

A Quantum- Secured Federated Learning Framework for Dynamic Security Assessment in Smart Grids

Heena S ¹, Suganthi T ²

¹M.E., Computer science and engineering & Bharathiyar Institute of Engineering for women, Salem. Email id: heenavinayaga163@gmail.com

² Assistant Professor, Computer science and engineering & Bharathiyar Institute of Engineering for women, Salem. Email id: suganthithangaveluss@gmail.com

Abstract—The contemporary clever grid integrates superior conversation technologies, allotted power resources, and clever monitoring structures to enhance strength device effectivity and reliability. However, the growing connectivity of clever grid factors exposes the machine to more than a few cyber threats, records privateness issues, and protection vulnerabilities. Dynamic Security Assessment (DSA) is critical for continually monitoring the steadiness and safety of energy structures underneath altering operational conditions. Traditional centralized computing device mastering strategies used for safety evaluation require giant quantities of records to be shared with a central server, which can also compromise privateness and gadget confidentiality.

Federated Learning (FL) offers a decentralized studying framework the place a couple of clever grid entities such as substations, power providers, and grid operators collaboratively instruct a international mannequin except sharing uncooked data. However, the verbal exchange of mannequin updates between members might also nonetheless be prone to cyber-attacks, information leakage, or malicious manipulation. To overcome these challenges, quantum cryptographic strategies can be built-in with federated studying to beautify conversation protection and guard mannequin parameters for the duration of collaborative training.

This lookup proposes QFDSA (Quantum Secured Federated Learning for Dynamic Security Assessment), which integrates federated studying with quantum-secured conversation mechanisms such as Quantum Key Distribution (QKD). The proposed machine ensures impenetrable alternate of mannequin updates amongst clever grid nodes whilst retaining statistics privacy. The framework improves cyber resilience, enhances real-time safety monitoring, and gives a dependable dynamic safety evaluation mechanism for cutting-edge clever grid infrastructures.

Keywords—Quantum federated learning, dynamic security assessment, smart grid, quantum computing

1. INTRODUCTION

The modern power grid is rapidly evolving into a smart grid, integrating advanced communication technology, intelligent monitoring systems, and distributed energy resources. These developments improve efficiency, reliability, and automation in power generation, transmission, and distribution. However, the increasing interconnection of devices and digital infrastructure also exposes the grid to various cyber security threats and operational vulnerabilities. Therefore, ensuring the dynamic security assessment of smart grid systems has become a critical research challenge.

Dynamic security assessment involves continuously monitoring and evaluating the operational stability of the power grid under different conditions such as load variations, equipment failures, and cyberattacks. Traditional centralized data analysis approaches require collecting large amounts of data from different substations and control centers. This centralized method can create privacy risks, communication overhead, and potential security breaches. To overcome these challenges, Federated Learning has emerged as a promising distributed machine learning technique that allows multiple entities to collaboratively train models without sharing their raw data.

While federated learning improves data privacy, the communication between participating nodes and the central server still faces potential cyber threats. To address this issue, advanced cryptographic methods inspired by Quantum Computing have been explored to strengthen communication security. One such technique is Quantum Key Distribution (QKD), which enables secure key exchange using the fundamental principles of quantum mechanics. Integrating quantum security mechanisms into federated learning framework can significantly enhance the protection of sensitive smart grid data.

This paper proposes QFDSA (Quantum Secured Federated Learning System for Smart Grid Dynamic Security Assessment), a framework that combines federated learning with quantum-secured communication to ensure reliable and privacy-preserving analysis of power grid data. The proposed system enables distributed grid nodes to collaboratively train machine learning model while maintaining strong encryption and secured at an exchange. By integrating quantum-secured communication with decentralized learning, the framework aims to enhance grid stability monitoring, cyber resilience, and real-time security assessment in modern smart grid environments.

The proposed approach contributes to the development of a secure, scalable, and intelligent smart grid infrastructure, capable of handling future energy demands while protecting critical power system data from cyber threats.

2. RELATED WORKS

In recent years, researchers have explored various techniques to enhance the security, privacy, and reliability of smart grid systems using advanced machine learning and distributed computing technologies. Several studies have focused on using

federated learning (FL) to address the challenges of data privacy and decentralized data ownership in smart grid infrastructures.

A secure federated deep learning framework was proposed to detect False Data Injection Attacks (FDIAs) in smart grids. In this approach, distributed grid nodes collaboratively train a detection model without sharing raw data. The method combines federated learning with cryptographic techniques to protect sensitive power system data during training and communication, improving both privacy and detection accuracy.

Another study introduced the FedDiSC framework, which uses federated learning to distinguish between cyberattacks and power system disturbances. The model utilizes deep autoencoder networks and privacy-preserving gradient quantization to enhance detection accuracy while reducing communication overhead among distributed power grid zones. Experimental results showed improved efficiency and secure collaborative learning without exposing sensitive operational data.

Researchers have also explored federated learning for anomaly detection in decentralized smart grid environments. A decentralized federated anomaly detection model based on peer-to-peer gossip protocols was proposed to overcome the limitations of centralized aggregation in traditional federated learning systems. The study demonstrated improved training efficiency and enhanced privacy protection while maintaining accurate attack detection in distributed power networks.

Another line of research focuses on integrating federated learning with advanced encryption techniques. For example, an IoT-based smart grid framework combined federated learning with homomorphic encryption to ensure secure processing of smart meter data. This approach allows energy consumption prediction and analysis while protecting user privacy by encrypting model parameters during communication between edge devices.

Additionally, federated learning has been applied to risk assessment and operational security analysis in smart grids. A data-driven privacy-preserving risk assessment framework uses deep learning models within a federated environment to evaluate grid security risks without requiring centralized data sharing. The approach ensures secure collaboration among grid operators while maintaining the confidentiality of operational data.

Despite these advancements, existing systems still face challenges such as secure communication between federated nodes, vulnerability to model poisoning attacks, and scalability issues in large power networks. These limitations highlight the need for stronger security mechanisms such as quantum-secured communication integrated with federated learning. Therefore, the proposed QFDSA framework (Quantum Secured Federated Learning System for Smart Grid Dynamic Security Assessment) aims to enhance the security and reliability of federated learning systems by incorporating quantum-based encryption techniques for protecting data exchange in smart grid environments.

3. PROPOSED METHODOLOGY

The proposed QFDSA framework integrates federated learning with quantum cryptographic techniques to create a highly secure dynamic security assessment system for smart grids. In this framework, each smart grid node such as substations, renewable energy sources, or control centers trains a local machine learning model using its operational data. Instead of sharing raw data, only model updates are transmitted to a central aggregation server.

To ensure secure communication, the system incorporates Quantum Key Distribution (QKD), which enables participants

to generate and share encryption keys using quantum communication channels. These keys are used to encrypt model updates before transmission. Quantum cryptography provides unconditional security because any attempt to intercept the communication will disturb the quantum states and be immediately detected.

The aggregated global model is then redistributed to all participating nodes for further training and dynamic security evaluation. By combining federated learning with quantum-secured communication, the proposed system ensures strong privacy protection, secure model exchange, and reliable real-time security assessment for smart grid operations.

3.1 Implementation Algorithm

The implementation of the Quantum Secured Federated Learning System for Smart Grid Dynamic Security Assessment (QFDSA) is designed to ensure secure, privacy-preserving, and efficient model training across distributed smart grid nodes. The algorithm combines federated learning with quantum-secured communication to protect sensitive grid data during collaborative learning. The following steps describe the operational workflow of the proposed system.

Algorithm: QFDSA for Smart Grid Dynamic Security Assessment

Step 1: Global Model Initialization

The central server initializes a global machine learning model for security assessment. This model will be shared with all participating smart grid nodes for local training.

Step 2: Establish Quantum-Secured Communication

A secure communication channel is established between the central server and distributed nodes using Quantum Key Distribution. This mechanism ensures that encryption keys are exchanged securely, preventing unauthorized interception or tampering.

Step 3: Local Model Training at Smart Grid Nodes

Each participating smart grid node receives the initialized global model and trains it locally using its own operational data. This process follows the principles of Federated Learning, where raw data remains within the local node and is not shared externally.

Step 4: Encryption of Model Updates

After local training, the nodes generate model parameter updates. These updates are encrypted using the quantum-generated encryption keys to ensure confidentiality and integrity during transmission.

Step 5: Secure Transmission of Model Updates

The encrypted model updates are securely transmitted to the central aggregation server through the established quantum-secured communication channel.

Step 6: Model Aggregation at the Central Server

The central server collects the encrypted updates from all participating nodes, decrypts them securely, and performs aggregation (such as weighted averaging) to combine the local model parameters into an improved global model.

Step 7: Global Model Update and Distribution

The updated global model is redistributed to all smart grid nodes for the next training iteration, improving the overall performance and accuracy of the system.

Step 8: Dynamic Security Assessment

Using the continuously updated global model, the system performs real-time smart grid dynamic security assessment to detect potential anomalies, cyberattacks, or system instability conditions, thereby enhancing the reliability and resilience of the smart grid infrastructure.

3.2 Module List

- Smart Grid Data Collection Module
- Federated Learning Training Module
- Quantum Key Distribution (QKD) Module
- Secure Communication Module
- Model Aggregation Module
- Dynamic Security Assessment Module
- Monitoring and Alert Module

3.3 Module Description

Smart Grid Data Collection Module

This module is responsible for gathering operational data from various smart grid components such as sensors, substations, smart meters, and renewable energy units. The collected information includes parameters such as voltage levels, current flow, power consumption, frequency variations, and fault indicators. This data forms the basis for training and evaluating the intelligent security assessment model used in the system.

Federated Learning Training Module

This module performs distributed machine learning training across multiple smart grid nodes using the concept of Federated Learning. Each participating node trains the model locally using its own operational data. Instead of sharing raw data with a central server, only model updates or parameters are transmitted, thereby preserving data privacy and reducing the risk of sensitive information exposure.

Quantum Key Distribution (QKD) Module

This module ensures secure key generation using Quantum Key Distribution, a quantum cryptographic technique that enables secure exchange of encryption keys. QKD leverages principles of quantum mechanics to ensure that any attempt to intercept the key during transmission can be detected thereby enhancing communication security in the smart grid network.

Secure Communication Module

The secure communication module ensures safe transmission of model updates between smart grid nodes and the central server. The encryption keys generated through the QKD module are used to encrypt and decrypt the transmitted information. This process protects the system from cyber threats such as eavesdropping, data tampering, and unauthorized access.

Model Aggregation Module

This module operates at the central server where model updates received from different nodes are combined to form an improved global model. Aggregation is performed using federated learning algorithms such as Federated Averaging (FedAvg). The aggregated global model is then redistributed to

the participating nodes for further training and continuous improvement.

Dynamic Security Assessment Module

This module analyzes the smart grid's operational state using the trained global model. It performs real-time evaluation of system stability, fault detection, and cybersecurity threats. By analyzing patterns in grid data, the module helps identify abnormal behaviors, potential failures, or malicious activities within the network.

Monitoring and Alert Module

The monitoring and alert module continuously tracks the overall security status of the smart grid infrastructure. If abnormal conditions, faults, or cyber threats are detected, the module automatically generates alerts and notifications for grid operators. This helps in taking timely corrective actions to maintain grid reliability and operational safety.

3.4 Flow diagram

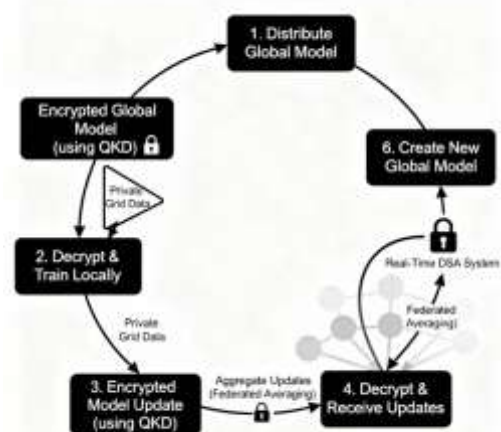


Fig no 1: Flow Diagram

4. RESULTS AND DISCUSSION

The proposed Quantum Secured Federated Learning System for Smart Grid Dynamic Security Assessment (QFDSA) was implemented to evaluate its performance in providing secure and reliable monitoring of smart grid operations. The system integrates Federated Learning with Quantum Key Distribution to ensure privacy-preserving collaborative learning and secure communication among distributed smart grid nodes. During the experimental evaluation, operational data such as voltage levels, power flow, and frequency variations were collected from multiple grid nodes and used for local model training. Each node trained the model independently without sharing raw data, thereby preserving data privacy and reducing communication overhead. The locally trained model updates were securely transmitted to the central server through a quantum-secured communication channel and aggregated to generate an improved global model.

The results demonstrate that the federated learning framework effectively detects abnormal grid conditions and potential cyber threats while maintaining high prediction accuracy. The integration of quantum key distribution further enhances the system by protecting model updates from interception or tampering during transmission. The trained global model continuously analyzes real-time grid data and performs dynamic security assessment to identify instability, faults, or

cyberattacks within the smart grid network. The system also generates alerts when abnormal conditions are detected, enabling grid operators to take timely corrective actions. Overall, the experimental results confirm that the proposed QFDSA framework provides a secure, efficient, and scalable approach for intelligent smart grid monitoring and dynamic security assessment.

Output



Fig no 2: Training dataset



Fig no 3: Dashboard



Fig no: 4 Federated Learning



Fig no 5: Realtime Monitoring



Fig no 6: QKD



Fig no 7: Threat Analysis



Fig no 8: Threat prediction

5. CONCLUSION AND FUTURE SCOPE

The proposed Quantum Secured Federated Learning System for Smart Grid Dynamic Security Assessment (QFDSA) provides a secure and intelligent framework for monitoring and protecting modern smart grid infrastructures. By integrating Federated Learning with Quantum Key Distribution, the system enables collaborative model training across distributed smart grid nodes while ensuring strong data privacy and secure communication. The framework allows local nodes to train models using their own operational data without sharing sensitive information, thereby reducing privacy risks and communication overhead. The secure communication mechanism further protects the transmission of model updates from cyber threats such as eavesdropping or data manipulation.

The experimental evaluation demonstrates that the proposed system effectively performs dynamic security assessment by analyzing real-time smart grid data and detecting potential faults, instability, or cyberattacks. The use of federated learning improves the scalability and efficiency of the system, while the quantum-secured communication ensures the integrity and confidentiality of data exchange. As a result, the QFDSA framework enhances the reliability, resilience, and cybersecurity of smart grid operations.

In future work, the system can be extended by integrating advanced deep learning models to improve anomaly detection accuracy and predictive analysis. The framework can also incorporate edge computing techniques to further reduce latency and enable faster local decision-making at grid nodes. Additionally, the integration of blockchain-based security mechanisms may further strengthen trust and transparency in the federated learning process. Expanding the system to support large-scale smart grid networks and real-time energy management applications will further enhance its practical applicability in next-generation power systems.

REFERENCES

1. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*. (Foundational paper on Federated Averaging - FedAvg).
2. Kairouz, P., McMahan, H. B., Avent, B., et al. (2021). Advances and Open Problems in Federated Learning. *Foundations and Trends® in Machine Learning*, 14(1–2), 1-210. (Comprehensive survey of FL, including security and privacy aspects).
3. Lo, H. K., Curty, M., & Tamaki, K. (2014). Measurement-Device-Independent Quantum Key Distribution. *Nature Photonics*, 8(8), 595-604. (Seminal paper detailing the MDI-QKD protocol).
4. Pirandola, S., et al. (2020). Advances in Quantum Cryptography. *Advances in Optics and Photonics*, 12(4), 1012-1236. (Comprehensive review of QKD protocols and technologies).
5. Xu, Y., et al. (2023). Adaptive resource allocation in Quantum Key Distribution (QKD) for federated learning. *2023 International Conference on Computing, Networking and Communications (ICNC)*. (Paper discussing QKD resource allocation for FL).
6. P Kundur, J Paserba, V Ajjarapu, G Andersson, A Bose, C Canizares, N Hatziaargyriou, D Hill, A Stankovic, C Taylor, T Van Cutsem, V Vittal. (2004). Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. *IEEE Transactions on Power Systems*, 19(3), 1387-1401. (Standard definitions for power system stability).
7. E Vaahedi. (2014). *Practical Power System Operation*. John Wiley & Sons. (Textbook covering practical aspects of grid operation, including DSA).
8. Liu, S., et al. (2021). Searching for the Devil in the Details: Learning Challenging Smart Grid Stability Boundary with Deep Learning. *IEEE Transactions on Power Systems*. (Example of deep learning for DSA).
9. Sapountzoglou, N., et al. (2020). Charting the landscape of federated learning for healthcare. *Frontiers in Digital Health*. (Survey illustrating FL applications in sensitive domains).
10. Bhagoji, A. N., et al. (2019). Analyzing federated learning through backdoor attacks. *Proceedings of the 22nd International Conference on Artificial Intelligence and Statistics (AISTATS)*. (Example paper on backdoor attacks against FL).
11. Nasr, M., Shokri, R., & Houmansadr, A. (2019). Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks. *Proceedings of the IEEE Symposium on Security and Privacy (SP)*. (Paper detailing inference attacks against ML models).
12. Scarani, V., et al. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3), 1301. (Review discussing practical security aspects of QKD implementations).
13. Cao, Y., et al. (2022). BB84 protocol for quantum key distribution network resource allocation. *Quantum Engineering*. (Example of QKD network resource management).
14. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*. (Example of modern dataset creation for security AI, analogous to grid data needs).