Blockchain-Based Decentralized Identity and Access Control for IoT-Enabled Distributed Energy Resources in Smart Grids

Pham Quy Duong
Master, National Institute of Digital Technology and Digital Transformation
Vietnam, Hanoi
pqduong@mst.gov.vn

Le Cuong
PhD, Electric Power University
Vietnam, Hanoi
cuongle@epu.edu.vn

***Abstract*—The accelerated deployment of distributed energy resources (DERs) within smart grids has resulted in the integration of millions of heterogeneous Internet of Things (IoT) devices, including smart meters, solar photovoltaic (PV) inverters, battery energy storage systems (BESS), and electric vehicle (EV) charging stations. These devices enable peer-to-peer energy trading, demand response, and real-time grid coordination. However, when managed through centralized identity and access management (IAM) systems, they introduce severe security vulnerabilities, including single points of failure, device impersonation, false data injection attacks, and limited auditability.**

This paper proposes a decentralised identity and access control framework that integrates W3C Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) with Hyperledger Fabric permissioned blockchain. Each DER device is assigned a unique DID and cryptographic key pair. Smart contracts implement a hybrid Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) model for device registration, role/attribute issuance, policy enforcement, and fine-grained authorisation. Secure communication between devices and the blockchain is facilitated by Message Queuing Telemetry Transport (MQTT) over Transport Layer Security (TLS).

A comprehensive security analysis demonstrates the framework's resistance to device spoofing, replay attacks, unauthorised access, insider threats, and single points of failure through immutable audit logs and multi-organization endorsement policies. The proposed design provides a practical pathway toward secure and scalable DER integration in smart grids, significantly enhancing trust, data integrity, and resilience compared with traditional centralised IAM solutions.

***Index Terms*—Blockchain; Decentralized Identifier (DID); Verifiable Credential; Hyperledger Fabric; Access Control; Smart Grid; Internet of Things (IoT); Distributed Energy Resources (DER); RBAC; ABAC.**

I. Introduction

The global transition toward decarbonised energy systems has accelerated the adoption of distributed energy resources (DERs), including rooftop solar photovoltaics, residential battery storage, and electric vehicle (EV) charging infrastructure. Projections indicate that by 2030, tens of millions of DER-connected IoT devices will participate in smart grid operations, including real-time metering, bidirectional energy flows, demand response programs, and localized energy markets [1]. These devices primarily use lightweight communication protocols such as MQTT to enable low-latency telemetry and control commands among prosumers, energy aggregators, and distribution system operators (DSOs).

However, the convergence of IoT and smart grids introduces significant security and trust challenges. Conventional centralized identity and access management (IAM) systems rely on a trusted third party (e.g., a utility-operated Public Key Infrastructure (PKI) or cloud IAM service) to issue credentials, validate identities, and enforce access policies. This model exhibits several critical limitations:

- Single point of failure: Compromising the central IAM server exposes all connected DER devices to attackers.
- Device impersonation and spoofing: Attackers can clone device identities or inject falsified meter data, leading to billing inaccuracies, grid instability, or market manipulation.
- Inadequate auditability: Centralized logs are susceptible to alteration or deletion by insiders or following a breach.
- Scalability bottlenecks: Millions of devices generating frequent authentication and authorisation requests can overwhelm central servers during peak events (e.g., extreme weather-driven demand response).
- Privacy erosion: The centralized collection of device attributes and consumption patterns enables detailed profiling of prosumers.

Recent high-profile incidents involving compromised smart meters and EV chargers have highlighted these risks, underscoring the urgent need for architectures that eliminate central trust anchors while preserving operational efficiency [2], [4].

Blockchain technology, particularly permissioned platforms such as Hyperledger Fabric, offers a compelling alternative by providing a tamper-proof, distributed ledger maintained by a consortium of known participants (DSOs, aggregators, and large prosumers). Smart contracts enable programmable, enforceable access policies executed identically across all endorsing peers. When combined with W3C Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), blockchain technology supports self-sovereign identity for devices. DER devices can prove ownership of their identity and attributes

without disclosing unnecessary information or relying on a central registry [14], [15].

This paper addresses the following research questions:

- Research Question 1: How can decentralised identity (DID + VC) enhance trust establishment among heterogeneous DER participants (prosumers, aggregators, DSOs)?
- Research Question 2: How can blockchain-based smart contracts effectively enforce fine-grained, context-aware access control policies that combine RBAC and ABAC for DER IoT devices?
- Research Question 3: To what extent does the proposed framework enhance data integrity, auditability, and system resilience compared with conventional centralised IAM architectures?

The primary contributions of this study are as follows:

- A novel decentralised identity management architecture tailored for DER IoT ecosystems, in which each device possesses a W3C-compliant DID anchored to Hyperledger Fabric.
- A hybrid RBAC+ABAC access control model implemented via multiple interacting smart contracts (chaincodes) that supports dynamic policy evaluation, VC verification, and immutable auditing.
- Detailed integration of secure MQTT-over-TLS communication with on-chain authorization for constrained DER devices.
- A comprehensive security analysis demonstrating the framework's resistance to key threats in smart grid environments through cryptographic identities, policy-enforcing smart contracts, and distributed ledger properties.

The remainder of the paper is organised as follows: Section II reviews related work and provides background on blockchain applications in smart grids and DER management, blockchain-based access control for IoT systems, decentralized identity technologies, and the Hyperledger Fabric platform. Section III presents the proposed decentralised identity and access control architecture. Section IV details the smart contract design. Section V provides a security analysis of the framework. Section VI discusses limitations and future directions, and Section VII concludes the paper.

II. Related Work

This section reviews existing literature on blockchain technology in smart grids and DER management, blockchain-based access control mechanisms for IoT, and the application of decentralized identity (DID) and Verifiable Credentials in IoT and energy domains. It identifies gaps that motivate the proposed framework.

A. Blockchain Applications in Smart Grids and DER Management

Early research on blockchain for smart grids primarily focused on peer-to-peer (P2P) energy trading and transactive energy markets. The Energiforsk report [1] provides a comprehensive survey of use cases, including local energy markets, flexibility trading, and grid service provision. It notes that blockchain has the potential to reduce intermediary costs and enhance transparency but highlights significant challenges in scalability, privacy, and device-level security.

Westphall and Martina [2] implemented a validated clean-energy trading platform on Hyperledger Fabric with anonymised buyers, achieving high throughput under loads of 5,000 sensors/buyers/sellers while analysing data generation rates and deployment costs. Shamaseen et al. [3] proposed a hybrid private-public blockchain framework incorporating a novel "Proof of Energy" consensus algorithm to mitigate the energy expenditure of Proof-of-Work, reporting 60.86 transactions per second (TPS) and an average latency of 3.4 seconds under a 10,000-transaction load. Mohanta et al. [4] developed a smart-contract-based scheme emphasizing data integrity and resistance to double-spending and forgery in IoT-enabled smart grids, with low computational (3.15 ms) and communication (992 bits) overheads.

These works demonstrate the viability of blockchain for market operations. However, they frequently assume pre-established device identities or rely on centralized registration steps, leaving the identity and access control layer underexplored.

B. Blockchain-Based Access Control for IoT Systems

Traditional IoT access control models (RBAC, ABAC, and CapBAC) become susceptible to centralisation when implemented at large scale. Zhang et al. [5] were among the first to develop smart-contract-based access control using multiple Access Control Contracts (ACCs), a Judge Contract, and a Register Contract on Ethereum, enabling both static policy validation and dynamic misbehavior detection. Namane and Ben Dhaou [6] provided a taxonomy distinguishing partially versus fully decentralised blockchain access control solutions and surveyed applications across healthcare, supply chain, and smart home domains. Yu et al. [7] pioneered the integration of ABAC with blockchain for IoT by conceptualising attribute tuples and policy tuples stored on the blockchain to support fine-grained, decentralised decision-making. Xu et al. [8] presented a comprehensive treatment of decentralised IoT access control using smart contracts for context-aware policies.

Hyperledger Fabric has emerged as the preferred platform for enterprise and industrial IoT deployments due to its modular architecture, pluggable consensus (Raft), and native support for attribute-based identity via the Fabric Certificate Authority (CA) and Membership Service Providers (MSPs). Iftekhar et al. [9] demonstrated an ABAC mechanism built solely from Fabric components for IoT devices on ARM64 architectures (Raspberry Pi), achieving secure access without external platforms. Shih et al. [10] designed three specialised smart contracts (Device, Policy, Access) for the Industrial Internet of Things (IIoT) supporting dynamic attribute updates and fine-grained authorisation. Gordijn et al. [12] extended Fabric to integrate multiple IDs, attributes, and policies with minimal performance impact for real-world access decisions.

Iftekhar and Cui [13] anchored device data hashes in Fabric to enable detection of any form of falsification.

These contributions establish strong foundations for policy-driven access control; however, they rarely integrate W3C DIDs or Verifiable Credentials, limiting true self-sovereignty and interoperability with emerging decentralised identity ecosystems.

C. Decentralized Identity (DID) and Verifiable Credentials in IoT and Energy

The W3C DID specification [14] defines a URI-based identifier (e.g., did:fab:device123) resolvable to a DID Document containing public keys, authentication methods, and service endpoints without requiring a central registry. Khayer et al. [15] examined the potential of blockchain for identity management in IoT, emphasising Physical Unclonable Functions (PUFs), zero-knowledge proofs, and reputation systems as complementary mechanisms. However, few studies have applied DID/VC specifically to DER IoT devices operating under the strict latency and regulatory constraints of smart grids.

The present work bridges these gaps by anchoring DIDs to Hyperledger Fabric (via custom chaincode), issuing role- and attribute-based VCs from authorised issuers (DSO, manufacturers), and enforcing hybrid RBAC+ABAC policies through smart contracts. This approach preserves the permissioned, high-performance characteristics of Fabric while adding the self-sovereign identity properties demanded by increasingly autonomous DER ecosystems.

D. Hyperledger Fabric for DER IoT Applications

Hyperledger Fabric is a permissioned blockchain framework designed for enterprise and consortium environments. Its modular architecture and permissioned nature make it particularly well-suited for critical infrastructure such as smart grids, where participants (DSOs, aggregators, and prosumers) are known and identifiable, unlike public blockchains that rely on anonymous participants and energy-intensive consensus.

Figure 1 illustrates the main components and the typical transaction flow in Hyperledger Fabric.

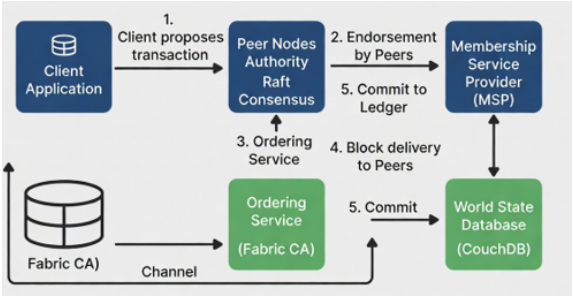

Fig. 1. Main components and the typical transaction flow in Hyperledger Fabric [11].

Key characteristics relevant to DER IoT deployments include:

- Permissioned Network and MSP: All participants are authenticated through Membership Service Providers (MSPs) before network access. This enables fine-grained organizational identity management aligned with the consortium governance model (DSO Organization, Aggregator Organization, and Prosumer Consortium Organization).
- Execute-Order-Validate Architecture: Transactions are executed (endorsed) by selected peers according to endorsement policies, ordered via Raft consensus, and validated before commitment. This separation supports high throughput and confidentiality suitable for control commands and telemetry.
- Chaincode (Smart Contracts): Business logic is implemented in general-purpose languages (Go, Java, Node.js). Four primary chaincodes are employed in this framework: DIDRegistry, VCRegistry, PolicyContract, and AccessControl (detailed in Section IV).
- Private Data Collections and CouchDB World State: Sensitive prosumer attributes are protected via private data collections visible only to authorized organizations, while public data supports rich JSON queries.
- Channels: Private sub-networks can isolate confidential transactions if required by regulatory or commercial constraints.

Fabric's support for attribute-based identity, pluggable consensus, and high-performance transaction processing underpins the proposed integration with lightweight MQTT gateways for constrained DER devices. The standard transaction flow (execute-order-validate) is assumed known [11]; the specific configuration and chaincode design for DER identity and access control are detailed in subsequent sections.

III. Proposed Architecture

Figure 2 illustrates the high-level architecture of the proposed blockchain-based decentralised identity and access control framework for DER IoT in smart grids.

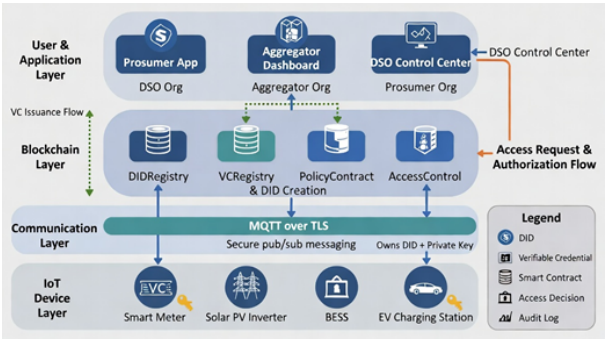

Fig. 2. High-level architecture of the proposed blockchain-based decentralised identity and access control framework for DER IoT in smart grids.

A. IoT Device Layer

Each DER device (smart meter, PV inverter, BESS, EV charger) generates its own DID (did:fab:¡unique-suffix¿) and

corresponding public/private key pair (Ed25519 or secp256k1) during onboarding. The private key never leaves the device (or its secure element). Devices expose a lightweight MQTT client over TLS 1.3. A local IoT Gateway aggregates multiple devices, performs initial signature verification, and submits transactions to Fabric via the Fabric SDK (or REST gateway) on behalf of constrained devices.

B. Communication Layer

MQTT topics are structured hierarchically (e.g., grid/zoneA/prosumer123/meter1/telemetry, grid/control/inverter456/setpoint). Access to publish or subscribe on sensitive topics is gated by the blockchain authorization service. Short-lived JWT-like tokens signed by the device's DID private key and containing a nonce/timestamp are used for MQTT broker authentication, while critical control commands are validated directly on-chain before execution.

C. Blockchain Layer (Hyperledger Fabric)

A permissioned Fabric network is operated by a consortium consisting of:

- DSO Organization (authoritative for grid stability policies)
- Aggregator Organization (manages prosumer fleets)
- Prosumer Consortium Organization (represents individual or community DER owners)

Each organization maintains two peer nodes. A Raft ordering service ensures crash-fault tolerance [11]. All participants share a single channel. Four primary chaincodes are deployed:

- DIDRegistry – stores and updates DID Documents (public keys, service endpoints).
- VCRegistry – manages issuance, revocation, and verification of Verifiable Credentials containing roles (e.g., "CertifiedProsumerDevice") and attributes (e.g., "maxExportkW", "locationZone", "certificationExpiry").
- PolicyContract – stores and evaluates hybrid RBAC+ABAC policies (e.g., "DSO operators may issue setpoints to inverters in their zone if grid frequency ¿ 49.8 Hz").
- AccessControl – core authorization engine that verifies DID signatures, resolves and validates VCs, evaluates policies, and emits immutable audit events.

World state is maintained in CouchDB for rich JSON queries. Private data collections protect sensitive prosumer attributes.

D. Application & User Layer

Prosumers interact via mobile/web apps that manage their devices' DIDs and VCs. Aggregators and DSOs operate dashboards that submit policy updates or bulk control commands. All actions affecting grid state or billing are recorded as Fabric transactions, providing non-repudiable audit trails.

IV. Smart Contract Design

Smart contracts (implemented as chaincode in Hyperledger Fabric) serve as the trusted, decentralised enforcement layer for identity management and access control. By encoding policies and verification logic directly on the blockchain, the system eliminates reliance on centralized policy decision points while ensuring transparency, immutability, and consistent execution across all network participants.

A. Conceptual Foundation

The smart contract design rests on three core principles:

- Decentralized Trust Anchor: Smart contracts act as a distributed, tamper-proof policy engine. Every authorization decision is executed identically on multiple endorsing peers and recorded on the immutable ledger.
- Hybrid RBAC + ABAC Model: The framework combines Role-Based Access Control (RBAC) (e.g., "DSO_Operator", "CertifiedProsumerDevice") with Attribute-Based Access Control (ABAC) (e.g., device location, current grid frequency, certification status). This hybrid approach provides both coarse-grained role management and fine-grained, context-aware authorization suitable for dynamic smart grid environments.
- Separation of Concerns: Identity registration, credential management, policy definition, and authorization decision-making are separated into specialized chaincodes. This modular design improves maintainability, auditability, and allows independent evolution of each component.

B. Structural Design

The smart contract layer consists of four interacting chaincodes deployed on a shared Fabric channel:

Figure 3 illustrates the overall smart contract architecture and the interaction flow between the four chaincodes.

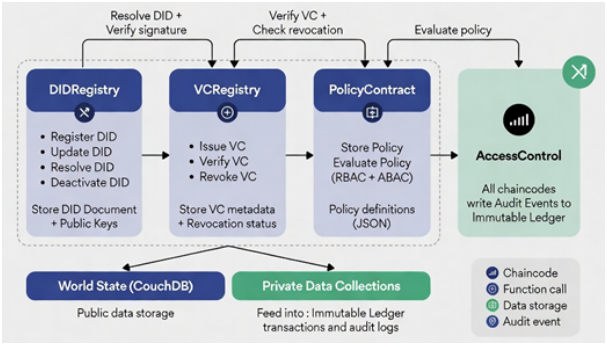

Fig. 3. Overall smart contract architecture and interaction flow between the four chaincodes (DIDRegistry, VCRegistry, PolicyContract, and AccessControl).

Data Storage Strategy:

- Public data (DID documents, policy definitions, audit events) is stored in the World State (CouchDB) for rich querying.

TABLE I
CHAINCODE RESPONSIBILITIES, DATA STORAGE, AND INTERACTIONS

Chaincode	Primary Responsibility	Key Data Stored on Ledger	Interaction with Other Chaincodes
DIDRegistry	Manage decentralized identifiers and public keys	DID Document, revocation status	Called by AccessControl
VCRegistry	Issue, verify, and revoke Verifiable Credentials	VC metadata, revocation registry	Called by AccessControl
PolicyContract	Store and evaluate hybrid RBAC+ABAC policies	Policy definitions (JSON)	Called by AccessControl
AccessControl	Core authorization engine (orchestrator)	Audit events (AccessGranted/AccessDenied)	Calls all other three chaincodes

- Sensitive attributes within Verifiable Credentials are stored using Private Data Collections, visible only to authorized organizations.

All chaincodes are developed in Go following Fabric best practices for determinism and security. They are invoked through the Fabric SDK by IoT gateways or authorized applications.

C. Application in DER IoT Environments

The smart contract design directly supports key operations in distributed energy resource ecosystems:

- Device Onboarding: A prosumer creates a DID for a new DER device and obtains a Verifiable Credential from an authorised issuer (e.g., DSO or manufacturer). Each step is immutably recorded on the blockchain.
- Secure Control Command Authorisation: Before a set-point command from the DSO or aggregator is applied to an inverter or BESS, the AccessControl chaincode verifies the requester's identity (via DID signature), role/attributes (via VC validation), and current context (e.g., grid status) against defined policies.
- Tamper-Proof Auditing: Every access decision, policy change, and credential issuance/revocation generates an immutable event on the ledger, providing strong non-repudiation and supporting regulatory compliance and forensic investigation.

This design addresses Research Question 2 (RQ2) by providing a transparent, immutable, and automatically enforced mechanism for decentralised identity and access control without depending on any central trusted third party.

V. SECURITY ANALYSIS

This section provides a qualitative security analysis of the proposed framework, demonstrating its resistance to prominent threats in DER-enabled smart grid environments. The analysis is based on the cryptographic foundations of DIDs/VCs, the distributed execution model of Hyperledger Fabric, and the hybrid policy enforcement logic.

A. Threat Model

We consider the following adversary capabilities, consistent with typical smart grid IoT threat models:

- Compromise of individual DER devices or IoT gateways (e.g., via physical access or firmware exploits).
- Network-level attacks: eavesdropping, message replay, man-in-the-middle (MITM) on MQTT channels.
- Attempted device impersonation or spoofing of legitimate DIDs.
- Malicious or compromised insiders within one consortium organization (e.g., a rogue aggregator employee).
- Attempts to bypass or tamper with access control policies.
- Denial-of-service attempts against the blockchain network or specific chaincodes.

We assume the underlying Fabric network (peers, ordering service) remains available and that at least a threshold of honest endorsing peers exists per the endorsement policy (e.g., majority of organizations).

B. Mitigation Analysis

Resistance to Device Spoofing and Impersonation

Each DER device holds a unique DID and private key that never leaves its secure element. All critical operations (telemetry publication, control command requests) are signed with this private key. The AccessControl chaincode verifies the signature against the public key in the on-chain DID Document before any further processing. An attacker without the private key cannot produce valid signatures, preventing impersonation even if device metadata is cloned.

Resistance to Replay Attacks

MQTT authentication uses short-lived JWT-like tokens containing a nonce and timestamp, signed by the device's DID private key. On-chain transactions include Fabric-generated timestamps and transaction IDs. The AccessControl and PolicyContract chaincodes reject requests with expired or previously seen nonces/timestamps. This bounds the window for replay to negligible duration under normal clock synchronization.

Resistance to Unauthorized Access and Policy Bypass

All authorization decisions are performed by the AccessControl chaincode, which (1) verifies the DID signature, (2) resolves and cryptographically validates the relevant VCs from VCRegistry, and (3) evaluates the hybrid RBAC+ABAC policy from PolicyContract. Decisions are executed on multiple endorsing peers according to the multi-organization endorsement policy. A single compromised peer or organization cannot unilaterally grant access. Policy definitions themselves are stored immutably and can only be updated via properly endorsed transactions.

Resilience Against Single Points of Failure

There is no central IAM server. Identity documents, credentials, and policies reside on a distributed ledger replicated across peers from multiple organizations. The Raft ordering service tolerates crash faults. Even if one organization's peers become unavailable, the remaining consortium members can continue operation (subject to endorsement policy). Private data collections ensure sensitive attributes are not exposed network-wide.

Mitigation of Insider Threats and Audit Log Tampering

Every access decision, credential issuance/revocation, and policy change emits an immutable event recorded on the ledger with full provenance (requester DID, timestamp, decision outcome, policy version). No single insider can delete or alter historical records. Private data collections restrict visibility of sensitive prosumer attributes to authorized organizations only. Consortium governance and multi-org endorsement further limit the ability of any single party to unilaterally alter system behavior.

Data Integrity and False Data Injection Prevention

While the framework primarily secures identity and access control, it indirectly protects data integrity: only authenticated and authorized devices can publish telemetry or receive control commands. All such interactions are logged immutably, enabling downstream detection of anomalies (e.g., via cross-correlation with grid state or billing systems).

C. Summary

The combination of self-sovereign cryptographic identities (DIDs), verifiable attribute/role credentials (VCs), and distributed policy-enforcing smart contracts on a permissioned blockchain provides strong, layered defenses against the identified threats. The design eliminates the single point of failure inherent in centralized IAM while preserving fine-grained, context-aware control required for safe DER operation. Quantitative performance evaluation under realistic attack scenarios and large-scale device populations is identified as important future work to complement this qualitative analysis.

VI. Limitations and Future Work

While the proposed framework offers a coherent architectural solution, several limitations must be acknowledged:

- The current work focuses on conceptual design, smart contract specifications, and qualitative security analysis. A full prototype implementation integrating physical smart meters, PV inverters, BESS, and SCADA systems has not yet been deployed; quantitative performance metrics (e.g., MQTT command latency, Fabric TPS under peak DER registration and authorization loads) therefore remain to be measured in realistic environments.
- The custom did:fab method, while functional for this prototype, should be aligned with emerging standardized methods (e.g., did:indy or did:web with Fabric anchoring) for broader interoperability and tool support.
- Latency introduced by on-chain authorization may require optimisation (e.g., edge decision caching, optimistic execution, or hybrid off-chain/on-chain models) for protection-class applications demanding sub-100 ms response times.
- The current VC revocation mechanism relies on simple on-chain lists. Large-scale deployments would benefit from privacy-preserving revocation registries (e.g., status lists with zero-knowledge proofs) to avoid leaking credential status information.
- Regulatory and governance frameworks for cross-border DER identity, liability, and data sharing are still evolving; consortium governance models require careful legal and contractual design alongside the technical architecture.

Recommended directions for future research include:

- Integration of zero-knowledge proofs to enable attribute verification without revealing raw values (e.g., proving "certificationExpiry ¿ now" without disclosing the exact date).
- Incorporation of dynamic oracles into policy evaluation to feed real-time grid state data (frequency, congestion, renewable output) directly into authorization decisions.
- Extension to support energy tokenisation and automated settlement processes, leveraging the same identity layer for seamless interoperability.
- Large-scale field pilot deployment in collaboration with DSO and aggregator partners to validate performance, usability, and regulatory compliance under operational conditions.

VII. Conclusion

This paper has proposed a decentralised identity and access control framework for IoT-enabled Distributed Energy Resources in smart grids, based on the integration of W3C Decentralised Identifiers (DIDs), Verifiable Credentials, and Hyperledger Fabric permissioned blockchain. The approach directly addresses the fundamental limitations of traditional centralized identity management systems—single points of failure, device impersonation, unauthorised access, and insufficient auditability—by leveraging self-sovereign cryptographic identities for DER devices and enforcing hybrid RBAC+ABAC policies through smart contracts.

The combination of decentralised identity standards and permissioned blockchains enables secure device registration, dynamic role and attribute management, and fine-grained, context-aware authorisation across heterogeneous DER devices (smart meters, solar PV inverters, BESS, and EV charging stations). Operating over secure MQTT communication, the framework supports trustworthy interactions among prosumers, energy aggregators, and distribution system operators while maintaining data integrity and transparency through immutable on-chain policy enforcement and audit logs.

By establishing a robust technological foundation that aligns W3C decentralised identity standards with Hyperledger Fabric, this work contributes to the development of resilient, secure, and consumer-centric smart grid architectures. As renewable

energy penetration and DER adoption continue to increase, such identity-centric security solutions are expected to play a critical role in enabling trusted peer-to-peer energy trading, demand response coordination, and real-time grid operations. Continued research and practical experimentation will be essential to fully realise the potential of decentralised identity and access control in future smart energy systems.

REFERENCES

[1] Energiforsk, "Blockchain for smart grid operations, control, and management," Energiforsk, Stockholm, Sweden, Tech. Rep. 2022:888, 2022.

[2] J. Westphall and J. E. Martina, "Blockchain privacy and scalability in a decentralized validated energy trading context with Hyperledger Fabric," Sensors, vol. 22, no. 12, Art. no. 4585, Jun. 2022.

[3] A. Shamaseen, M. Qatawneh, and B. Elshqeirat, "Smart grid system based on blockchain technology for enhancing trust and preventing counterfeiting issues," Energies, vol. 18, no. 3, Art. no. 1352, Feb. 2025.

[4] B. K. Mohanta et al., "Smart-contract-based blockchain-enabled decentralized scheme for improving smart-grid security," Internet of Things, vol. 30, Art. no. 101811, 2025.

[5] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," arXiv:1802.04410, 2018.

[6] S. Namane and I. Ben Dhaou, "Blockchain-based access control techniques for IoT applications," Electronics, vol. 11, no. 13, Art. no. 2125, Jul. 2022.

[7] H. Yu, T. Chen, and J. Wang, "A blockchain-based access control mechanism for IoT," in Proc. 2022 6th Int. Conf. Electronic Information Technology and Computer Engineering (EITCE), Xiamen, China, 2022, pp. 25–30.

[8] R. Xu, Y. Chen, and E. Blasch, "Decentralized access control for IoT based on blockchain and smart contract," in Blockchain for Distributed Systems Security, S. S. Iyengar et al., Eds. Hoboken, NJ, USA: Wiley, 2019, ch. 23.

[9] A. Iftekhar, X. Cui, Q. Tao, and C. Zheng, "Hyperledger Fabric access control system for Internet of Things layer in blockchain-based applications," Entropy, vol. 23, no. 8, Art. no. 1054, Aug. 2021.

[10] D.-H. Shih, T.-W. Wu, M.-H. Shih, G.-W. Chen, and D. C. Yen, "Hyperledger Fabric access control for industrial Internet of Things," Applied Sciences, vol. 12, no. 6, Art. no. 3125, Mar. 2022.

[11] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," arXiv:1801.10228, 2018.

[12] D. Gordijn, R. Kromes, T. Giannetsos, and K. Liang, "Combining ID's, attributes, and policies in Hyperledger Fabric," arXiv:2207.01599, 2022.

[13] A. Iftekhar and X. Cui, "Anti-tamper protection for Internet of Things system using Hyperledger Fabric blockchain technology," arXiv:2109.07074, 2021.

[14] World Wide Web Consortium (W3C), "Decentralized identifiers (DIDs) v1.0: Core architecture, data model, and representations," W3C Working Draft, Oct. 2020. [Online]. Available: https://www.w3.org/TR/did-core/

[15] B. Khayer, S. Mirzaei, H. Alavizadeh, and A. S. Shahraki, "Blockchain for secure IoT: A review of identity management, access control, and trust mechanisms," IoT, vol. 6, no. 1, Art. no. 65, 2025.