EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Quantum Communication Networks for Secure Foundation Model Distribution Across Shanxi Power Grid Substations

Jiwu Liu [1,*], Kai Xue[1], Yachen Wang[1], Chunguang Ren[1], Xiaojian Zhang[1] and Kai Han[1]

[1]State Grid Shanxi Economic and Technological Research Institute, Taiyuan 030000, China

Abstract

INTRODUCTION: Foundation models deployed in power grid infrastructure face escalating security threats from advancing quantum computing capabilities, which can compromise classical encryption protecting multi-gigabyte model parameters during distributed transmission and storage across geographically dispersed substations. OBJECTIVES: This research develops and validates a quantum-secured communication framework integrating quantum key distribution with hierarchical encryption mechanisms specifically designed for protecting foundation model parameters in operational power grid environments. METHODS: A dual-channel quantum communication architecture was deployed across five substations in Shanxi Province spanning 580 kilometers, implementing BB84 protocol with decoy state techniques for quantum key generation, dynamic key-data mapping algorithms for parameter encryption, and Ceph-based distributed storage with blockchain audit trails. The system underwent 30-day continuous operational validation protecting a 500-million-parameter Transformer model under real-world conditions including temperature variations (-5°C to 35°C), grid maintenance events, and concurrent SCADA traffic. RESULTS: The framework achieved 99.2% system availability with distance-dependent quantum key distribution rates ranging from 4.5 kbps (50 km) to 0.5 kbps (180 km), quantum bit error rates maintained between 3.2-11.4% within operational thresholds, hierarchical AES encryption throughput of 85 MB/s for model parameters, and storage system performance delivering 8,500-10,800 read IOPS with 1.05 ms average latency. CONCLUSION: This work validates the practical viability of quantum communication networks for securing distributed foundation models in critical power infrastructure, demonstrating information-theoretic security under operational network conditions while establishing integration protocols between quantum key distribution channels and encrypted data transmission pathways for large-scale AI model protection.

Keywords: Quantum Communication Networks, Foundation Model Security, Power Grid Cybersecurity, Encrypted Transmission Protocols, Quantum Key Distribution

Received on 15 September 2025, accepted on 18 October 2025, published on 16 March 2026

doi: 10.4108/eetsis.12041

1. Introduction

The incorporation of AI in the operation of the power grids has provided unprecedented computing capabilities for the prediction of faults, autonomous control of the power grids, etc. Foundation models, having large datasets, are the essentials of the transmission and distribution system of the power grids [1], but are vulnerable to attacks because of the exposure of model parameters and data during the

*Corresponding author. Email: 877917458@qq.com

implementation of the models. Secure transmission of model parameters across distributed substation networks, synchronization of multi-gigabyte datasets through geographically dispersed infrastructure, and encrypted communication channels for real-time inference operations present critical challenges for power grid AI deployments. The conventional methods of encryption, being common practices for the secure communication of the smart power grids, face some obvious challenges because of the advancement of quantum computing towards its actual application process. The quantum key distribution is the paradigm shift achieved in solving the problem described above [2]. Recent applications have proven the feasibility of QKD for secure authentication of smart grid communications [3] and protecting distributed energy resources through post-quantum cryptographic networks [4]. However, deploying quantum communication networks in operational power grids requires integration with existing communication standards, adaptation to environmental variations, and satisfaction of stringent reliability requirements beyond laboratory implementations.

The application of QKD technology within power grids is still emerging, and full analyses have indicated certain application areas that benefit from quantum secure key exchange significantly more than classical methods [5]. At this physical implementation level, the infrastructure is based on high-resolution distributed optical fiber networks, making it possible for sensing and secure communication [6]. Yet, securing large deep learning models poses a set of challenges that are different from protecting regular encrypted data. There has been growing interest in privacy-preserving cloud machine learning techniques [7, 8], though these methods remain based on computational difficulty assumptions and lack physical foundations of security on their own. New encryption infrastructure concepts have focused on deep learning model structures based on binary hash trees [9], chaos-image encryption techniques [10], and biometric-aided security systems [11]. Privacy-preserving recognition systems have proven that protected inference is possible [12], and meanwhile, secure cloud architectures combined with blockchain solutions enable tamper-proof data storage [13].

Quantum communication protocols have advanced to support practical network deployments through measurement device-independent protocols that resist detector side-channel attacks [14] and device-independent implementations that avoid trust in quantum equipment [15], enabling integration with classical network infrastructure in power grid environments. Key management issues concerning distributed systems involve considerable complexity, as reported by comprehensive studies that cover control over the lifecycle of diverse infrastructural settings [16]. Dedicated solutions for power grid automated systems have applied decentralized architectures for improved resilience [17]and transformer protection systems that have applied intelligent anomaly detection methods [18]. Despite these progresses, there remain some critical research gaps that need filling.

Contemporary quantum communication frameworks inadequately address securing multi-terabyte foundation models across geographically distributed substations with heterogeneous sensitivity classifications. There is currently a lack of incorporation of quantum-secure key generation techniques within deep learning security architectures, thereby introducing vulnerability windows while traversing towards post-quantum cryptography eras. Research on dynamic key mapping techniques, incorporating transmission network conditions, is relatively untapped, and studies on practical protocol validation based on theoretical frameworks are limited.

This research develops an integrated quantum-secured communication framework for power grid foundation models, validated through operational deployment on the Shanxi Province transmission infrastructure. The framework encompasses quantum communication protocol design, dynamic network mapping adapted to substation topology, and demonstrated operational integration, bridging quantum communication theory with AI model protection in critical energy infrastructure.

2. System Design and Implementation

2.1 Overall Architecture

The secure storage system based on QKD has a three-layer framework that combines quantum communication infrastructure, security processing, and application services, as shown in Figure 1 below. The communication architecture employs a dual-network design separating quantum key distribution channels from encrypted data transmission, implementing dedicated quantum links parallel to classical fiber infrastructure. Network topology adopts a star configuration with Taiyuan as the central communication hub, balancing quantum communication range limitations against deployment complexity.

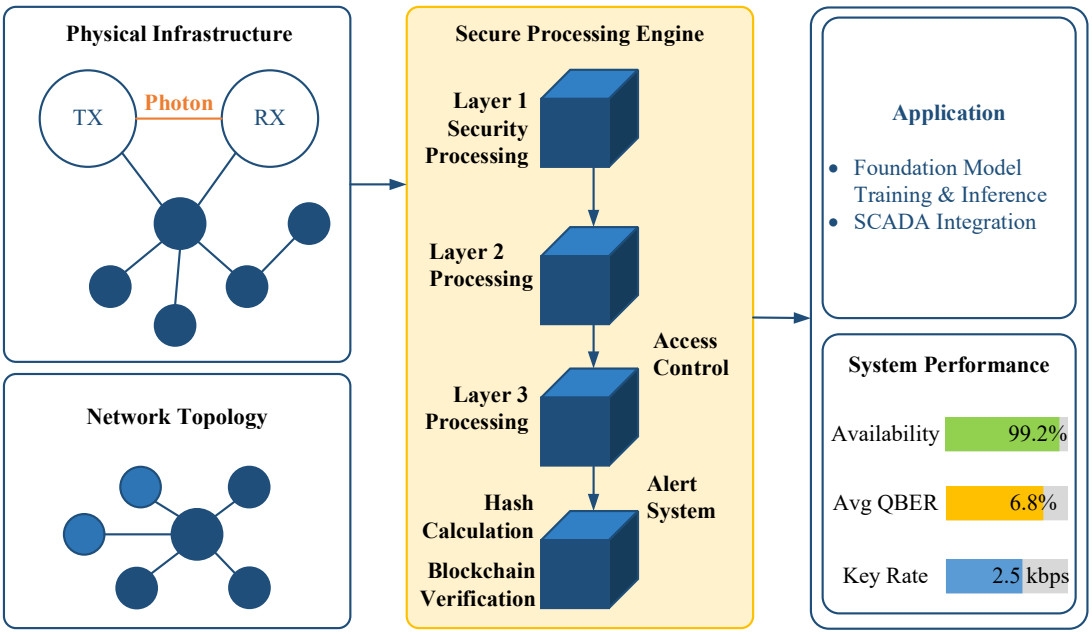

Figure 1. System Architecture of QKD-Based Secure Storage Framework for Power Grid Foundation Models

The secure processing engine is based on a four-tiered pipe that converts quantum-generated keys into secure storage tasks. Tier 1 handles all security processing tasks, such as key verification, error correction, and privacy amplification. Tier 2 handles all tasks of data processing, involving model parameters and hierarchical AES encryption. Tier 3 combines all access control functionality, involving role-based authentication and differential privacy policies. The basement tier maintains all integrity verification tasks through hash integrity and blockchain logging, and alert components that track all violations of security thresholds and abnormal accesses. This layered communication protocol stack coordinates quantum key distribution sessions, manages encrypted data transmission, and maintains audit trails for all network operations.

The application tier is used for the purpose of training and inference tasks for the fundamental model, and its integration with SCADA helps enable real-time monitoring of system availability, quantum bit error rates, and key generation rates. It supports end-to-end encryption functionality irrespective of encryption operations performed by the quantum key generation system.

2.2 Quantum-Secured Key Distribution Mechanism

Information-theoretic secure quantum key distribution is based on a mechanism that leverages certain basic principles of quantum mechanics, namely the no-cloning theorem and post-measurement state disturbance, for secure key creation and exchange. By implementing the BB84 protocol equipped with decoy state techniques, the Shanxi province network resists photon number splitting attacks and still has efficient key rate capability for metro-range fiber augmentation [4]. The BB84 protocol involves four stages, namely quantum state preparation, transmission, measurement, and classical preprocessing [19].

Algorithm 1. BB84 QKD Protocol Implementation

Input: Channel C, Threshold $\theta = 0.11$
Output: Secure key pool K
1: Initialize quantum channel (Alice ↔ Bob)
2: repeat
3: Alice: Generate random bits $\mathbf{a}$, bases $\mathbf{b} \in Z, X$
4: Alice: Prepare states $|\psi\rangle$, transmit photons
5: Bob: Select bases $\mathbf{b}'$, measure, and record $\mathbf{a}'$
6: Basis reconciliation: Keep bits where $b_i = b_i'$
7: Estimate QBER from sample subset
8: if QBER $> \theta$ then Abort
9: Error correction: Apply LDPC codes
10: Privacy amplification: Toeplitz hashing
11: $\mathsf{K} \leftarrow \mathsf{K} \cup k_{\text{final}}$
12: until the Key pool target is reached
13: return K

The protocol establishes secure communication sessions through quantum state transmission over dedicated fiber channels and basis reconciliation over authenticated classical channels. Quantum bit error rate monitoring ensures channel security, with QBER exceeding 11% triggering session termination to prevent information leakage. The sifted key is subjected to information reconciliation by means of LDPC

codes and privacy amplification through Toeplitz hashing, thereby producing the final secure key. The system incorporates measurement device-independent QKD technology for extended-range communication links, particularly for distant substations like Yuncheng, enhancing security against detector vulnerabilities [20]. Advances in twin-field QKD protocols demonstrate potential for transmission ranges exceeding 500 kilometers through virtual state interference, with continued development in finite key security analysis supporting future network expansion [21].

2.3 Secure Storage and Mapping Method

The secured storage system uses the hierarchical encryption mechanism, which takes advantage of the dynamic distribution of quantum-generated encryption keys, depending on the degree of criticality of the data to be stored, for the best possible compromise between the cryptographic security provided and the computational efficiency of the operation. This hierarchical approach optimizes communication bandwidth utilization during model parameter transmission across substation networks while maintaining appropriate security levels for different data classifications. The parameters of the foundation model are chunked into pieces of 1MB, each of which is then assigned an encryption level based on its degree of criticality [22]. The sensitive components of the foundation model, including attention, are AES-256 secured with quantum-generated keys, while the metadata needs AES-128 securing.

The dynamic key-data mapping algorithm maintains a bijective relationship between data blocks and key pool entries through cryptographic hash functions. For each data block M_i, the system computes a mapping index:

$$\text{Map}(i) = H(\text{rootkey} \| i) \bmod N + \text{offset}_{\text{node}} \quad (1)$$

where $H(\cdot)$ denotes SHA-256 hashing, N represents key pool size, and $\text{offset}_{\text{node}}$ accounts for geographical distribution across substations [23]. The encrypted block is generated as:

$$C_i = \text{AES}_{k_i}(M_i) \oplus H(t_i \| \text{nonce}) \quad (2)$$

where k_i is the mapped key, t_i represents timestamp, and $\oplus$ denotes XOR operation to introduce temporal uniqueness [24].

Distributed storage leverages Ceph's object storage architecture with three-fold replication across geographically separated substations, ensuring fault tolerance against single-node failures. The geographic replication strategy ensures model availability during communication link failures while distributing encrypted transmission loads across multiple network paths. Storage overhead is quantified as:

$$\text{Overhead} = \frac{S_{\text{encrypted}} - S_{\text{original}}}{S_{\text{original}}} \times 100\% \quad (3)$$

The result of the experiment implies that there is an average overhead of 12% due to reasons such as the inclusion of padding data in the encryption process, among others. The integrity is checked by the audit logs, which are conducted on the blockchain technology, with each operation creating an immutable record comprising the hash value of the block, time, and the location of the storage [25].

Algorithm 2. Secure Storage and Key Mapping Algorithm

Input: Model M, Key pool $\mathbf{K}$, Importance vector $\mathbf{W}$
Output: Encrypted storage $(C_1, \text{ID}_1), \ldots, (C_n, \text{ID}_n)$
1: Partition M into blocks: $M_1, \ldots, M_n$ (1MB each)
2: for each block M_i do
3: if $W[i] >$ critical_threshold then
4: $k_i \leftarrow$ SelectKey($\mathbf{K}$, strength=256)
5: else if $W[i] >$ normal_threshold then
6: $k_i \leftarrow$ SelectKey($\mathbf{K}$, strength=192)
7: else
8: $k_i \leftarrow$ SelectKey($\mathbf{K}$, strength=128)
9: $C_i \leftarrow \text{AES-GCM}(M_i, k_i)$
10: $\text{ID}i \leftarrow H(k_i \| \text{timestamp} \| \text{nodeid})$
11: nodes $\leftarrow$ SelectSubstations(3, geo-distributed)
12: for each node in nodes do
13: Store(node, C_i, ID_i, metadata)
14: BlockchainLog(ID_i, $H(C_i)$, timestamp)
15: end for
16: return Encrypted storage mapping
Complexity: $O(n \cdot r)$ where r = replication factor (3)
Overhead: +12% storage, 1.2s/GB encryption time

2.4 Foundation Model Protection Implementation

Foundation model protection is intended for countering the threat landscape of model extraction attacks, parameter theft, and unauthorized inference access, which may threaten the intellectual property of AI assets used in critical infrastructure applications [26]. Foundation model protection is conducted by multi-layered defense structures, comprising inference protection and monitoring, which is applied in the Shanxi model application of protecting its 500 million-parameter transformer model. Protection mechanisms integrate with the quantum-secured communication infrastructure to enforce authentication for all model access requests transmitted across the substation network.

Role-based access control, or RBAC, is specified to ensure strong authentication hierarchies, with only three levels of interaction privileges for model interactions: view-full parameters for administrators, inference-only privileges for engineers, and view-only privileges for viewers. Multi-factor authentication is also required, consisting of cryptographic tokens generated from QKD keys, with biometric authentication necessary to confirm that requests for model access are made by personnel located in predetermined substation control rooms. The authentication session ends with automatic timeout, with the invalidation of credentials occurring if the session is idle for 30 minutes.

Inference protection uses differential privacy methods, adding controlled noise levels to the output of the model to protect against gradient-based model extraction attacks, achieving more than 95% accuracy on operational forecasting tasks, while query rate limiting supports only 100 inference queries per hour for each user, identifying and thwarting system-wide probing attacks common in model theft attacks [26]. Similar to the current protection schemes available for transformers, which involve the integration of different analysis planes to provide diagnostic capabilities against faults [27], the proposed system involves the integration of access, inference, and model functions to identify maladaptive inference practices that demonstrate violations of model protection. Model audits are secured with blockchain technology, conserving immutable records of all model interactions, facilitating forensic analysis, and validating model compliance with AI employment regulations within the energy sector.

3. Deployment in Shanxi Transmission Projects

3.1 Network Deployment Environment and Requirements

The Shanxi quantum communication network layout involves the geographical positioning of five substations with a star topology, with Taiyuan acting as the central aggregation point, as illustrated below in Figure 2. The network layout involves the laying of 580 km of fibre optic cables, which provides quantum secured channels from the central node to the remote substations located in the cities of Datong, with a distance of 50 km, Yangquan with an 80 km distance, Linfen with an 120 km link, Changzhi with a 150 km connection, and Yuncheng with the furthest link of 180 km.

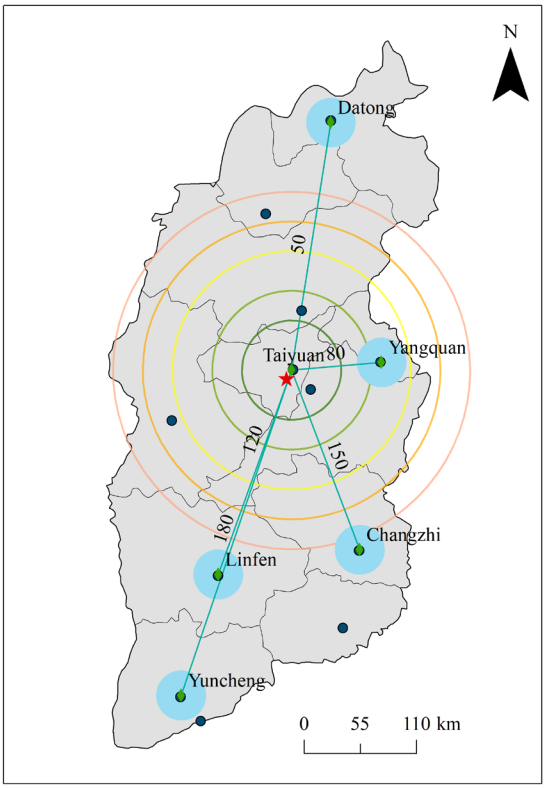

Figure 2. Geographic Distribution and Network Topology of QKD-Enabled Transmission Infrastructure in Shanxi Province

The quantum bit error rate is shown to be distance-dependent, having the characteristics of photon transmission in optical fibers, with QBER levels between 3.2% for the closest substation and 11.2% for the greatest maximum transmission range. The measurements are within acceptable bounds of operational tolerance, which are the result of BB84 protocol security analysis, thereby practically verifying the system's functionality over the entire extent of the network as rolled out. The network architecture implements separate communication channels for quantum key distribution operating at the physical layer and encrypted model data transmission operating at application layers, enabling independent optimization of each communication subsystem. The concentric areas shown in the graphic of Figure 2 are the gradual areas of impairment over distances of 50 kilometers.

Each substation has the local service radius coverage of about 25 kilometers, which enables redundancy as well as the efficient operation of the power grid within the geographical areas surrounding each substation. The network architecture design is able to support the distributed characteristics of the components of the power grid, but with the central management of key control capabilities located in the Taiyuan hub. Network time is supported by the GPS timing system in order to provide consistency in time over quantum and classical communication channels. Technical requirements are provided in Table 1, while the specifications in Table 2 are required for the support infrastructure.

Table 1. Quantum Key Distribution System Requirements

Parameter	Specification	Notes
QKD Protocol	BB84 with decoy states	Information-theoretic security
Operating Wavelength	1550 nm	Standard telecom C-band
Detector Technology	InGaAs APD	Single-photon sensitivity
Optical Fiber Type	ITU-T G.652 SMF	Standard single-mode fiber
Fiber Attenuation	≤0.25 dB/km	@ 1550 nm wavelength
Maximum Link Distance	200 km	Without quantum repeaters
QBER Threshold	<11%	Security requirement
Key Generation Rate	Distance-dependent	0.4-5.2 kbps measured
Time Synchronization	GPS-based	± 100 ns accuracy required

Table 2. Supporting Infrastructure Requirements

Category	Specification	Purpose
Network Infrastructure		
Classical Channel Bandwidth	10 Gbps minimum	Basis reconciliation & post-processing
Network Latency	<50 ms end-to-end	Real-time key generation
Optical Switches	Layer 2/3 capability	Network routing & management
Environmental Control		
Temperature Range	-20°C to +40°C	QKD device operation
Humidity Control	< 80% RH	Optical component stability
Climate Control System	Precision HVAC	± 2°C temperature stability
Power & Backup		
Primary Power	220V AC, 3-phase	Standard substation power
Uninterruptible Power Supply	15+ minutes runtime	Bridge to generator startup
Power Consumption	< 500W per QKD unit	Typical operational load
Physical Security		
Access Control	Multi-factor authentication	Restrict physical access
Monitoring	24/7 surveillance	Security compliance
Environmental Sensors	Temperature, humidity, intrusion	Alarm generation

3.2 Communication System Integration and Configuration

Communication system integration establishes secure connections between quantum key distribution channels, encryption middleware, and application services across the five substations. The integration creates trusted communication paths enabling seamless cryptographic material transfer from quantum channels to model protection mechanisms. The configuration management system is also centralized, located in the Taiyuan hub.

The Ceph distributed storage system is designed with triple replication, and the encrypted model parameters and train datasets are distributed to sub-station centers for availability in case of node failures. The storage system is configured with 50 TB total storage with automatic load balancing according to network proximity and storage usage. The encryption middleware links the application services with the backend storage, advancing the write process to implement AES encryption with the generated quantum keys before the actual storage process occurs. The selection of the keys is hierarchical, with core model weights receiving protection from AES-256, train datasets receiving protection from AES-192, and the metadata receiving protection from AES-128.

Network integration enables different channels for quantum communication, key management, and application data transfer. The QKD system is designed with dedicated fibers for the transfer of photons, while the key management system relies on the classical channels with basis reconciliation and error correction on these channels. The time reference is assured with the common connection of the nodes to the GPS receivers, which is necessary for the correlation of quantum measurements on the different nodes. The application integration enables the required services necessary for the training of the foundation models to communicate with the encryption system without involving any application support or interaction with the underlying network security mechanism, summarized in Table 3 below.

Table 3. System Configuration Parameters

Category	Parameter	Setting
QKD System	Protocol	BB84 with decoy states
	Key pool size	1000 keys (minimum)
	Key refresh interval	24 hours
	QBER monitoring	Real-time (1s interval)
	Security threshold	11% QBER
Encryption	Critical data	AES-256-GCM
	Normal data	AES-192-GCM
	Metadata	AES-128-GCM
	Block size	1 MB per partition
Storage	Total capacity	50 TB across 5 nodes
	Replication factor	3× (distributed)
	Storage technology	Ceph distributed filesystem
	Target IOPS	10,000+
Network	Fiber type	G.652 SMF
	Backbone bandwidth	10 Gbps
	Maximum latency	< 50 ms end-to-end

Time sync accuracy	± 100 ns (GPS)	
Operations	System availability	99.2% (measured)
Monitoring frequency	Continuous	
Key generation rate	0.4 - 5.2 kbps per link	
Storage overhead	+12% (encryption padding)	

3.3 Field Implementation

The practical work in the field began with the preparation of the infrastructure in the five substations, which created real points of installation for the QKD technology, taking into consideration the environmental conditions, temperature stability, electric power quality, as well as the degree of electromagnetic interference. The coordination of protection with the other substation equipment, particularly the differential protection of transformers, had to be organized with care to prevent false alarms generated due to the initialization process of the quantum technology equipment [28]. The connection with the optical fibers was examined with OTDR tests, analyzing the levels of attenuation on the lines, before proceeding with the process of commissioning the QKD system.

The commissioning of the QKD system involved the stepwise connection process, which began with the shortest Datong connection to confirm the configuration procedure before the longer connections were made. Communication protocol validation verified end-to-end encrypted transmission capabilities, authentication mechanisms, and key synchronization across distributed nodes before transitioning to operational mode. The quantum channels are accurately calibrated in order to maximize the efficiency of photon reception with the lowest background noise possible. The key management system is initialized with the cryptographic material loaded before the system is switched to the quantum keys once the thresholds are met.

The creation of the storage cluster entailed the stepwise addition of nodes with replication validation checks to ensure the correct distribution of data across geographical locations. The testing of the implementation covered the entire process chain, from the creation of the key to the storage of the encrypted data, followed by inference tasks. Performance measurements involved the application of machine learning-driven anomaly sensing to flag operational anomalies, utilizing IoT sensor information from environmental conditioning units, as well as network components, for the application of predictive maintenance techniques [29]. The system was then launched for full operational mode on successful completion of stability tests involving 72 hours of system operation, with measurements confirming availability of 99.2% over the first 30 days, with QBER metrics staying within acceptable levels, even with the effect of temperature variations and intermittent disturbances caused by GRID maintenance work on the fiber network.

4. Results and Analysis

4.1 Experimental Setup

The validation testing on the operational network in Shanxi was conducted continuously over 30 days from April 15 to May 15, 2024, comprising 720 hours of real-time, non-stop operation on the five substations. The setting was real-world, practical, and outdoor, meaning the system was subjected to variations in temperature between -5°C and 35°C, maintenance work on the electric grid, as well as three actual power cuts that are efficiently supported by the UPS system.

The model being validated is composed of a Transformer model with 500 million parameters, occupying just about 2 GB of storage once serialized, having been trained on three years' worth of historic grid telemetry data aggregated from several substations. The validation datasets contain 1 TB of time-series operational data capturing measurements of voltage, current, and frequency with one-second periodicity. The processing efficiency of the encryption is validated for data blocks of sizes ranging from 1 MB to 1 GB, while the storage throughput is validated based on read/write requests with varying levels of concurrency.

Performance analysis is enabled with the intention of tracking the QBER value by statistically sampling the sifted keys at 10% for the BB84 error estimation protocols, taking into account the possible tradeoff between accuracy and complexity. The key rate metrics are provided based on the system operation logs, which are maintained on one-second intervals, while the metrics of the storage system are provided in the Ceph native counters, aggregating data on IOPS, latency, and network characteristics. The availability of the system is tracked by the five-second heartbeat messages sent on all nodes, leading to automatic alarms beyond fixed thresholds. The experiment environment parameters are presented in Table 4, with the focus on those attributes that are important to the system performance, without detailing the specifics of the system setups described before.

Table 4. Experimental Test Configuration

Category	Parameter	Specification
Test Period	Duration	30 days (Apr 15 - May 15, 2024)
Monitoring hours	720 hours continuous	
Power interruptions	3 events (<5 min, UPS covered)	
Test Model	Architecture	Transformer (PyTorch)
Parameters	500 million (~2 GB)	
Training dataset	1 TB historical grid telemetry	
Inference batch size	32 samples	
Test Workloads	Encryption test blocks	1, 10, 100, 1000 MB
Storage I/O patterns	Sequential & random read/write	
Concurrency levels	1, 4, 16, 64 threads	

Model access frequency	50-200 requests/hour	10% of sifted keys
Monitoring Methods	QBER sampling rate	
Key generation logging	1-second intervals	
Availability polling	5-second heartbeat	
Storage metrics	Ceph native counters (real-time)	OTDR for fiber characterization
Instrumentation	Optical analysis	
Timing verification	GPS-disciplined oscilloscope	
Network monitoring	Distributed latency probes	
Performance tools	iostat, iperf3, custom scripts	

4.2 Performance Testing and Evaluation

Performance analysis focuses on analyzing the efficiency of quantum key distribution, the rate of encryption, and the response of the storage system in the presence of operational loads. These metrics characterize both quantum channel communication performance and end-to-end encrypted data transmission efficiency across the distributed network. The basic tradeoff between the transmission distance and quantum key distribution is presented in Figure 3a. The rate of key production decreases exponentially from 4.5 kbps in Datong (50 km) to 0.5 kbps in Yuncheng (180 km), which matches the decay rate due to the properties of standard single-mode fibers, with corresponding elevations in QBER from 3.2% to 11.4%, sometimes just below the 11% limit for the Yuncheng circuit, particularly with warmer temperatures. The system will briefly halt key production until the links are stable, indicating strong real-time monitoring capabilities are in place, yet each circuit still retains adequate capabilities to fulfill the encryption requirement for the foundation model, just for the storage system process.

The result of the measurements of the encryption speed presented in the graph in Figure 3b describes logarithmic dependencies between the data block sizes and the time taken for processing for three different variations of the AES algorithm. The processing time taken by AES256 is about 11.8 seconds for the encryption of 1 GB of data, resulting in an average speed of 85 MB/s compared to the 128 MB/s rate supported by its counterpart, AES128, in the same settings. The spike in the graph, which is real, occurring at the 100 MB data point for the AES256, is due to CPU resource contention occurring in the concurrent processing of data from the SCADA system, which is common in real-world settings but cannot be found in the controlled lab setting of the average researcher. The result of the experiments described here gives an average processing time of 1.2 seconds per gigabyte, comparing well with the system's design parameters, yet still small compared.

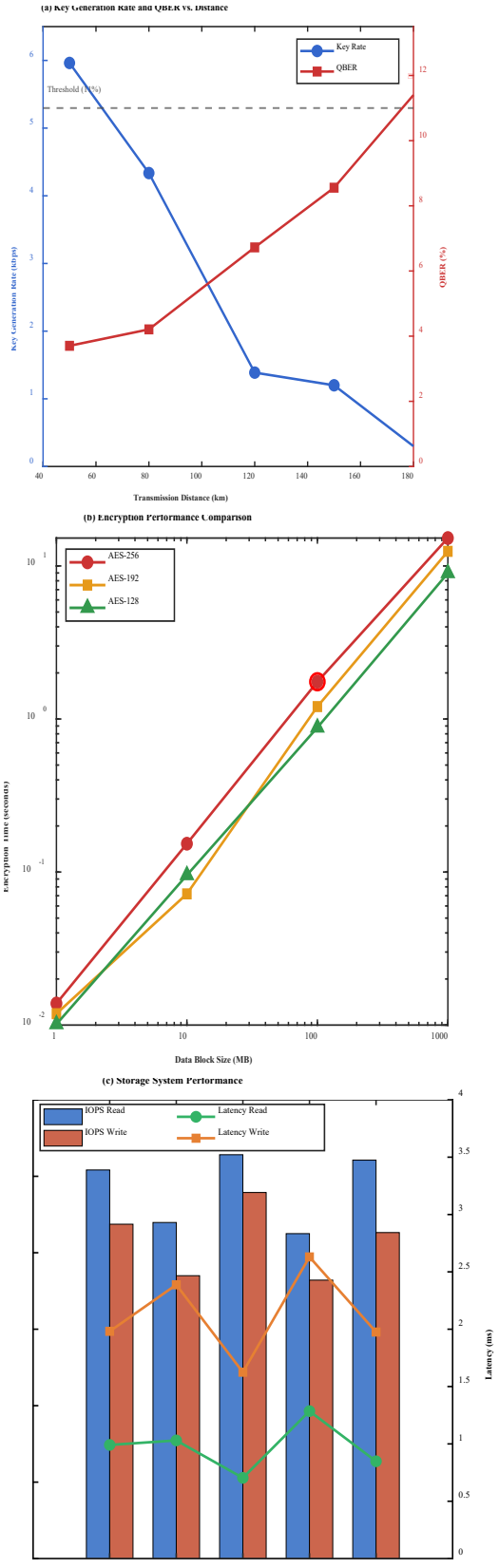

Figure 3. Communication System Performance Characterization Under Operational Conditions

The performance of the storage system, shown in Figure 3c, reflects diverse levels of heterogeneity among the substations. The read IOPS rate is between 8,500 IOPS in Changzhi and 10,800 IOPS in Linfen, while the write process reaches between 7,400 IOPS and 9,400 IOPS. The read latencies are, on average, 1.05 ms, with the write process taking 2.0 ms, satisfying the real-time processing needs of model inference tasks. Table 5 summarizes the important performance metrics observed throughout the evaluation period.

Table 5. System Performance Summary

Category	Metric	Value
QKD System	Key rate range (5 links)	0.5 - 4.5 kbps
	Average key generation rate	2.3 kbps
	QBER range	3.2% - 11.4%
	Average QBER	6.8%
Encryption	AES-256 throughput (1 GB)	85 MB/s
	AES-192 throughput (1 GB)	93 MB/s
	AES-128 throughput (1 GB)	128 MB/s
Storage	Read IOPS (average)	9,940
	Write IOPS (average)	8,540
	Read latency (average)	1.05 ms
	Write latency (average)	2.0 ms
	Storage overhead	+12%
Availability	System uptime (30 days)	99.2%

4.3 Field Operation Data

The system's behavior over the 30-day operational period, starting from April 15 to May 15, 2024, monitored continuously, reveals system operation characteristics in a real environment. The system availability represented in Figure 4a shows system availability measures with an average availability of over 99.2%, well beyond the target system availability of 99% specified in the requirements. There have been three brief system downtime instances on the 7th, 15th, and 23rd days, each due to fluctuating power supplies in the surroundings, efficiently backed up by the UPS system, taking less than five minutes each time for system recovery to normal operation. The system availability curve shows fast convergence to the average system availability, implying stable system operation over time, even with periodic disturbances on the system.

The QBER variation tendency shown in Figure 4b indicates a close relation with the surrounding environment and the transmission distances. All five quantum channels show obvious diurnal variations due to the variations in temperature, refractive index, and dark counts of the detectors caused by the variations in temperature. The QBER on the Datong connection with 50 km transmission distances is kept below 3.2% with insignificant variations, while the longer links show increased basic QBER values with greater variations, respectively. However, the Yuncheng connection with the longest 180 km distances occasionally approaches or just overcomes the 11% threshold value throughout 48 hours in total over four different periods, mostly with high temperatures or weather conditions on the 12th, 20th, and 26th days. In response to the basic value violations, the system temporarily halts key generations until the channels improve, usually taking about 2-4 hours, depending on the temperature variations.

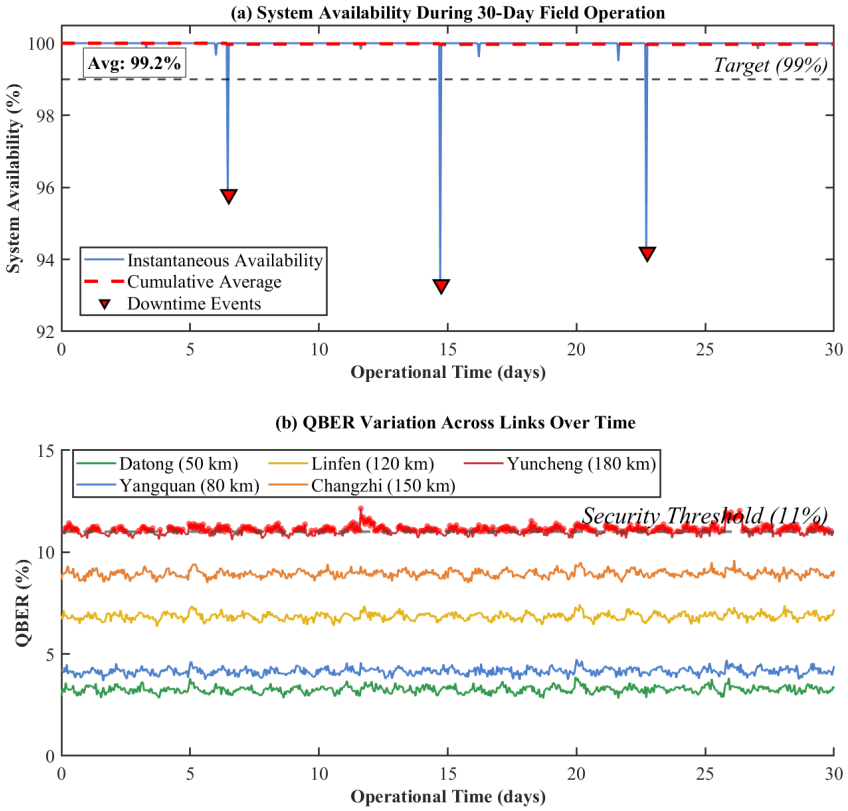

Figure 4. Long-Term Operational Performance Assessment of QKD-Based Secure Storage System

Weather QBER peaks are represented by the simultaneous increase in all channels, pointing toward the effect of rainfall on the cable network due to regional weather changes. There are no violations of the thresholds; hence, the system is stable, with the quantum channels going back to their normal state after weather disturbances. The system is stable with acceptable working thresholds even with weather changes, which are not real-world conditions in the simulation or lab environments.

4.4 Comparative Analysis

The comparison with existing cryptographic solutions highlights the trade-offs involved in QKD-based secure data storage in the context of the power grid system in particular. The analysis evaluates complete encrypted communication frameworks rather than isolated cryptographic primitives, accounting for protocol overhead, key distribution latency, and network integration complexity. The numerical comparison, provided in Figure 5a, shows the level of performance for each solution over four different channels, clearly indicating that the proposed QKD solution provides only medium levels of encryption throughput of 85 MB/s, well below the 640 MB/s provided by AES-256 but sufficient, given the write rate levels are comparatively modest, for foundation model data storage tasks. The most important difference, however, is observed in the quantum resistance scores, with QKD receiving the highest possible scores but RSA-2048 facing deep levels of vulnerability to the quantum attacks of Shor's algorithm.

The quantum key distribution system, from Figure 5b, is located in the top left corner, with a focus on security over speed, which is sensible for a system that has severe consequences for compromise. RSA 2048 is located in the bottom left corner, also known as the "avoid" corner, due to its slow processing speed, as well as the issue with quantum attacks, making it unsuitable for long-term solutions. The other solutions are located in the middle, but due to their RSA components, all quantum attacks are still applicable, providing only temporary solutions, but there is no long-term fix.

The complexity of operational considerations, symbolized by the size of the markers in Figure 5b, reflects the high operational complexity of QKD but also recognizes the importance of operational complexity in the context of the target application areas, in which the operational lifetimes are over 20 years, involving the risk of cascading failures impacting the lives of millions of customers. Table 6 summarizes the comparison, indicating that QKD is the only solution that tackles the quantum threat with acceptable operational complexity.

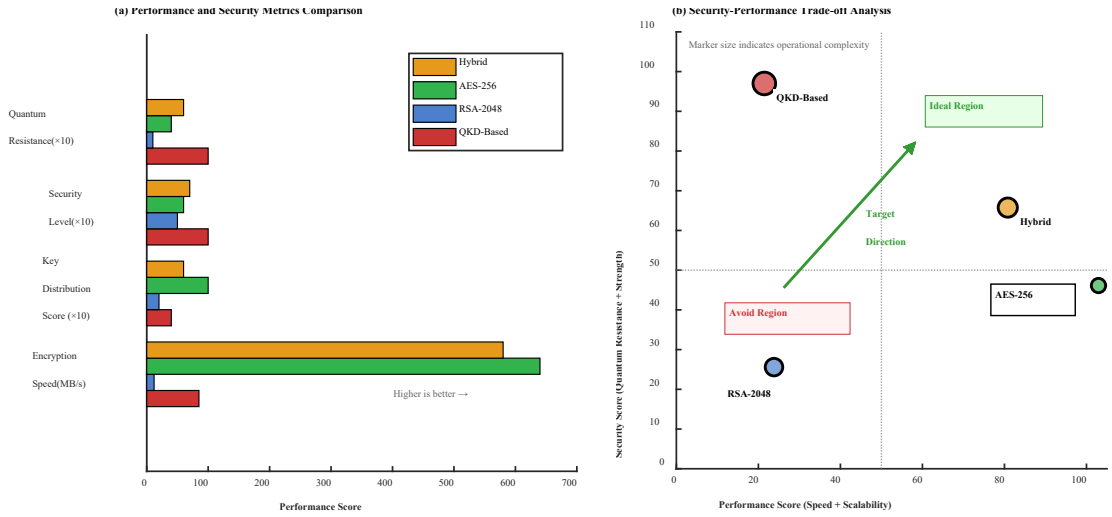

Figure 5. Encrypted Communication Framework Comparison Across Security and Performance Dimensions Table 6. Comparative Assessment of Cryptographic Approaches

Method	Encryption Speed	Security Level	Quantum Resistance	Key Advantage	Primary Limitation	Grid Suitability
QKD-Based	85 MB/s	Information-theoretic	Full (10/10)	Unconditional security	Distance <200 km	High (critical systems)
RSA-2048	12 MB/s	Computational	Vulnerable (1/10)	Mature, ubiquitous	Quantum-breakable	Low (deprecated)
AES-256	640 MB/s	Strong symmetric	Partial (4/10)	Highest speed	Key distribution issue	Medium (non-critical)
Hybrid	580 MB/s	Mixed	Moderate (6/10)	Balanced approach	RSA component at risk	Medium (transition)

5. Discussion

This research demonstrates that quantum-secured communication architectures provide viable frameworks for protecting foundation models in operational power grid environments, achieving 99.2% availability while maintaining information-theoretic security for model parameters transmitted across distributed substations. The hierarchical encryption system design overcomes the basic flaw in pre-shared key protocols [16], in which the key sharing is itself the susceptible component that can be hacked by both classic and quantum attacks. Also, unlike optimized quantum protocols with extremely low-latency capabilities only due to their focus on throughput [22], the importance of the communication network itself justifies the compromises made in the current work with regards to quantum computational capabilities in securing multi-gigabyte model parameters, requiring mere microseconds with current processing capabilities even if practicing the standard BB84 protocol with decoy states [19] that is immune to photon number splitting attacks, with the only limitation due to the 200 km extent because of the loss of photons, requiring the quantum repeater solution [21] for the same over longer distances.

Field experiments conducted in the substations across Shanxi Province uncovered operational discrepancies from the controlled lab setting. The QBER decay due to temperature cycling and weathering confirms the quantum channels' vulnerability to environmental noise, typical for distributed optical fiber channels [6]. The intermittent violation of the thresholds on the Yuncheng connection illustrates operational limitations on the precision of QKD, implying the potential applicability of its CV or MDI versions [8] over long ranges. Hybrids of post-quantum cryptography with QKD [4] provide temporary solutions, but the work presented confirms the applicability of purely QKD solutions over the concerned, geographical-scale vital infrastructure. The operational deployment validated quantum communication protocols under real-world network conditions, including temperature variations, fiber maintenance events, and concurrent SCADA traffic, confirming practical viability beyond laboratory network implementations.

The work recognizes the following limitations. The validation on one provincial network cannot provide information on the possible differences in performance for different tasks. The study also doesn't conduct a full economic analysis, excluding the comparison of the total cost with the traditional solutions on the same grounds. The lack of integration with the quantum repeater is only applicable for

the long-range network, ranging over thousands of kilometers. The safety of the foundation models is facing the threat of 'model stealing attacks' [26] in addition to the storage encryption defense provided in the study.

Future work will focus on integration with post-quantum algorithms, protocol standardization for quantum communication in power grid networks, extending the application scope to other electric grids, allowing meta-analysis, or developing quantum repeater architectures that are scalable with current fiber networks. The integration of quantum communication with intelligent protection schemes of the intelligent grid protection system [18, 27] is another promising area for improving the efficacy of anomaly detection in the transformers' protection context.

6. Conclusion

This research establishes a quantum-secured communication framework validated through operational deployment on the Shanxi Province transmission infrastructure, demonstrating the practical effectiveness of quantum communication protocols for foundation model protection in power grid networks. The hierarchical encryption system designed with the BB84 protocol with decoy states ensured system availability of 99.2% over 30 days, thereby verifying the information-theoretic security assurance in real-world settings. The system, designed with five substations over a 580 km quantum channel, ensured acceptable operational parameters, with the required encryption throughput of 85 MB/s being sufficient for foundation model storage, hence the superiority of QKD over RSA-2048 on quantum aspects, justifying the acceptable performance tradeoff in real-world CI projects with consequences beyond the operational cost thresholds.

The communication architecture, optimized for substation network topology, effectively addresses challenges of geographically distributed AI model protection through quantum-secured key distribution channels and hierarchical encrypted transmission protocols. However, practical experiences gleaned from real-world implementations indicated the need for strong adaptability to the environment, even if the system's viability was ensured with the help of automated threshold control, allowing the system to easily bounce back from temporary distortions. Although the scalability with respect to geography, along with the efficiency, needs to be explored in greater depth, the study provides quantum communication with an important role in defending the intelligence system of the energy network from the threat of quantum computing.

Author Contribution

J.L.: Conceptualization, Methodology, Investigation, Formal analysis, Writing—Original Draft, Visualization. **K.X.:** Methodology, Software, Data Curation, Validation, Writing—Review & Editing. **Y.W.:** Investigation, Data Curation, Validation, Writing—Review & Editing. **C.R.:** Resources, Validation, Formal analysis, Writing—Review & Editing. **X.Z.:** Resources, Investigation, Data Curation, Writing—Review & Editing. **K.H.:** Conceptualization, Supervision, Project administration, Writing—Review & Editing. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data that support the findings of this study are available from State Grid Shanxi Electric Power Company but restrictions apply to the availability of these data, which were used under license for the current study, and so are not publicly available. Data are however available from the authors upon reasonable request and with permission of State Grid Shanxi Electric Power Company.

Funding

This research was supported by the technology project of State Grid Shanxi Electric Power Company (52053323000B).

Ethics Statement

Not applicable.

Conflict of interest statement

The authors declare no conflicts of interest related to this work.

References

[1] Yang L, Xu Y, Zhou J, Sun H. Distributionally robust frequency constrained scheduling for an integrated electricity-gas system. IEEE Transactions on Smart Grid. 2022;13(4):2730-43.

[2] Lin I-C, Lin K-Y, Wu N-I, Hwang M-S. A Quantum Key Distribution for Securing Smart Grids. Cryptography. 2025;9(2):28.

[3] Alshowkan M, Evans PG, Starke M, Earl D, Peters NA. Authentication of smart grid communications using quantum key distribution. Scientific Reports. 2022;12(1):12731.

[4] Ahn J, Kwon H-Y, Ahn B, Park K, Kim T, Lee M-K, et al. Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd). Energies. 2022;15(3):714.

[5] Grice W, Olama M, Lee A, Evans P. Quantum key distribution applicability to Smart grid cybersecurity systems. IEEE Access. 2025.

[6] Li Y, Xin C, Jia Z, Han X, Huang Y. Deformation measurement based on high resolution distributed optical fiber sensing and conjugated beam method. Optik. 2021;241:167065.

[7] Almosti AM, Rahman MH. Analysis of Data Privacy Breaches Using Deep Learning in Cloud Environments: A Review. Electronics. 2025;14(13):2727.

[8] Rodríguez E, Otero B, Canal R. A survey of machine and deep learning methods for privacy protection in the internet of things. Sensors. 2023;23(3):1252.

[9] Rohhila S, Singh AK. Using binary hash tree-based encryption to secure a deep learning model and generated images for social media applications. Future Generation Computer Systems. 2025;166:107722.

[10] Singh OP, Singh KN, Singh AK, Agrawal AK. Deep learning-based image encryption techniques: fundamentals, current

trends, challenges and future directions. Neurocomputing. 2025;612:128714.
[11] Byeon H, Shabaz M, Surbakti H, Keshta I, Soni M, Bhatnagar V. Deep learning and encryption algorithms based model for enhancing biometric security for artificial intelligence era. Journal of Ambient Intelligence and Humanized Computing. 2024:1-14.
[12] Tanwar VK, Raman B, Rajput AS, Bhargava R. SecureDL: A privacy preserving deep learning model for image recognition over cloud. Journal of Visual Communication and Image Representation. 2022;86:103503.
[13] Haque SMU, Sofi SA, Sholla S. A privacy-preserving deep learning framework for highly authenticated blockchain secure storage system. Multimedia Tools and Applications. 2024;83(36):84299-329.
[14] Wang W, Tamaki K, Curty M. Measurement-device-independent quantum key distribution with leaky sources. Scientific reports. 2021;11(1):1678.
[15] Le Roy-Deloison T, Lobo EP, Pauwels J, Pironio S. Device-independent quantum key distribution based on routed Bell tests. PRX Quantum. 2025;6(2):020311.
[16] Rana S, Parast FK, Kelly B, Wang Y, Kent KB. A comprehensive survey of cryptography key management systems. Journal of Information Security and Applications. 2023;78:103607.
[17] Yi J, Huang W, Huang L, Huang G, Zheng G, Li Y. Decentralized storage technology of network information security level secret key of distribution automation terminal. Discover Applied Sciences. 2025;7(6):564.
[18] Jahromi MZ, Khalaf M, Kassouf M, Kundur D. Towards a more secure reconstruction-based anomaly detection model for power transformer differential protection. Frontiers in Energy Research. 2024;12:1444697.
[19] Saeed MH, Sattar H, Durad MH, Haider Z, editors. Implementation of qkd bb84 protocol in qiskit. 2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST); 2022: IEEE.
[20] Mizutani A, Tamaki K, Ikuta R, Yamamoto T, Imoto N. Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol. Scientific reports. 2014;4(1):5236.
[21] Currás-Lorenzo G, Navarrete Á, Azuma K, Kato G, Curty M, Razavi M. Tight finite-key security for twin-field quantum key distribution. npj Quantum Information. 2021;7(1):22.
[22] Li Y, Zhang P, Huang R. Lightweight quantum encryption for secure transmission of power data in smart grid. IEEE Access. 2019;7:36285-93.
[23] Callejo P, Gramaglia M, Cuevas R, Cuevas A. A deep dive into the accuracy of IP Geolocation Databases and its impact on online advertising. IEEE Transactions on Mobile Computing. 2022;22(8):4359-73.
[24] Nasser AM, Ma D. SecMonQ: An HSM based security monitoring approach for protecting AUTOSAR safety-critical systems. Vehicular Communications. 2020;21:100201.
[25] Aliev H, Kim H, Choi S. A scalable and secure group key management method for secure V2V communication. Sensors. 2020;20(21):6137.
[26] Raj A, Varma D, Arora C. Examining the Threat Landscape: Foundation Models and Model Stealing. arXiv preprint arXiv:250218077. 2025.
[27] Sayed AS, Nabil EM, Abdelaziz AY, Bajaj M, Zaitsev I. An enhanced protection scheme for power transformers integrating alpha plane analysis. Scientific Reports. 2025;15(1):8683.
[28] Shah AM, Bhalja BR, Patel RM, Bhalja H, Agarwal P, Makwana YM, et al. Quartile based differential protection of power transformer. IEEE transactions on power delivery. 2020;35(5):2447-58.
[29] Presciuttini A, Cantini A, Costa F, Portioli-Staudacher A. Machine learning applications on IoT data in manufacturing operations and their interpretability implications: A systematic literature review. Journal of Manufacturing Systems. 2024;74:477-86.