from 2000–2023. – 2026.
5. Ochilova S., Berdiyev G., Xujaqulov N. Fraktal nazariyasiga asoslangan musiqa kompozitsiyasining tahliliy usullari //Journal of Transport. – 2025. – Т. 2. – №. 3. – С. 136-139.
6. Alimov U., Zohirov Q., Berdiyev G. WAYS TO DEVELOP COORDINATION SKILLS IN KURASH //Mental Enlightenment Scientific-Methodological Journal. – 2024. – Т. 5. – №. 09. – С. 9-14.
7. Pardayeva G.A., Raximqulov FUQAROLAR MUROJAATLARINI STATISTIK TAHLIL QILISH UCHUN AXBOROT TIZIMINI ISHLAB CHIQISH // UNIVERSAL AKADEMIK VA KO'P FANLI TADQIQOTLAR JURNALI. – 2026. – Т. 4. – №. 32. – С. 87-90.
8. Qodirov B. TALABALARDA KOMPLEKS MA'LUMOTLAR BAZASI KOMPETENSIYALARINI RIVOJLANTIRISH UCHUN TIZIMLANGAN PEDAGOGIK STRATEGIYALAR //Osiyo ilmiy tadqiqotlar va innovatsiyalar jurnali. – 2026. – Т. 5. – №. 1. – С. 143-147.
9. Pardayeva G. A., Choriyev B. S., Sulaymonova D. B. SUN'IY INTELLEKT TEKNOLOGIYALARIGA ASOSLANGAN RAQAMLI TA'LIMDA ADAPTIV O'QITISH METODIKASINING NAZARIY MODELI VA AMALIY ASOSLARI //Inter education & global study. – 2025. – Т. 3. – №. 10 (1). – С. 256-265.