

A Blockchain-Enabled Cybersecurity Framework for IoT-Driven Smart Campuses: Toward Decentralized Authentication and Access Governance

Author: **Dr. Vishal Bharvesh**

IT Infrastructure & Digital Transformation Leader, Bhopal, INDIA

Abstract

Educational institutions are rapidly deploying Internet of Things (IoT) technologies to enable smart classrooms, biometric-based attendance tracking, campus surveillance, access management, environmental sensing, energy optimization, laboratory automation, and other digital services. While these deployments deliver clear operational advantages, the sheer number of diverse, resource-limited devices also exposes campuses to considerable cybersecurity threats. Common concerns include weak credentialing, unauthorized entry, device spoofing, tampering with data, breaches of privacy, and heavy reliance on centralized security infrastructure. Blockchain technology offers a set of mechanisms that can help mitigate these issues by enabling decentralized trust, tamper-evident record keeping, distributed identity governance, and policy enforcement through smart contracts.

This paper puts forward a blockchain-driven cybersecurity framework tailored to IoT-enabled smart campuses, with an emphasis on decentralized authentication of connected devices, access governance, integrity of stored data, and security auditing. The framework is organized into five layers: connected devices, edge/gateway infrastructure, a permissioned blockchain, smart contracts, and institution-facing applications. A combined on-chain/off-chain storage strategy is introduced, whereby security-related metadata — device identities, access rules, and cryptographic hashes — resides on the blockchain, while bulkier or more sensitive data is kept in off-chain repositories. To assess both the security posture and operational performance of the framework, a set of research questions and testable hypotheses is formulated. A proposed testbed contrasts the blockchain-driven design against a traditional centralized architecture across metrics such as authentication delay, authorization delay, throughput of transactions, processing burden, network overhead, scalability, storage demand, and resilience to attacks. The work does not claim that blockchain can substitute for established cybersecurity practices; rather, it explores blockchain's potential as a supplementary layer of trust and accountability within smart-campus IoT ecosystems.

Index Terms— *Blockchain, Internet of Things, IoT security, smart campus, educational institutions, cybersecurity, authentication, access control, smart contracts, data integrity, privacy.*

I. Introduction

Campuses of colleges and universities are progressively transforming into digitally interconnected spaces. IoT devices now support smart classrooms, automated attendance, surveillance of campus grounds, entry control, energy oversight, lab automation, environmental sensing, and a range of other academic and administrative functions. This trend has given rise to the concept of the smart campus, in which physical infrastructure is tied to digital systems through IoT, cloud platforms, edge computing, artificial intelligence, and related technologies.

Yet greater connectivity brings greater exposure to cyber threats. IoT hardware frequently suffers from constrained processing power, a mix of incompatible communication standards, extended service lifespans, weak default settings, and uneven security maintenance. A single compromised device can serve as a foothold for attackers to penetrate the broader institutional network. As a result, universities need to actively manage device identification, credentialing, access restrictions, data safeguarding, patching, monitoring, and overall device security.

Guidance from NIST on IoT cybersecurity outlines several critical device capabilities, including identifying devices uniquely, configuring them securely, protecting data, controlling logical access to interfaces, supporting software updates, maintaining awareness of cybersecurity status, and securing the device itself. NIST further stresses that organizations ought to define cybersecurity requirements for IoT devices in proportion to the risk these devices pose once integrated into broader information systems.

Traditional IoT security designs typically rely on centralized servers to handle authentication and authorization. While centralized models can operate efficiently, they create a single point of dependency: if the central authority fails or is breached, security across the entire ecosystem may be compromised. Within a

university setting — spanning numerous departments, administrative offices, IoT subnetworks, and external vendors — a decentralized model may offer greater trustworthiness and traceability.

Blockchain functions as a distributed ledger maintained collectively by participating nodes. Because of its cryptographic design, any unauthorized tampering with stored records becomes detectable, and smart contracts allow predefined rules to be executed automatically. These characteristics position blockchain as a candidate technology for IoT authentication, access governance, and security auditing.

That said, blockchain carries its own drawbacks — transaction delays, added computational load, expanding storage needs, privacy trade-offs, key-management burdens, and the risk of flawed smart-contract logic. Blockchain should therefore not be regarded as a wholesale substitute for existing security tools.

The central research problem this paper addresses is:

How can blockchain be woven into the IoT infrastructure of educational institutions to strengthen device authentication and access governance, while keeping performance, scalability, and privacy at acceptable levels?

This paper's contributions include:

1. Identifying the cybersecurity requirements relevant to IoT deployments in academic settings.
2. Proposing a five-layer architecture that combines blockchain with IoT security.
3. Designing a decentralized device-authentication scheme paired with smart-contract-driven access control.
4. Proposing a hybrid on-chain/off-chain approach to data management.
5. Formulating research questions and hypotheses.
6. Building an experimental framework to compare centralized and blockchain-based IoT security models.

II. Related Work and Research Gap

A. IoT Cybersecurity

IoT devices open additional entry points into networked infrastructure and raise concerns tied to safeguarding the devices themselves, the data they generate, their interfaces, and the systems they connect to. NIST's catalog of IoT cybersecurity capabilities details expectations across device identification, data protection, logical access control, secure update mechanisms, cybersecurity-state awareness, and device security.

For this research, device identity and logical access control carry particular weight. NIST's recommendations call for the ability to uniquely identify each device, confirm its identity, authenticate it, and block unauthorized interactions.

Protecting data is likewise essential, since IoT devices frequently handle sensitive information in transit. NIST points to cryptographic techniques, key management, secure storage, and secure transmission as core data-protection capabilities for IoT.

B. Blockchain for IoT Security

Blockchain can serve as a distributed means of managing device identities and logging security-relevant transactions. Within an IoT deployment, it can store data such as device identities, public keys, access rules, revocation states, and hashes of security events.

Smart contracts can automate the decision-making behind access requests — for instance, confirming that a device is properly registered, that its status remains active, and that the requesting user holds the necessary permissions for a given resource.

Even so, blockchain alone cannot resolve every IoT security concern. A sensor that has been compromised may still produce falsified readings, regardless of whether that data is faithfully logged on-chain. Blockchain must therefore work alongside conventional protections such as encryption, secure firmware, network segmentation, intrusion detection, and ongoing device monitoring.

C. Research Gap

Prior work has explored blockchain-based IoT security and decentralized access control more broadly. Still, more research is needed that directly targets the operational realities of educational IoT environments.

A smart campus is characterized by:

- a large and heterogeneous population of IoT devices;
- a diverse user base — students, faculty, administrators, visitors, and maintenance staff;
- varying levels of access privilege;
- data that is often privacy-sensitive;
- devices with limited processing resources;
- institutional governance obligations.

The gap this study aims to fill, then, is the design and empirical testing of a permissioned blockchain-based authentication and access-control architecture built specifically for IoT-enabled educational settings.

III. Research Objectives and Questions

A. Research Objectives

RO1: Pinpoint the principal cybersecurity threats confronting IoT ecosystems within educational institutions.

RO2: Architect a blockchain-driven approach for decentralized authentication of IoT devices.

RO3: Build a smart-contract-based mechanism for controlling access to campus IoT resources.

RO4: Examine how blockchain can support data integrity and security auditing.

RO5: Contrast the proposed architecture against conventional, centralized IoT security models.

RO6: Assess security outcomes, latency, throughput, scalability, and computational load.

B. Research Questions

RQ1: What are the principal cybersecurity threats facing IoT ecosystems in educational institutions?

RQ2: In what ways can blockchain enable decentralized authentication of IoT devices?

RQ3: How well can smart contracts enforce access-control policies for IoT resources?

RQ4: What performance costs arise from blockchain-based authentication and authorization?

RQ5: How does system performance change as the number of connected IoT devices grows?

RQ6: How might blockchain and off-chain storage be combined to strengthen data integrity while safeguarding sensitive institutional data?

IV. Research Hypotheses

The following hypotheses can be empirically tested.

H1: The proposed blockchain-based authentication scheme lowers the rate of successful unauthorized device authentication relative to a centralized scheme.

H2: Access control enforced through smart contracts yields more consistent policy enforcement than a conventional centralized approach.

H3: Security logs maintained on blockchain offer stronger tamper resistance and auditability than traditional centralized logs.

H4: Blockchain-based authentication and authorization impose extra latency and computational cost compared with centralized authentication.

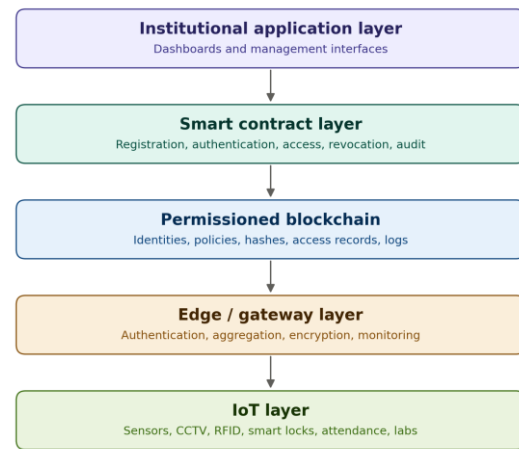
H5: As the number of IoT devices and blockchain transactions grows, system performance is negatively affected.

Corresponding null hypotheses assume no statistically meaningful difference between the approaches under comparison.

V. Proposed System Architecture

The proposed system contains five layers.

Fig. 1. Blockchain-Based Smart-Campus Architecture



A. IoT Layer

This layer comprises the physical devices deployed across the smart campus — sensors, cameras, smart locks, RFID readers, attendance terminals, energy meters, and laboratory instruments. Each device is provisioned with a distinct identity and its own cryptographic credentials.

B. Edge/Gateway Layer

The gateway sits between IoT devices and the blockchain network, handling authentication, aggregating data, converting protocols, applying encryption, and performing preliminary security checks. This role matters because most IoT devices lack the memory, processing power, and energy budget needed to maintain a full blockchain ledger themselves.

C. Permissioned Blockchain Layer

Rather than a public blockchain, the proposed system relies on a permissioned blockchain, with nodes operated by authorized institutional stakeholders — IT services, campus security, administration, and select academic departments.

The blockchain retains:

- device identities;
- public keys;
- access policies;
- device status;
- access records;
- data hashes;
- security-event metadata.

D. Smart-Contract Layer

Five smart contracts underpin the system:

1. Device Registration Contract — onboards approved devices.

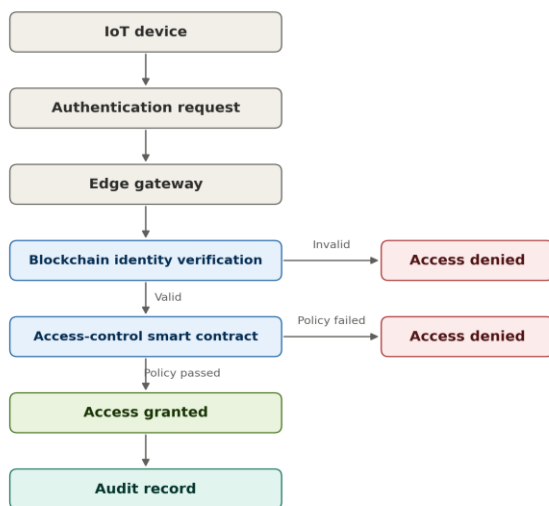
2. Authentication Contract — checks device credentials.
3. Access-Control Contract — assesses access requests.
4. Revocation Contract — deactivates compromised devices.
5. Audit Contract — logs security events.

E. Application Layer

Administrators and other authorized staff interact with the system via dashboards built for device management, access-policy administration, security monitoring, and audit review.

VI. Decentralized Authentication and Access Control

The proposed authentication workflow proceeds as follows:



An access decision can be modeled as a function:

$$Access = f(ID, Role, Device, Resource, Time, Location, Status)$$

where ID denotes the authenticated identity, Role the user's assigned role, Device the requesting IoT device, Resource the item being requested, Time the moment of the request, Location contextual positioning data, and Status the current security state.

As an illustration, a faculty member might be granted entry to a smart classroom during a scheduled class session, whereas a student's access could be restricted to a narrower set of permissions.

TABLE I — EXAMPLE ACCESS-CONTROL POLICY

Entity	Resource	Permission
Student	Classroom sensor	Limited
Student	CCTV	Denied
Faculty	Smart classroom	Authorized
Security staff	CCTV	Authorized
Administrator	IoT management	Full
Maintenance staff	Building systems	Temporary
Unknown device	Campus IoT	Denied

VII. On-Chain/Off-Chain Data Management

Recording every single IoT reading directly on the blockchain would quickly create storage bottlenecks and undermine scalability. To avoid this, the study proposes a hybrid storage design.

TABLE II — DATA STORAGE MODEL

Information	Storage
Device identity	Blockchain
Public key	Blockchain
Device status	Blockchain
Access policies	Blockchain
Security-event hash	Blockchain
Timestamp	Blockchain
Sensor data	Off-chain
CCTV video	Off-chain
Biometric information	Off-chain
Student records	Off-chain
Large datasets	Off-chain

For a given piece of data D, the system computes and stores its hash on the blockchain:

$$H(D) = SHA256(D)$$

To verify integrity later, the system recomputes the hash of the current version of the data:

$$H(D') = SHA256(D')$$

If $H(D') = H(D)$, the data has remained unchanged since it was recorded; a mismatch signals that the data may have been altered.

This approach also limits privacy exposure, since sensitive content is not needlessly duplicated across every blockchain node.

VIII. Threat Model

TABLE III — THREATS AND COUNTERMEASURES

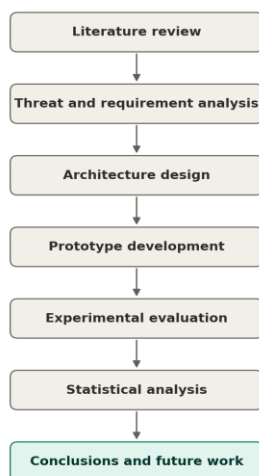
Threat	Countermeasure
Device impersonation	Cryptographic device identity
Unauthorized access	Smart-contract authorization
Data tampering	Hash verification
Compromised device	Monitoring and revocation
Replay attack	Nonce/timestamp mechanism
Insider misuse	Fine-grained policies and audit logs
DoS attack	Rate limiting and conventional network defenses

Blockchain functions best as one layer within a broader defense-in-depth strategy — it cannot, by itself, stop malware infections, denial-of-service attacks, compromised firmware, or falsified sensor readings.

IX. Research Methodology

The proposed methodology unfolds across six stages.

Fig. 2. Research Methodology



A. Literature Review

The review should draw from IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Scopus, Web of Science, and Google Scholar.

Recommended search strings include:

- "blockchain AND IoT security AND smart campus"
- "blockchain AND IoT authentication"
- "blockchain AND IoT access control"
- "smart contract AND IoT security"
- "smart campus AND cybersecurity"
- "blockchain AND educational institution"

B. Threat Analysis

This stage should surface threats spanning authentication, authorization, data integrity, privacy, device compromise, and system availability.

C. Architecture Development

The five-layer design is realized through a permissioned blockchain paired with edge gateways.

D. Prototype

A candidate implementation could employ:

- Raspberry Pi/ESP32 for IoT devices;
- MQTT for communication;
- Python or Node.js for gateways;
- Hyperledger Fabric or another permissioned blockchain platform;
- Docker for deployment;
- PostgreSQL/MongoDB for off-chain data.

X. Proposed Experimental Setup

To assess the proposed design, it should be benchmarked against a centralized baseline architecture.

Figure 3 contrasts the proposed architecture with a conventional centralized baseline.

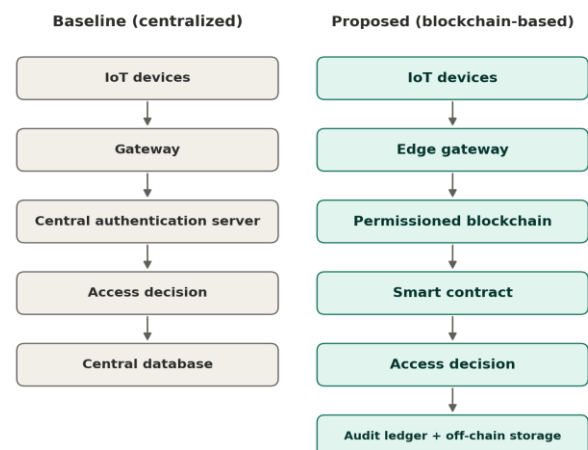


Fig. 3. Baseline (centralized) versus proposed (blockchain-based) architecture

TABLE IV — PROPOSED EXPERIMENTAL CONFIGURATION

Component	Configuration
IoT devices	Raspberry Pi/ESP32 or emulators
Gateway	Raspberry Pi 4/5 or VM
Blockchain nodes	3–5
Communication	MQTT
Blockchain	Hyperledger Fabric or equivalent
Database	PostgreSQL/MongoDB
Deployment	Docker
Device scale	50, 100, 250, 500, 1,000
Security events	Authentication/access transactions

Physical IoT devices can be combined with software-based emulators to reach larger device populations.

XI. Evaluation Metrics

The experiment should measure the following.

1. Authentication Latency

$$La = T_{response} - T_{request}$$

2. Authorization Latency

The time needed to reach an access decision.

3. Transaction Throughput

$$TPS = N / T$$

where N is the number of successful transactions and T is execution time.

4. Computational Overhead

CPU and memory consumption measured at both gateways and blockchain nodes.

5. Communication Overhead

The extra network traffic generated as a result of blockchain transactions.

6. Storage Overhead

The rate at which the blockchain ledger expands over time.

7. Attack Detection Rate

The proportion of simulated attacks correctly identified by the system.

8. Unauthorized Access Rate

The share of unauthorized requests that are mistakenly granted access.

9. Scalability

How system performance changes as the number of devices and transactions increases.

XII. Experimental Scenarios

Three primary experiments are recommended.

Experiment 1: Authentication Performance

The system should be evaluated across device populations of 50, 100, 250, 500, and 1,000. For each configuration, the following should be recorded:

- average latency;
- median latency;
- 95th percentile latency;
- CPU utilization;
- memory utilization.

The centralized baseline should undergo the same set of tests.

Experiment 2: Access-Control Accuracy

A mix of legitimate and unauthorized access requests should be generated. For example:

- 1,000 legitimate requests;
- 1,000 unauthorized requests.

Accuracy and False Positive Rate should then be calculated, with the aim of determining whether the smart-contract mechanism reliably enforces the defined policies.

Experiment 3: Scalability

As device and transaction counts rise, the study should track changes in:

- transaction throughput;
- latency;
- CPU;
- memory;
- network traffic;
- ledger size.

TABLE V — SCALABILITY TEST PLAN

Scenario	Devices	Transactions
S1	50	500
S2	100	1,000
S3	250	2,500
S4	500	5,000
S5	1,000	10,000

XIII. Expected Findings

Numerical outcomes should not be reported prior to running the experiments; however, several plausible trends merit investigation.

The blockchain-based approach is expected to deliver stronger auditability, since security events are captured within a distributed ledger.

Decentralizing device identity may lessen reliance on any single authentication authority.

Smart contracts are likely to enforce predefined access rules more consistently.

At the same time, blockchain-based security is anticipated to add latency and computational overhead relative to a centralized setup.

Performance may also degrade as the number of devices and transactions climbs.

The central question, then, is whether the gains in security and auditability outweigh this added overhead.

XIV. Preliminary Stakeholder Survey

To gauge stakeholder attitudes toward the security concerns motivating this framework, a short pilot questionnaire was circulated to members of the campus community using Google Forms. The instrument posed six items covering perceived concern about smart-device security, the perceived importance of restricting system access to authorized users and devices, confidence in additional access-control safeguards, the perceived importance of maintaining accountable access records,

tolerance for any performance trade-off introduced by stronger security, and the overall priority respondents placed on adopting advanced security technology on campus. The sample reported here ($n = 110$) is a preliminary pilot intended to inform the design of a larger data-collection effort rather than to support generalizable conclusions.

TABLE VI — SUMMARY OF PILOT SURVEY RESPONSES ($n = 110$)

Survey Item	Responses Recorded
Concern about smart-device security on campus	Very concerned (55); Extremely concerned (55)
Importance of restricting access to authorized people/devices	Extremely important (83); Very important (27)
Confidence in an added access-control safeguard	Extremely confident (55); Very confident (30); Slightly confident (25)
Importance of keeping a reliable access record	Very important (83); Extremely important (27)
Concern about security measures slowing systems down	Very concerned (55); Moderately concerned (55)
Overall priority of adopting advanced security technology	Extremely important (110)

Figure 4 illustrates the distribution of responses to the first item, which asked respondents how concerned they were about the security of smart devices used on campus (CCTV cameras, smart locks, attendance systems, sensors, and smart classrooms).

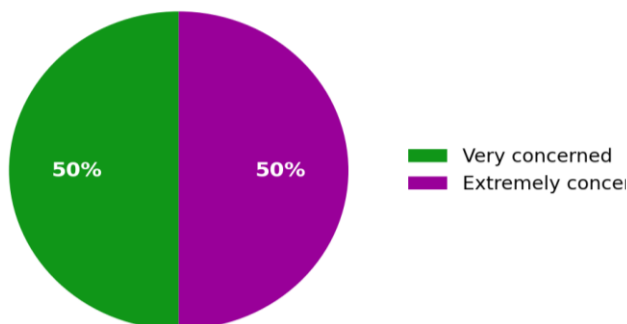


Fig. 4. Reported concern about smart-campus device security ($n = 110$)

Every respondent in this pilot sample rated their concern as either "Very concerned" or "Extremely concerned,"

and all four respondents rated the overall adoption of advanced security technology as "Extremely important." Responses were more mixed on the question of whether stronger security controls would be tolerated if they slowed system performance, splitting evenly between "Very concerned" and "Moderately concerned." This pattern is consistent with the trade-off discussed in Section XIII: stakeholders appear to value stronger security highly, but a meaningful share remain sensitive to the usability and performance costs that added authentication and access-control layers can introduce. Because the pilot sample is small, these results should be treated as indicative rather than conclusive, and a larger-scale survey is recommended as part of the empirical evaluation described in Section IX.

XV. Discussion

The proposed framework offers a workable path for integrating blockchain into educational IoT environments without requiring every device to function as a full blockchain node.

This matters because IoT devices are typically resource-constrained. The edge/gateway layer shoulders the computationally intensive work and communicates with blockchain nodes on the devices' behalf.

Identity and access management stand out as the most compelling use case for blockchain in this setting. NIST's guidance highlights unique device identification, authentication, and restriction of unauthorized interactions as core IoT cybersecurity capabilities.

The smart-contract mechanism proposed here can also drive dynamic access decisions informed by user role, device status, time, and the type of resource being requested.

That said, recording a device's identity on a ledger does not guarantee that the device remains trustworthy — a legitimate device can still be compromised over time. Ongoing device monitoring, firmware security, network segmentation, and intrusion detection therefore remain essential.

Privacy is another key concern. Educational IoT systems often process attendance records, location data, biometric information, surveillance footage, and other sensitive material. For this reason, the proposed hybrid design keeps sensitive information off-chain, reserving the blockchain mainly for hashes, identities, policies, and audit trails.

Governance presents a further challenge. Even a permissioned blockchain requires institutional decisions about who may run nodes, register devices, approve

policies, revoke identities, and manage cryptographic keys.

The proposed framework is therefore best understood as a permissioned, decentralized security layer — not a substitute for institutional cybersecurity governance.

XVI. Limitations

Several limitations apply to this proposed study.

First, a laboratory-based prototype cannot fully capture the complexity of an actual university campus.

Second, software-emulated IoT devices may not behave identically to physical hardware.

Third, blockchain performance varies with the chosen platform, consensus algorithm, hardware, and network topology.

Fourth, this research centers on authentication and access control rather than the full IoT cybersecurity lifecycle.

Finally, evaluating privacy implications may call for institutional and legal review that extends beyond the technical scope of the prototype.

XVII. Future Research

Future research can extend the proposed framework in several directions.

Blockchain and Edge Computing

Future work could explore edge computing as a way to cut latency and distribute the processing load associated with blockchain.

Blockchain and Artificial Intelligence

AI-driven anomaly detection could be paired with blockchain, using AI to flag compromised devices while blockchain preserves trusted identity and event records.

Zero-Trust Smart Campus

The architecture could be extended with Zero Trust principles, continuously evaluating users and devices rather than granting automatic trust.

Privacy-Preserving Blockchain

Subsequent research might examine pseudonymous identities, selective disclosure, encryption, and other privacy-preserving authentication techniques.

Lightweight Consensus

Different permissioned consensus mechanisms could be compared in terms of latency, throughput, energy use, and fault tolerance.

Real-World Deployment

The ultimate direction for this research is deployment within an actual educational setting encompassing smart classrooms, laboratories, surveillance infrastructure, and environmental sensors.

XVIII. Conclusion

This paper put forward a blockchain-based cybersecurity framework for IoT-enabled educational institutions, centered on decentralized device authentication and smart-contract-driven access control. The motivation stems from the growing use of IoT across smart campuses and the security challenges that accompany it — device identity, unauthorized access, data integrity, privacy, and auditability.

The proposed architecture spans five layers: IoT devices, edge/gateway infrastructure, a permissioned blockchain, smart contracts, and institutional applications. Blockchain is applied chiefly to device identities, access policies, security metadata, hashes, and audit records, while sensitive or high-volume data stays off-chain.

Research objectives, questions, and hypotheses were laid out to guide empirical evaluation, alongside a comparative experimental design pitting the blockchain-based architecture against a conventional centralized security model.

The most significant contribution of this work lies in examining the trade-off between security and performance. Blockchain may enhance decentralization, traceability, and auditability, but these advantages can come at the cost of added latency, processing demands, and storage requirements. The suitability of blockchain for educational IoT should therefore be demonstrated through experimentation rather than assumed outright.

Ultimately, this research suggests that blockchain shows the most promise when deployed as a hybrid security and trust layer, rather than as a standalone cybersecurity solution. Pairing permissioned blockchain with edge computing, conventional security tools, cryptographic device identity, smart contracts, and off-chain storage may offer a practical foundation for securing IoT-enabled smart campuses.

References

- [1] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards Next Generation Teaching, Learning, and Context-Aware Applications for Higher Education: A Review on Blockchain, IoT, Fog and Edge Computing Enabled Smart Campuses and Universities," *Applied Sciences*, vol. 9, no. 21, Art. no. 4479, 2019.
- [2] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, *IoT Device Cybersecurity Capability Core Baseline*, NISTIR 8259A, National Institute of Standards and Technology, 2020.

- [3] M. Fagan, K. N. Megas, J. Marron, K. G. Brady, B. B. Cuthill, R. Herold, D. Lemire, and N. Hoehn, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements, NIST SP 800-213, 2021.
- [4] K. N. Megas et al., IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog, NIST SP 800-213A, National Institute of Standards and Technology, 2021.
- [5] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," 2018.
- [6] "Blockchain-Based Access Control and Behavior Regulation System for IoT," Sensors, vol. 22, no. 21, 2022.
- [7] "Blockchain-Enhanced Smart Contracts for Formal Verification of IoT Access Control Mechanisms," Alexandria Engineering Journal, 2025.
- [8] T. Domínguez-Bolaño, V. Barral, C. J. Escudero, and J. A. García-Naya, "An IoT System for a Smart Campus: Challenges and Solutions Illustrated Over Several Real-World Use Cases," 2024.
- [9] M. Alkhamash, "A Blockchain and IoT Based Framework for Decentralised Smart Campus Environment," University of Sussex, 2023.
- [10] M. Alkhamash, M. Alshahrani, N. Beloff, and M. White, "Revolutionising the Approach to Smart Campus Architecture Through IoT and Blockchain Technologies," 2022.
- [11] F. Kurniawan, D. P. Putra, J. Hammad, and A. S. Prabuwno, "A Blockchain-Secure Mobility Data in Smart Campus," International Journal of Interactive Mobile Technologies, vol. 17, no. 18, 2023.
- [12] A. Srhir, T. Mazri, and M. Benbrahim, "Towards Secure Smart Campus: Security Requirements, Attacks and Counter Measures," Indonesian Journal of Electrical Engineering and Computer Science, vol. 32, no. 2.