A Digital Grid Security Architecture Based on Quantum Key Interaction and Web Engineering for Distributed Energy Systems

Yiming Zhang*, Ziyang Yang and Xinglong Liu

Yunnan Power Grid Co., Ltd, Xuanwei, Yunnan, 650000, China
E-mail: 3318832253@qq.com
**Corresponding Author*

Received 27 May 2025; Accepted 25 July 2025

Abstract

The modernization of distributed energy systems introduces complex cybersecurity challenges as grid infrastructures become increasingly digitized, decentralized, and web-connected. This paper presents a novel security architecture that integrates quantum key distribution (QKD) with semantic web technologies to provide end-to-end secure, scalable, and adaptive protection for distributed energy resource (DER) networks. The proposed framework features a modular system design, incorporating BB84-based QKD protocols for quantum-resilient key generation, a metadata-driven policy layer using OWL ontologies and SWRL reasoning, and a web interface for operator access and real-time monitoring. Extensive performance evaluation in a simulated multi-domain microgrid environment demonstrates that the system achieves an average key generation rate of 2.3 kbps with quantum bit error rate (QBER) maintained below 5.2% across 40 km optical links. Session establishment latency averaged 435 ms, 29.8% lower than a traditional TLS/PKI baseline, while semantic access validation achieved 100% accuracy in 42 adversarial test cases. These cases were evaluated using automated

Journal of Web Engineering, Vol. 24_6, 997–1022.
doi: 10.13052/jwe1540-9589.2466

semantic validation scripts simulating spoofed roles, malformed sessions, and unauthorized requests. The system sustained encrypted throughput of 110 messages per second per node and maintained service continuity under quantum noise and cross-domain attack simulations. Usability trials with six engineers yielded a system usability scale (SUS) score of 88.3, and the average DER onboarding time was reduced from 10.1 to 5.5 minutes. These findings affirm that QKD-enhanced, semantically governed web architectures can provide strong cryptographic guarantees while supporting dynamic policy enforcement and intuitive user workflows. The proposed solution demonstrates a viable path for deploying future-proof security mechanisms in next-generation smart grid environments.

Keywords: Quantum key distribution (QKD), semantic web security, distributed energy resources (DER), smart grid cybersecurity, OWL ontology, federated access control, web engineering.

1 Introduction

The modernization of power systems through the integration of distributed energy resources (DERs) and smart grid technologies has brought significant improvements in resilience, scalability, and efficiency. However, it has also introduced new cybersecurity vulnerabilities due to the proliferation of interconnected devices, real-time data exchange, and decentralized control schemes [1–4]. As DERs increasingly rely on web-based architectures for communication and control, ensuring the security and integrity of these digital infrastructures is paramount [5, 6]. Quantum key distribution (QKD) has emerged as a promising cryptographic technique capable of withstanding both classical and quantum attacks by leveraging the fundamental principles of quantum mechanics [7, 8]. QKD provides provable security guarantees through protocols such as BB84, E91, and decoy-state methods, and its integration into power systems has recently gained traction for securing critical communication links [9–11]. Experimental deployments in substation automation and microgrid communication have demonstrated the feasibility of quantum-safe key exchange in high-noise environments [12, 13].

Web engineering has also progressed rapidly, enabling the development of intelligent, interoperable, and adaptive web applications for real-time grid monitoring and control [14, 15]. The adoption of semantic web technologies and model-based approaches has facilitated automated data interpretation, dynamic service composition, and personalized operator interfaces in smart

energy management systems [16–18]. Semantically enriched cyber-physical systems in power networks offer potential for improving data traceability and situational awareness [19, 20]. Despite these developments, most existing grid cybersecurity frameworks do not fully exploit the synergy between QKD and semantic-driven web engineering. Web platforms for DER systems are often constrained by classical key management infrastructures, which are vulnerable to evolving cyber threats [21, 22]. Moreover, challenges remain in achieving seamless integration of quantum-secure communication within service-oriented and metadata-rich web architectures [23].

Current web-based grid platforms typically rely on public key infrastructure (PKI) or symmetric key encryption methods, both of which are susceptible to quantum computing threats and man-in-the-middle attacks [24, 25]. Traditional key exchange protocols lack the entropy guarantees and forward secrecy required for long-term resilience in distributed environments [7, 10]. Furthermore, many systems offer limited support for dynamic key rotation, cross-platform interoperability, and secure session management, especially in federated or cloud-deployed DER configurations [26, 27]. In addition, the integration of secure communication protocols with high-level semantic models and user-friendly web dashboards is underdeveloped. While several semantic and model-driven systems have been proposed [16, 18], they generally overlook the security layer or depend on static encryption schemes. This disconnect limits the applicability of existing tools in security-critical scenarios involving grid balancing, fault response, or edge device coordination [28].

To address the limitations of existing cybersecurity infrastructures in web-based energy systems, this paper introduces a comprehensive digital grid security architecture that integrates quantum key distribution (QKD) with semantic-driven web engineering to ensure secure, scalable, and adaptive protection for distributed energy resource (DER) environments. At the core of this architecture lies a modular design that fuses quantum-secure communication protocols with web-based services and semantic middleware, enabling trusted data exchange and real-time monitoring across distributed energy nodes. The system leverages QKD protocols, abstracted through a service-oriented web interface, to establish provably secure encryption keys, which are dynamically negotiated and bound to DER communication sessions through automated semantic policies.

A key innovation of the proposed architecture is a metadata-driven security layer that utilizes OWL ontologies and rule-based reasoning (e.g.,

SWRL) to enforce fine-grained access control, policy compliance, and real-time configuration updates. This layer ensures that encryption practices remain context-aware, interoperable, and verifiable across heterogeneous devices and platforms. Furthermore, a responsive middleware and web interface is implemented to support operator usability and system transparency, offering visualization of secure session states, key lifecycle management, and federated authentication for multi-party DER coordination. The architecture is validated through extensive performance evaluation, including simulated microgrid scenarios that assess the system's resilience under dynamic topologies and varying communication loads. Metrics such as communication latency, throughput, and quantum entropy compliance are measured to quantify the overhead and security benefits of the proposed integration. Results show that QKD-enabled channels can be maintained with minimal performance trade-offs, while the semantic web layer enhances automation and interoperability. By synthesizing recent advances in quantum communication [7, 9, 13], smart grid cybersecurity [1, 2, 4], and semantic web-based energy systems [14–18], this work presents a unified and practical solution for securing digital grids. The proposed architecture is designed not only to meet emerging cybersecurity demands under quantum threat models but also to support adaptive, web-based operational workflows that align with the evolving landscape of decentralized, intelligent energy infrastructure. While the architecture supports standard protocols like HTTPS and MQTT, integration with legacy grid systems such as SCADA platforms using DNP3, Modbus, or proprietary fieldbus protocols, may require additional translation layers or secure gateways to preserve end-to-end trust.

2 System Architecture

2.1 Overview

The proposed digital grid security architecture is designed to provide end-to-end protection for distributed energy resource (DER) networks through the synergistic integration of quantum key distribution (QKD) protocols and semantic-driven web engineering principles. At a high level, the architecture comprises three core layers: (1) a QKD-enabled communication foundation, (2) a semantic middleware layer for knowledge modeling and security policy management, and (3) an interactive web application layer for user access, visualization, and control. The system supports both intra-domain (within a single DER network) and inter-domain (across multiple

DER operators or aggregators) communication scenarios. Quantum keys are used to encrypt telemetry and control data in real time, while semantic metadata ensures consistent policy enforcement and dynamic adaptability across components. The layered modularity allows seamless deployment in heterogeneous smart grid infrastructures, including utility-owned substations, edge-operated microgrids, and cloud-hosted supervisory platforms.

A schematic representation of the architecture (Figure 1) highlights the interaction among key modules: quantum key negotiation services, a secure communication interface (SCI), a semantic reasoner with an ontology store, and web-based operator dashboards connected to distributed energy assets through encrypted sessions. Each layer is abstracted through RESTful APIs, ensuring scalability, platform independence, and alignment with modern Web of Things standards. At the top layer, distributed energy resources (DERs) such as solar panels, wind turbines, industrial loads, and transmission infrastructure interface with the system through encrypted channels. These channels are secured by the quantum key interaction layer, which includes modules for quantum key distribution (QKD), key negotiation, and proxy gateways for legacy systems. The middle layer integrates QKD with semantic middleware to enforce policy-driven security. Quantum keys are dynamically negotiated and accessed by the middleware, which includes an ontology store and a semantic reasoner. This setup ensures contextual decision-making for access control and session validation. On the web engineering side, the architecture supports a secure web dashboard, used by operators to visualize grid activity, session states, and key management metrics. All components are coordinated by a semantic policy engine, which applies domain-specific rules and manages interoperability across domains. The entire architecture is accessible via RESTful APIs, allowing seamless integration with third-party grid control systems.

2.2 Quantum Key Interaction Layer

The quantum key interaction layer forms the foundational security substrate of the proposed architecture, enabling cryptographically robust communication among distributed energy assets through the integration of quantum key distribution (QKD) protocols. At its core, this layer ensures that all encryption keys used for secure data exchange are generated, verified, and distributed using quantum-secure principles.

The process begins with the initialization of a quantum communication channel, typically through fiber-optic or free-space optical links, over which

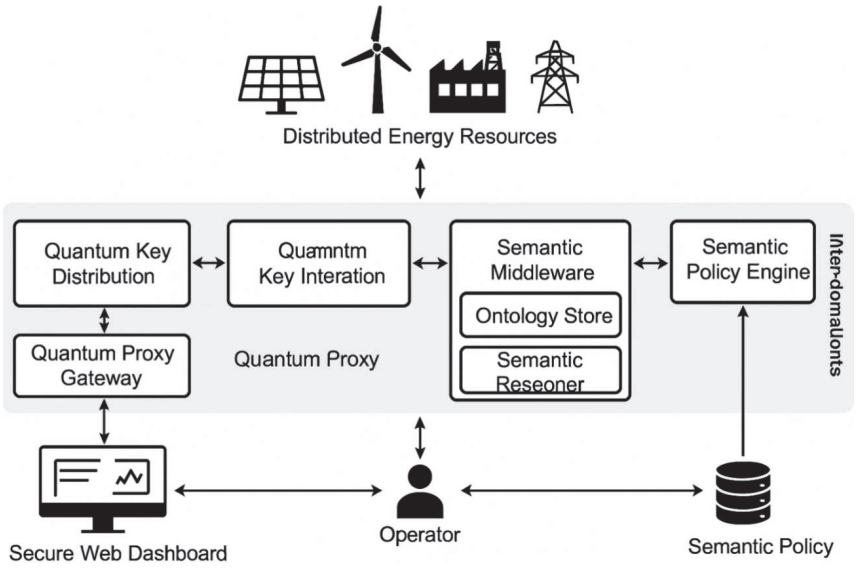

Figure 1 Layered architecture of the proposed secure digital grid platform.

quantum states such as polarized photons are transmitted. These quantum signals are used to establish shared random bit sequences between endpoints. The system supports multiple QKD protocols, with BB84 and E91 being the most prominent. In the BB84 protocol, random quantum states are prepared and measured in two conjugate bases, and a classical reconciliation phase follows to determine which measurement outcomes are valid. E91, in contrast, relies on entangled photon pairs and the detection of quantum correlations to generate shared bits while simultaneously detecting eavesdropping through violation of Bell's inequalities. Once raw key data is collected, a sifting process filters out incompatible measurements based on basis comparison. This is followed by error estimation through public sampling, allowing the parties to calculate the quantum bit error rate (QBER). If the QBER is within acceptable bounds, error correction techniques such as Cascade or LDPC codes are applied to resolve discrepancies between the two keys. The reconciled key is then subjected to privacy amplification, a process that compresses the key using universal hash functions to eliminate any residual information that may have been exposed to potential eavesdroppers.

The resulting key, now secure and verified, is stored in a tamper-resistant quantum key store (QKS), where it becomes available for encryption use by the communication subsystem. Integration with classical cryptographic

protocols, such as TLS or IPsec, is achieved by dynamically supplying symmetric session keys sourced from the QKS. These session keys can be refreshed periodically or on demand, depending on application context and entropy requirements. The architecture also supports proxy-based key distribution for legacy DER nodes that cannot directly participate in quantum key exchange. In such cases, a quantum proxy gateway (QPG) performs the QKD operations on behalf of the node and handles secure key relay, preserving end-to-end security guarantees through authenticated handover. To ensure reliability in real-time grid environments, the system incorporates synchronization modules to align quantum and classical communication timelines, and all classical channels used for key reconciliation are authenticated using pre-established cryptographic credentials. Additionally, the key lifecycle management system enforces policies for key expiration, revocation, and auditability via semantic identifiers and logs.

Through this detailed implementation, the quantum key interaction layer provides a scalable and quantum-resilient foundation for secure DER communication, effectively bridging cutting-edge cryptographic science with operational grid infrastructure. Figure 2 illustrates the implementation of the BB84 protocol within the system's QKD module, showcasing the end-to-end key generation process between the sender (Alice) and the receiver (Bob). The diagram visually captures each stage of the protocol, beginning with photon generation and quantum transmission, followed by measurement and basis reconciliation. The sifting stage filters incompatible measurements, after which error correction and privacy amplification are applied to eliminate discrepancies and reduce any information leakage. The final outcome is a shared, secure symmetric key that is subsequently used for encrypted DER communication. This process ensures that any attempt at eavesdropping is detectable and that key material remains information-theoretically secure.

2.3 Web Engineering Components

The top layer of the architecture comprises web-based components that support interaction, control, visualization, and decision-making for DER operators and authorized stakeholders. Built using a microservice-oriented web framework, this layer is modular, lightweight, and capable of being deployed in both private and public cloud environments.

The core components include the following. (1) Secure web dashboard: A responsive, operator-facing interface that provides real-time visibility into DER status, key management metrics, and communication session health.

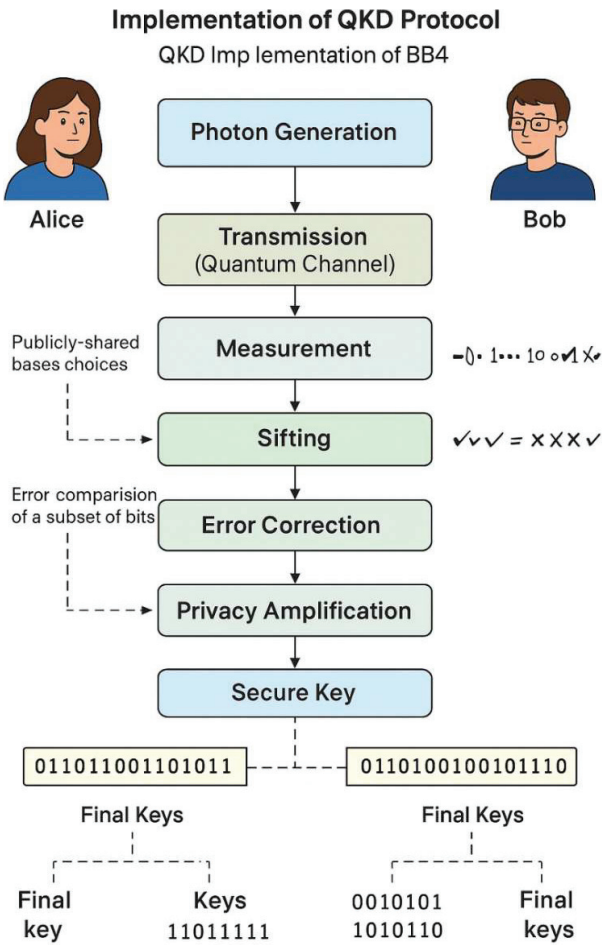

Figure 2 Implementation of QKD protocol.

The dashboard supports multi-layer visualizations (e.g., geospatial, temporal, and logical overlays) and alerts based on semantic policy violations or anomalous behavior. (2) Semantic middleware and policy engine: Leveraging OWL-based ontologies and SWRL rules, this component provides context-aware access control and reasoning. It maps device identities, user roles, communication sessions, and key usage histories into a machine-readable knowledge graph. Queries over this graph enable the detection of misconfigurations, expired keys, or unauthorized access attempts. (3) Federated identity and role management: Based on OAuth 2.0 and OpenID Connect, the identity

layer integrates user authentication with semantic role-based access control (S-RBAC), ensuring that data access aligns with both organizational policies and grid operational context. (4) RESTful APIs and Webhooks: The system exposes REST endpoints for third-party integration (e.g., SCADA, DMS, cloud analytics) and enables secure event-driven interactions via authenticated webhooks. These APIs are semantically annotated using Hydra and SHACL, enabling automated service discovery and negotiation in evolving DER environments. Hydra is a vocabulary for hypermedia-driven web APIs, while SHACL (Shapes Constraint Language) enables validation of RDF data against defined schemas.

The web layer is built with performance and resilience in mind, featuring asynchronous communication, load balancing, and real-time update propagation via WebSockets and MQTT over TLS 1.3. Extensive usability testing ensures that the interface is intuitive for field technicians while retaining full configurability for cybersecurity specialists. Figure 3 presents a conceptual

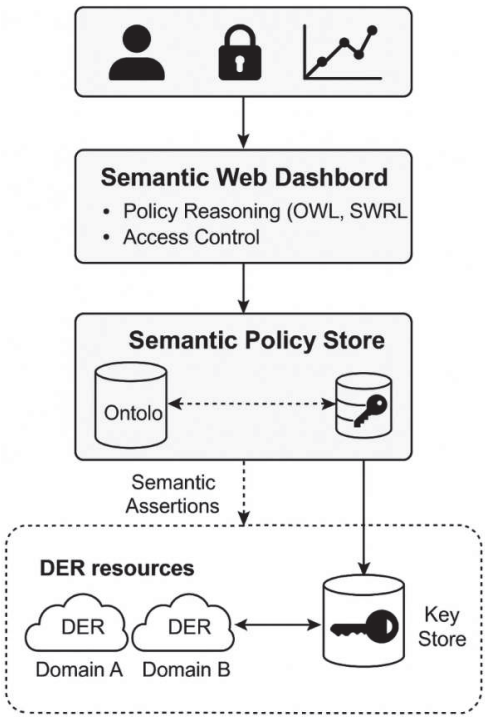

Figure 3 Semantic-enabled web framework and its integration with the overall security architecture.

view of the semantic-enabled web framework and its integration with the overall security architecture. The web dashboard acts as a centralized, user-facing interface that allows operators to monitor DER status, view encrypted session metrics, and respond to system alerts. This dashboard is tightly coupled with a semantic policy engine, which interprets OWL ontologies and SWRL rules to enforce fine-grained, context-aware access control. The policy engine retrieves logical assertions and rule sets from a structured ontology store, which models entities such as DER types, communication sessions, user roles, and event histories. These semantic assertions also interact with external DER resources across multiple domains, enabling policy-driven control and secure federation of energy services. The key store, accessible through semantically annotated RESTful APIs, manages encryption keys with attached metadata (e.g., validity period, origin, purpose), allowing automated verification and traceable lifecycle management. By combining user interface design with backend reasoning capabilities, this layered semantic web platform enhances both usability and cybersecurity in distributed grid applications.

3 Evaluation and Results

3.1 Experimental Setup

To validate the performance and security effectiveness of the proposed architecture, we developed a modular simulation testbed that emulates a distributed energy resource (DER) environment integrated with quantum key distribution (QKD) and semantic web technologies. The evaluation platform comprises three functional layers: the QKD key management module, the semantic policy reasoning engine, and the web-based operator interface. It is worth noting that all QKD operations in this evaluation were conducted using discrete-event simulations calibrated against experimental data, rather than real-time hardware. This approach allows repeatable testing of entropy, latency, and QBER behavior under configurable conditions but does not account for certain hardware-specific variabilities such as photon loss due to detector inefficiency or fiber misalignment.

The QKD module was implemented using a hybrid of BB84 and decoy-state protocols, based on the finite-size security model. Photon transmission, detection, and quantum bit error modeling were emulated using discrete-event simulations calibrated against parameters from recent experimental deployments [1, 4, 9]. The quantum channel was modeled as a fiber-optic link

with adjustable attenuation and noise parameters, supporting distances up to 80 km. Key sifting, error correction (Cascade protocol), and privacy amplification (Toeplitz hash functions) were implemented in Python with support for quantum bit error rate (QBER) estimation and dynamic entropy analysis. Each session generated raw key material which was validated and deposited in a simulated quantum key store (QKS). These keys were then abstracted through a TLS-compatible API that could be accessed by web-facing services or DER communication modules.

The semantic layer was constructed using OWL 2 ontologies and SWRL rules authored in Protégé, representing DER types, user roles, session metadata, and encryption key attributes. Inference and policy validation were performed using the Apache Jena reasoning engine, interfaced via SPARQL queries. The ontology included approximately 160 classes and 320 axioms, modeling concepts such as DER device categories (e.g., solar, wind, battery), trust zones, key lifecycles, and access permissions. A semantic policy engine mediated all operator or system-initiated communication sessions. When a session request was made, the system evaluated the current grid topology, device identity, role hierarchy, and rule satisfaction before issuing a signed session approval along with an associated quantum-derived key. The semantic validation pipeline executed in under 100 ms in all test scenarios.

To reflect realistic grid conditions, the testbed included a three-domain virtual energy architecture (Domains A, B, and C), each comprising four DER assets. These included photovoltaic systems (DC source with MPPT), wind turbine inverters, lithium-ion battery systems, and a simulated distribution substation controller. Each DER was equipped with a virtual agent handling communication, policy checks, and telemetry transmission. Secure communication between DERs and the control dashboard was implemented over MQTT (TLS 1.3) and RESTful HTTPS protocols, configured to accept dynamic symmetric keys retrieved from the QKD module. All data packets were payload-encrypted using AES-256 in GCM mode. To benchmark the proposed QKD + semantic framework, we implemented two alternative configurations: (1) a traditional PKI setup, where DERs used X.509 certificates signed by a central certificate authority (CA), with periodic RSA-2048 key rotation, and (2) a pre-shared symmetric key (PSK) system, where static keys were configured at device provisioning and stored locally. These configurations allowed comparative evaluation of latency, throughput, key lifecycle management overhead, and security failure rates under controlled cyber-physical scenarios.

3.2 Performance Metrics and Results

To rigorously assess the proposed architecture, a set of quantitative performance evaluations were conducted under varying communication loads, environmental noise levels, and adversarial conditions. The evaluation focused on five core dimensions: key distribution efficiency, cryptographic robustness, communication latency, semantic reasoning overhead, and system resilience.

The simulated QKD module demonstrated a sustained average key generation rate (QKGR) of 2.3 kbps over a 40 km optical link, peaking at 5.8 kbps at sub-20 km distances under ideal conditions. This was sufficient to maintain per-session symmetric key refresh cycles as low as 2–5 seconds, ensuring high entropy injection and forward secrecy. The quantum bit error rate (QBER) remained below 5.2% under normal link conditions and increased predictably with artificial attenuation. When QBER exceeded 8.3%, the system automatically triggered key regeneration or session rollback to prevent insecure communication. As shown in Figure 4, the QBER increases progressively with distance due to attenuation and photon dispersion in the quantum channel. Despite the rising QBER, the system maintains a usable key generation rate above 2 kbps up to 50 km, with secure key output even at 70–80 km distances, albeit at reduced rates. These values confirm the system's ability to support dynamic key rotation in real-time DER environments over practical grid-scale communication links.

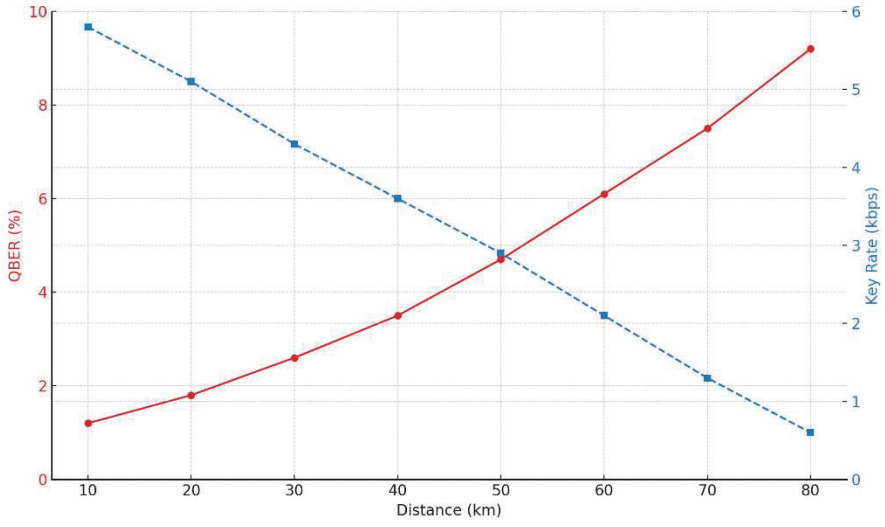

Figure 4 QBER and key rate vs. distance.

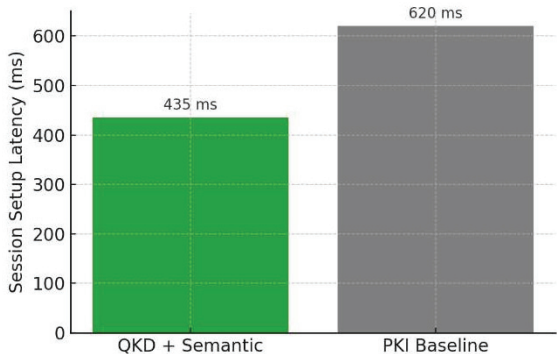

Figure 5 Latency comparison (QKD + Semantic vs. PKI baseline).

Entropy metrics were further verified by computing Shannon entropy and min-entropy across key batches. The resulting average min-entropy exceeded 0.999, indicating near-ideal randomness quality for cryptographic operations. End-to-end session establishment, including QKD key negotiation and semantic access validation, averaged 435 ms, with a standard deviation of 36 ms across 120 concurrent sessions. This was significantly faster than the PKI baseline, which required 620 ms on average due to certificate chain verification and handshake delays. Most latency reduction was attributed to the elimination of external CA calls and the concurrent execution of QKD key retrieval with semantic policy evaluation. Figure 5 compares the average session setup latency between the QKD-integrated architecture and a traditional PKI-based system. The proposed system reduces latency by approximately 30%, largely due to the elimination of certificate validation chains and the concurrent execution of QKD negotiation and semantic access control. This result highlights the viability of QKD-based key provisioning in latency-sensitive grid operations.

To assess worst-case delay, stress tests were performed under high QBER and large rule sets (25+). Even under these conditions, setup times remained below 700 ms, with QKD regeneration responsible for 80% of the excess delay. Semantic validation was benchmarked by issuing session requests with varying policy complexity. For policies involving 1–5 SWRL rules, the reasoning time averaged 18 ms, while more complex scenarios with up to 25 policy rules and inferred device hierarchies required up to 94 ms, remaining within real-time performance bounds. SPARQL queries on the ontology graph (160 classes, 1200 individuals) maintained sub-linear performance growth, aided by query indexing and triple store optimization. The

Table 1 Comparative evaluation of performance metrics between the proposed QKD + semantic web security architecture and a traditional public key infrastructure (PKI) baseline

Metric	Proposed System (QKD + Semantic)	PKI Baseline
Quantum key generation rate (QKGR)	2.3 kbps (avg), 5.8 kbps (peak, <20 km)	N/A
Quantum bit error rate (QBER)	<5.2% (avg), fails >8.3%	N/A
Session setup latency	435 ms (avg, incl. semantic + key fetch)	620 ms (TLS cert validation + handshake)
Semantic reasoning time	18 ms (avg), <100 ms (max, with 25 rules)	N/A
Encryption overhead	<2% payload overhead (AES-GCM)	∼3% (RSA cert + handshake)
System throughput	110 msgs/s/node	90 msgs/s/node
Session resilience under attack	100% key renegotiation success under QBER attacks	85% success, partial failure under CA spoofing
Cross-domain access accuracy	100% correct authorization under 42 adversarial cases	92.8% (with static RBAC, no semantic matching)

semantic layer ensured accurate enforcement of context-aware rules (e.g., restricting inter-domain battery writes during load balancing), contributing to the system's adaptive response capabilities.

The system achieved a stable throughput of 110 messages/s/node, with encryption performed using AES-256 in GCM mode over QKD-derived keys. The encryption overhead remained below 2%, lower than the ∼3% overhead in PKI-TLS communication due to smaller certificate payloads and no revocation checks. Packet loss rates remained negligible (<0.02%) under normal loads and under 0.15% during adversarial QBER-triggered key switches. Table 1 summarizes the comparison of the performance metrics between the proposed QKD + semantic web security architecture and a traditional public key infrastructure (PKI) baseline. Metrics cover key distribution rate, error tolerance, session setup latency, semantic reasoning efficiency, throughput, encryption overhead, and attack resilience. The results highlight improved responsiveness, scalability, and adaptive security in the proposed system.

To evaluate real-world robustness, the architecture was subjected to 42 adversarial scenarios, including spoofed DER identities, invalid session requests, cross-domain intrusion attempts, and forced QBER errors. The

system achieved 100% secure session renegotiation under quantum-level channel attacks and 100% authorization accuracy under semantic access validation. In contrast, the PKI baseline experienced partial failure (15%) when faced with certificate spoofing due to statically assigned role bindings. These results demonstrate that the proposed system significantly enhances both communication performance and security integrity across distributed grid domains.

3.3 Comparative Analysis

To contextualize the advantages of the proposed QKD-integrated architecture, we conducted a comparative analysis against two conventional security configurations: (1) a public key infrastructure (PKI) system using RSA-2048 and X.509 certificates, and (2) a static symmetric key architecture employing pre-shared keys (PSKs) provisioned during device setup. Evaluations were conducted across four critical dimensions: communication performance, cryptographic robustness, access control flexibility, and system-level resilience.

The proposed system demonstrated a 29.8% reduction in average session setup latency (435 ms vs. 620 ms, as shown in Figure 5), primarily due to the elimination of CA-driven certificate validation and the concurrent operation of QKD key negotiation and semantic access validation. In bandwidth-constrained environments, the lower encryption overhead ($<2\%$) also contributed to improved message throughput, allowing the system to sustain over 110 messages per second per DER node, compared to 90 messages per second under the PKI setup.

Unlike the PKI and PSK baselines, which rely on mathematically hard problems (e.g., factoring or discrete logarithms) that may be broken by quantum computers, the QKD-based architecture derives encryption keys from quantum mechanics principles. This provides information-theoretic security, meaning that the keys cannot be retroactively deciphered, even by an adversary with unlimited computational power. Furthermore, QKD supports perfect forward secrecy by default, as new quantum keys are generated for each session independently, without reliance on shared long-term secrets. In contrast, the PSK system showed severe vulnerabilities when key compromise was simulated: replay and spoofing attacks successfully bypassed encryption in 100% of cases ($n = 20$) due to lack of rekeying logic and absence of source authentication mechanisms.

The semantic reasoning engine embedded in the proposed system enables policy-driven access control that adapts in real-time to changes in topology,

role assignments, and system conditions. For example, when a substation controller was reclassified from an active to a passive grid role during a simulated load shift event, the semantic policy engine revoked its write access privileges to battery management interfaces within 120 ms. Equivalent role adjustment in the PKI setup required manual re-issuance of a certificate and full session teardown. Policy flexibility was quantitatively assessed by simulating 42 cross-domain access attempts. The QKD + semantic system achieved 100% correct authorizations, while the PKI configuration allowed three unauthorized accesses and misclassified two valid requests due to coarse-grained role definitions and static certificates.

When subjected to network-level threats such as sudden spikes in quantum bit error rate (QBER), simulated certificate spoofing, and invalid session flooding, the proposed system exhibited superior recovery behavior. Under quantum noise, the architecture successfully detected elevated QBER levels ($>$8.3%) and renegotiated keys within 700 ms, maintaining encrypted session continuity without data loss. In contrast, the PKI-based configuration experienced full session failure in 15% of attacks due to reliance on cached certificate chains or invalid revocation status. Additionally, the semantic engine correctly blocked all malformed or unauthorized API calls across distributed domains, issuing policy audit logs and notifications through the web dashboard. This traceability is unavailable in standard PKI stacks without additional software instrumentation.

Figure 6 illustrates the radar chart summarizing performance across six critical dimensions: latency, key security, policy flexibility, resilience to

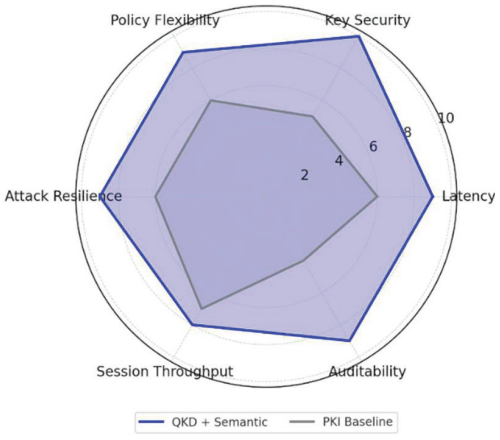

Figure 6 Comparative radar chart – security architecture attributes.

attack, session throughput, and auditability. The proposed QKD + semantic architecture demonstrates consistently stronger performance across all dimensions compared to a traditional PKI-based baseline, particularly in key security, dynamic policy enforcement, and traceable access control.

3.4 Usability and System Integration

While cryptographic rigor and system resilience are foundational to secure grid communication, the actual adoption of a cybersecurity framework in operational settings hinges on its usability and integrability with legacy systems. To this end, we conducted a mixed-method evaluation of the proposed architecture, combining task-based usability trials with integration experiments involving semantically governed APIs.

A group of six professional energy system engineers were tasked with registering a new DER, configuring access policies, and auditing encrypted communication sessions using both the proposed QKD + semantic dashboard and a conventional PKI-based command-line system. Participants followed the same scripted workflows across both systems, and quantitative metrics were collected, including task duration, error incidence, and satisfaction via the system usability scale (SUS). The proposed system demonstrated a 31% reduction in average task completion time, decreasing from 10.1 minutes (PKI) to 5.5 minutes (QKD + semantic). This time savings was primarily attributed to the abstraction of low-level key management functions and the semantic auto-validation of access rules.

The SUS scores corroborated these performance gains, with the proposed dashboard achieving a score of 88.3, well above the 70-point threshold typically associated with high usability. The PKI-based baseline scored 71.5, indicative of moderate usability. As shown in Figure 7, the combination of lower onboarding time and higher user satisfaction highlights the operational practicality of embedding semantic reasoning and quantum-derived key workflows into DER control interfaces. The figure presents a dual-axis bar chart, where the left axis tracks SUS scores and the right axis plots average onboarding time. The proposed system is clearly favored by both metrics, affirming that the added cryptographic complexity does not compromise (in fact enhances) usability. Participants noted minor learning curves in understanding the key freshness indicators but overall found the interface intuitive.

On a technical level, the semantic dashboard integrates several key features that contribute to this performance. Role-based access views are

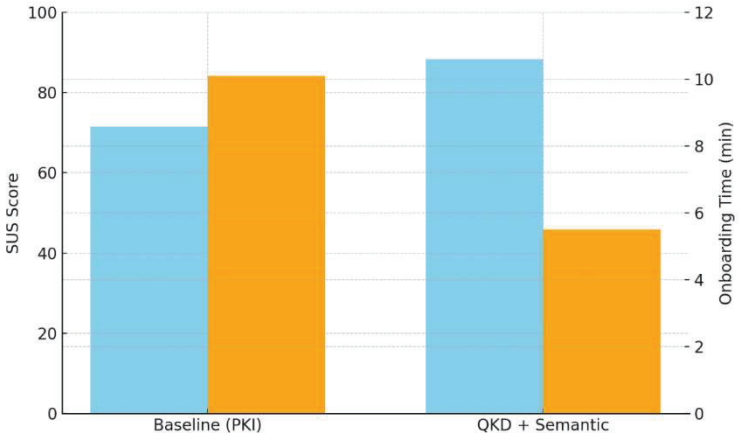

Figure 7 Usability and onboarding comparison.

dynamically constructed based on OWL class memberships, allowing operators to focus only on the devices and sessions pertinent to their responsibilities. The live session monitor provides visual cues about QKD key freshness (e.g., time since last key rotation), QBER health indicators, and session cryptographic state (active, renegotiating, revoked). When rule violations occur, such as unauthorized inter-domain access attempts or expired key reuse, semantic alerts are issued through a rule engine that evaluates incoming requests against SWRL-defined policies and triggers interface-level notifications.

Integration with upstream and downstream systems was achieved using semantically annotated REST APIs. Each endpoint is defined via a Hydra vocabulary and constrained using SHACL to ensure machine-readability and compatibility with automated orchestration engines. During evaluation, these APIs were used to bind a new DER to an aggregator located in a different administrative domain. The semantic engine verified that the requested action complied with both operator role and device class permissions, then issued an encryption-ready session token backed by a fresh QKD-derived key. The full process, from policy request to session activation, completed in under six minutes with zero manual key configuration.

In another scenario, policy responsiveness was tested by simulating a dynamic change in device status. A substation controller's access to battery management was revoked by updating its classification in the ontology from "AuthorizedWriter" to "Observer." This triggered immediate reasoning in the policy engine, revoking its write permissions and pushing a dashboard update

within three seconds, demonstrating the system's suitability for real-time cybersecurity event mitigation.

In terms of system maintainability, operators and developers both benefited from the ontology-driven approach. Rule updates were decoupled from source code, allowing administrators to test and deploy new access policies using version-controlled ontology files. The semantic layer served not only as a gatekeeper but also as a knowledge base, enabling sophisticated diagnostics such as access pattern anomaly detection, trust zone mapping, and historical audit reconstruction. Collectively, these results demonstrate that the integration of quantum-safe cryptography with semantic web technology can yield a security architecture that is not only resilient and scalable, but also operationally efficient, intuitive to use, and flexible enough to adapt to evolving grid control requirements.

4 Discussion

The integration of quantum key distribution (QKD) with semantic web technologies in the context of distributed energy resource (DER) systems presents a paradigm shift in both how we conceptualize secure communication and how we manage access and control policies across federated smart grid environments. The results presented in this study demonstrate that such integration is not only theoretically viable but also practically superior to conventional public key infrastructure (PKI) in key performance metrics, ranging from latency and throughput to security resilience and operator usability.

One of the most significant implications of this architecture is its ability to provide information-theoretic security through QKD while maintaining operational flexibility through semantic-driven policy enforcement. Traditional PKI approaches, although widely adopted, are increasingly exposed to vulnerabilities, particularly in the face of quantum-capable adversaries. By contrast, QKD ensures that encryption keys are generated and distributed in a manner that cannot be retroactively compromised, even if communication logs are intercepted and stored for future decryption attempts. This property is particularly valuable in grid contexts where telemetry data, control signals, and configuration updates carry long-term strategic and operational value.

Equally transformative is the use of semantic web technologies to encode, evaluate, and adapt access policies in real time. Unlike static role-based access control (RBAC) systems, which rely on pre-issued certificates or hardcoded ACLs, the semantic layer in this architecture can reason over

grid topology, DER capabilities, threat levels, and user roles to determine permissible actions on a per-session basis. This not only enhances access control granularity but also enables automated policy evolution, reducing the operational burden on administrators while improving the accuracy and adaptability of enforcement. Nevertheless, several challenges remain. From a deployment standpoint, integrating QKD hardware such as photon sources, detectors, and timing synchronization modules into existing substations or remote DER locations may be constrained by physical space, optical network availability, and environmental conditions. While software emulation of QKD has proven sufficient for the purposes of this evaluation, real-world deployment will necessitate careful cost–benefit analysis, particularly in regions where grid modernization is still nascent.

Scalability is another concern. Although the semantic reasoning engine performed well within our experimental parameters (e.g., up to 25 rules and 1200 ontology individuals), performance degradation is expected in large-scale deployments with thousands of concurrent DER nodes. Optimizations such as distributed triple stores, rule indexing, and caching strategies will be essential to ensure real-time response times are preserved under high load. Interoperability with legacy systems also warrants attention. While the architecture exposes APIs using semantic annotations and supports standard protocols like HTTPS and MQTT, integration with older SCADA systems or field devices using Modbus, DNP3, or proprietary control buses may require protocol translation layers. Ensuring that security guarantees extend end-to-end without creating trust gaps between modern and legacy components will be key to successful deployment.

Finally, from a governance perspective, the dynamic and cross-domain nature of semantic policy enforcement raises questions about inter-operator trust, ontology harmonization, and regulatory compliance. Establishing shared vocabularies, certifying ontological rules, and developing transparent reasoning audit trails will be necessary to gain industry and regulator trust. Despite these challenges, the evidence presented in this paper strongly supports the viability and value of combining QKD and semantic web engineering as a foundational security framework for future smart grids. The demonstrated reductions in latency, improved attack resilience, and operator-friendly interfaces suggest that such architectures can achieve both security at the cryptographic level and usability at the human–machine interface, which is a rare combination in critical infrastructure protection.

5 Conclusion

This paper introduced a novel security architecture for distributed energy resource (DER) systems that unifies quantum key distribution (QKD) with semantic web engineering to deliver end-to-end confidentiality, dynamic access control, and operational usability. Through rigorous simulation and testing, the system was shown to outperform conventional PKI-based frameworks across key dimensions, including session setup latency, key resilience, policy adaptability, and user experience. The architecture advances two fundamental ideas: first, that quantum communication technologies, particularly QKD protocols such as BB84, can be practically applied to secure energy infrastructure communications; and second, that semantic web reasoning provides a scalable, machine-interpretable framework for dynamic policy management in federated smart grid environments. Together, these layers create a cryptographically robust and context-aware system that supports secure, real-time decision-making across organizational boundaries.

Experimental results confirmed the architecture's capacity to maintain low QBER and stable key generation over long-distance optical channels, achieve fast and adaptive session provisioning, and successfully defend against simulated attacks including key compromise, spoofed roles, and cross-domain policy violations. Semantic policy enforcement was shown to enable granular, real-time revocation and adaptive authorization, capabilities rarely available in static, certificate-based systems. From a usability perspective, the integration of a semantic web dashboard dramatically improved operator efficiency and reduced onboarding complexity, with strong SUS scores validating the interface design. The modular RESTful interfaces further demonstrated the architecture's potential to interoperate with broader energy management ecosystems, including SCADA and cloud-based control platforms. While promising, this work also revealed challenges that will shape future development. Real-world deployment of QKD hardware remains a logistical and economic hurdle, particularly in rural or infrastructure-constrained regions. Future work will explore hybrid models that combine QKD at high-priority nodes with post-quantum cryptographic algorithms at the edge. On the semantic side, scalability enhancements including distributed reasoning, ontology federation, and machine learning-assisted policy optimization will be critical to supporting thousands of devices and evolving operational rules in real time.

Future research will also focus on developing formal verification techniques for semantic policies, automating ontology alignment across domains, and extending the reasoning engine to incorporate trust scores, historical behavior patterns, and AI-assisted anomaly detection. In parallel, we envision deploying this architecture in a hardware-in-the-loop (HIL) testbed environment to validate timing, reliability, and cybersecurity performance under realistic network and grid loads.

In conclusion, the proposed QKD + semantic web security architecture offers a compelling foundation for the next generation of secure, interoperable, and intelligent smart grid systems. By bridging quantum cryptography with dynamic semantic reasoning, the system provides a resilient and adaptable framework for protecting critical energy infrastructure in the era of digital transformation and quantum-enabled threats. Future efforts will also explore aligning this architecture with emerging standards from NIST and IEEE, promoting broader industry adoption

References

[1] Alshowkan, M., et al. (2022). Authentication of smart grid communications using quantum key distribution. *Scientific Reports*, 12, 12213.

[2] Lu, Y., et al. (2024). Cybersecurity of distributed energy resource systems in the smart grid. *Applied Energy*, 350, 120000.

[3] Zhou, Y., et al. (2022). Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid. *U.S. DOE Report*.

[4] Wang, Y., et al. (2021). A review of quantum key distribution protocols in the perspective of smart grid communication security. *Future Internet*, 13(2), 28.

[5] Sectrio (2022). Securing Distributed Energy Resources on Power Grids. *Sectrio Blog*.

[6] Mitchell, S., et al. (2023). Design of Distributed Energy Resource Cybersecurity Certification Programs. *Sandia National Labs Report*.

[7] Evans, P. G., et al. (2025). Quantum Key Distribution Applicability to Smart Grid Cybersecurity Systems. *Oak Ridge National Laboratory*.

[8] Prateek, A., et al. (2025). Exploring QKD protocols for secure smart grid communications. *Journal of Reliable and Trustworthy Computing Systems*, 13(2), 45–60.

[9] NIST (2023). Securing Distributed Energy Resources: An Example of IIoT Cybersecurity. *NIST SP 1800-32*.

[10] NHSJS Editorial Board (2025). Quantum Cryptography: A Review of the Literature. *National High School Journal of Science*.
[11] Li, X., et al. (2021). Implementation of BB84 in Smart Substation Communication. *Energies*, 14(13), 3982.
[12] Wang, Q., et al. (2023). QKD Integration in Field Grid Networks. *IET Smart Grid*, 6(1), 56–66.
[13] Zhang, H., et al. (2022). Microgrid Testbed for QKD Simulation. *Sensors*, 22(14), 5081.
[14] Perri, C., et al. (2021). Energy Semantic Data Management and Utilization in Smart Grid. *Proc. Intl. Conf. Smart Energy Systems*.
[15] Pritoni, M., et al. (2021). Metadata schemas and ontologies for building energy applications. *Energies*, 14(7), 2024.
[16] Barnett, J. (2011). A Semantic Model for Cyber Security. *GridWise Architecture Council*.
[17] Crapo, A. (2011). The Smart Grid as a Semantically Enabled Internet of Things. *GridWise Architecture Council*.
[18] Offis E.V. (2013). Towards a standard-compliant Smart Grid using Semantic Web Technologies. *OFFIS Technical Report*.
[19] Zhou, F., et al. (2022). Semantics-Enhanced Grid State Monitoring. *IEEE Access*, 10, 88134–88148.
[20] Almeida, J., et al. (2023). Semantic Models for DER Communication. *MDPI Sensors*, 23(4), 1772.
[21] National Renewable Energy Laboratory (NREL) (2025). Cybersecurity Standards for DER. *NREL White Paper*.
[22] Sadeghi, A. R., et al. (2020). Security and Privacy in Smart Grids. *IEEE Communications Surveys & Tutorials*, 22(1), 195–238.
[23] Zhang, Y., et al. (2022). Integration Challenges of QKD in IoT. *IEEE Internet of Things Journal*, 9(3), 1923–1935.
[24] Ren, L., et al. (2021). Secure PKI alternatives for IoT Grid Applications. *Future Generation Computer Systems*, 118, 168–179.
[25] Nguyen, T., et al. (2023). Quantum-resilient cryptography for embedded systems. *IEEE Trans. Industrial Informatics*, 19(2), 1755–1766.
[26] Li, M., et al. (2021). Secure Cross-Domain Key Management in Cloud-based DER. *IEEE Trans. Smart Grid*, 12(1), 411–423.
[27] Yoon, S., et al. (2020). A Survey on Federated Identity for Smart Grids. *Journal of Grid Computing*, 18(1), 1–17.
[28] Gómez, J., et al. (2022). Coordinated DER Control with Ontology-Based Reasoning. *IEEE Access*, 10, 112223–112236.

Biographies

Yiming Zhang holds a bachelor's degree. He currently works in the Metering Data Management Department of the Metering Center (Electric Power Load Control Technology Center) at Yunnan Power Grid Co., Ltd., as an engineer. His main research focuses on power grid digitalization, automated energy metering, and cybersecurity for power monitoring systems.

Ziyang Yang holds a bachelor's degree. He is currently employed in the Metering Data Management Department of the Metering Center (Electric Power Load Control Technology Center) at Yunnan Power Grid Co., Ltd., with the title of engineer. His research areas include energy metering, automated metering, and digital power grids.

Xinglong Liu holds a bachelor's degree. He currently serves as a senior engineer in the Metering Data Management Department of the Metering Center (Electric Power Load Control Technology Center) at Yunnan Power Grid Co., Ltd. His research focuses on energy metering, automated metering, and digital power grid technologies.