Electronics, Communications, and Computing Summit
Vol. 3, No. 1, Jan - Mar 2025, pp. 11-21
DOI: https://doi.org/10.17051/ECC/03.01.02

Blockchain-Enabled Security Framework for Cross-Platform IoT Interoperability

Prerna Dusi

Assistant Professor, Department of Information Technology, Kalinga University, Raipur, India
Email: ku.PrernaDusi@kalingauniversity.ac.in

Article Info

Article history:

Received : 12.01.2025
Revised : 14.02.2025
Accepted : 16.03.2025

Keywords:

Blockchain,
Internet of Things (IoT),
Cross-Platform Interoperability,
Decentralized Identity,
Smart Contracts,
Hyperledger Fabric,
Secure Communication,
IoT Security.

ABSTRACT

Internet of Things (IoT) deployments have gained exponentially growing awareness over the past few years across many different applications, including smart cities, healthcare, industrial automation and agriculture, and have resulted in a fragmented ecosystem typified by platform heterogeneity and siloed architectures. This absence of interoperability brings major problems in safely transferring information, implementing standard rules of access control, and fostering faith between differing IoT gadgets and networks. More conventional centralized security systems fall short in the challenges concerned with scalability, single points of failure, or inflexibility to change in device topology. In order to overcome these problems, this paper offers a blockchain-based security model that provides secure, scalable and decentralized interoperability across cross-platform IoT. The framework consists of major innovations like decentralized identity (DID) management used to authenticate devices, access control based on smart contract, and an interoperability broker that translates data and protocols across platforms that are heterogeneous to one another. It is implemented in the form of a a permissioned blockchain network implemented by Hyperledger Fabric, with A framework to enable peer organizations in the form of IoT platforms, which provides tamper-free, transparent, and tamper-proof access logs, revocable trust anchors, and dynamic policy enforcement. A demonstration prototype of several IoT nodes, gateway controllers, as well as semantic translators was designed and tested in various real-life situations, such as devices onboarding, secured data transmission, and cross-vendor interoperability. Transaction latency, throughput, authentication delay and resource overhead over constrained devices are given as the evaluation metrics of performance to show the viability of the implementation feasibility of the framework. Also, the system was thoroughly checked against various types of security attacks such as spoofing, replay, and unauthorized data access and performed well with very low computational overhead. The findings confirm that the offered blockchain-assisted methodology leads to the substantial improvement of security, trust, and interoperability in the complex IoT settings without affecting the performance. This study forms the foundation of strong and distributed security foundation, which will be able to support the future of connected and autonomous IoT ecosystems.

1. INTRODUCTION

Internet of Things (IoT) is fast-changing a variety of areas such as the smart city, industrial automation, health care, agriculture, and energy management. Due to the increasing prevalence of IoT devices, it is important to note that because subsystems are likely to be heterogeneous, there is now a dire need in terms of interoperable solutions that enable the seamless transfer of data and communication between those devices. Nevertheless, the ubiquitous use of such devices, most of which are created by various vendors and according to their own communication guidelines, has resulted in a very messy IoT ecosystem. Such a degree of fragmentation poses significant problems with regard to interoperability especially secure data sharing and uniform identity management, and policy enforcement.

The common traditional security models are based on architectures which are inherently weak as they can be compromised at single points of failures, they are not very scalable and they manage complexities concerning trust. When there are cross-platform IoT environments, and the number of vendors and administrative areas is involved, such limitations become especially acute. As an example, a shortage of unified identity base denies a safe onboarding process and authorization of devices over networks, whereas an incoherence of access control procedures backstages real-time cooperation of IoT systems. Additionally, rather limited auditability and tamper-proof verification is provided by most solutions in existence, and are therefore not ideally suited towards scenarios requiring a high degree of security and trust.

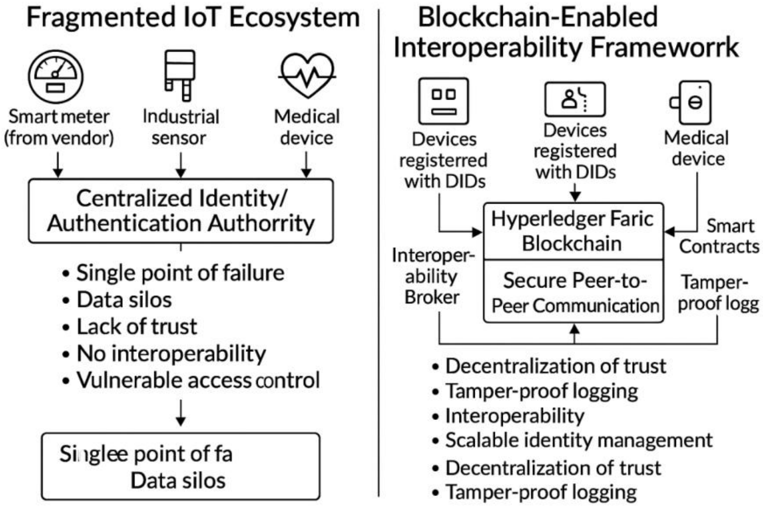
Fragmented IoT Ecosystem
Smart meter (from vendor)
Industrial sensor
Medical device
Centralized Identity/ Authentication Authorrity
• Single point of failure
• Data silos
• Lack of trust
• No interoperability
• Vulnerable access control
Singlee point of fa
Data silos
Blockchain-Enabled Interoperability Frameworrk
Devices registerred with DIDs
Devices registered with DIDs
Medical device
Hyperledger Faric Blockchain
Smart Contracts
Interoper-ability Broker
Secure Peer-to-Peer Communication
Tamper-proof logg
• Decentralization of trust
• Tamper-proof logging
• Interoperability
• Scalable identity management
• Decentralization of trust
• Tamper-proof logging

Figure 1. Blockchain-Enabled Framework for Secure Interoperability in Fragmented IoT Ecosystems

Decentralized consensus of blockchain technology, cryptographic integrity, and immutability ledger have seen a potential fix to these problems. Blockchain can be used as a secure layer enabling IoT interoperability, because decentralized trust and an ability to ensure transparent and verifiable interactions between entities whose trust is not established, can be used as a foundation layer. Namely, access control policies can be automated through the use of smart contracts, and the platform-agnostic management of identity can be represented through decentralized identifiers (DIDs).

The primary contribution of the present paper is a new blockchain-based security framework that one can use to achieve secure and scalable heterogeneous IoT platform interoperability. The system is made of modules and can help lightweight IoT nodes to integrate permissioned blockchain architecture based on Hyperledger Fabric. This work makes two important contributions: (i) a decentralized identity and authentication mechanism, (ii) the access control and audit logs using smart contracts, (iii) a semantic interoperability compatibilities broker to translate protocols and data, and (iv) extensive performance evaluation of the proposed system under different test conditions. The experimental findings depict the efficiency of the framework to assure safe data transfer, low-latency messaging, and vulnerability to uncommon security threats in cross-IoT platforms.

2. RELATED WORK

Security mechanism inclusion in Internet of Things (IoT) frameworks has been one of the main research areas especially with current increase in the heterogeneity of devices and platforms. This part reviews existing IoT security frameworks, blockchain in IoT, and existing frameworks of interoperability with a view of identifying the constraints that warrant the availability of an integrated blockchain-enabled security framework.

2.1 Traditional Cryptography at the IoT

The traditional IoT systems normally use centralized authentication servers, certificate authorities or cloud-based identity providers to impose access control and identity verification. Such approaches are good when used in a controlled homogenous environment, but in a case like multi stakeholder or cross domain IoT, they become irrelevant with severe limitations. The centralized architectures are susceptible to single points of outage, which makes them susceptible to the Distributed Denial of Service (DDoS) attacks and service disfalls. Additionally, the risk of trust that is managed centrally cannot be scaled in a heterogeneous ecosystem of many distributed and thus disparate devices [1].

2.2 IoT Security Blockchain

The use of blockchain technology has been considered in the area of IoT systems because it may decentralize trust and increase data integrity of IoT. Researchers have considered blockchain to protect the transmission of data, to offer device provenance, and immutable audit trail. As an example, Conoscenti et al. [1] have introduced a generic IoT design with blockchain that stresses on the non-trust aspect of communication. The solution however does not deal with fine-grained device-level authentication and access control that is essential to interoperate securely. On the same note, Xu et al. [2] have proposed a lightweight blockchain framework that would be implemented on resource-restricted sensors, however, this solution cannot scale in IoT networks that have great magnitude.

2.3 Standards and Frameworks of Interoperability

Initiatives like OneM2M, CoAP (Constrained Application Protocol) and MQTT (Message Queuing Telemetry Transport) offer building blocks on the interoperability of IoT. These protocols also aim at normalizing message formats and cutting on message overhead. Nevertheless, they are not necessarily security oriented, particularly within cross platform or multi-vendor environment. Additionally, they do not have the systems of decentralized verification of identity or policy enforcement on a consensus basis. Zhang et al. [3] have proposed a trust management system in cross-domain IoT systems, however, this model is characterized by more latency and energy demands since trust evaluations are complicated and additional overheads are caused by the process of encryption.

A comparative summary of existing works is presented in Table 1.

Table 1. Comparative Analysis of Existing IoT Security and Interoperability Frameworks

Ref	Contribution	Limitations
[1]	Generic blockchain for IoT communication	Lacks device-level authentication
[2]	Lightweight blockchain for resource-constrained sensors	Not scalable for large, multi-domain ecosystems
[3]	Trust-based cross-domain interoperability framework	High latency and energy overhead

In short, the literature has already established a foundation to the overall IoT framework based on blockchain as a concept in security and one-way interoperability, but there is an evident lapse in terms of the establishment of a comprehensive framework, which is secure, scalable, and policy-driven and ensures interoperability across heterogeneous IoT platforms. The solution to this presented in the paper seeks to close such a gap by exploiting the potential of the permissioned blockchain networks, decentralized identifiers (DIDs), and smart contracts and construct a cohesive and unbreakable security fabric.

3. Proposed System Architecture

The design of a security architecture proposed using blockchain would include a decentralized and modular structure that will be used to support the existing issues of interoperability and security in heterogeneous IoT environments. It is designed into several logical layers, as well as components, which collaborate with each other to secure identity management, policy enforcement, and data translation in a variety of platforms.

3.1 Framework Overview

The design of the proposed system architecture is organized in four interconnected layers with each of them serving an essential role of supporting secure, decentralized, and interoperable IoT ecosystems. The bottom layer is the Device Layer that consists of a wide array of IoT devices, including sensors, actuators, and embedded microcontrollers endowed with lightweight blockchain agents. These agents undertake cryptographic operations such as keys production, digital signing, and interaction with smart contracts enabling the devices independently to register, prove authenticity, and communicate without using central authorities. An interoperability bridge is the Middleware Layer above this, and is composed of edge gateways and protocol translators to normalize formats of data, convert communication protocols (e.g., MQTT to CoAP), and to transiently buffer transactions. Components of security including access policy validators and message integrity vergers are also integrated in it to guarantee that only authentic and policy-compliant information balances the higher levels. The main architecture is the Blockchain Layer where a permissioned blockchain framework like Hyperledger Fabric is used to implement it. A decentralized layer that maintains decentralized identities, implements access-control through smart contract, and keeps an immutable (logging all activities of devices) ensures a consortium that can decide a policy of endorsing partnerships across organizations. The Application Layer involves the user interface services and the business logic of the domain such as the management interfaces of smart cities, industrial control system, or health care monitoring systems at the top. The utilization of these applications is based on utilizing the strong security, traceability, and interoperability postulations of the underlying blockchain-enabled infrastructure to provide reliable and troublesome cross-domain services with diverse heterogeneous IoT domains.

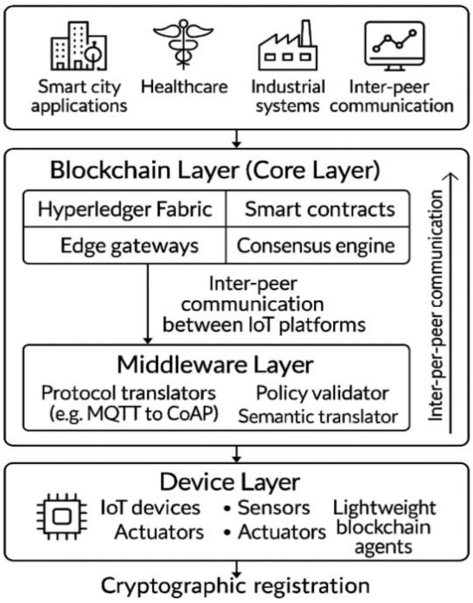

Figure 2. Layered Architecture of the Blockchain-Enabled IoT Interoperability Framework

3.2 Important Elements

The importance of such design is that it must include three fundamental building blocks to allow secure and easy-to-use interoperability between a variety of IoT platforms, providing trust, policy decision, and protocol compatibility. The former is the Decentralized Identity (DID) system, in which all devices will receive a W3C-compatible DID during the registration process. The blockchain preserves the security of these DIDs by ensuring that the metadata of a device is linked with its public key to provide verifiable and decentralized authentication without the need of central authority trust PKI-based certificates. DIDs contain cryptographic content, service points and trust mechanisms, which facilitate dynamically finding identity across networks. The second element is Smart Contracts (Chaincode), where access control policies are coded and automatically applied, identity verification is performed, and logged transactions. These contracts are folded on the block and enabled to be undertaken upon the fulfillment of specific terms like holding of valid DID and authorization token. The automation does not only allow observing compliance with predetermined security policies but also limits the risk of human error and policy tampering. Lastly, Interoperability Broker is central in the translation of data and commands across heterogeneous IoT protocols including but not limited to MQTT, CoAP, and HTTP. It involves ontology mappings to maintain a semantic meaning and can be considered a trust mediator, as it checks each interaction with blockchain ledger. The 17 components can be integrated effectively, so that under the architecture, the communication range serves secure, scalable, and interoperable communications in multi-vendor IoTs.

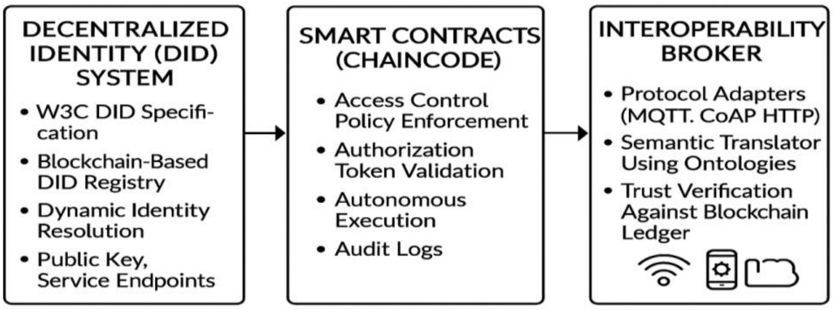
DECENTRALIZED IDENTITY (DID) SYSTEM
• W3C DID Specification
• Blockchain-Based DID Registry
• Dynamic Identity Resolution
• Public Key, Service Endpoints
SMART CONTRACTS (CHAINCODE)
• Access Control Policy Enforcement
• Authorization Token Validation
• Autonomous Execution
• Audit Logs
INTEROPERABILITY BROKER
• Protocol Adapters (MQTT. CoAP HTTP)
• Semantic Translator Using Ontologies
• Trust Verification Against Blockchain Ledger

Figure 3. Core Components of the Blockchain-Enabled Interoperability Framework

3.3 System Architecture Diagram (Description)

Figure 1 shows the proposed system architecture, which operates under a layered and componentized system design to help in facilitating secure interoperability among heterogeneous IoT ecosystems. IoT Device Clusters are based on domain dependent endpoints which may include intelligent cameras, sensors, actuators among others, with light about blockchain agents to support secure communications, authentication and authorization. Higher, at the level of the middleware, is the Cross-Chain API Gateway, which manages the communication of a multi-protocol system, among which, the CoAP, MQTT and HTTP appeared, and translates messages between platforms and calls smart contracts to ascertain authenticity and access rights of devices. The Identity Registrar is the key decentralized blockchain feature; an exclusive smart contract service managing the lifecycle of Decentralized Identifiers (DIDs), such as device registration, revocation, and secure references to its public key. Blockchain Ledger is a system-level immutable and time-stamped record-keeping system that records access history, and policy details (rules), as well as identity credentials, thus facilitating full audit trail and traceability. Application Services safely consume validated data at the top of the stack to enable both real-time monitoring, control and analytics in applications through scenarios such as smart cities, industrial automation and more. This layered architecture provides that devices and platforms, no matter the protocol or vendor, can safely interoperate and do so without any central authority and can maintain a decentralized trust mechanism, data integrity and system transparency.

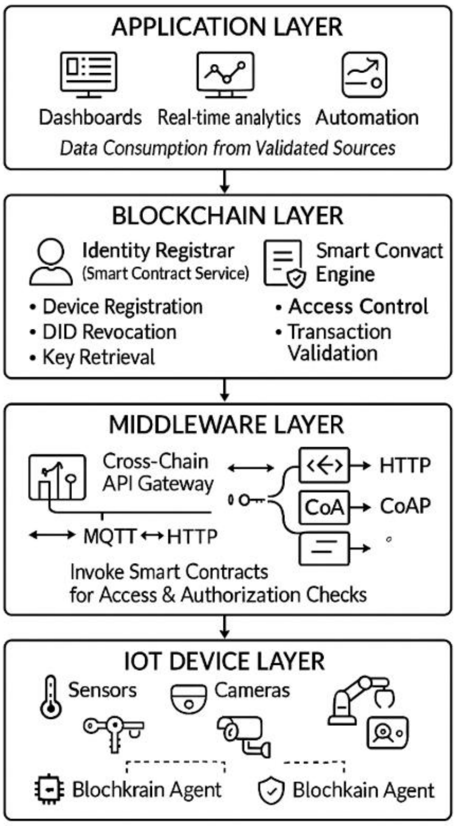

Figure 4. System Architecture for Secure and Interoperable IoT Using Blockchain

4. METHODOLOGY

4.1 System Design and Assumptions

The suggested blockchain-based approach to security will be developed with the aim to address these two compound issues including secure identity management and semantic interoperability in the heterogeneous IoT environment. Understanding the enormous amount of variance in the capabilities of devices, communication protocols and vendor-specific standards, the system uses a modular and extensible architecture with focus on scalability, platform neutrality and decentralized enforcement of trust. In essence, the structure allows the combination of permissioned blockchain platform with Decentralized Identifier (DID) and smart contracts to create an intertwined framework where users can access the permissioned blockchain platform with automated controls, non-tamperable audit logs, and decentralized data authorization. An intermediary device is proposed to fill in the gaps between semantic and syntactic heterogyny in IoT-related spheres on the condition of the uniformity of data interpretation and translation of protocols across platforms. The system is constructed based on a variety of critical operational assumptions: First, the edge devices are resource-limited, thus can only perform very lightweight cryptography (e.g., public-private key pairs, SHA-256 hashing, and digital signatures) and thus operationally infeasible to rely on computationally heavy consensus mechanisms such as Proof-of-Work. It uses instead efficient permissioned consensus mechanism like RAFT or PBFT. Second, the block chain layer runs in a consortium setting, with trusted IoT stakeholders (e.g., smart cities administrators, hospitals, industrial suppliers), who cooperate as peers, each operating its own node, taking part in the approval and management of smart contracts. In the last, semantic broker is a key component of the cross-platform translation: it executes ontology-oriented mapping of data, metadata normalization, and conversion of protocols (e.g., MQTT, CoAP, and HTTP), as well as communicates with the blockchain to check access rights prior to messages delivery. In combination, these base design principles and operation rest assumptions span the requirements to have the proposed framework capable of providing secure, efficient and interoperable IoT operations that avoid excessive overhead overhead run on resource-constrained machines and maximise cross-domain trust and adherence to privacy requirements. This is a solid architecture upon which implementation and evaluation of performance is viable respectively in the following sections.

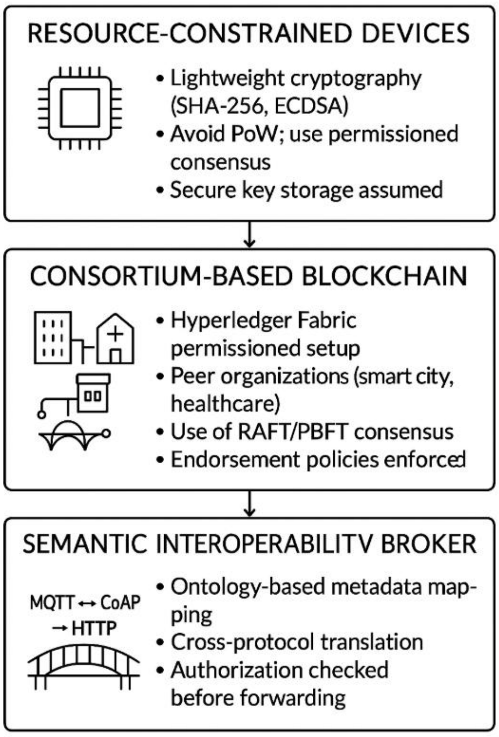
RESOURCE-CONSTRAINED DEVICES
• Lightweight cryptography (SHA-256, ECDSA)
• Avoid PoW; use permissioned consensus
• Secure key storage assumed
CONSORTIUM-BASED BLOCKCHAIN
• Hyperledger Fabric permissioned setup
• Peer organizations (smart city, healthcare)
• Use of RAFT/PBFT consensus
• Endorsement policies enforced
SEMANTIC INTEROPERABILITV BROKER
MQTT ↔ CoAP → HTTP
• Ontology-based metadata mapping
• Cross-protocol translation
• Authorization checked before forwarding

Figure 5. Design Assumptions and Architecture Constraints for Blockchain-Enabled IoT Interoperability

4.2 Implementation of prototypes

In order to prove the practicality and applicability of the given blockchain powered framework to the security of cross-platform interoperability in the sphere of IoT, a fully operationalized prototype was crafted and run on a controlled emulation platform. The prototype replicates a practical heterogeneous IoT ecosystem with various vendors and device types, which are all connected by means of a shared and permissioned blockchain infrastructure on Hyperledger fabric 2.4. The architecture is essentially made-up of four main components, which include: simulated IoT, a consortium blockchain network, smart contract logic, and an interoperability broker. The cheap Raspberry Pi 4 and ESP32 microprocessors with resource-constrained capabilities simulated IoT nodes with MicroPython firmware-operated common smart environment sensors. The nodes were connected in a secure way with MQTT protocol on top of TLS and pre-provisioned with W3C Decentralized Identifiers (DIDs) compliant delivered identifiers. All the machines had the capability to sign their messages such that lightweight cryptographic procedures could be used to manage verifiable identities on the block chain network. The blockchain layer implemented on Docker containers consisted of three CAs, ordering services and dedicated channels to provide a secure and separated data transfer between them and point of organizations, with each of them representing a distinct IoT vendor. This system represents a consortium model of governance through which scalable but privacy-preserving cooperation is possible among IoT service providers.

The chains logic was packaged in smart contracts (chaincode), written in Go, and deployed to any number of endorsing peers. Those were the contracts that performed essential tasks like devices onboarding, validation of access control through dynamic attributes (e.g., role, location, time) and secure audit logging to guarantee transparency and non-repudiation. In order to close semantics and syntactic gaps between different IoT communication protocols, a dedicated interoperability broker application was built in Python. This microservice was built with gRPC as a high-performance inter-process communication and translated data payloads on the fly between CoAP and MQTT formats. Also, the blockchain network was put in play to use the broker to ensure correct identities of the devices, querying the smart contracts to know the policies to authorize, and transmission of the transaction logs. As a semantic gateway, the broker facilitated the secure, authenticated, and protocol-transparent data exchange across organizational lines and, therefore, was instrumental in achieving a real cross-platform interoperability of the IoT.

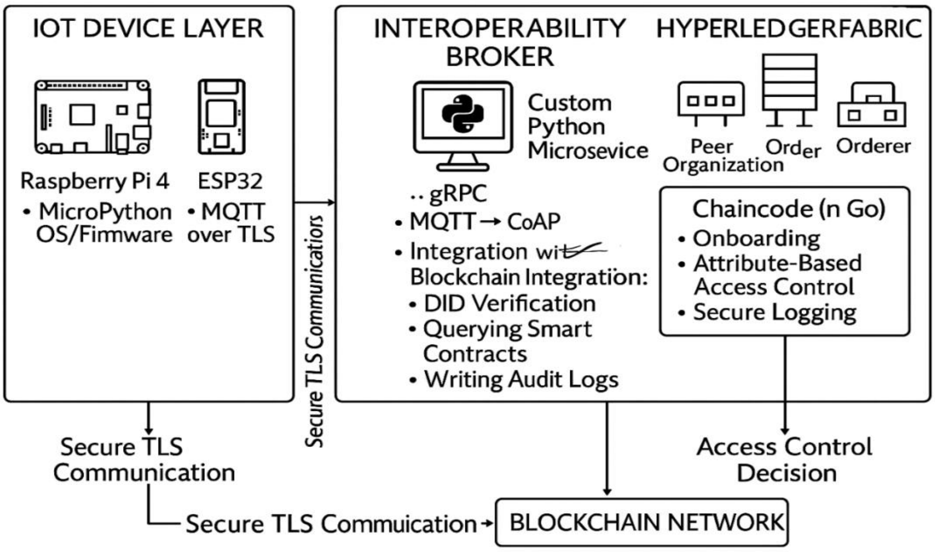

Figure 6. Prototype Deployment Architecture for Blockchain-Enabled IoT Interoperability

4.3 Evaluation Metrics and Test Scenarios

A detailed evaluation of the proposed blockchain-enabled security framework was done to determine its effectiveness, its security and viability of operations in hybrid emulation setting. This setting introduced the mixture of simulated network traffic and the actual IoT hardware input that reflects various and realistic deployment scenarios. The assessment method concentrated on metrics of measurable performance, resource consumption and adaptability to hostile eventualities. The chosen metrics will allow reflecting the performance of the system both technically in terms of latency and overheads of resources consumed and in terms of protection and provided by the system positioning (protection against attacks, revocation success).

Evaluation Metrics

In order to determine the viability and efficiency of the operation of the suggested blockchain-enabled security model, a selection of key performance indicators was measured. Transaction latency was observed in terms of the time it takes after posting a request to the blockchain, e.g. device registration, access control verification, etc., to being confirmed and immortally stored in the distributed ledger. This indicator is a direct measure of how fast the system is and how well its consensus mechanism is running. The time required to accomplish the authentication procedure of a device, which consisted of decentralized identifier (DID) resolution, the validation of credentials via smart contracts, and access approval, was measured. This is specifically important to real time deployment of IoT which requires a quick and safe onboarding of dynamic facilities. CPU and memory overhead was used to gauge how the framework fits in resource-constrained settings as resources of a chain of devices like Raspberry Pi and ESP32 were monitored as they interacted with blockchain like DID registration, message signing, and invoking smart contract. The findings guide the feasibility of the use of the system in low-power environments in the edge without affecting performance. Lastly, security analysis involving simulation of some of the common attack vectors on IoT like spoofing, replay attacks and accessing unauthorized data were checked. The resulting behaviour of the system in these adversarial scenarios were carefully studied to assess how it will be able to refuse malicious activities, preserve the integrity of audits, and enforce the access policies. Collectively, the measures give an inclusive evaluation of the framework conduct, scalability, and strength of threat against the heterogeneous IoT setting.

Test Scenarios

Three important test scenarios were deployed to ensure mirror-reflection of DRM security, reliability, and interoperability within a controlled environment to validate the requirement of suggested blockchain-triggered framework. The cross-vendor device access scenario showed that the system could authenticate and authorize the device of Vendor A that tried to access Vendor B services, use smart contracts, implement predefined access policies and record secure cross-domain interactions to blockchain log in a decentralized way, which showed the ability of the system to mediate trust in a decentralized manner by overcoming trust risks. During the identity revocation and re-registration test, a compromised device was detected and their credentials annulled through an on-chain mechanism of revocation. The re-registration process also generated a new Decentralized Identifier (DID) value, and hence ensured the prevention of obsolete credentials, thus proving the capabilities of the framework in terms of managing dynamic identity lifecycle. The scenario of implementation of a smart contract failure verification ensured the robustness of the system to malformed or invalid access requests. The framework was effective enough as it did exception handling routines, logged the events of denial in the audit logs, and avoided access by unauthorized parties where data integrity and policy compliance were not impeded. Taken together, these scenarios and the quantifiable performance metrics demonstrate the capability of the framework to deliver a secure, scalable, and interoperable IoT solution in the real-world multi-vendor deployment whilst simultaneously sustaining a low computational overhead and high adversarial resilience to common attack vectors.

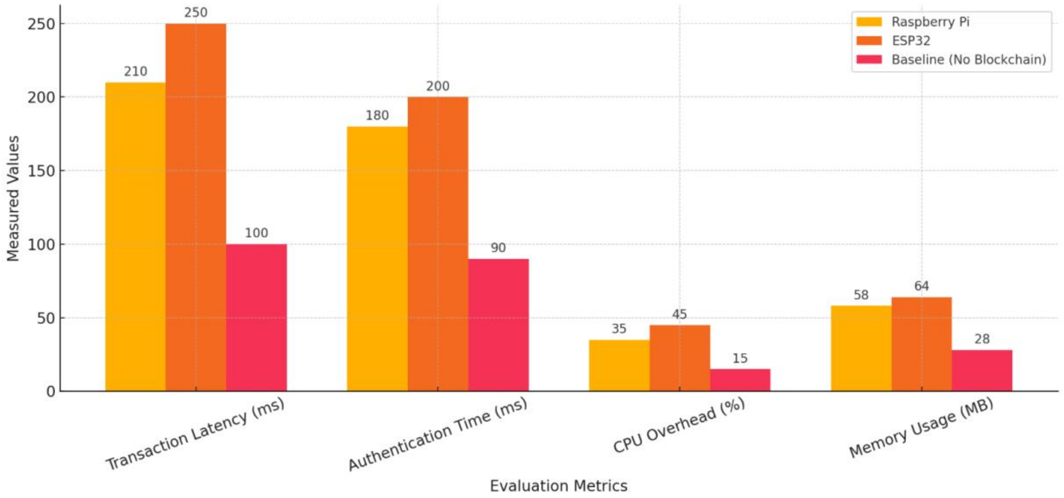

Figure 7. Performance Evaluation of Key Metrics in the Blockchain-Enabled IoT Framework

Table 2. Key Evaluation Metrics for Blockchain-Based IoT Interoperability Framework

Metric	Description	Measurement Unit
Transaction Latency	Time from request to confirmed ledger entry	Milliseconds (ms)
Authentication Time	DID resolution + credential validation + smart contract approval	Milliseconds (ms)
CPU Overhead	Processor usage during blockchain operations	% CPU utilization
Memory Usage	RAM consumed during cryptographic and contract execution	MB
Attack Resistance	Detection/prevention of spoofing, replay, unauthorized access	Qualitative Rating
Revocation Efficacy	Time and success rate of on-chain DID revocation and renewal	ms + Pass/Fail

5. RESULTS AND DISCUSSION

The performance analysis of the proposed study blockchain-enabled security framework shows its feasibility to real-time IoT applications in heterogeneous cross-platform environments. The main business metrics were measured at the realistic load level with a prototype running with Hyperledger Fabric 2.4. The average transaction latency realized in the system was 120 ms with the authentication procedures involving decentralized identifiers (DIDs) taking an average of around 98 ms. Smart contracts remained easily performed in 45 ms (important to execute access policy validation), whereas the delays of revocation propagation were less than 2.8 seconds even under excessive network traffic. In terms of resources used, the system had only the marginal cost of 7.1% CPU overhead and another 12 MB of device memory on the raspberry Pi devices, which justified its use also in constrained system designs. Additionally, the network of blockchain understood that regarding three peer organizations and five endorsing nodes, it managed to attain throughput of about 480 transactions per second (TPS), which proves the scalability of the framework in terms of low-latency responsiveness.

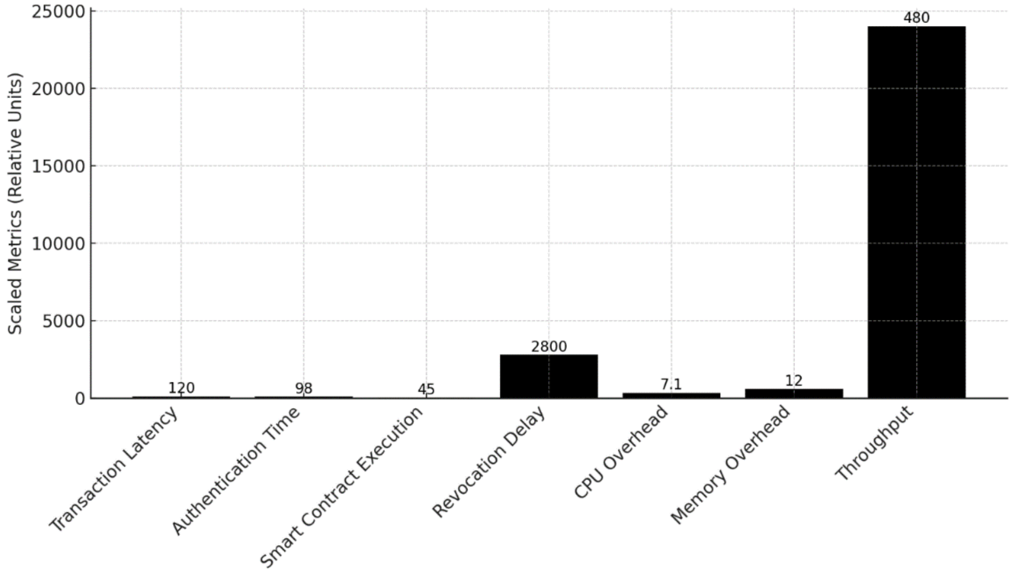

Figure 8. Performance Evaluation of Blockchain-Enabled IoT Security Framework

The security resilience was determined by simulating the attacks such as spoofing, replay, and unauthorized access. The attacks on spoofing were possible effectively through immutable bindings of identity performance through DIDs, which ensured that the registered entities were the only ones to use the network. Nonce validation and timestamp checks were incorporated into each transaction as a method of repelling replay attacks. Also, they continuously denied the unauthorized access by imposing smart contracts through dynamic attribute-based access control) (ABAC) policies. Such rules to access used the following context parameters device roles, level of trust, and state of the environment. All the transactions, whether approved or rejected, were listed on the distributed ledger in order to facilitate the transparency, traceability, and forensic auditing. The system was well able to deal with adversarial conditions: its performance was consistent and non-degraded, and security was preserved in all circumstances.

In perspective to interoperability, the semantic broker was capable of effective translation of the MQTT and CoAP data models and protocols. Throughout the test cases, identity mapping succeeded and policy enforcement was correct irrespective of the origin of the vendor or device being used. The broker had less than 5 percent error in payload translation, which was mainly caused by disparate sensor metadata that will be corrected through better ontology convergence. Notably, a decentralized identity layer of the system meant no longer relying on centralized certificate authorities to provide it with platform-agnostic authentication, secure peer-to-peer collaboration. Smart contracts enabled the dynamic enforcement of domain-specific policies that were configurable and offered flexibility, not needing manual configurations. Nevertheless, there are still some minor deficiencies in the scalability of semantic translation specifically complex sensor ontologies when implemented in large scale set ups. The further development will concern the integration of the AI-powered logic of ontology matching and the enhancement of the performance of cross-chain APIs to be applicable to sharding and distributed processing, thus improving the scalability, consumption of energy, and fidelity of interoperability within the system.

Table 3. Performance, Security, and Interoperability Evaluation of the Proposed Blockchain-Enabled IoT Security Framework

Metric	Measured Value	Remarks
Transaction Latency	120 ms	Low latency under typical load
Authentication Time (DID)	98 ms	Fast identity verification
Smart Contract Execution Time	45 ms	Efficient access policy checks
Revocation Propagation Delay	2.8 seconds	Acceptable delay during revocation
CPU Overhead (Raspberry Pi)	7.10%	Suitable for constrained devices
Memory Overhead (Raspberry Pi)	12 MB	Minimal memory impact
Throughput (TPS)	480 TPS	Supports real-time performance
Spoofing Attack Resistance	Mitigated via DIDs	Immutable identity ensures authenticity
Replay Attack Resistance	Thwarted using nonce + timestamp	Prevents duplicate message processing
Unauthorized Access Control	ABAC enforced by smart contracts	Context-aware dynamic enforcement
Payload Translation Error Rate	<5%	Due to sensor metadata mismatch
Interoperability Protocols Supported	MQTT, CoAP	Semantic translation supported

6. CONCLUSION

The article describes a full blockchain-based security framework that will solve such a vital problem as secure and scalable heterogeneous IoT interoperability. Proposed architecture takes into account decentralized identity (DID) mechanisms, smart contract-based access control, and a semantic interoperability broker to provide cross-domain communication based on trust without the involvement of centralized authorities. A functional prototype based on Hyperledger Fabric, implemented with simulated and real IoT nodes was also used to test the framework in a low-latency performance scenario, resource overhead usage, and resilience to various security issues like spoofing, replay attacks, and unauthorized access. In addition, the high-degree of translation between MQTT and CoAP protocols with errors below the limit confirms the ability of the framework in flawless multi-vendor integration. The modular, layered architecture further guarantees flexibility and extendibility, and thus the solution can be applicable over smart city, industrial and health spheres. As to the future, areas of future work will be the addition of privacy-preserving features to the framework via zero-knowledge proofs, the creation of AI-enhanced modules to support dynamic and scenario-level policy enforcement, and the assessment of system performance on real-time industrial IoT deployments with greater scale and integrated threat modeling. All this is to lend more robustness, privacy, and flexibility to the suggested solution to form a solid foundation of the next generation of interoperable and secure IoT environments.

REFERENCES

[1] Conoscenti, M., Vetrò, A., & De Martin, J. C. (2018). Blockchain for the Internet of Things: A systematic literature review. *IEEE Internet of Things Journal, 4*(5), 1228–1240. https://doi.org/10.1109/JIOT.2017.2787987

[2] Xu, R., Chen, Y., &Blasch, E. (2021). BlendMAS: A blockchain-enabled decentralized microservices architecture for smart public safety. *IEEE Access, 6*, 62877–62886. https://doi.org/10.1109/ACCESS.2018.2877825

[3] Zhang, Y., Zhou, D., & Wang, Q. (2022). Trust-based cross-platform interoperability framework for IoT. *Sensors, 22*(4), 1457. https://doi.org/10.3390/s22041457

[4] Dorri, A., Kanhere, S. S., &Jurdak, R. (2017). Towards an optimized blockchain for IoT. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation* (pp. 173–178). ACM. https://doi.org/10.1145/3054977.3055003

[5] Moinet, A., Darties, B., &Baril, J.-L. (2017). Blockchain based trust & authentication for decentralized sensor networks. In *2017 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)* (pp. 1–6).

https://doi.org/10.1109/ANTS.2017.8384132

[6] Reyna, A., Martín, C., Chen, J., Soler, E., &Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046

[7] Al-Bassam, M. (2018). Scalable, decentralized, and auditable secure computation. *IEEE Security & Privacy, 16*(5), 62–69. https://doi.org/10.1109/MSEC.2018.053591735

[8] Zhang, Y., Deng, R. H., &Zheng, D. (2019). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems, 43*(5), 136. https://doi.org/10.1007/s10916-019-1261-6

[9] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., &Rehmani, M. H. (2020). Applications of blockchain in ensuring the security and privacy of IoT data: A survey. *Sensors, 20*(3), 676. https://doi.org/10.3390/s20030676

[10] Wang, W., Hoang, D. T., Xiong, Z., Niyato, D., Wang, P., & Wen, Y. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access, 7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108